Douglas Salane
Center for Cybercrime Studies
John Jay College of Criminal Justice
The City University of New York

Greater New York Dental Meeting
Javits Center
November 29, 2011

Computer Security in an Insecure World
A Disclaimer

- The views presented here are solely those of the speaker and do not necessarily reflect the views of The John Jay College Criminal Justice or The City University of New York.
Center for Cybercrime Studies
(what we do)

- Academic Security Researchers (latest in security, policy and privacy)
- Security Practitioners (IT security, corporate security and privacy executives, forensic firms and legal firms)
- Law Enforcement Practitioners (FBI, Secret Service, NYPD Cyber Crime Squad, prosecutors’ offices, FDIC, FTC)
- Support College’s degree programs in computer information system (B.S.) and Forensic Computing & Security (M.S.)
- Community Outreach
Aims of the Presentation

- Raise Awareness of Information Security Challenges
- Provide examples of some of the threats
- Introduce basic security concepts and the security process
- Review some of the obvious things that need to be done but are often neglected
New Technologies, New Threats

- “It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness, it was the epoch of belief, it was the epoch of incredulity, it was the season of light, it was the season of darkness, it was the spring of hope, it was the winter of despair...”

- Charles Dickens, *A Tale of Two Cities*
Valiena Allison got a call from her bank on a busy morning two years ago about a wire transfer from her company’s account. She told the managers she hadn’t approved the transfer. The problem was, her computer had.

As Allison, chief executive officer of Sterling Heights, Michigan-based Experi-Metal Inc., was to learn, her company computer was approving other transfers as she spoke. During hours of frantic phone calls with her bank, Allison, 45, was unable to stop this cybercrime in progress as transfer followed transfer. By day’s end, $5.2 million was gone.

She turned to her bank, a branch of Comerica Inc. (CMA), to help recover the money for her metal-products firm. It got all but $561,000 of the funds. Then came the surprise: the bank said the loss was Experi-Metal’s problem because it had allowed Allison’s computer to be infected by the hackers.

“At the end of the day, the fraud department at Comerica said: ‘What’s wrong with you? How could you let this happen?’” Allison said.
$9 Million ID Theft Scheme Alleged
Duo Charged in Retail Scam that Spans 15 Years
Tracy Kitten, Managing Editor
October 18, 2011

Georgia authorities say they made key arrests in an identity theft investigation that has connected crimes going back 15 years, totaling $9 million.

The Criminal Intelligence Unit of the Cherokee County Sheriff’s Office, with help from the U.S. Secret Service, arrested Robert Smith, 46, of Atlanta, and R of Roswell, Ga., for their alleged involvement in ID theft cases that targeted victims throughout the United States. During the arrests, authorities seized more than $500,000 cash along with what has been defined as high-end retail property, including a 1999 Lexus and a Harley Davidson motorcycle.

Smith has been charged with five counts of Identity Fraud, 1 count of Conspiracy to Commit Identity Fraud, 1 count of Conspiracy to Commit Retail Property Fencing and 1 count of Violation of the Georgia RICO Act. Hill faces charges of Conspiracy to Commit Retail Property Fencing and Violation of the Georgia RICO Act.

More than 8,000 compromised identities have been linked to Smith and Hill. According to the Cherokee County CIU, identities were compromised from within system, with suspects using counterfeit driver’s licenses to establish credit through retailers such as Best Buy, Target, Sam’s Club, Wal-Mart, Home Depot and eBay for cash.

More arrests are expected.

ID Theft Connects Fraud

The arrests came just days after the U.S. District Attorney’s Office in Queens, N.Y. announced closure of the biggest ID theft takedown in U.S. history. [See Bi

The scheme, which allegedly involved five organized crime rings with ties to Europe, Asia, Africa and the Middle East, resulted in financial losses exceeding $1

It’s just another example showing how ID theft crimes are growing.

