WLAN & 802.11 SECURITY

Presented

by

Brian Mansfield

Chief Wireless Consultant
The Mansfield Group, LLC

June 18, 2002
Internet Developers Group
Netscape Communications
Mountain View, CA

The Mansfield Group, LLC

www.itvshop.com/wlan-security

WLAN Security Services

1. 802.11 Network Integration

- 802.11 security threat assessments
- WLAN site surveys & new installations
- WLAN security design & implementation

2. WLAN Security Workshops

- Public security workshops
- Private security workshops (Industry/Organization Specific)

UPCOMING WORKSHOPS

Wireless LAN & 802.11 Security Workshops:

LOS ANGELES	**July 11, 2002**
CHICAGO	**August 13, 2002**
NEW YORK	**August 15, 2002**
REGISTRATION:	**www.itvshop.com/wlan-security**

INTRODUCTION:

SECURITY GOALS

1. **Authentication** - Prevent unauthorized network access & identify authorized users

2. **Confidentiality** - Use of encryption to ensure privacy of data

3. **Data Integrity** - Protect against modification or destruction of data

3 DRIVERS OF WLAN SECURITY

1. Inherent WLAN Vulnerabilities

2. 802.11 Task Group i

- Short term WEP fixes (TKIP, MIC)
- Long term 802.11 fixes (802.1x, AES)
- Backward compatibility

3. Vendor Solutions

- Standards based (EAP-TLS, TTLS)
- Pre-standards based (TKIP, MIC)
- Proprietary

I. INHERENT WLAN SECURITY VULNERABILITIES

INTRODUCTION:

INHERENT SECURITY VULNERABILITIES

802.11 signals sent → **PUBLIC AIRWAVES**

Spread spectrum → **DE-MODULATED**

Open Auth/ Null → **DEFAULT**

INTRODUCTION:

INHERENT SECURITY VULNERABILITIES

BSS Networks	→	**SAME SSID**
MAC ID Filtering	→	**SENT IN THE CLEAR w/WEP**
Shared Secret Authentication	→	**HACKED**

INTRODUCTION:

INHERENT SECURITY VULNERABILITIES

Rogue APs	→	**ATTACK WEAPONS**
Laptops	→	**WILL BE LOST**
802.1X Authent.	→	**STATELESS PROTOCOL**

INTRODUCTION:

INHERENT SECURITY VULNERABILITIES

ADDITIONAL ISSUES:

- No user identification and authentication (only machine)
- No per session or per user encryption solution
- Vulnerability to disassociation attacks
- No central authentication, authorization, and accounting support
- RC4 stream cipher is vulnerable to known plaintext attacks
- No support for extended authentication; token cards; certificates/smart-cards; one-time passwords; biometrics; etc.
- Key management issues (ie. re-keying global keys)

WEP GOALS

1. Prevent unauthorized network access
2. Provide data privacy
3. Maintain data integrity

ALL 3 CAN BE COMPROMISED

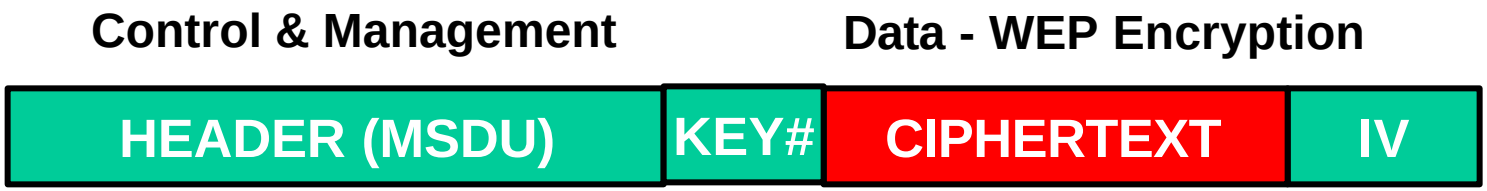
THE WEP PROBLEM:

WEP ENCRYPTION

WEP ONLY PROTECTS DATA

NOT

PHYSICAL LAYER TRANSMISSIONS



RTS, CTS, ACK, SSIDs, MAC ID
Assoc Request, Beacons,
Probe Requests/Response

THE WEP PROBLEM:

