Laptop and Mobile Device Security

Presented By

Eric Jernigan, CISSP, CISM
PCC Information Security Manager
Eric Jernigan

- Information Security Manager
- Office: (503) 977-4896
- Email: eric.jernigan@pcc.edu
- 7+ years in Information Security practice
- 10 years Intelligence/counter-intelligence, homeland defense (security)
- CISSP: Certified Info Systems Security Professional
- CISM: Certified Info Security Manager
Laptops vs. Mobile Devices

For this presentation consider Laptops and Mobile devices as synonymous

- All Shapes and Sizes
- Hotspots
- Wi-Fi Phones
- Most still build security in as a afterthought or after consumer pressure
Computer Threats

Mobile Computers are more vulnerable to these threats
Mobile Device Theft

The theft of desktop PC’s has fallen in recent years while the theft of laptops steadily increased.
Laptop Hustle

- http://www.youtube.com/watch?v=Gb3ZiTJkCaA
Targeted Locations

- Colleges and Universities
- Automobiles
- Libraries
- Airports
- Hotels and Conference Centers
- Company Offices
- Hospitals
Danger Areas

- At a check-out counter
- While engrossed in a telephone conversation
- While paying the cashier at a cafe or restaurant
- As you sleep or read a newspaper between flights or in a library
- In a crowded restroom
- At the x-ray conveyer
- Loading the car
Wireless Attacks

- [http://www.youtube.com/watch?v=pgBHjZUKW54](http://www.youtube.com/watch?v=pgBHjZUKW54)
Man-in-the-Middle Attack

- Makes it seem that two computers are communicating with each other
  - Actually sending and receiving data with computer between them
  - Active or passive

Diagram:

- Target
- AP
- Server
- Dual-Card Attacker

Intercepting transmissions
Denial of Service (DoS)

- Network unavailable from flood of requests
- Wireless DoS attacks are different:
  - **Jamming**: Prevents wireless devices from transmitting
  - Forcing a device to continually dissociate and re-associate with AP
Wireless Attack Surface

Signal emitted from a single access point.
Additional PDA/Smartphone Threats

Malware Delivery Vectors for Mobile Devices

1. Physical media (SD card, memory stick)
2. Synchronization with PC
3. Wireless LAN or LAN network connection
4. Telephony/mobile network data service (SMS, MMS, WAP)
5. Peer-to-peer connectivity (Bluetooth, IR)
Environmental threats

- Home environment usually has more variables (food, pets, kids)
- Each new location for a mobile device means an area assessment should occur
- “Is Your Cat Infected with a Computer Virus?”
  - “…the strangest thing of all happened: the LCD display on the pet ID computer froze and displayed the ominous message: .All your pet are belong to us.."
The Mobile Security “Perfect Storm”

Fastest Growing Device Segment: Smart phone growth = 77%
Other mobiles = 27%
Mobiles out ship PC’s 5:1 in 2006
(Source: Canalys for H1’05 to H1’06, IDC & Gartner)

Increasing Mobile Device Threats: Mobile virus variants have doubled every 6 months since 2004
(235 mobile virus variants in H1’06)
(Source: Symantec Security Response)

IT is Organizing:
Mobile/wireless IT spending likely to exceed IT budget growth in many organizations:
12.5% avg. growth rate
(Source: Gartner)

Enterprise Faith: 80% of companies are allowing corporate data on devices, yet continue to not secure the data*

Outdated Thinking: 75% of companies have not addressed smart phone security*
(60% cite security as biggest mobility obstacle*)

* Q1 2006 Symantec survey conducted by Economist Intelligence Unit

Source: Symantec Mobile Enterprise Security
REAL RISKS

RISKS AND DANGERS
Why Should PCC Care About Your Mobile Device being compromised?

- **Operational & financial burdens**
  - Money better spent on students and programs

- **Costs of remediation**
  - Controls more expensive when change is reactive

- **Legal liability**
  - Loss of federal funding, State/Federal fines

- **Negative effect on public confidence**
  - The most expensive cost
British defense chief says stolen laptop with personal data could have been targeted

The Associated Press
Published: January 21, 2008

LONDON: British Defense Secretary Des Browne told lawmakers Monday he could not discount the possibility that a stolen laptop containing sensitive details on 600,000 prospective military recruits had been specifically targeted for theft.

