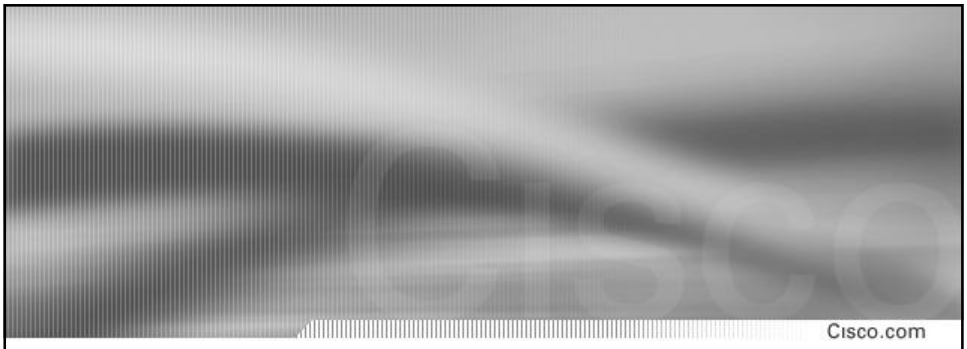


Wireless LAN Security

Franjo Majstor
fmajstor@cisco.com
EMEA Consulting Engineer

Agenda

Cisco.com

- **WLAN Security Primer**
- **Dynamic key mechanisms**
- **RC4 usage WEP Enhancements**
- **Future directions**

War driving …

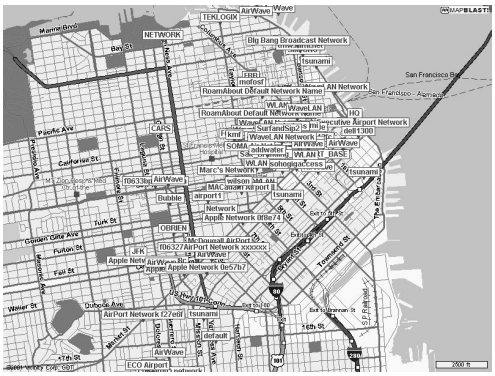
Cisco.com

… is possible as it has been proven by "War driving" exercise in SFO:

= cruising with a car + laptop + WLAN card

+ GPS scanning for (unprotected) 802.11 wireless networks.

+ Perl script to log the SSID, AP's MAC address, best S/N ratio and location (GPS).



www.personaltelco.net/index.cgi/WarDriving

3

Wire Equivalent Privacy (WEP)

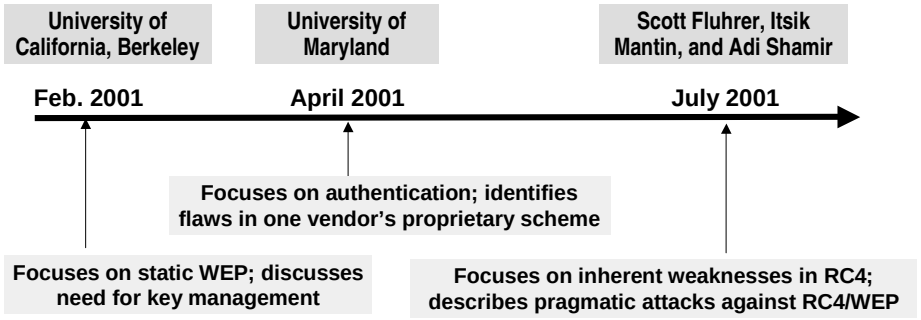
Cisco.com

- **Uses the RC4 stream cipher of RSA Data Security for encryption.**
- **RC4 Keystream = (24 bits IV , WEP Key)**
- **Key must be shared by both the encrypting and decrypting endpoints.**
- **IEEE 802.11b has chosen to use 40-bit keys. Several vendors Cisco support 128-bit WEP encryption with their WLAN solutions. Cisco in HW (3 % degradation only)**
- **Key distribution or key negotiation is not mentioned in the standard.**

