Emory Unplugged
Emory’s Wireless LAN Infrastructure

Stan Brooks CWNA, CWSP
Emory Network Communications
stan.brooks@emory.edu
AIM-Y!-MSN: WLANstan

Copyright Stan Brooks 2007. This work is the intellectual property of the author. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the author. To disseminate otherwise or to republish requires written permission from the author.
Outline

- Connecting to Emory’s wireless network
- Emory’s wireless network scope
- Wireless information & resources
- Wireless security at home & on the road
  - Why you need it
  - How to achieve it
Wireless Connection Methods

- **EmoryUnplugged**
  - Best and safest connection method available
  - Need Emory NetID/password for authentication
  - WPA/WPA2-Enterprise
    - Encrypted & Authenticated
    - Requires some initial configuration the first time you connect
    - Turn on your laptop & go for subsequent sessions

- **EmoryGuest**
  - Good for iPhones and other devices that can’t do WPA-Enterprise
  - Limited functionality guest connection
    - Web-surfing ONLY and bandwidth-limited
    - Re-authentication required every 4 hours
  - Unencrypted
Connecting to EmoryUnplugged

- **Windows (XP/Vista)**
  - Unless you use Windows Zero Config, each manufacturer’s client is different.
    - May need to experiment to achieve connectivity
  - The latest drivers solve a lot of the connectivity issues we’ve seen.
    - Obtain from the laptop or Wi-Fi card vendor
    - Reference drivers can address some obscure issues
      - Obtain from the chipset manufacturer

- **Mac**
  - Usually it just works.

- **Other OS’s (Linux) & Devices (PDAs or tablets)**
  - Must support EAP-PEAP-MSCHAPv2 for authentication
  - Use **EmoryGuest** if unable to connect through **EmoryUnplugged**
Personal Wireless Device Registration

- **PWD’s**: Personal (non-computer) Wireless Devices
  - iPhones, PDAs (Win/Palm/other), and other devices
  - PWD’s are able to use *EmoryGuest* without using a browser to log in through the guest access captive portal.

- Available wherever *EmoryGuest* or *EHC Guest* access is available.

- The same guest access limitations apply to PWDs.
  - Limited bandwidth (500kbps)
  - Limited services (Web/Secure Web, VPN)

- Manual registration process
  - Bring device to GBS Information Services or Clean Room in the North Decatur Building for registration.

*This is considered an experimental or “Beta” service*
EmoryUnplugged – Wireless Footprint

- Wireless Coverage in over 130 buildings and outdoor areas
- Full coverage in the Goizueta Business School
- Detailed maps at AAIT’s website
- Best way to check – Open your laptop and look for EmoryUnplugged or EmoryGuest
Wireless Information & Resources

http://www.it.emory.edu/wireless

- This URL has links to
  - Maps
  - Policies
  - FAQs
  - Getting Started instructions/PDFs for Mac’s & PC’s
  - Links to Software Express for free install scripts
There are 3 main areas to address:

1) Protect data as it travels from source to destination
2) Protect the client from unauthorized access
3) Protect the network from unauthorized/compromised users
Safe HotSpot Wireless Computing

Assume the network connection is *HOSTILE* - practice safe computing!

- **Enable/use Personal Firewalls**
  - Properly configured for “Internet” or untrusted connection
- **Configure your Wireless Client for security**
  - Do NOT connect to non-preferred wireless networks (usually off by default)
  - Do NOT automatically connect to an open wireless network – Set client to ask you (On Demand/Manual)
  - Just Say No to Ad-Hoc Networks (They are REALLY BAD for security reasons)
- **Encrypt your traffic**
  - WPA / WPA2-Enterprise (probably not available at hotspots)
  - Virtual Private Networks - VPNs
    - Use Emory VPN services to encrypt your traffic when connected to open networks
      - SSL VPNs (Emory’s FirePass VPN: [https://vpn.emory.edu](https://vpn.emory.edu))
      - PPTP or IPSec (Emory’s PPTP VPN: vpn.service.emory.edu)
    - Corporate VPN

*Remember: HTTP, POP3, IMAP, FTP, Telnet and other protocols send credentials and data as clear text, so encrypt to be safe!*
Security Tip for Windows

- Windows “Probes” for **ALL** networks in its “Preferred Networks” List
  - Windows will attempt to automatically connect to **ANY** network in its “Preferred Networks” list – including Ad Hoc Networks
  - Any successful association (connection) with a wireless network is automatically added to the “Preferred Networks” list
  - To prevent unintended connection to fake or “Trojan” APs, set Open and Unauthenticated network connections to “On-Demand” or “Manual”
Safe SOHO Wireless Computing

- On your clients:
  - Do NOT connect to non-preferred wireless networks
  - No Ad-Hoc Networks (Ad-Hoc networks are REALLY BAD for security)

- On your router:
  - Please, Please, Please! - Change your router’s default configuration
    - CHANGE THE PASSWORD FROM THE DEFAULT
    - Change the SSID from the default
      - Choose an SSID that does not identify you or your geographic location
    - Set the channel to 1, 6, or 11 to reduce interference
  - Read the directions and set up WPA-PSK or WPA2-PSK
    - Choose a difficult to guess and long (32+ character) passphrase that has upper/lower case, numbers, and punctuation.
      - Example: “Emory\University/Rox*My<2>smallW0RLD!!!Yeah!”
    - WPA-PSK can be subject to dictionary attacks, so misspelled words, added punctuation and longer keys will help mitigate this type of attack – just make it easy for YOU to remember
Recap

- Emory’s Wireless Network scope
- How to connect to Emory’s Wireless Network
  - EmoryUnplugged
  - EmoryGuest
- Web resources for more information
- Protecting yourself when connecting at Wi-Fi hotspots & at home
Questions

Stan Brooks – stan.brooks@emory.edu