Real-World Wireless Network Security

What We Want

- Easy to use
- Broad compatibility
- Low administrative overhead
- No special client software

What We Have

- Wi-Fi drivers overcomplicate the task of setting SIDs or WEP keys
- Current Wi-Fi systems do not include any unique client identifiers
- VPNs, LEAP, 802.11x, etc. require certain cards, drivers and operating systems, tend to be complex and unreliable, and it will be years before we can assume otherwise

The Compromise

We cannot trust wireless clients any more than general Internet hosts and will not waste time pretending otherwise

Wireless Setup

- Stock 802.11b
- Broadcast SID
- No WEP
- Access points on a highly-untrusted VLAN

Registration

- The first time a system is connected, all outbound web requests will be redirected to a registration page
  (See http://www.net.cmu.edu/netreg/)
- Registration provides limited accountability by restricting access to people who already have accounts.
- A side benefit is the security warning every user will see during the registration process

Registration Details

- DHCPD v3 allows you to serve different IP ranges to known MACs
- Unregistered MACs are assigned a separate IP range with a special DNS server, 30 second lease times and no internet access
- The registration web server's IP is returned for every DNS request

Registration Details

- The registration web server issues a redirect for any HTTP request to the HTTPS server `netreg.example.edu` to avoid browsers caching our page instead of the real `www.nytimes.com`
- After authenticating the user's MAC is added to the registered client list in dhcpd.conf

Security

- Registered clients are behind NAT and a firewall to protect the internal network from abuse
- Snort sensor inside the NAT layer
- Rate-limiting 802.11b is an exercise in optimism but we should do it anyway

Security Details

- Open internet access limited to the ports used by encrypted protocols for web (443), email (993, 995), and ssh (22)
- Unencrypted HTTP is diverted to squid
- Windows and Mac file sharing limited to two secured servers
- Everything else is dropped

Known Problems

- Registration can be bypassed using MAC spoofing
- Potentially nasty things may be tunneled over SSL ports
- SMTP AUTH requires client support

Future Directions

- Compromise on ease of use and security by allowing PPTP, IPSec or PPPoE users greater access
- Use of per-host bandwidth allocation
- Automatic de-registration after long periods of inactivity
- Automatic reaction by the IDS to add firewall rules for hosts which demonstrate worm, spammer or kiddie behaviour