4

Papers on WLAN Security

Cisco.com

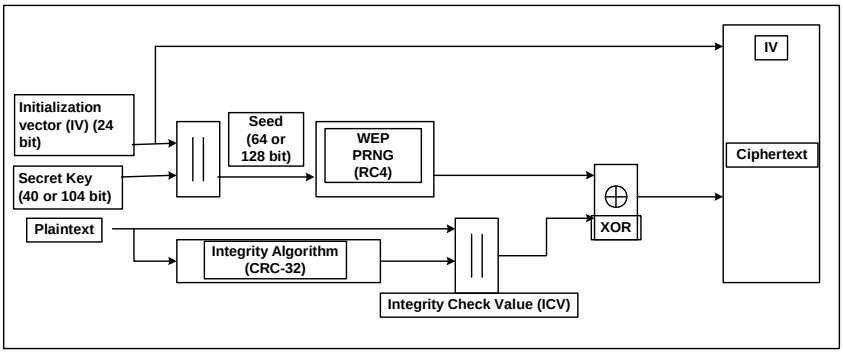


* "In practice, most installations use a single key that is shared between all mobile stations and access points. More sophisticated key management techniques can be used to help defend from the attacks we describe…"
– University of California, Berkeley report on WEP security, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

5

802.11b WEP Encryption

Cisco.com



6

UC Berkeley Attack

Cisco.com

- **Bit Flipping**

  Bits are flipped in WEP encrypted frames, and ICV CRC32 is recalculated.

- **Replay**

  Bit flipped frames with known IVs resent.

  AP accepts frame since CRC32 is correct

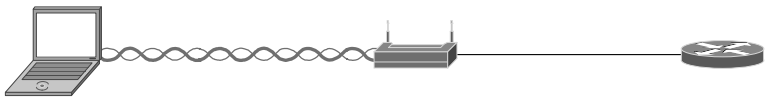
  Layer 3 device will reject, and send predictable response

  Response database built and used to derive key

7

UC Berkeley Attack

Cisco.com



Bit Flipped frame Sent

Frame passes ICV forwarded to Dest MAC

Upper Layer protocol fails CRC sends predictable error message to source MAC

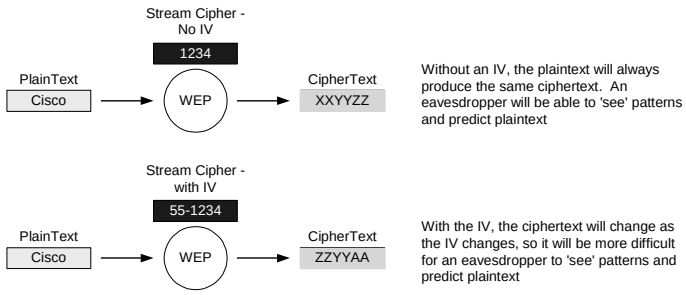
AP WEP encrypts response and forwards to source MAC

Attacker anticipates response from upper layer device and attempts to derive key

8

What is an IV?

Cisco.com



- **Same plaintext packet should not generate same ciphertext packet**
- **IV is random 24 bits long string (24 bits + 104 bits WEP key = 128 bits) and changes per packet**

9

What is a ‘Weak’ IV?

Cisco.com

- **In the RC4 algorithm the Key Scheduling Algorithm (KSA) creates an IV based on the base key**
- **A flaw in the WEP implementation of RC4 allows ‘weak’ IVs to be generated**
- **Those IVs ‘give away’ info about the key bytes they were derived from**
- **An attacker will collect enough weak IVs to reveal bytes of the base key.**

10

Fluhrer-Mantin-Shamir (FMS) paper

Cisco.com

Key recovery possible due to statistical analysis of plaintext and 'weak' IV

- **Attacks leverage 'Weak' IVs**

  A large class of weak IVs can be generated by RC4

  Attacks based on this paper are mainly Passive attacks, but can be more effective if coupled with active attack.

  www.crypto.com/papers/others/rc4_ksaproc.ps

- **Major Implementations of attacks**

  http://airsnort.sourceforge.net/

  http://wepcrack.sourceforge.net/

11

Airsnort

Cisco.com

- **Capture enough packets**
- **Crack phase**
- **For every byte of the key, there are 256 weak IVs.**
- **13 key bytes * 256 = 3315 packets to get all weak keys**
- **You do not need sometimes all of the weak keys to break the WEP key**

