802.11i: The User Perspective

Or

How I Learned to Stop Worrying about War Chalkers and Love WLANs

NIST WLAN Security Meeting

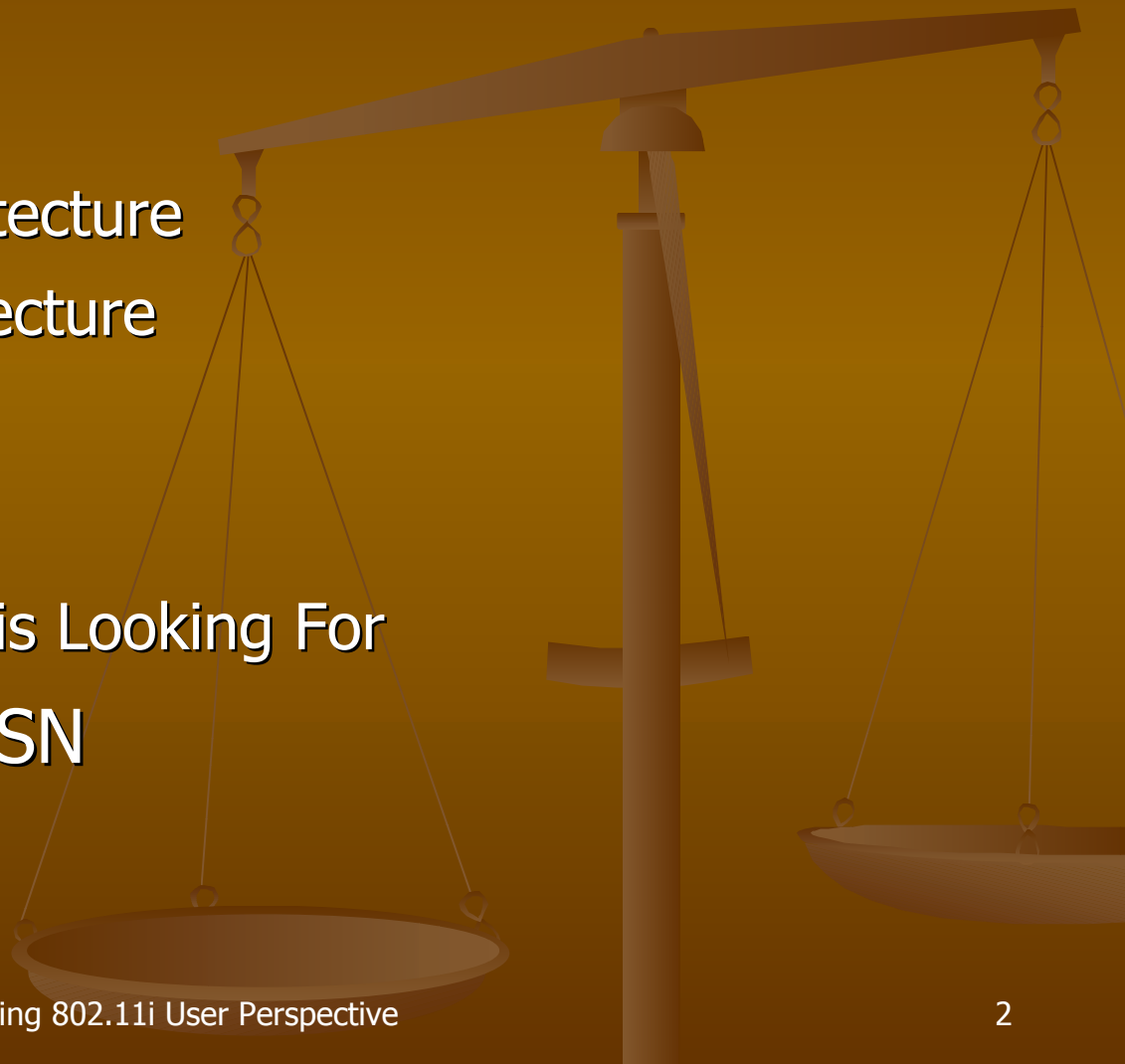
December 4-5, 2002

Stephen T. Whitlock
stephen.whitlock@boeing.com

Paul Dodd
paul.dodd@boeing.com

Agenda

- Steve
  - Background
  - Current Architecture
  - Target Architecture
- Paul
  - Test Results
  - What Boeing is Looking For
- Migration to RSN



