

Remote Computing Safety

Mark Smylie Hart – CITES Security Officer
GIAC Certified Intrusion Analyst

30 November, 2005

Remote Computing Safety

Topics for today:

Wireless Connectivity

On-Campus vs. Off-Campus
Shoulder Surfers
Sniffers and Rogues

Home Connectivity

Dialup vs. Broadband

Encryption

WEP vs. WPA
VPN Usage

Remote Computing Safety

Fundamentals:

Trust no-one

Strong Passwords

Firewall EVERY network connection

AntiVirus Software

SpyWare/AdWare Protection

Software Vendor Patches

Common Sense

Remote Computing Safety

One more fundamental concept:

'He who knows the Enemy and Himself will never be defeated in a hundred battles.'

-Sun Tzu
The Art of War

Know your enemy – What would an attacker want? What would he be looking for? Where would he hide?

Know yourself – What is your password? What do you do on your computer? What do you do for the University? Where are you sitting right now?

Remote Computing Safety – Wireless Networking

Where do you use Wireless?

Coffee Houses

The Union

Airports

Hotels

Home

When you connect to a network, **KNOW** what you're connecting to.

Access Points vs. Ad-Hocs

The two networks look different in the Windows Wireless Networking helper utility, and even more information is available if you run a utility such as NetStumbler (www.netstumbler.com).

Remote Computing Safety – Wireless Networking

Beyond the *type* of network you connect to, it's important to know where you are physically.

Hotels and Airports are prime territory for attackers.

Hotels: Wireless sniffing can capture your login/password information and data packets can be reconstructed to reveal whatever you were doing.

Airports: Huge potential for information theft. Once you close your computer to board your plane, an attacker has lots of quality time with your account info. Also be on the lookout for shoulder surfers.

If you're not using your wireless connection, turn it off!

Remote Computing Safety – Home Connectivity

Dialup

Attack threat exists, but not as severe. Password loss should still be seen as an issue.

Broadband

Default configuration of some operating systems may make computers on broadband connections **MORE** vulnerable to attack.

Patch your system with extreme prejudice!

Wireless at home?

Default configuration of access points you purchase at Store of Choice is **VERY** insecure – the manufacturer wants it to be easy to use.

Default configuration of some operating systems can leave you exposed to attack from a poorly configured laptop that happens to be walking by your house.

Remote Computing Safety – Home Connectivity

What can you do about insecure wireless?

See a qualified therapist

Driver and Firmware Updates

MAC Filtering

SSID (Service Set Identifier) Broadcast

WEP (Wired Equiv. Protection) vs. WPA (Wi-Fi Protected Access)

If you must share resources at home, share responsibly (configure your firewall to allow sharing to your subnet only...specify subnet!!)

By default, windows wants to share to everyone – don't let it.

Remote Computing Safety – Home Connectivity

What can you do about insecure wireless?

There are many resources available to help you get the job done.

CITES HelpDesk (244-7000 / consult@uiuc.edu)

On-Site Consultants (333-8628 / onsite@uiuc.edu)

Contact the vendor

World of Windows Networking (<http://wown.com>)

Remote Computing Safety – Encryption

WEP – Wired Equivalent Privacy

“...The bottom line for wireless networks is that you can't count on WEP to provide even minimal security...”

-Matthew S. Gast

802.11 Wireless Networks-The Definitive Guide (O'Reily)

(Open = Open!)

Coffeehouses and Airports aren't typically using WEP because of the complexity in setup (must cater to a lower, more common denominator).

Know your environment and enable your firewall.

Remote Computing Safety – Encryption

UIUC VPN Client

QuickConnect – the University’s wireless network available in most public spaces – only allows the following functions:

<u>Service</u>	<u>Port #</u>
SSH/SFTP	22
Email	25
Secure Email	993/995
Web Traffic	80/8080
Secure Web Traffic	443
Network Time	123
VPN's	500
Printing	515
Instant Messaging (AOL/MSN)	5190/1863
Remote Desktop (Windows)	3389

Remote Computing Safety – Encryption

UIUC VPN Client

Install the UIUC VPN Connector (www.cites.uiuc.edu/vpn)

The VPN creates an encrypted tunnel between your machine and the University's network that would be very difficult to penetrate by an attacker.

The VPN Client will allow you to connect securely from anywhere and allow you full network connectivity...as if you were sitting at your desk.

Also, the VPN Client will allow you to remain connected to the network for 24 hours straight (auto-disconnect after 90 minutes of inactivity).

QuickConnect will disconnect you after one hour unless the VPN client is running – very frustrating if you start an email at 59:42

Remote Computing Safety - Conclusions

Fundamentals:

- **Trust no-one and use Common Sense!**
- **Create a Strong Password**
- **Firewall EVERY network connection**
- **Keep your AntiVirus Software up-to-date**
- **Keep updated with Software Vendor Patches**
- **Know your computer's 'normal' behavior**
- **Use the UIUC VPN Client EVERY time!**

Beyond that...

- **Use the CITES HelpDesk as a resource (244-7000)**
- **Don't forget about the good people at Google**

Remote Computing Safety

Thanks for coming!

Send feedback to:
securitysupport@uiuc.edu