12

Deployment issues with 802.11b today

Cisco.com

- **Lack of integrated User administration**
  - Integration with existing user administration tools required (RADIUS, LDAP-based directories)
  - Identification via User-Name easier to administer than MAC address identification
- **Lack of Key management solution**
  - Static keys difficult to manage on clients, access points
  - Proprietary key management solutions require separate user databases

Solution: 802.1x
IEEE standard-in-progress for port-based network access control
Leverages existing standards: EAP (Extensible Authentication Protocol), RADIUS

13

EAP Defined - RFC 2284

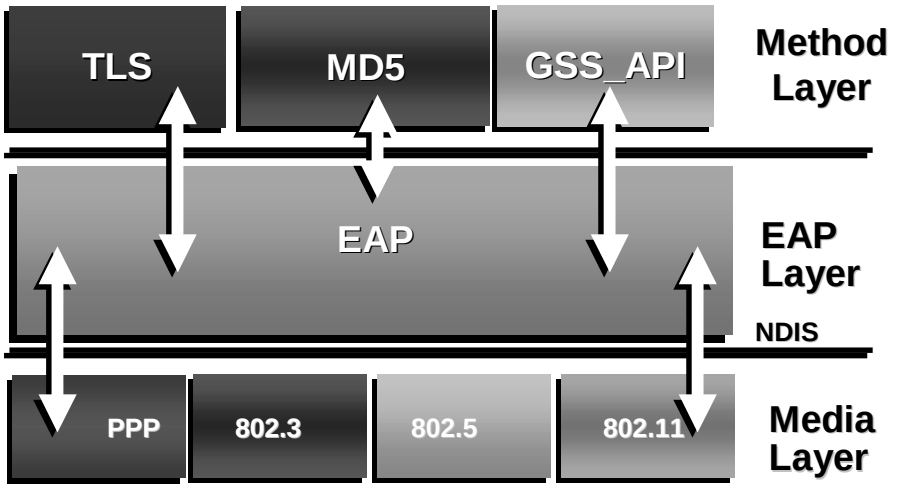
Cisco.com

- **Extensible Authentication Protocol is a extension of CHAP/PAP within PPP**
  - Support multiple “authentication” schemes:
    - plain password hash (MD5)
    - token cards
    - GSS-API (Kerberos)
    - TLS (based on X.509 certificates)