In the Smith and Hill case, what stands out is the length of time the scheme spanned. But Julie Fergerson, a board member of the Identity Theft Resource Center Council, says the timeline is not so surprising. Banks and retailers likely picked up on and traced fraudulent activity years ago. “But it’s hard to hand that over to
Cybercrime Extracts $399,000 from Florida Dentist’s Account; Internet Security Awareness Could Have Thwarted Attack

New KnowBe4 Case Study Examines Telephony Denial-of-Service (TDoS) Attack, a Cybercrime Tactic That Floods Victims’ Phone Lines While Cyberheist Is Underway

Clearwater, Fla. (PRWEB) April 25, 2011

According to a new case study published by the Internet Security Awareness Training (SAT) firm KnowBe4, a telephony denial-of-service (TDoS) attack against a semi-retired St. Augustine dentist served as a smokescreen for a nearly $400,000 cyberheist.

In November 2009, Robert Thousand Jr. began receiving a flood of calls to his business, home and mobile phone lines. The calls consisted of a 30-second recorded message from a sex hotline. What appeared to be a phone service issue turned out to be far more sinister. The following month, Thousand discovered that five transfers totaling $399,000 had been made from his TD Ameritrade retirement account. When the FBI investigated his case, it became apparent that the TDoS attack was intended to prevent Thousand’s broker from reaching him while the criminals committed their cyberheist.

TDoS is a form of denial-of-service (DoS) attack. When the calls come from multiple sources, it is known as a distributed denial-of-service (DDoS) attack. The high volume of automated calls prevents victims from making or receiving legitimate calls, thereby denying them use of their phone service. In Thousand’s case, the cybercriminals set up a number of VoIP accounts and used automated dialing to inundate his phone lines. While that was happening, they initiated the transfers that drained his retirement account.

Thousand was not the only victim to be targeted in such a manner. Others reported similar telephony DoS attacks.

“Before the cybercriminals launched their TDoS attack, they found a way to obtain Dr. Thousand’s Ameritrade account information and password.”
Android Threats Surge With Infected Third-Party ‘Angry Birds’ Apps:
Tech

By Sarah Frier - Nov 15, 2011

In the era of the personal computer, Apple Inc. (AAPL)'s machines were often less vulnerable to security threats than the alternatives. That may also be the case with the rise of smartphones.

Google Inc. (GOOG)'s Android operating system for mobile devices has had an almost sixfold increase in threats such as spyware and viruses since July, according to Juniper Networks Inc. (JNPR) That may increase the perception that Apple devices are safer than smartphones and tablets that run on Android, said Juniper.

"You're not going to see nearly the number of infections on Apple as you see on Android," said Dan Hoffman, who leads a team tracking mobile threats for Sunnyvale, California-based Juniper, the second-largest maker of networking equipment.

Most of the growth in Android threats comes from applications, or apps, available from sites not associated with Google's Android Market, according to data Juniper collected as of Nov. 10. Apple doesn't face the same issue because iPhone and iPad owners can only get applications from Apple's App Store, which is controlled by the company.

"The open nature of the Android system makes it more susceptible to attack," Hoffman said in an interview. "If it's on a third-party site, Google can't remove it."

Making malware is easier with Android software because the applications aren't checked, the source code is open and the apps can be sold on external sites, Hoffman said. Android is free and available for download by anyone, while Apple screens each application added to its store. With Android growing faster than Apple's system, it appeals to hackers seeking greater reach, he said. Of the thousands of infected Android apps, 55 percent contain spyware, which can gather data from phone use.

