The Convergence of Ubiquity: The Future of Wireless Security

William A. Arbaugh
Department of Computer Science and UMIACS
University of Maryland
College Park, MD
waa@cs.umd.edu
http://www.cs.umd.edu/~waa
Talk Overview
(with apologies to Dickens)

• Wireless Networking Overview
• Why Wireless Security is Different
• Hop by Hop vs. End to End

• The Ghosts of Wireless Security Past
• The Ghosts of Wireless Security Present
  • Wi-Fi Protected Access
  • Denial of Service

• The Ghosts of Wireless Security Future
  • Trends
  • Interworking
  • Device security
Wireless Networking is Experiencing Exponential Growth

19,482 for 2002 according to Gartner Dataquest 1/03

WLAN Shipments

Source: In-Stat/MDR, 7/02
WLAN Sales

2,320 for 2002 according to Gartner Dataquest 1/03

Source: In-Stat/MDR, 7/02
Wireless Networking

• The next Internet, or
or the next Bubble?
The Future of WLAN’s?

- 4G?
- Hot spot coverage only ala Boingo et. al?
- Or some sort of overlay blend?
- Regardless- the rapid growth will continue.
WLAN Urban Legend

- 802.11b is “secure” because it uses frequency hopping or spread spectrum!
- Using IPsec or SSH is all that’s needed to provide complete security!
- I haven’t heard of anyone’s WLAN being exploited—so I’m OK!
- All of the known attacks require a sniffer which is difficult to find and expensive. Thus, you’re safe!
- Attacking WLANs requires expensive and specialized tools!
The Threat

• In general, there are four threat classes:\footnote{Modifications to the model originally proposed by \cite{Abraham et al.}}:
  • Journeymen (Class 0)
  • Experts (Class 1)
  • Insiders (Class 2)
  • Well funded professionals (Class 3)
Why Wireless Security is Different

- An attacker has access to the transport medium of your network!
- Essentially elevates the experts to an insider (higher threat)
The Wireless Threat

Used with permission from KARS: http://www.ittc.ku.edu/wlan/
Hop by Hop vs. End to End

• End to end security is necessary, but only sufficient if and only if strong mutual authentication occurs.

• PEAP attack [Asokan, et.al.]

• Human factors, e.g. “Social Engineering”

• Requires global non-forgeable identity
• End to End cannot guarantee availability!
• Routing attacks
• Michael DoS (We’ll see this later)
Wired Equivalent Privacy

- What exactly does that mean?
- My guess:
  - Prevent unauthorized use (access control, authentication, and integrity)
  - Prevent unauthorized disclosure (confidentiality)
  - Prevent unauthorized eavesdropping (Not likely to happen in consumer wireless)
Identity

- The current standard only uses the MAC address as a form of identity.
  - Unfortunately, the MAC address is malleable and further compounded by inadequate cryptographic binding [Walker, Borisov et. al., Arbaugh et. al.].

- The future standard uses two forms of identity: MAC address at the link layer, and a user ID at the network layer.
  - Requires cryptographic binding between the two ID’s [Mishra et. al.].

**nb.** History buffs will remember that the AMPS (Cellular) system made the same mistake with the equipment serial number (ESN).
Access Control

- **MAC access control lists**
  - *MAC address is forgeable* [Arbaugh et. al.]
- Proprietary “closed network” used a shared secret as access token.
  - *Access tokens broadcast in the clear in management frames* [Arbaugh et. al.]

nb. Here the reliance on the expense/difficulty in eavesdropping as a security mechanism is again a mistake the cellular community made.
Integrity

- The lack of any message authenticity mechanism, or the reliance on error detection (CRC) for integrity protection.
  - A linear CRC combined with a linear combiner, XOR, allows “bit flipping” [Borisov et. al.].
WEP Block Diagram

Encryption Key $K$
Init. Vector $IV$
Plaintext data byte $P$

Pseudo Random byte $b$

RC4

Ciphertext data byte $C$

Decryption works the same way: $P = C \oplus b$
Confidentiality

- IV space is only $2^{24}$
  - Creates Depth [Walker, Borisov et. al.]
  - $c_1 \oplus c_2 = (p_1 \oplus r) \oplus (p_2 \oplus r) = p_1 \oplus p_2$
- Lack of Replay protection combined with stream cipher
  - Asynchronous known plaintext attack [Walker, Borisov et. al.]
  - Synchronous known plaintext attack [Arbaugh]
- IV as first part of key
  - Induces several classes of weak IV’s. The most damaging being when the IV is of the form $<n, FF, x>$ [Fluhrer et. al.]
Mitigating FMS

- Most all vendors have implemented IV filtering to prevent FMS attacks.
- Reduces IV space from $2^{24}$ to $2^{18}$ in some cases.
- Prevents FMS attack that required on average several hours, but ....
- Reduces the work-factor of a previous attack (Inductive Chosen Plaintext) from 18 hours to 80 minutes!!!
Authentication

- The use of a challenge response system covered by a Vernam cipher.