14

EAP Architecture

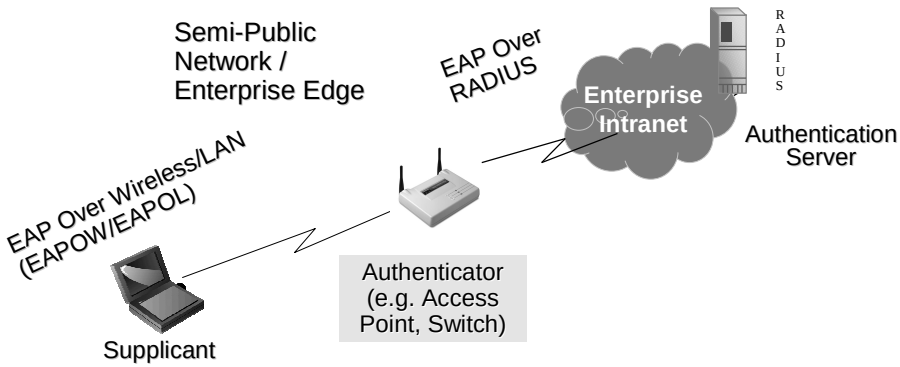
Cisco.com



15

EAP Centralized User-Based Authentication

Cisco.com

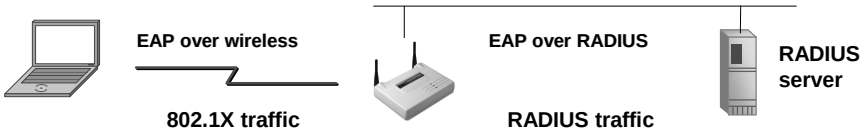


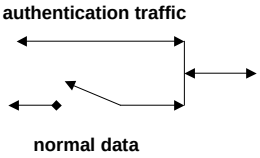
16

Before EAP Start

Cisco.com

802.11 association complete; data blocked by AP





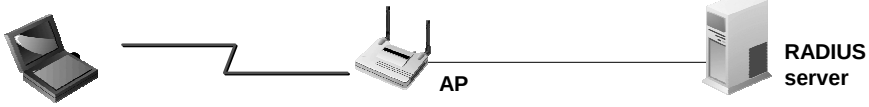
AP encapsulates 802.1x traffic into RADIUS traffic, and visa versa

AP blocks everything but 802.1x-to-RADIUS authentication traffic

17

EAP-TLS

Cisco.com



EAPOL Start →		Start process
← EAP-Request/Identity		Ask client for identity
EAP -Response/Identity (UserID) →		Provide identity
	Access request →	Pass request to RADIUS
← EAP-TLS		Perform sequence defined by EAP-TLS
....		
EAP-TLS →		
key Client receives or derives session key		key
	← Access success	Pass session key to AP
← EAP success		Start using WEP
← EAPOW key		Deliver broadcast key, encrypted with session key

18

IEEE 802.1x Defined

Port based network access control

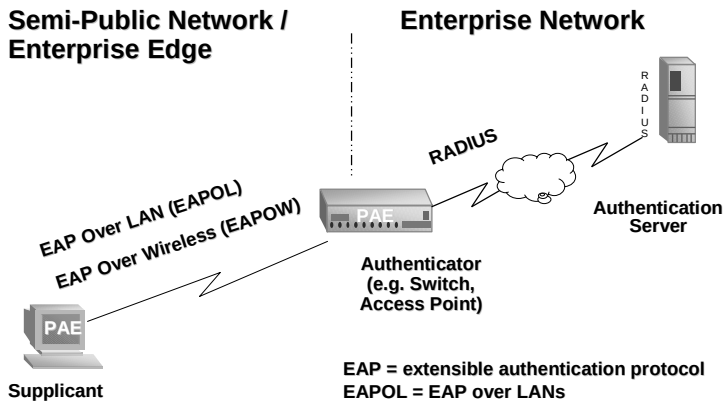
Cisco.com

- **802.1x is an IEEE Standard in progress for Port Based Network Access Control, EAP based**
- **Falls under 802.1 NOT 802.11**
- **NETWORK standard, not a wireless standard**
- **Provides Network Authentication, NOT encryption**
- **Improved authentication: username/password**
- **Works on 802.3 LAN switch or 802.11b WLAN AP**
- **To be used for centralized user administration**
- **Is PART of the 802.11i draft**

19

IEEE 802.1X Terminology

Cisco.com

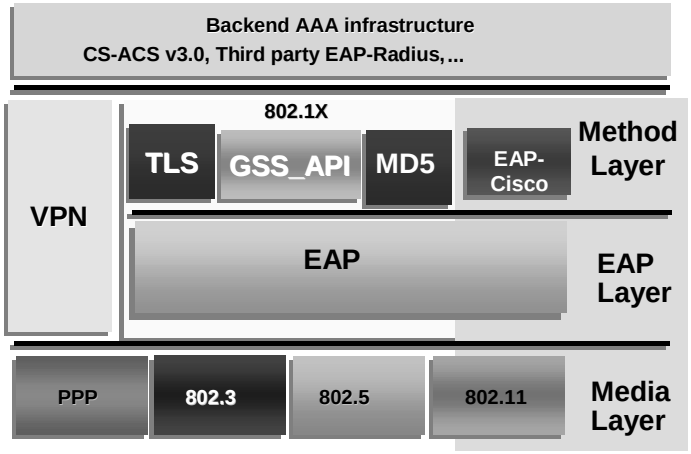


EAP = extensible authentication protocol
EAPOL = EAP over LANs
PAE = port access entity
Port = network access port
RADIUS = remote authentication dial in user service