Increasing Market Share

Google, based in Mountain View, California, and Apple, based in Cupertino, are vying for control of a smartphone market as computing evolves from desktop machines to mobile devices. While Apple has championed a closed system in which it makes its own hardware and doesn't share its operating system, Google has opted for an open approach, allowing companies such as Samsung Electronics Co. and
Mobile Malware Development Continues To Rise, Android Leads The Way
Filed Under: Android, GTC Blog

November 15, 2011

What happens when anyone can develop and publish an application to the Android Market? A 47.8% increase in Android malware samples since July 2011. These days, it seems all you need is a developer account, that is relatively easy to anonymize, pay $25 and you can post your applications. With no upfront review process, no one checking to see that your application does what it says, just the world’s largest majority of smartphone users skimming past your application’s description page with whatever description of the application the developer choose to include. Sure, your application can be removed after the fact—if someone discovers that it is actually malicious and reports it. But, how many unsuspecting people are going to download it before it is identified as malicious and removed? This is precisely what is playing out in the mind of mobile malware developers today.

This approach has led to major increases in research into and discovery of vulnerabilities with in the Android platform as the delivery mechanisms of mobile malware. In our annual Malicious Mobile Threats Report, report, Juniper found a 430% increase in Android malware from 2008 to the summer of 2010. We have since seen exponential growth in Android malware over the last several months. The Juniper Global Threat Center found that the months of October and November are shaping up to see the fastest growth in Android malware discovery in the history of the platform. The number of malware samples identified in September increased by 20% over the number of known Android malware samples. October showed a 110% increase in malware sample collection over the previous month and a striking 171% increase from what had been collected up to July 2011.

In addition to an increase in the volume, the attackers continue to become more sophisticated in the malware they write. For instance, in the early spring, we began seeing Android malware that was capable of leveraging one of several platform vulnerabilities that allowed malware to gain root access on the device, in the background, and then install additional packages to the device to extend the functionality of the malware. Today, just about every piece of malware that is released contains this capability, simply because the vulnerabilities remain prevalent in nearly 90% of Android devices being carried around today. Attackers know this, and they’re using it to gain privilege escalation on the device in order to gain access to data and services that wouldn’t otherwise be available.

The majority of malicious applications target communications, location, or other personal identifying information. Of the known Android malware samples, 55%, acts in one way or another as spyware. The other major type of attack, which make up 44%, are SMS Trojans, which send SMS messages to premium rate numbers owned by the attacker in the background of a legitimate application, without the person’s knowledge. Once these messages
Mobile Computing

- 400% Increase in malware in Android Apps from 2009 to 2011
- Fall 2011 – doubling of malware each month
- 55% spyware, 45% SMS Trojans
- Android phones 60% of the mobile market
- Convenience and efficiency versus risks
FOREIGN SPIES STEALING
US ECONOMIC SECRETS
IN CYBERSPACE

Report to Congress on Foreign Economic Collection
and Industrial Espionage, 2009-2011

October 2011
Why is it Getting Out of Hand?

- Systems are too complex to secure
- New systems are rushed to market
- Internet’s design
- Lack of social and governmental controls
- Widespread availability of PII (social engineering and identity theft)
Cybercrime

- Organized activity that’s now mainly profit motivated – it’s not just hacking anymore

- Access to extraordinary tools and resources via a growing underground economy (Botnet services, ATM skimmers, custom software with support.)

- Growing market for contraband especially PII and financial information (Carding Sites)

- Transnational nature of the crime
A False Sense of Security

- We are usually in a comfortable safe place when online.
- We are too trusting on the Internet – we are just not aware of how unsafe it is.
- We are lulled by quick obvious rewards and ignore the longer term risks.
- On-line services now are essential – we have no choice but to accept the risk.
Privacy and Security

Can you be secure when

- Anyone can know just about anything about you?
- You cannot control the parties that have access to your personal information nor how they use it?
- Erroneous information about you cannot be corrected?
- Time no longer heals all wounds – your digital footprint lives on in perpetuity?
The Need to Know
(A Fundamental Security Principal)

- In military operations individuals are given access only to information needed to perform their work.

- Limit access to sensitive information and limit the damage due to compromises by a trusted insider.

- We limit access to information because we do not know how it will be used.

