Security Enhancements to Strengthen RC4-Based WEP Static Keys

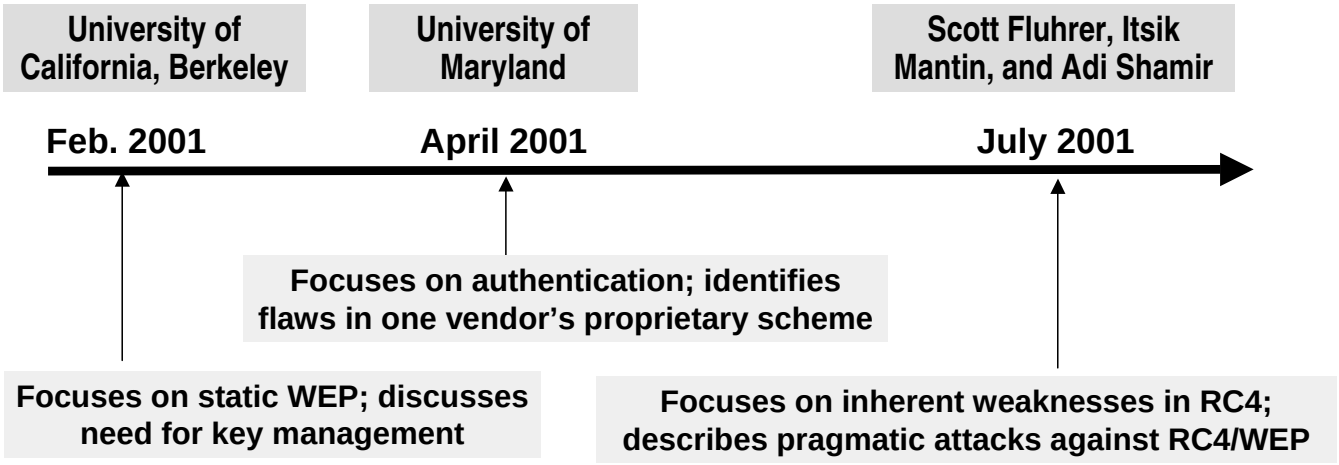
Franjo Majstor
K.U.Leuven, Dept. of Computer Science, DistriNet

franjo.majstor@student.kuleuven.ac.be
franjo@cisco.com

Agenda

- **Quick intro**
- **Dynamic key mechanisms**
- **RC4 usage WEP Enhancements**
- **Future directions**

WLANs & Security



* "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

Security Issues with WEP

- **Stateless Protocol (Replay Attack)**
- **Linear Checksum - Packet Modification (bits flip)**
- **IV Reuse (Collision)**
- **Bad IV for RC4 (Airsnort, WEPCrack,…)**

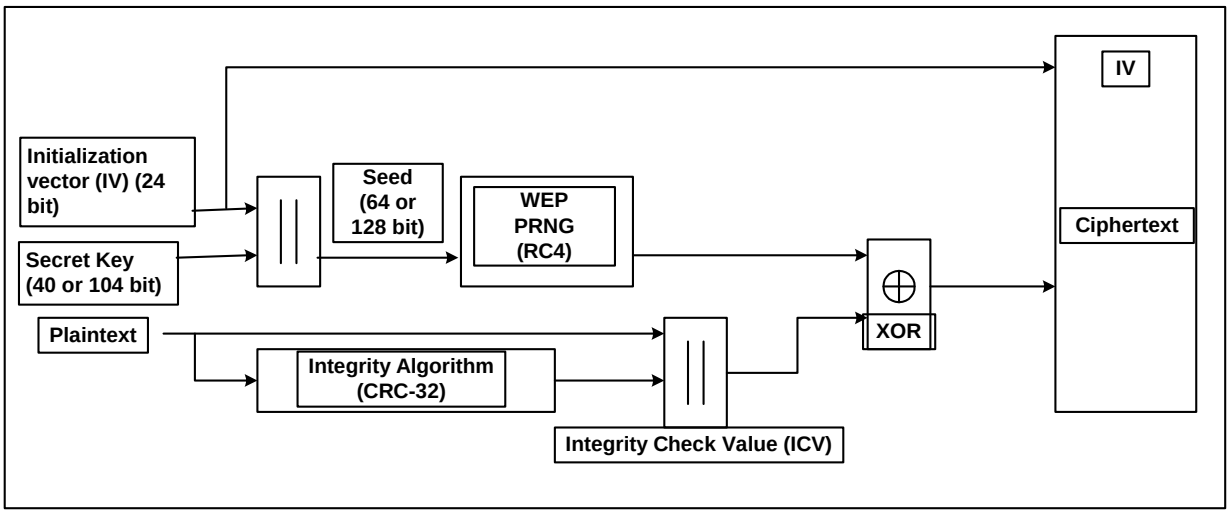
Already explained at:

www.esat.kuleuven.ac.be/cosic/seminars/seminars_text.html

New ones:

- **Dachb0den Labs:**
  www.dachb0den.com/projects/bsd-airtools/wepexp.txt
- **An Initial Security Analysis of the IEEE 802.1x Standard**
  www.cs.umd.edu/~waa/1x.pdf

802.11b WEP Encryption



Deployment issues with 802.11b today

- **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

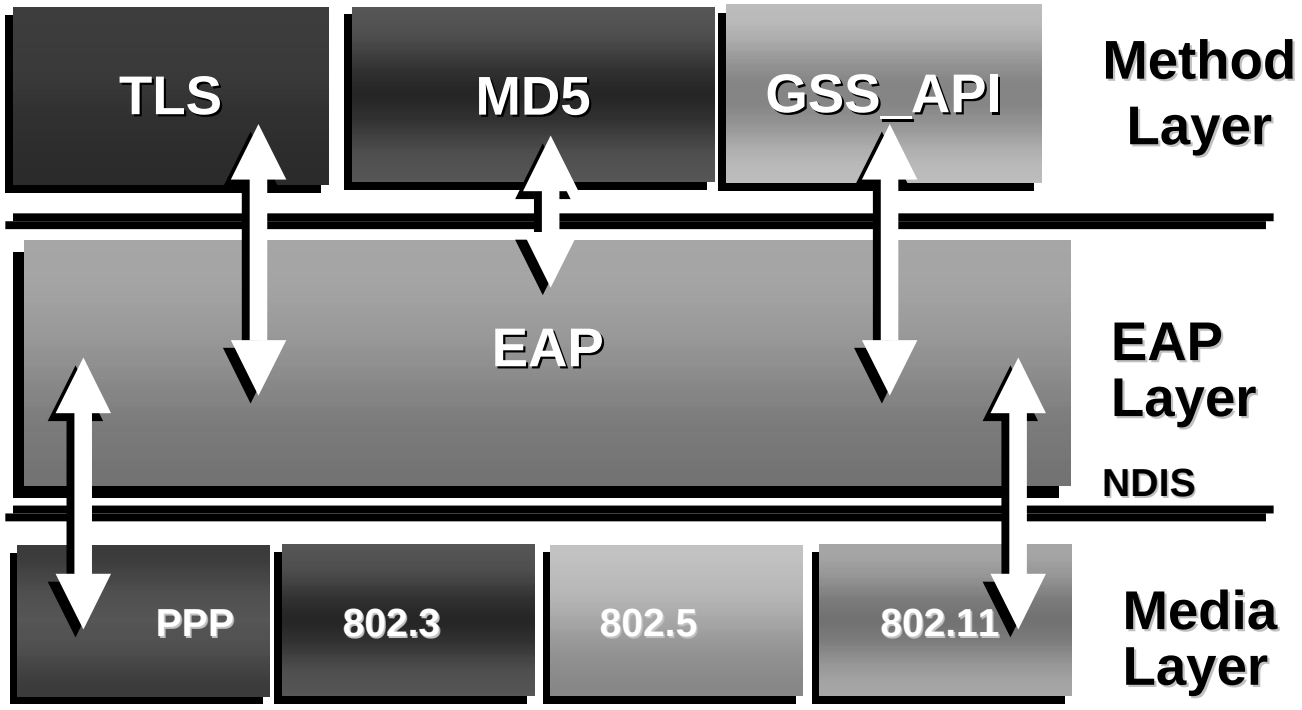
  Proprietary key management solutions require separate user databases