20

New WLAN Security Framework

Cisco.com



21

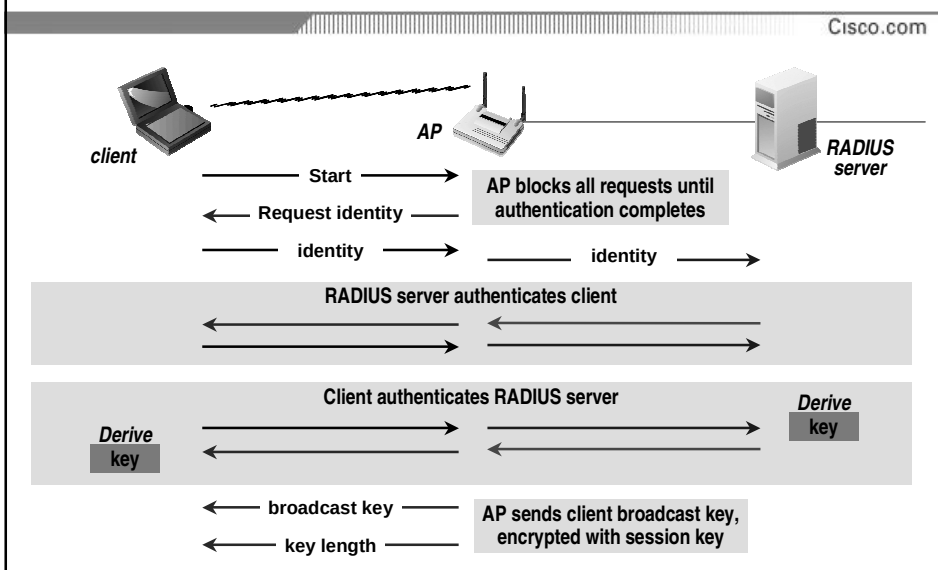
EAP-Cisco Defined

Cisco.com

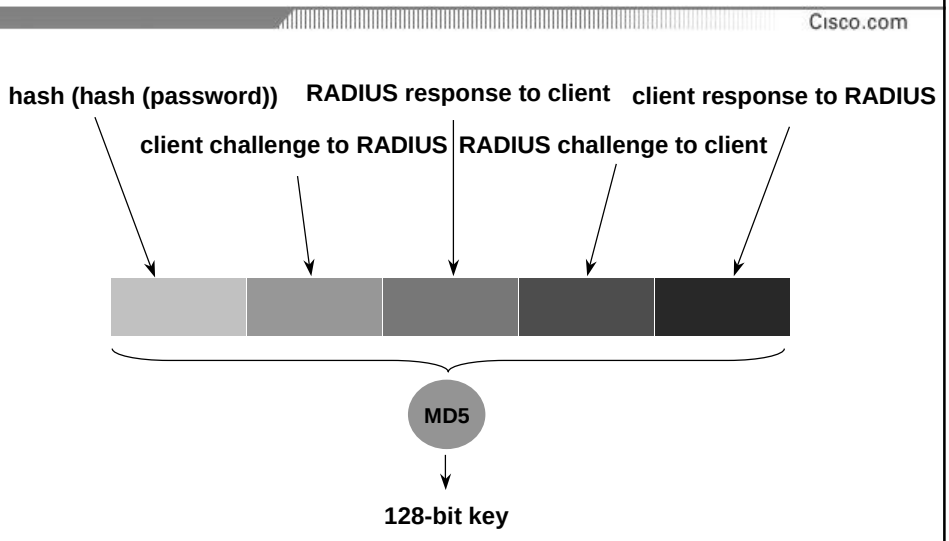
- **No native EAP support currently available on legacy operating systems (Win 95/98/NT)**
- **EAP-MD5 *does not* do mutual password authentication, uses *static keys only***
- **EAP-TLS supports *dynamic keying* but is too intense for security baseline feature-set (requires PKI/CA, *certificates*)**
- **EAP-Cisco supports mutual password based authentication and *dynamic keying***