Background

- Initial deployment
  - Ad-hoc implementations
    - Rapid growth (~1000 Access Points, 90% in Factory)
    - Endless variety of client devices
    - WEP encryption used inconsistently
    - No WLAN security architecture or policy
    - Deployed as extensions of the wired network
  - Caused the Access Points to be shut down in Aug 2001 while security architecture and policies were developed

Uses

- Flight line assembly
  - Moving aircraft assembly line requires wireless connections to workstations
  - Wireless wearable computers provide information directly to workers
- Conference rooms
  - WLANs provide consistent access to mobile workers
- Office areas
  - WLANS simplify cabling and provide ubiquitous coverage

Client Types

- Laptops and other computers
  - Can use existing and future solutions
- Resource challenged devices
  - Palm, Pocket PC, Bar Code scanners, etc
  - Can use some security solutions
- Devices without a user interface
  - Printers, embedded machine controllers
  - Automated device authentication needed
- Really, really dumb devices
  - Sensors, RFID tags
  - No OS, no crypto support, etc.

Current Architecture

- Network Services named as sole wireless LAN provider
- WLANS treated as untrusted networks
  - Partitioned from wired network
  - Access via VPNs using two-factor authentication and encryption
  - Increased application security
- WEP required
  - Reduces exposure
  - Provides legal barrier
- Wireless policy established
  - Ad-hoc WLANs not permitted

Issues

- IEEE 802.11 Wired Equivalent Privacy (WEP) protocol lacks effective security
  - Group-keyed access control
  - No user authentication
  - Flawed encryption
  - Radio signals extend beyond Boeing property
  - Interception is hard to detect
- VPN solution is unwieldy
  - Limited availability of VPN client software
  - VPN's require frequent reconnection

Target Architecture

- Embrace IEEE 802.11i Robust Security Network (RSN) standard to enable WLANs to be trusted
  - Native per-user access control
  - Native strong authentication (e.g. token cards, certificates, and smart badges)
  - Native strong encryption
  - RSN Availability unknown
- Evaluate and deploy Wi-Fi Protected Access
  - In testing now

Early Test Results of WPA

- First testing of beta software was in September 2002
  - ✓ Supports 802.1x/PEAP, with Dynamic WEP or TKIP
  - ✓ Supports Safeword token cards and Soft Token
  - ✗ Only works with W2k SP3+ and WXP clients
  - ✗ Did not support VLAN's
  - ✗ Did not support network login at the GINA
  - ✗ Did not support existing Boeing user certificates

Client Test Results

- Only works with W2k SP3+ and WXP clients
  - Windows 2000 SP1 is our current default for laptops and desktops
  - Windows CE? Pocket PC? Pocket PC 2002? Unix flavors? Linux? PalmOS?