Browne said data — including details of candidates’ religions and some banking records — was not encrypted. The computer was snatched from the car of a Royal Navy recruitment officer in Birmingham, in central England, on Jan. 9.

“We have no reason to believe that this theft was specifically targeted against the officer or to acquire the laptop for the data held on it, but we cannot wholly discount this,” Browne said.

Nashville laptop theft may cost $1 million

With Social Security numbers at risk, county officials offer registered voters in Tennessee county a year of free identity theft protection at the cost $10 per account

By Robert McMillan, IDG News Service
January 14, 2008

The theft of a laptop containing Social Security numbers of Nashville, Tenn.-area voters is expected to cost local officials about $1 million as they roll out identity-theft protection to those affected.

County officials say that thieves broke into Davidson County Election Commission offices on the weekend before Christmas, smashing a window with a rock and then making off with a $3,000 router, a digital camera, and a pair of Dell Latitude laptops containing names and Social Security numbers of all 337,000 registered voters in the county.

County election officials began notifying residents of the breach on Jan. 2, and the local government is offering victims one year of identity-theft protection.

Marty Greenleaf is concerned his personal information was on the laptop that disappeared at Salt Lake Community College.

“I’m upset that they’re not telling me everything that happened,” Greenleaf said. The school called him early last week and instructed him to change the password he uses to access his student page on the SLCC Web site due to a possible security breach.

SLCC acknowledged a laptop had been stolen, but spokesman Joy Tlou said the school is still unsure whether the laptop taken from the Continuing Education of SLCC’s Miller campus in Sandy contained internal log-in information for about 1,000 students, faculty and staff.

“We know which computer it was and we are trying to ascertain what information was on that computer,” Tlou said.

DigiKam 0.9.3

Thefreeware 3.1.1

Ubuntu 15.10

Firefox 41.0.1

LibreOffice 4.4.3

Notepad++ 6.6.9

Thunderbird 41.0.1
The (partial) Legal Landscape

- GLBA
- FERPA
- HIPAA
- SB 583 Consumer Identity Theft Protection Act

Relevant federal bills under consideration in the U.S. House and Senate:

- *Identity Theft Protection Act*
- *Data Accountability and Trust Act*
- *Personal Data Privacy and Security Act*
- *Data Security Act of 2007*
Legal Liability

- Plaintiffs have sought relief under numerous legal theories
  - Negligence: Elements – duty, breach, injury, causation
  - Defense: intervening criminal act
  - Breach of contract
  - Invasion of privacy
  - Breach of fiduciary duty
  - Negligence *per se*

*If you were a victim what would you have done?*
CUNY THEFT THREATENS STUDENT IDS

By YOAV GONEN Education Reporter

November 1, 2007 -- As many as 20,000 current and former CUNY students are at risk of identity theft after a laptop with their names and Social Security numbers was stolen from a financial-aid office in Midtown, The Post has learned.

The potential breach angered students, who were sent letters Oct. 19 urging them to contact their credit-card companies and take other steps to protect themselves.

"It's ridiculous," said Ken Krivac, of Queens, whose 19-year-old daughter had attended Queensborough Community College. "It's a young girl starting off in life and everything's been compromised."

His daughter said the timing couldn't be worse.

"I was trying to get a job and they weren't able to do a background check" because of her credit alerts, she said.

University officials said they reported the apparent theft to police "recently," but they could not pinpoint a date. The letters put the disappearance of the laptop as "last week."

Officials said the missing laptop had not been functional and that any sensitive data it contained was password-protected.

"We have no reports the laptop's hard drive, which contained Social Security information, has been accessed," said a CUNY spokesman.
What’s wrong with this?

- http://www.youtube.com/watch?v=qj5wJeU4x-k&feature=related
REAL SOLUTIONS

DEFENSIVE MEASURES
What Now?