SHARED KEY AUTHENTICATION

WEP AUTHENTICATION & ENCRYPTION ARE COMBINED

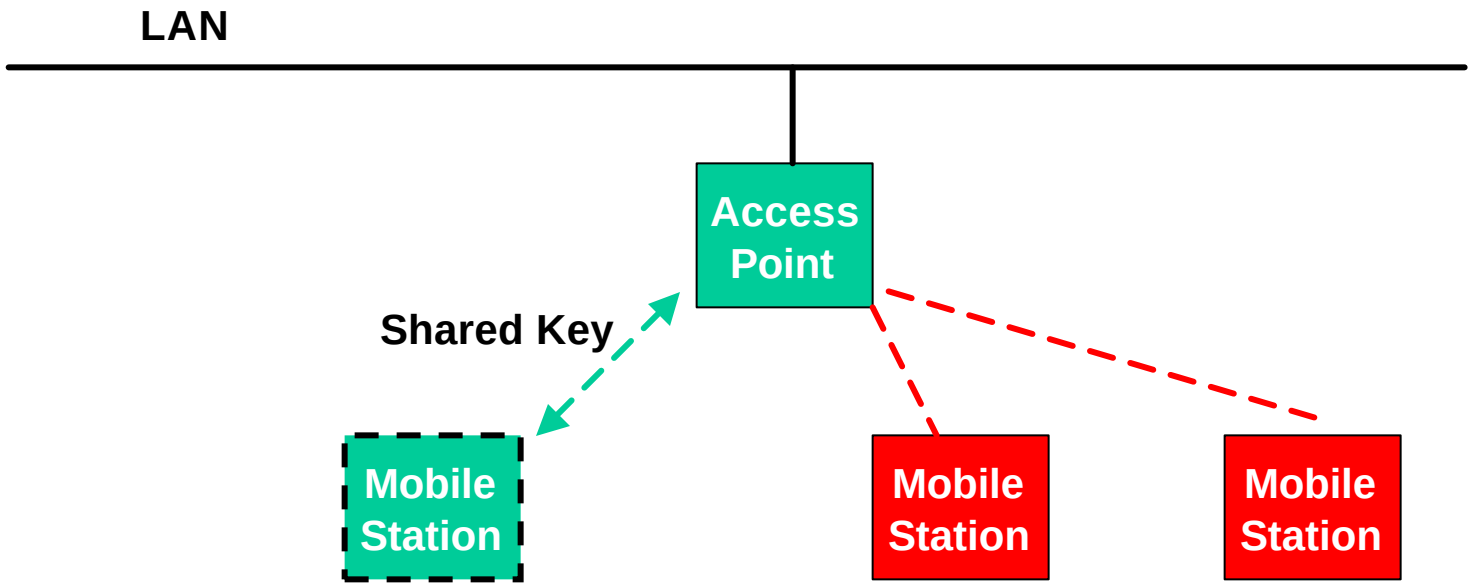
IF ONE BREAKS…

...SO DOES THE OTHER!

THE WEP PROBLEM:

SHARED KEY AUTHENTICATION

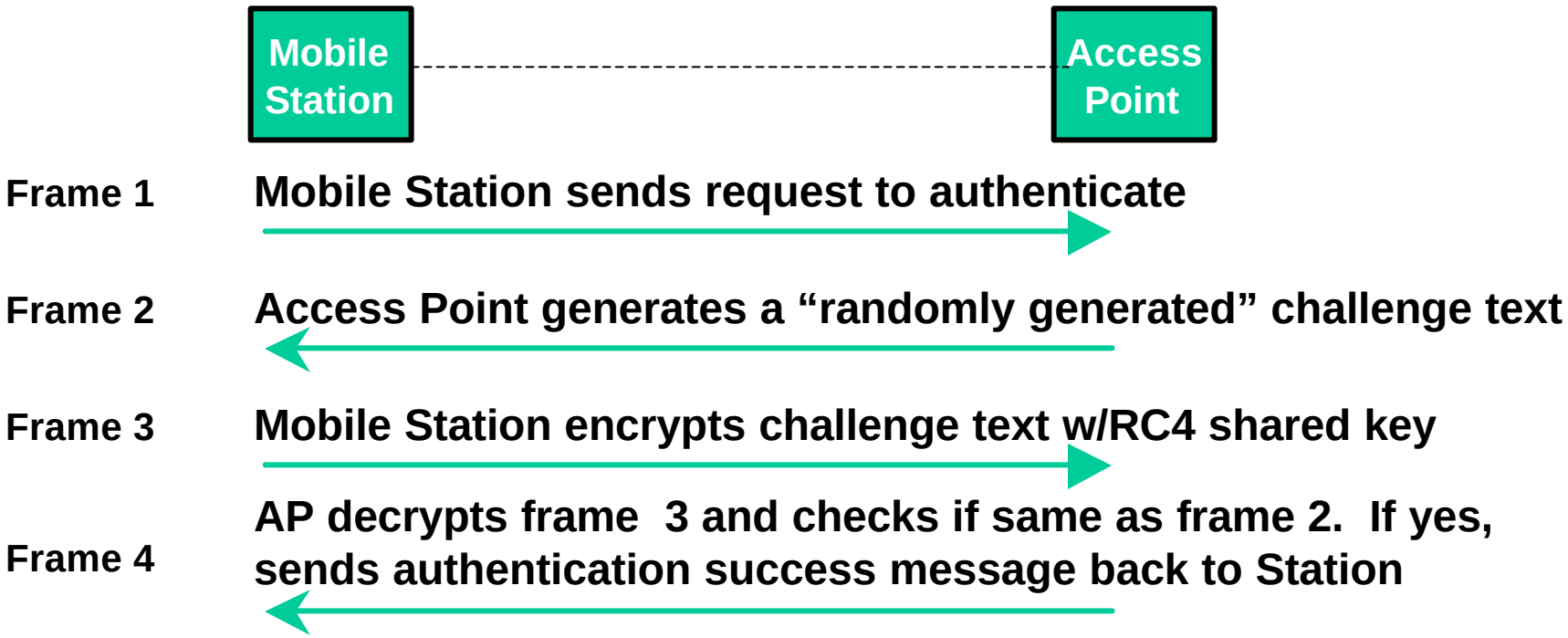
Client and AP have same 40/128 bit encryption key or “shared secret”



THE WEP PROBLEM:

SHARED KEY AUTHENTICATION

Authentication built using encryption primitive/ Challenge-Response



IEEE 802.11 Standard, 1999 Edition, Paragraph 8.1.2.1

II. 802.11 TASK GROUP i

802.11 TASK GROUP i

Enhanced Security Mechanisms

Defining the interaction between 802.1X and 802.11 standards

- **Scope:** Enhance the 802.11 Medium Access Control (MAC) with security mechanisms
- **Status:** Ongoing - (Security portion of the TGe (QOS) was moved to the TGi May 2001)

http://grouper.ieee.org/groups/802/11/

RECENT TGi MEETINGS

March 11 - 15 - St. Louis, Missouri

- TGi draft 2.0 created and went to LB (#35) on 3/25
- Motion to replace AES-OCB mode w/CBC- MAC - FAILED
- Discussion on 802.1X MiM attack - > develop EAP state machine

May 13-17 - Sidney, Australia

- LB #35 preliminary voting: 257 votes received:

  90 yes

  112 no

  55 abstain

- Over 1200 comments received. Comment resolution ongoing

ROBUST SECURITY NETWORK (RSN)

- **TGi defines two classes of security algorithms for 802.11**
  1. **Pre-RSN security Network**
  2. **Robust Security Network**
- **RSN security consists of two basic subsystems:**
  1. **Data privacy mechanisms:**
     - **TKIP - rapid re-keying to patch WEP for minimum privacy**
     - **AES encryption - robust data privacy for long term.**
  2. **Security association management:**
     - **.1X authentication - replacing 802.11 authentication**
     - **.1X key management - to provide cryptographic keys**