Authentication Test Results

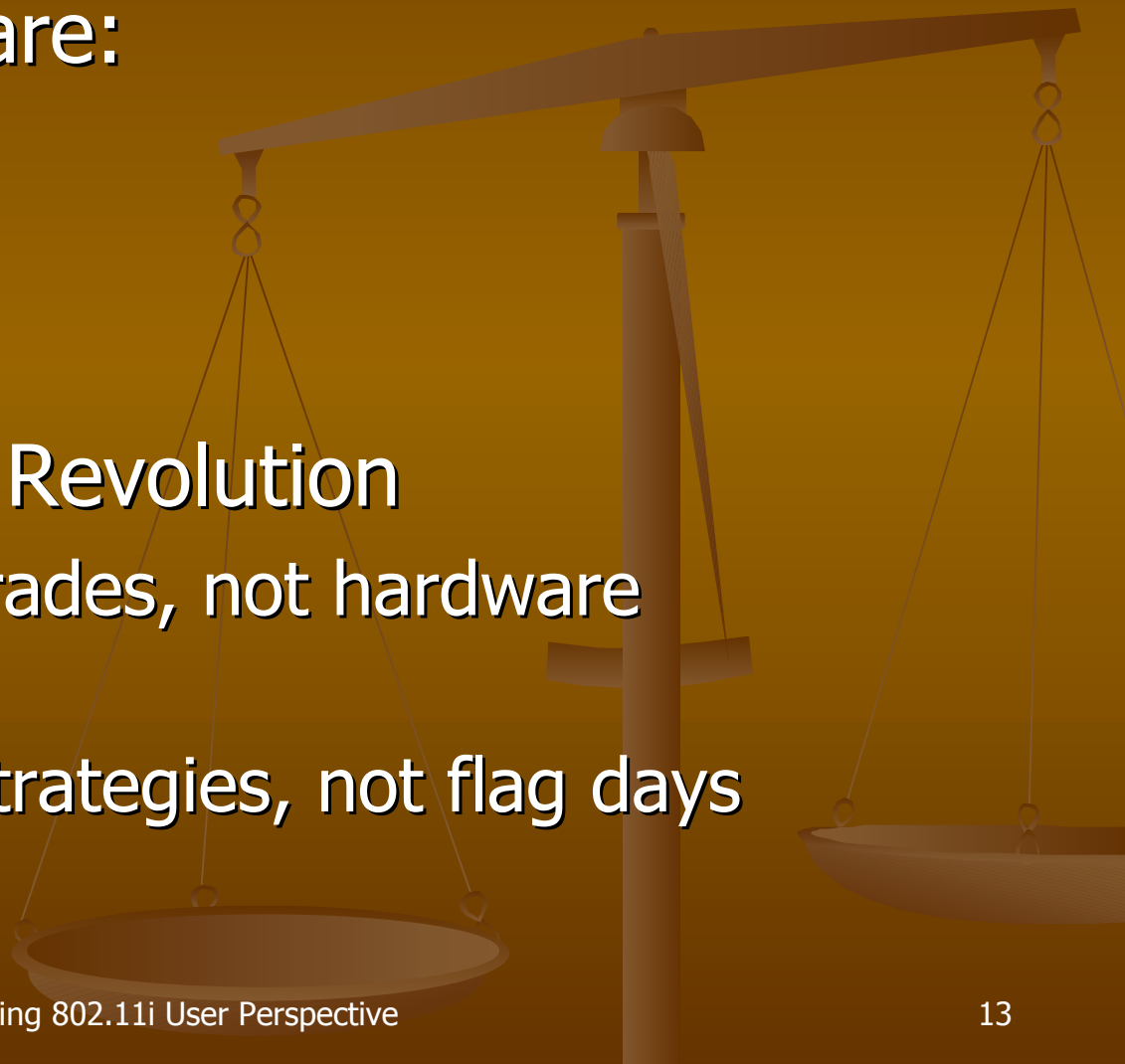
- ✓ Can switch between hard tokens and soft tokens on the fly
- ✗ Requires certificates to have a "Client Authentication" Extended Key Usage (EKU) field which is not in production Boeing certificates
- ✗ Can't switch between token card (PEAP) and certificate (EAP/TLS) authentication without first logging in with cached credentials
- ✗ PEAP supplicants battle each other for control

Infrastructure Test Results

- ✓ Newer software release now supports VLAN's
- ✓ Software-only upgrade to AP's and RADIUS server
- ✗ AP and RADIUS server configuration is complex and difficult

What Boeing is Looking For

- Our Priorities are:
  1. Usability
  2. Security
  3. Affordability
- Evolution, not Revolution
  - Software upgrades, not hardware replacements
  - Coexistence strategies, not flag days