- Assume someday you will lose or misplace your mobile device
- Be Aware of your environment
- Limit the amount of sensitive or personal information contained on the mobile or wireless
- Act NOW to protect all electronic data on Mobile Devices
Our Responsibilities

Be Aware of:

- Your working environment— even if working at home
- How you handle information
- The people around you
- How you communicate
- Know and understand PCC security policy and standards. (developed and to be distributed)
Limit Exposure On Mobile Devices

Is the private information accessed for a necessary business / academic reason?

Does the information need to be accessed on a mobile device? Does it need to be stored on it?

Be aware of Metadata

- “Afterimage” of accessed information residing in a device’s memory or application, not readily viewed but easy to retrieve.
WHY?
• It is YOUR responsibility to backup your files.
• You can accidentally delete needed files.
• Files can become unreadable/corrupt.
• You could suffer a hard drive crash and not be able to even boot up your machine.
• In short, because it’s not a matter of IF you will ever need to recover files, but WHEN.
Backing Up your Data

– Backup your files at least once a month. You can schedule backups

– Use Network backup
  • Use your department (H: Drive) and Personal drive (F: Drive) for important files
  • No extra storage media required

– Single keystroke recovery (rollback to a known good state)
  • Examples
    – Backup and Restore Center – Integrated in Windows
    – Apple Time Machine - integrated OS X Leopard
    – Acronis True Image 11 Home - $49.00
    – Deep Freeze - $45.00
Backing Up your Data

• If your Mobile Device (laptop, PDA, etc.) is your primary computer, you should have a separate device as a secure, backup device

• Keep the “backup” device in a separate, secure location

• If you use a mobile device for backup (e.g., a memory stick), then encrypt all sensitive data and store separately
Encrypt Your Disk

- Software is available to provide whole disk encryption for your mobile device
- Automatically encrypted or decrypted without any user intervention
- No data stored on an encrypted volume can be read (decrypted) without using the correct password
- Entire file system is encrypted (e.g., file names, folder names, contents of every file, free space, meta data, etc)
- Ensure password is in a secure location

http://www.truecrypt.org/

Cost: FREE
Encryption Options

• Some other options:
  – Vista Bitlocker
  – FileVault still a built in option for Mac OSX
  – Free Compusec [www.ce-infosys.com](http://www.ce-infosys.com)
On The Road

- Don’t rely upon hotel or conference staff to lock up a meeting room during a lunch break
- Stay only in hotels that use card-activated locks for room entry doors
- Use the hotel safe to protect your laptop while you are away from your room
- Don’t place your device on the bellman’s cart
- If you leave your laptop in your room, don’t advertise its presence - store it out of sight in luggage or sock drawer
- Always check your seat after traveling
- In the airport, always keep your laptop within your sight line.
Wireless Defense

- Only connect to secure wireless networks
  - Secure networks will be noted with the gold lock icon
  - PCC’s wireless network is not designed for security- be wary of what you access
- Connect only to networks you know and trust
- Limit what sites you visit when using wireless networks
- Don’t access sensitive information on unsecured access points while traveling – Bad time to be in Banner!
- There may be “imposter” PCC networks. Be careful.
Wireless Defense

1. Change the default password and SSID on your router
2. Enable WPA (WPA2 if available) on router and wireless device
3. Use MAC address filtering
4. Don’t broadcast SSID
5. Prohibit Peer-to-peer (Ad Hoc) networking

See the vendor guide for specific instructions on how to do these steps.

(note using an SSID name like “hacker” or similar may deter the casual access thief but may entice the dedicated criminal)
Mobile Security Strategies

PCC issued computer / mobile device:
- Ensure TSS has a record of your computer on file and that it has the needed safety measures installed.

Personal computer / mobile device:
- Record the make, model and serial number of the device and return the completed warranty card to the manufacturer. Print System Info Sheet. Photographs are helpful. Keep these documents with your records.
Mobile Security Strategies

• Maintain overall security practices such as updating the OS, Anti-Virus, firewall, IDS, etc.