- Modern communications services try grab all the information they can.
Fair Information Practices (www.ftc.gov)

- (1) Notice/Awareness (no secret collection)
- (2) Choice/Consent (how data used)
- (3) Access/Participation (who will access data)
- (4) Integrity/Security (correct data)
- (5) Enforcement/Redress (FTC)
Pew Internet & American Life Project – Why Americans Use Social Media

- 66% of on-line adults use social media, e.g., Facebook, Twitter, MySpace or LinkedIn, to communicate with family members and friends
- About 17% of 30-64 year olds use it to connect with others with a similar hobby or interest
Privacy and the Social Networking Site Business Model

- Highly targeted advertising
- Sharing user information is essential for revenue
- Trust relationships with friends
- Apps, connections, site links – still difficult to opt out of information sharing
Privacy Considerations

- State of Privacy – the intimacy of the group
- Short term benefits versus long term risks
- Who will have access to what you post?
  - Your friends?
  - Their friends?
  - Adversaries/Thieves?
Social Network Exploits

- Facebook – recent spam incident, Zone Alarm
- IEEE Computer – High probability of receiving spam.
- IEEE Computer – Non negligible probability of exposure to links pointing to sites with malware.
Mobile Phones
Privacy and Security Concerns

- GPS tracking
- The problem with Apps
- Exploits go where the action and money is
- Dramatic increase in on-line banking as the preferred method for banking
Protection Focus

INFORMATION ASSURANCE
- Information
- Information Systems

COMPUTER SECURITY
- Technology
- Hardware, Software and Networks
Key Components of IA

- People (security conscious staff)
- Technology (computer security)
- Operations (office systems)
Protecting Information

- Availability
- Integrity
- Confidentiality
- Authentication
- Non-Repudiation
Securing Information and Information Systems

- Risk Assessment
- Protect
- Monitor and Detect
- React
What a Business Must Do

- Know critical assets and operations to protect; try to anticipate the threats
- Devise policies to protect critical assets and operations
- Implement policies and monitor for compliance (systems, people and operations)
- Plan for attack response and remediation
- Know when and where to seek help from security firms and law enforcement
An Expanding Regulatory Environment

- HIPPA (digital medical records)
- PCI-DSS (if you take credit cards)
- Data breach legislation (44 states)
- Increasing restrictions on and penalties for mishandling consumer PII
HIPAA security regulations
Protecting patients’ electronic health information

Dentists who transmit certain patient health information electronically will have to comply with the recently released security regulations mandated by the Health Insurance Portability and Accountability Act of 1996, or HIPAA. Fortunately, compliance will not be mandatory until April 2005, so dentists will have plenty of time to adopt practices necessary for compliance.

There is a key difference between the security regulations and the HIPAA privacy regulations. Both sets of regulations apply only to dentists who are “covered entities.” In order to be a covered entity, a dentist must transmit certain patient health information electronically, using a format established by the HIPAA transaction standards. However, the HIPAA privacy regulations apply to all communications—electronic, written or oral—of patients’ protected health information. In contrast, the security regulations apply only to electronic protected health information, or PHI.

Under the HIPAA regulations, PHI is defined as information that identifies a patient and relates to that person’s health, health care or payment for health care. Any dentist who is a covered entity will have to adopt the protections for electronic PHI contained in the security rule.

The final version of the security regulations was modified by the U.S. Department of Health and Human Services, or DHHS, to more closely reflect the requirements of the privacy regulations. Thus, a dentist who has implemented measures to comply with the privacy regulations already may have taken some of the steps needed to comply with the security regulations.

Similar to the privacy regulations, the security regulations allow covered entities flexibility to adopt implementing measures that are appropriate for that particular covered entity. That means that a small private dental practice will not need to take the same measures to comply with the security regulations as will a hospital or an insurance company. In deciding what security measures to adopt, a covered entity must consider the following factors:

- the size, complexity and capabilities of the covered entity;
- the covered entity’s technical infrastructure, hardware and software security capabilities;
- the costs of security measures;
- the probability of and degree of potential harm from potential risks to electronic PHI.