What Boeing is Looking For

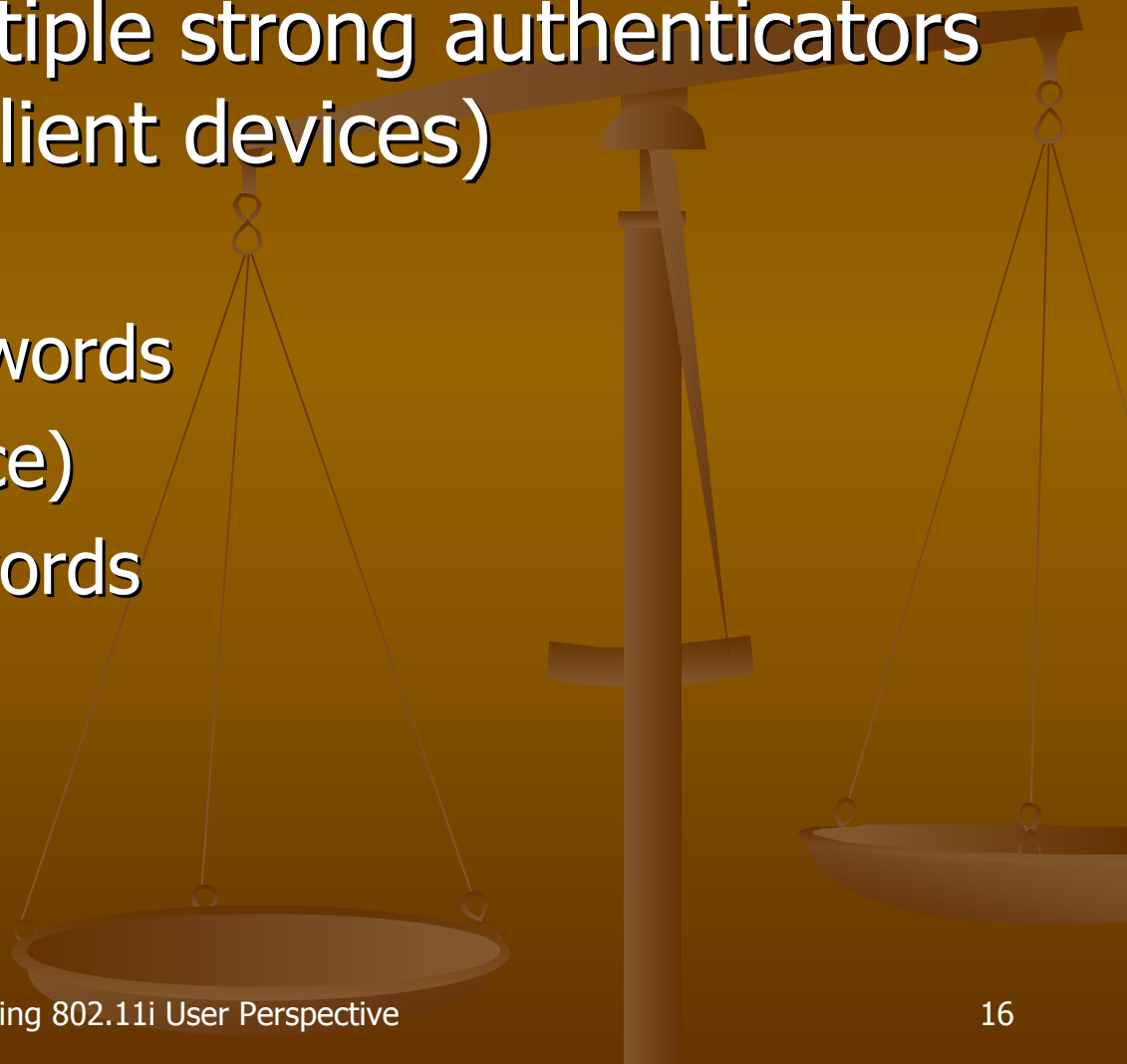
- Our users are mechanics, technicians, and engineers
  - Not just office workers
- Our environment is mobile and fluid, with hazardous substances and devices that are subject to being dropped
  - No open device ports (e.g. smart card, USB)
  - Can't depend on standard keyboards

What Boeing is Looking For

- Most clients will be bar code scanners, RFID tags, embedded controllers, handheld computers, and PDA's
  - Not just laptops
  - No touch labor to configure or admin
- Computers are tools that are shared
  - No assumption of cached credentials, or a single authentication type

What Boeing is Looking For

- Support for multiple strong authenticators (for users and client devices)
  - ✓ Certificates
  - ✓ One Time Passwords
  - ✓ Biometrics (voice)
  - ✗ No static passwords