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

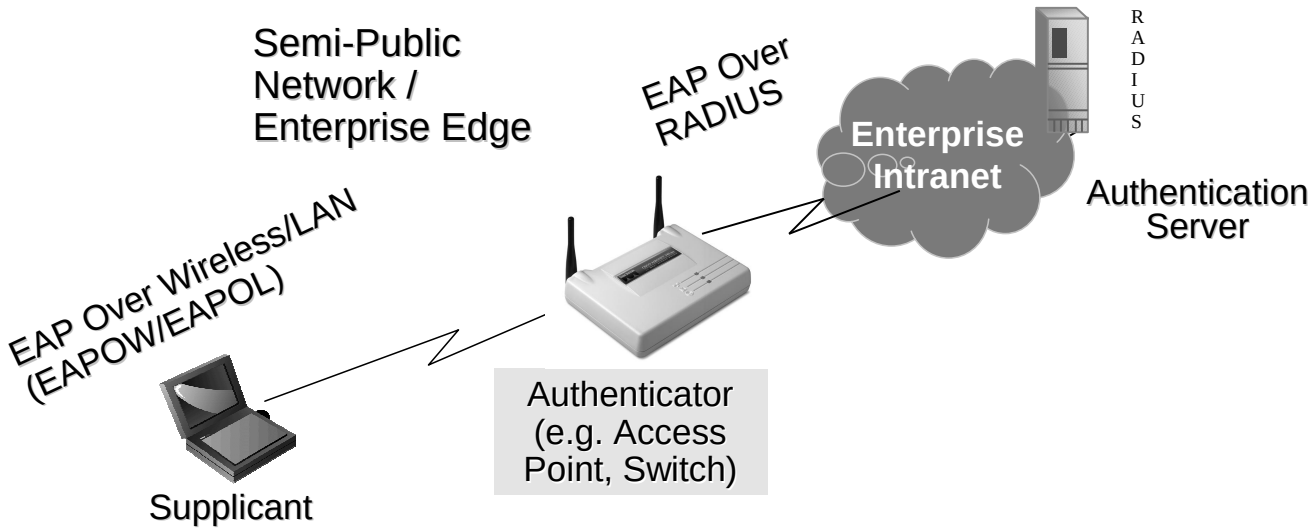
EAP Defined - RFC 2284

- **Extensible Authentication Protocol is an 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)**

EAP Architecture

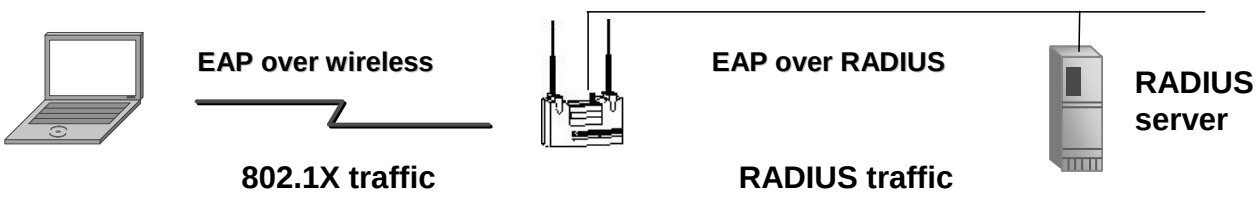


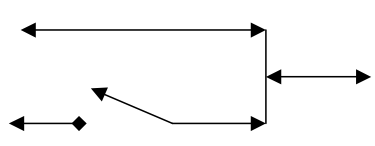
EAP Centralized User-Based Authentication