The security regulations contain standards with both “required” implementation specifications and “addressable” implementation specifications. While the required implementation specifications are mandatory, the addressable

BY PETER M. SFIKAS, J.D.
Warning: HIPAA has teeth and will bite over healthcare privacy blunders

New government fine structure plus random auditing make healthcare privacy lapses even less acceptable

By Tim Greene and Ellen Messmer, Network World
September 09, 2011 09:13 AM ET

Healthcare organizations that are performing risk assessments as a way to craft patient-privacy policies might want to consider a new potential attack vector: federal regulators.

Later this year, the Department of Health and Human Services is expected to start auditing up to 150 health providers at random through December 2012 in an effort to find medical entities that fail to comply with HIPAA and HITTECH regulations about how personal data must be handled securely.

IN THE NEWS: Stanford Hospital investigating patient data leak

While the audits don’t represent attacks on the personally identifiable information (PII) the regulations are supposed to protect, they do expose non-compliant providers to the potential for heavy fines and reputation-damaging publicity.

For instance, earlier this year Massachusetts General Hospital paid $1 million to settle a patient-privacy complaint with HHS due an employee leaving patient records in a subway car.

That’s a big switch from the way healthcare privacy regulations have been handled since 2003, says Abner Weinsaeb, president of HIPAA Group, a compliance consultancy to healthcare organizations. Until this year, HHS had received about 50,000 complaints but levied no fines, preferring to take remedial actions instead, he says.

Levying fines now has an upside for HHS, says Kelly Hagan, a healthcare attorney with law firm Schwabe, Williamson & Wyatt in Portland, Ore. - the agency gets a cut of whatever auditing, marks a sea change for what healthcare CIOs and CISOs face when dealing with HIPAA. “Suddenly HIPAA has teeth and is willing to bite,” Hagan says.

Despite this, instances of healthcare data breaches continue to flourish. Just this week, it was revealed that emergency room records from Stanford Hospital in Palo Alto, Calif., were students can hire help to do schoolwork.

MORE ON HEALTHCARE TECHNOLOGY: High-tech healthcare technology gone wild

Last year, HHS received 207 reports of breaches involving more than 500 individuals, according to a report to Congress last week. And there are growing incentives for criminals to data can be sold to criminals interested in perpetuating identity theft, he says, but more lucrative are schemes to commit medical identity theft.

That’s when stolen patient data is used to obtain medical care for someone else, which not only bilks insurers but also taints the medical record of the individual whose identity is stok victim never received.
Special Considerations

- Protecting your client’s data
- Work securely with your financial institution
- Be sure data needed to run the office is always available
- People are the key
GE Healthcare Intros Cloud EMR For Small Practices

The software-as-a-service GE Centricity Advance e-medical record system will help small medical practices comply with healthcare reform's "meaningful use" requirements.

By Marianne Kolbasuk McGee InformationWeek
June 15, 2010 03:56 PM

GE Healthcare is often associated with e-medical record and other clinical information systems used in hospitals and larger healthcare facilities. But the vendor Tuesday introduced for small, independent doctor practices a new Web-based, cloud version of its Centricity EMR software.

GE Centricity Advance is a new software-as-a-service offering that includes integrated e-medical records, practice management applications, and a patient portal.
The Little Things Get You

- Weak Passwords
- Using an Windows Admin account
- Not following standard practices (updates for OS and anti-virus software)
- Ignoring telltale signs (slow computer)
- People not following or not aware of basic security policies
People – the critical link

- All staff must be security conscious
- Training and constant reminders are an essential part of the security process
- Recent costly, notable data breaches at RSA Security and HB Gary, preeminent security firms - victims of highly targeted phishing attacks
The ACH transaction (ID: 87234325), recently sent from your bank account (by you or any other person), was rejected by the Electronic Payments Association.