TASK GROUP i STATUS

- .1x had 11 drafts - TGi is on D2
- Suggest going through D2.0 line by line before next LB
- AES-OCB now called “Wireless Robust Authentication Protocol” (WRAP)
- “Transient-Security Network” (TSN) - spec for legacy equipment (WEP) compatibility
- Comments still not resolved cover the following topics:
  - Solution for Ad-hoc association unclear
  - Lack of de-authentication at the MAC level.
  - RSN definition
  - AES Mode
  - Key distribution protocols

RECAP

- TKIP & MIC are short term WEP fixes implemented by firmware and software upgrades for existing WiFi devices
- 802.1X stateless protocol EAP state fixes under way by IETF PPP-EAP WG
- EAP-TLS client in Win XP; Support for .1x by August
- TTLS - secure authentication by either EAP-TLS or legacy authentication systems (Funk Software)
- PEAP under development to support end to end secure roaming (Microsoft, RSA Security, Cisco)
- AES is long term layer 2 encryption solution to replace RC4

III. 802.11 Protocol Analyzers & IDS Systems

PROTOCOL ANALYZERS & IDS

- **AiroPeek by Wildpackets**

  http://www.wildpackets.com
- **AirDefense**

  http://www.airdefense.net/
- **AirMagnet**

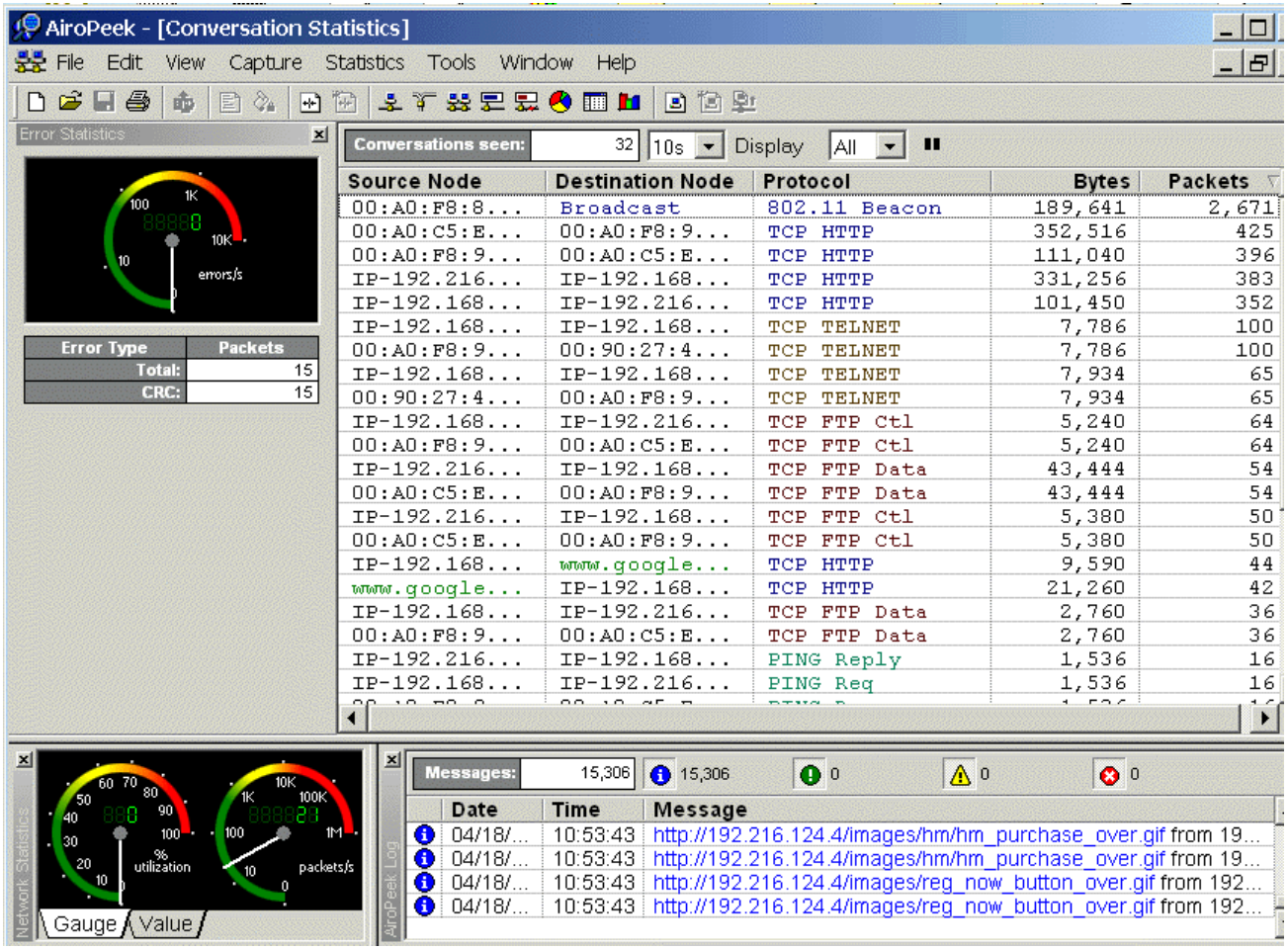
  http://www.airmagnet.com
- **Berkeley Varitronics Systems**