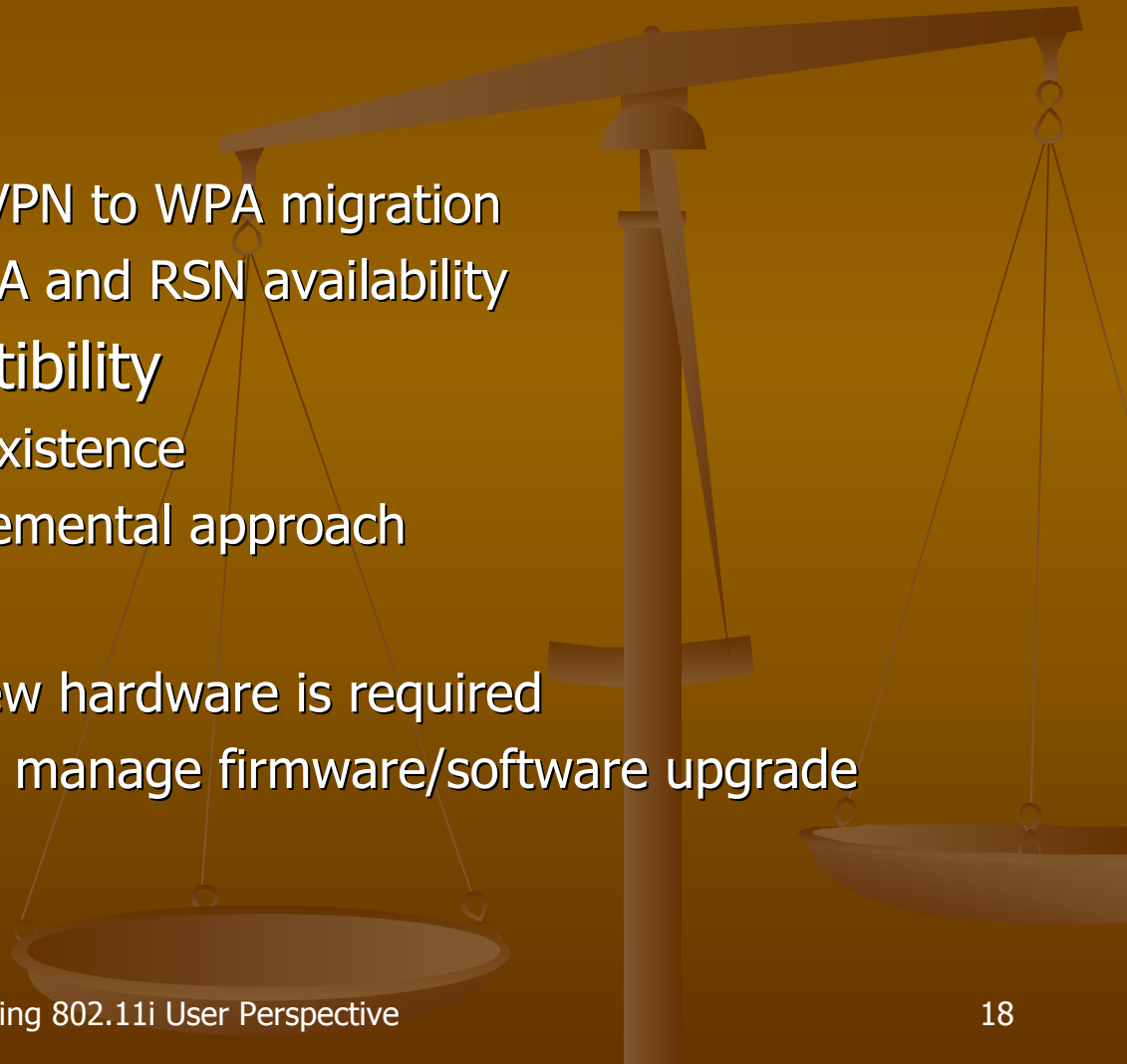


What Boeing is Looking For

- Flexible networks
  - Devices that can easily transition between Ad-hoc and Infrastructure mode
  - Assembly support WLAN inside the fuselage could become a fly-away WLAN upon delivery
- Secure Ad-Hoc networks (IBSS)
  - Print to the nearest printer
  - Detachable UI (screen, microphone)

Moving from WPA to RSN

- Depends on
  - Timing
    - Progress of WEP/VPN to WPA migration
    - Time between WPA and RSN availability
  - Backwards compatibility
    - WPA and RSN coexistence
    - Availability of incremental approach
  - Migration process
    - Whether or not new hardware is required
    - Ability to remotely manage firmware/software upgrade



Moving to RSN – Continued

- Benefits of RSN in order of interest
  1. P2P security
  2. Connection reestablishment
  3. AES
- Likely scenario
  - Implement new AP installations using 3 VLANs (WEP/VPN, WPA, and RSN)
  - Gradually migrate existing APs to add an RSN VLAN
  - Client devices will upgrade independently, based on business need