• Keep your browser set to at least Medium security, consider security add-ons (such as No-Script and SiteAdvisor)

• Consider creating and logging on to your computer with a lower privileged account when surfing the web
Additional Measures

- Install security updates for the operating system.
- Disable CD booting in your BIOS.
- Assign a password to your BIOS.
- Disable any guest accounts.
- Rename the default Administrator account.
- Use a secure password. (Upper and lowercase letters, numbers, and symbols)
Additional Measures

- Maintain antivirus and anti-spyware tools. Run frequent scans.
- Encrypt important files or better the whole disc.
- Never open attachments in emails from parties you do not know.
- Avoid downloading "freeware", unless the source is known to you.
– CyberAngel - Alerts unauthorized access to the computer/Locks communication ports to prevent access to the Internet/Notifies monitoring center from where the computer has called.

www.sentryinc.com
Aftermarket Items

USB Grenade
Alarm system (loud)

...Not Vista Compatible
A Case For Obscurity

Where’s the Mobile Device?

- Keep a laptop in a satchel, briefcase or other nondescript bag

- Never leave a laptop unattended in a motor vehicle where visible. Trunks are a last resort

I’m sorry; I should have given links!
Cables Locking Systems

- Cables are attached to the security slots provided in most laptops. Anchor the laptop to a table or desk with the cable.

Price: $10 - $50

http://us.kensington.com/
Alarm Devices

- Attaches to carrying cases, luggage, or notebooks equipped with a security lock slot
- Retractable steel cable retracts into plastic housing at the press of a button
- 95-100db alarm siren activated when lock is engaged; alarm sounds when cable is severed and when motion sensor is armed and triggered; alarm is deactivated when combination lock is released

Price: $20-$50

http://www.dobermanproducts.com/products.htm
Tracking Software

CompuTrace – In use on PCC issued laptops

• Software undetectable and tamper-resistant
• Tracks computer
• Erases the Hard Drive remotely

• PCC Help Desk can verify if you have it on yours

http://www.absolute.com

http://www.lojackforlaptops.com/
Report incidents

If your laptop has been lost or stolen or otherwise compromised. Report it immediately

• **TIME IS CRITICAL**

• Report incidents to any of the following
  – Information Security - 977-4896
  – Help Desk ext. 977-4400
  – Public Safety 977-4902 (including personal mobile devices)
  – Your campus support team

A lost/stolen/compromised mobile device may be forgivable... unless it isn’t reported
Why go through TSS to get a mobile device?

- Ease of ordering
- Compatibility with PCC services
- Hardware parts/Software load/Loaners
- Features/department prices
- Security Assurance
- Support

Other brands support is YOUR responsibility and services may not be available in some cases.

http://intranet.pcc.edu/finance/purchase/dell.htm
Often the weakest link in security is the human
Sometimes it is the strongest

- “The security protocols used to protect the data when loaded onto the laptop were appropriate to the potential harm that might result from inappropriate access to the personal data in question. We are satisfied, based on the information provided, that the key to the encryption software used on the laptop was not stored anywhere on the laptop or elsewhere. We do not see a threat.”
Be Safe, Be Cool!

Eric Jernigan
Information Security Manager
Office: (503) 977-4896
Email: eric.jernigan@pcc.edu
Resources

• Additional Laptop Security Tips
  – http://www.securityfocus.com/infocus/1186

• Ordering a PCC laptop
  – http://intranet.pcc.edu/finance/purchase/dell.htm
  – http://intranet.pcc.edu/its/policies/pcpurchasing.htm

• Backup Solutions
  – http://www.faronics.com/
Resources

- Encryption Software
  - http://www.truecrypt.org/
  - http://www.freewarepalm.com

- Alarm Devices

- Tracking Software
  - http://www.lojackforlaptops.com/
  - http://www.absolute.com

- General Tools
  - http://noscript.net/
  - http://www.siteadvisor.com
• RFID threats paper “Is your cat infected with a computer virus”
  – http://www.rfidvirus.org/papers/percom.06.pdf