22

EAP-Cisco Steps: Mutual Authentication

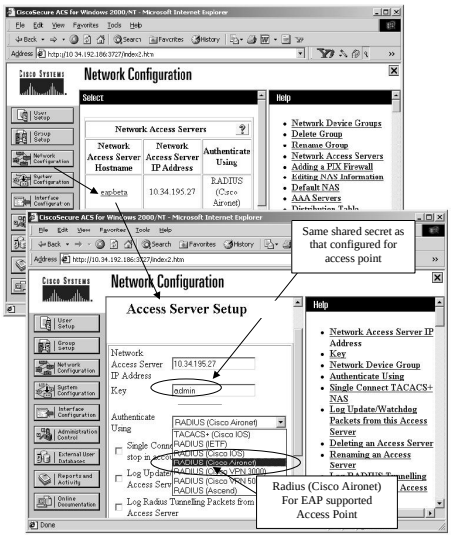


Deriving the Session Key



What Does the RADIUS Server Perform

Cisco.com



- **WEP key is calculated by the RADIUS server, only after the authentication is completed**
- **The key is passed to access point for THAT single authenticated client; this is a *session* key**
- **Client calculates the same WEP key**
- **Key is *never* transmitted over RF**

How Often to Change Key

Cisco.com

- **Every time a client roams to a new AP, it will go through the same authentication and get new WEP session key**
- **RADIUS server will also require a new authentication / key at a pre-defined time interval (Attribute 027, Session -Timeout)**
- **This provides different and totally unique WEP key to each client**

Security Enhancements for RC4 Based WEP

Cisco.com

- **Security Enhancements to Strengthen RC4-Based WEP Keys**
  - **Message Integrity Check (MIC)**
  - **Key Hashing or Temporal Key (TK) of TKIP**
  - **Linear Initialization Vector (IV) Sequencing**
  - **Broadcast Key rotation**

27

Message Integrity Check

Cisco.com

- **The MIC will protect WEP frames from being tampered with and being replayed .**
- **The MIC is based on Seed value, Destination MAC, Source MAC, and payload.**

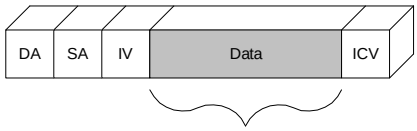
  Any change to these will change MIC value
- **Unlike CRC32, MIC uses a hashing algorithm to stamp frame.**