Canceled transaction

Transaction ID: 87234325
Reason of rejection See details in the report below

Transaction Report report_1609.pdf.zip (ZIP archive, Adobe PDF)

ESET NOD32 Antivirus warning, version of virus signature database 6476 (20110919)

Warning, ESET NOD32 Antivirus found the following threats in the message:

report_1609.pdf.zip > ZIP > report_1609.pdf.exe - Win32/TrojanDownloader.Chepvil.A trojan - was a part of the deleted object
Step into the Future of PAYMENTS

PAYMENTS 2012 is the premier educational event of its kind, offering the most current, concise, practical, and real-world information you need to address the myriad issues and opportunities available in today's rapidly changing payments environment.

Attend and expand your knowledge

---

News Headlines

- Limited Speaking Opportunities for PAYMENTS 2012 Still Available
- NACHA Launches Microsite for ACH Messaging Resources - http://direct.nacha.org
- Fraudulent Emails Appearing to Come from NACHA
- Expedited Processing and Settlement RFC: December 12 Deadline
- NACHA Welcomes Silicon Valley Bank as a Direct Financial Institution Member
- Cyber Attack Against Payment Processes Exercise (CAPP)

---

Events

- Webinar: Why FIs Should Care About Healthcare - The Legislation, Opportunities & Impacts - November 10, 2011, 1:30 p.m. - 3:00 p.m. EASTERN. - Register Now
- PAYMENTS 2012 April 29 - May 2, 2012

---

ePayments Marketplace

Utilize NACHA's localized directory of companies to find exactly what you are looking for.
WEBMAIL EXCEED LIMIT

Quantitative Methods Faculty [QMF@LISTSERVER.JJAY.CUNY.EDU] on behalf of Henrietta Wilson [henrietta.wilson@SEH.OX.AC.UK]

To: QMF@LISTSERVER.JJAY.CUNY.EDU

You forwarded this message on 11/20/2011 12:10 AM.

Dear Webmail Account User,

This message is updated webmail service team center
to all a messaging subscribers / webmail users. We are
to improve our database and e-mail center due to
unusual activities identified in our mail system, we
are deleting all unused webmail account, to create a space
for new.

To avoid this problem, you are advised to verify your email
account by clicking on the link below.
http://mailupgradecladermailer.tk/webmail-verify/

Thank you.

The System Administrator, Management Team.

Information from ESET NOD32 Antivirus, version of virus signature database 6643 (20111120)

The message was checked by ESET NOD32 Antivirus.

http://www.eset.com
Welcome to the IC3

The Internet Crime Complaint Center (IC3) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C), funded in part by the bureau of justice Assistance (BJA).

Filing a Complaint with the IC3

The IC3 accepts online Internet crime complaints from either the actual victim or from a third party to the complaint. We can best process your complaint if we receive accurate and complete information from you. Therefore, we request that you provide the following information when filing a complaint:

- Your name
- Your mailing address
- Your telephone number
- The name, address, telephone number, and Web address, if available, of the individual or organization you believe defrauded you.
- Specific details on how, why, and when you believe you were defrauded.
- Any other relevant information you believe is necessary to support your complaint.
Auction Fraud: I saw it on the Internet, I made a payment, what I got was not what I saw or I never received anything.

Counterfeit checks: Made possible by inexpensive, excellent duplicating facilities.

credit fraud: Web sites that collect credit card or other payment credentials

Investment fraud: e.g., pump and dump schemes.
Steps to Avoid Fraud

- When making purchases on-line, know with whom you are dealing.
- If it looks too good to be true, it probably is.
- Delete unsolicited e-mails that request personal information or contain attachments.
- Use a credit card for on-line purchases.
- Monitor account statements regularly; report discrepancies immediately.
Center for Cybercrime Studies (contact information)

- [http://www.jjay.cuny.edu/centers/cybercrime_studies/index.php](http://www.jjay.cuny.edu/centers/cybercrime_studies/index.php)

- [www.jjay.cuny.edu](www.jjay.cuny.edu)
  Academics, Research Centers and Institutes

Douglas Salane
dsalane@jjay.cuny.edu