- Eavesdropping on a single successful authentication provides the attacker the ability to authenticate at will [Arbaugh et al., Borisov et al., Walker]
The Ghosts of Wireless Security Present
Wi-Fi Protected Access (WPA)

- Announced early of this year by WECA
- Available real soon now
- Essentially a subset of IEEE draft
- Designed to support legacy equipment via new firmware and drivers
WPA

- Confidentiality: Per-packet keying via TKIP
- Message Authenticity: Michael algorithm via TKIP
- Access Control: IEEE 802.1x
- Authentication: EAP/TLS
WPA Commentary

- WPA will provide a tremendous increase in security.
- However, WPA is based on several new and domain specific protocols.
- As such- it SHOULD only be considered as an interim solution until Robust Security Network, aka WPA2, equipment becomes available.
RSN aka WPA2

- Due “Real Soon Now” - actually product won’t ship until Q3 or Q4 2004.
- Will require hardware upgrades to support AES in most cases (some of the newer cards/AP’s may not).
• Confidentiality: Per-packet keying via TKIP or AES CCMP

• Message Authenticity: Michael algorithm via TKIP or AES CCMP

• Access Control: IEEE 802.1x

• Authentication: EAP/TLS
Both WPA and RSN

- will provide tremendous improvements in Confidentiality, Integrity, Authentication, and Access Control
- but ......
- Availability will remain an issue
Denial of Service

- **ALL** past, current, and future Wi-Fi standards are susceptible to Denial of Service attacks at multiple layers.
  - **Layer 3 (EAP DoS)**
  - **Layer 2 (Michael DoS, unauthenticated management frames)**
  - **Layer 1 (CTS, Power Save)**
The Ghosts of Wireless Security Future
Trends

- Computing devices shrinking and becoming more capable
- Networks becoming ubiquitous
- Users becoming more mobile
- Content becoming active
- Software defined radios appearing
What is Interworking

- Interworking permits the user to transparently roam between different networks—usually with different PHY and administrative domains.
Transparent Roaming / Interworking

CDMA

WLAN
Why is Interworking Important?

- Ubiquity: User’s are demanding continuous connectivity.
- Ease of use requirements demand transparency.
- Sound business practice (and user privacy requirements) demand security.
Interworking Properties

- Security
- Transparency
- Simplicity

Availability
- User’s :-) $$
- Denial of Service
- Fraud
- User Complaints

Denial of Service $\times$
Wireless Device Security and Firewalls

- In the future everything will radiate- your fridge, your picture frame, even down to small parts (RFID).

- Most of these devices will also have IP addresses- Imagine the headline:

  Amazon DoS’d by Fridges, Toasters and phones - oh my!
Current Environment

- Small and large companies using Firewalls and anti-virus as the ONLY means of protection.
- Many home users connect via cable or DSL with no protection.
- Users are moderately mobile (Discrete Operation)
  - Laptops while traveling
  - VPN used to connect to office
- This simple operating model has created a significant management problem
Some of the Problems with Firewalls
Today’s Firewall

- Not as effective as a decade ago because of multiple “piercings”
- User mobility creates potential vector for malice
- Active content
- User “creativity”
- Crappy software
- Peer to Peer programs
Future Environment

- Dramatic increase in mobility (always on)
- Ubiquity of network access
- Ubiquity of more powerful computing devices
- IPv6, i.e. every device has a routable IP address
- Active content increasing
- Peer to Peer increasing
Future Environment

- Devices may require multiple management sources
  - A handset may need to receive updates from the manufacturer,
  - The developers of installed applications, and
  - Receive user and/or organizational data
Future Environment

- Management will become **significantly** more difficult
- Separation of management instructions is a **MUST**,
- Many organizations will want to be “**in the loop**” on all management instructions,
- Devices are “**always on**”
Conclusions

- Things are bad, but they are getting better. However, numerous challenges exist before we can have complete and secure ubiquitous computing.