28

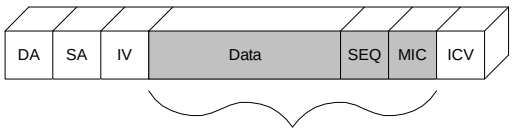
Message Integrity Check

Cisco.com

WEP Frame - No MIC



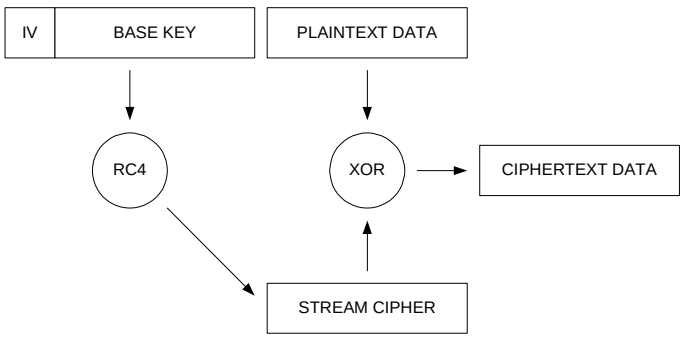
WEP Frame - MIC



29

The WEP Encryption Process

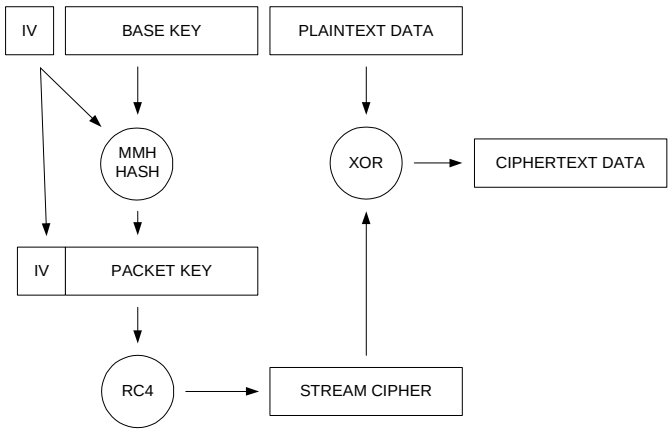
Cisco.com



30

WEP Key Hashing

Cisco.com



31

Broadcast Key Rotation

Cisco.com

- **Static Broadcast Key is vulnerable to FMS attack over time**
  - **Similar to static WEP Keys**
- **Using Broadcast Key rotation will prevent static WEP users from functioning correctly.**
- **Broadcast Key = Hash (seed, ap_mac_addr, nboots)**

32

Linear IV Sequencing

Cisco.com

- **Instead of random collision times, move through the IV listing in a linear fashion**
- **Broadcast key must be rotated before utilizing the entire IV space (~min 2.03h, optimal 10h)**
- **Added benefit is that if packet is using the previous IV, it will be rejected because the transmitter is expecting the next linear IV**

33

Static WEP vs. EAP-TLS vs. EAP-Cisco

Cisco.com

Attack	WEP	EAP-TLS	IV Hashing	MIC	Broadcast Key Rotation	EAP-Cisco
IV Reuse/Collision	✗				✓	
CRC32 bit-flipping	✗			✓		
CRC32 replay	✗			✓		
Authentication forging	✗					✓
FMS Attack	✗		✓			
Rogue AP	✗					✓
Dictionary attack	✗	✓				

34

IEEE 802.11i Security

- **Passed 1st letter ballot (Draft currently at version 1.6)**
  - **Fixes to WEP (Software)**
  - **AES proposals (new HW)**
    - **All MIC/IV Hash/IV Sequencing/Rapid Rekey to informative text:** passed
    - **Replace WEP2 with TKIP :** passed
  - **TKIP (Temporal Key Integrity Protocol)**
    - **Text/hash function/MIC etc is Work in Progress.**
- **grouper.ieee.org/groups/802/11/Reports/tgi_update.htm**

35

Questions?

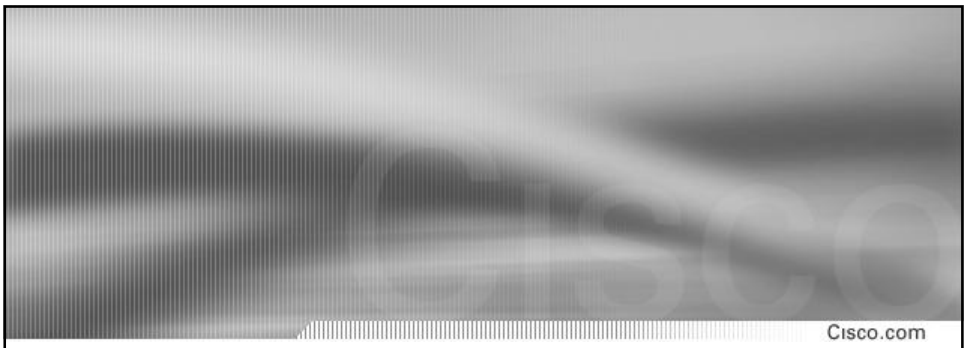
Cisco.com

References

Cisco.com

- **Wireless LAN Security**
  Cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm
- **802.11 security flaws description info from Berkley University**
  www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf
- **Paper from S. Fluhrer (Cisco Systems), I. Mantin and A. Shamir**
  www.crypto.com/papers/others/rc4_ksaproc.ps
- **An Initial Security Analysis of the IEEE 802.1x Standard**
  www.cs.umd.edu/~waa/1x.pdf
- **Wireless sniffers:** www.personaltelco.net/index.cgi/WirelessSniffers
- **IEEE 802.1X:** grouper.ieee.org/groups/802/1/pages/802.1x.html
- **EAP:** www.ietf.org/rfc/rfc2284.txt & www.ietf.org/rfc/rfc2716.txt

37



Cisco.com

Thank you!

Franjo Majstor
fmajstor@cisco.com
EMEA Consulting Engineer

