Cyber Security for Mobile Devices and Social Networking Sites
By Dan Steward M.S. MCSE, RHCE
Vanderbilt University—Institute For Software Integrated Systems
Mobile Devices—CyberSecurity

- Best Practices in Smartphone and Laptop Security
- Smartphones
- Laptops
- Netbooks
Vanderbilt University—Institute For Software Integrated Systems
Research Institute
Research Scientists
Conduct Research in Model Integrated Computing
Develop Applications with Grant Funds provided by DoD, Boeing, Darpa, private businesses to name a few
Research Scientists are Ph.d Instructors in the School of engineering and computer science at Vanderbilt University as well as advisors for students pursuing their doctorates.

- Very Busy People
- Travel extensively around the United States and the world
- Mobile Devices, i.e. smartphones and laptops are a way to stay in touch
Before the advent of the smartphone, researchers had to wait until they were able to use their laptops back at the hotel when traveling to check their email and to gain access to the internet.

Due to the secure nature of the sites where they travel, in most cases they are not allowed to use their laptops...
They use the smartphone/pda to check email, send email, calendaring, address books or contacts, music, photos, voice memo, compass and other apps at their fingertips.

Main application is email used to access an Exchange Server or Linux Post fix.

Utilize Active Sync via the smartphone to IMAP email and calendars to the phone.
Researchers also use their mobile devices for tethering (use phone as modem) to connect the laptop to the mobile broadband and also for Wifi and local development.
How Secure Is the Cyberspace

- What are some cyber threats
- What are some of the best practices for securing mobile devices
What Are Some Network Security threats for laptops

- Hotel Networks not secure
- Unencrypted hotel or public networks such as Starbucks or Panera bread.
- Improperly configured firewalls
- Lack of VPN clients
- Unsecured lost or stolen laptops
Things to Do To secure Your Laptop Data

- Store only what is necessary on your laptop
- Spreadsheets, financial data and other personal data such as ssn’s should be on an encrypted share or drive
- Protect data passing over a network from eavesdropping,
- When using Web accessed email use HTTP over SSL
Things to Do To secure Your Laptop Data—cont)

- Configure secure email certificates and encryption for email—Comodo
- Configure a personal firewall on the laptop such as the one that comes on Windows XP, Windows Vista or Windows 7. Windows 7 Professional firewall blocks incoming and outgoing ports that you specify
- Configure Bluetooth connections to only allow authorized access.
- TrueCrypt and PGP third party file and disk encryption.
Things to do to secure your laptop--continued

- Ensure that your data is backed up on a regular basis just in case your disk dies.
- Finally you should keep your system up to date with patches, operating system and anti-virus updates.
Think of a smartphone as a laptop
The only difference is they access the internet via a cellphone carrier
Best Practices for Smartphone Security

- The biggest threat to smartphone data loss is losing it.
- Always have your smartphone password protected.
- If you don’t have to, don’t store sensitive data on your smartphone.
- Use a VPN Client on your smartphone.
- Encrypt the data on your smartphone.
- If your smartphone is lost or stolen, call your carrier, some carriers have a way to remotely wipe and lock the smartphone.
Best Practices for Smartphone Security

- Can Smartphones get viruses or worms?
  - The answer is yes
  - They typically arrive via email or sms
  - Just as with any other PC, you should keep the software to your smartphone up to date
  - All major cellphone vendors have some sort of anti-virus software.
- Do not jailbreak your phone
- Do not install SSH on your smartphone w/o changing the root password.
Smartphone security

- Just as with your laptop, netbook or pc, do not click on a link in an email or text from a source you are unfamiliar with.
- Another method of installing malicious software on the smartphone, is sending a link via SMS, that looks like it comes from the carrier.
- Be careful when using your smartphone with wi-fi.
- Disable wi-fi and bluetooth unless you absolutely need it.
Securing your Social Networking Portal

- What is a social networking portal
- Facebook
- MySpace
- Twitter
- LinkedIn
Social networking sites sometimes referred to as “friend-of-a-friend” sites, build upon the concept of traditional social networks where you are connected to new people through people you already know.

Social networking sites differ, but they all have one thing in common, they allow you to share some information about yourself, and they provide some form of communication either in the form of email, chat, forums or instant messaging.

Some call them “communities” or groups of users with similar interests.
What are some risks facing Social Networking Sites

- Many of the social networking sites have very laxed default private settings.
- HTML should be disabled inside of comments.
- Most all Social Networking sites share by default all profile information.
- Social Networking sites allow you to link to offsite content, which could potentially be malicious.
What Securing Implications Do Social Networking Sites provide

- Sites encourage you to offer a certain amount of personal information.
- People tend not to exercise the same amount of caution as they would when first meeting a stranger, because:
  a. the internet provides a sense of anonymity
  b. the lack of physical interaction provides a false sense of security
  c. people offer information that was only initially intended for a friend not for strangers
  d. they want to offer insights to impress potential friends or associates
Limit the amount of personal information you post, for example your address or where you work or your routine.

Keep in mind that the internet is a public entity. Even though you post something, it may still be in cache on another person’s machine.

Be wary of strangers, limit the types of people that are allowed to contact you on these sites.

Be skeptical of what you read online. People lie and exaggerate.
How to protect yourself from risks on Social Networking sites–cont

- Evaluate your default settings
- Use Strong passwords
- Check privacy policies
- Use and maintain antivirus software
7 Things to stop doing now on Facebook

- Using a weak password
  a. avoid simple names or words found in a dictionary
  b. mix upper and lower case letters numbers and symbols
  c. Password should be at least eight characters long, insert numbers and letters in the middle of a word: e.g. hO27usES!

- Do not leave your full birthdate in your profile
  a. its an ideal target for identity thieves

- Overlooking useful privacy controls
  a. For almost everything in your profile, you can limit access
  b. Limit access to friends or friends of friends.
7 Things to stop doing on Facebook

- Do not post your child’s name in photo tags or captions
- Don’t mention that you’ll be away from home
  a. its like putting a no one’s home sign on your door at home
- Don’t allow search engines find you
- Do not allow youngsters to use Facebook unsupervised.