  http://www.bvsystems.com/Products/WLAN/Hornet/hornet.htm
- **Internet Security Systems 802.11 Wireless Scanner**

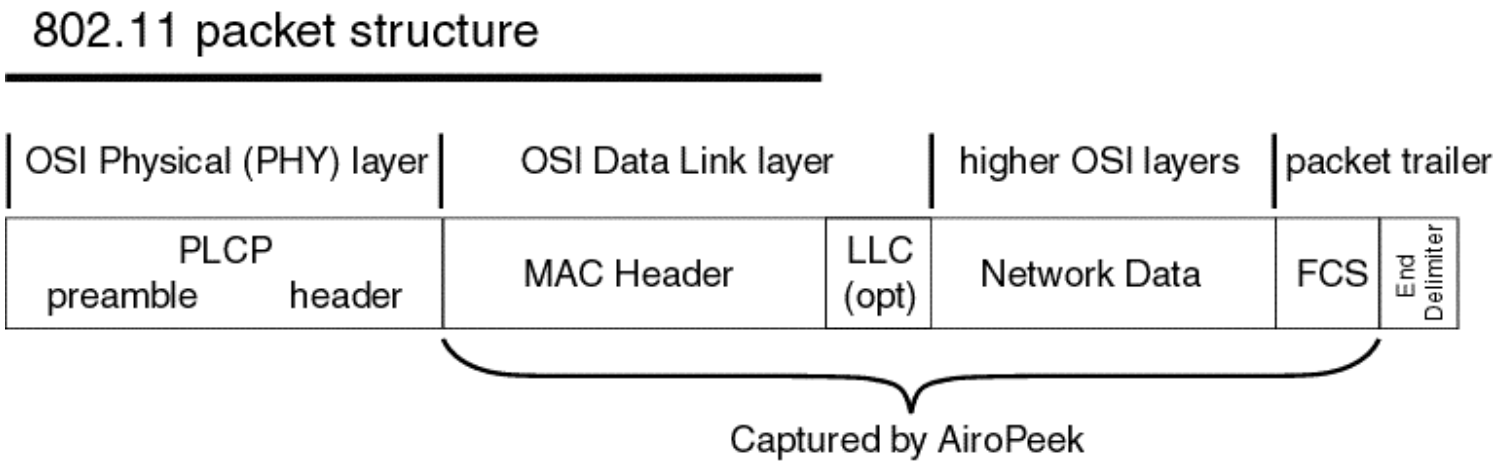
  http://www.iss.net/products_services/
- **Sniffer Technologies Sniffer Wireless**

  http://www.sniffer.com/products/default.asp#sniffer-wireless

AiroPeek by WildPackets



AiroPeek by WildPackets



AiroPeek by WildPackets

- Captures packets above the physical layer (MAC, LLC, IP, TCP, ect)
- Scans channels - Logs Peers; Identifies nodes & protocol traffic/signal strength
- Captures mgmt, control, data packets (Ack, Probe response/request, association, SSID, MAC)
- Custom filters machines/rogue APs
- Filters IP addresses/conversations/decode WEP
- www.wildpackets.com

802.11 SECURITY NEWSLETTER

802.11 Security Newsletter

www.itvshop.com/wlan-security