Before EAP Start

802.11 association complete; data blocked by AP

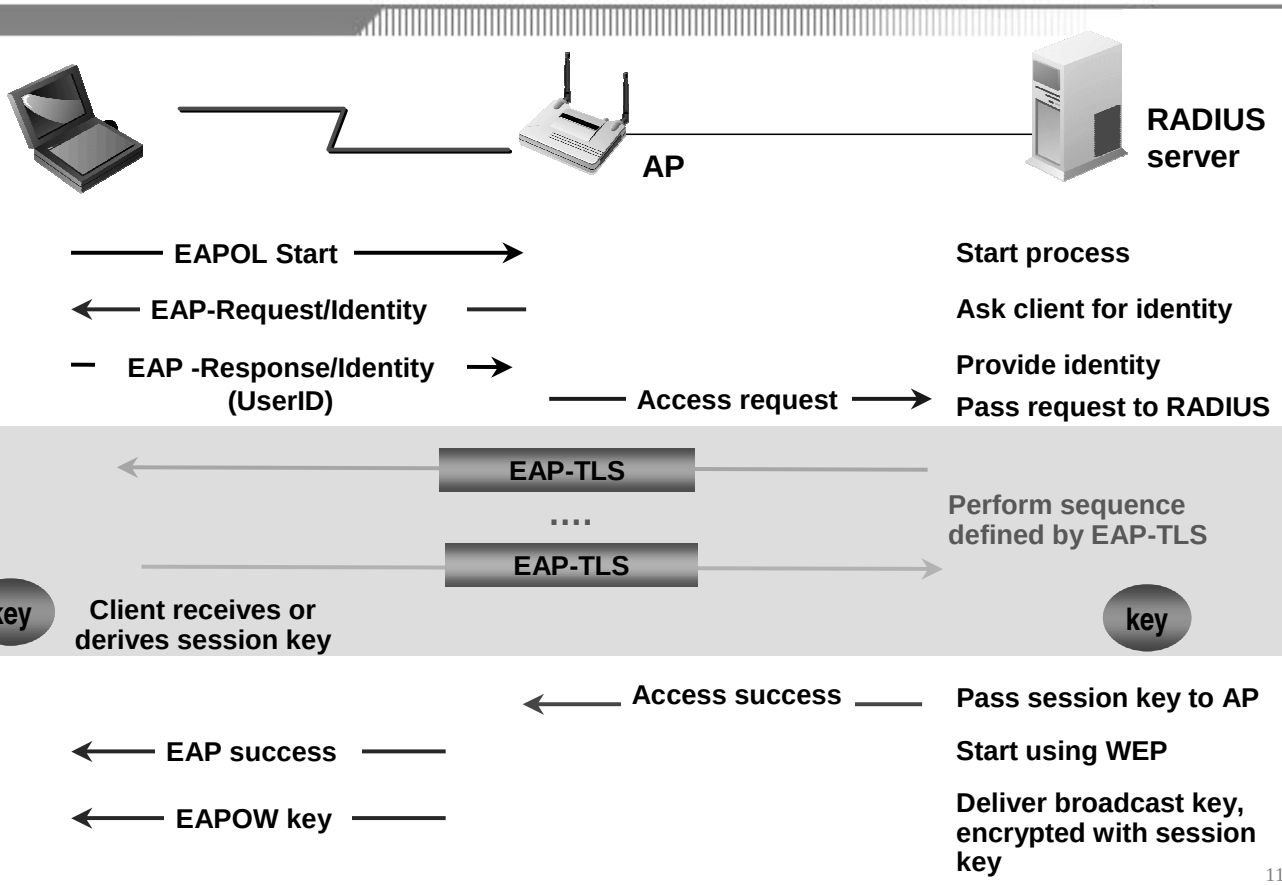




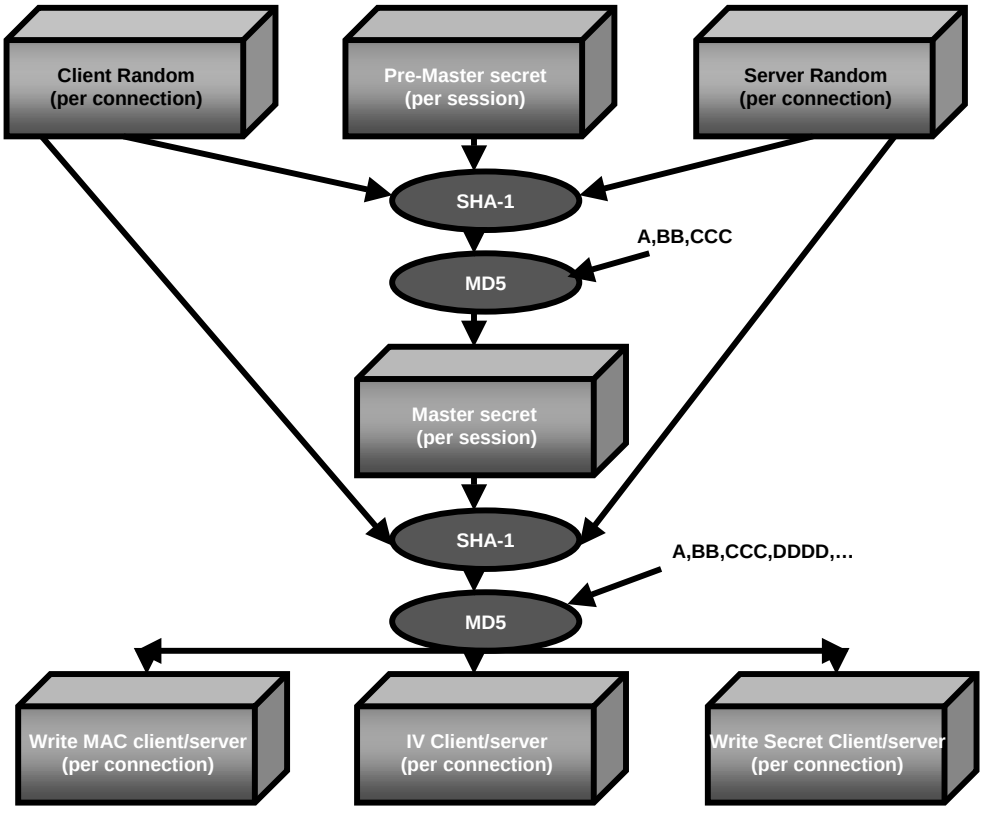
AP encapsulates 802.1x traffic into RADIUS traffic, and vice versa

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

EAP-TLS



Key material generation - TLS



Key material generation (EAP-TLS)- RFC2716

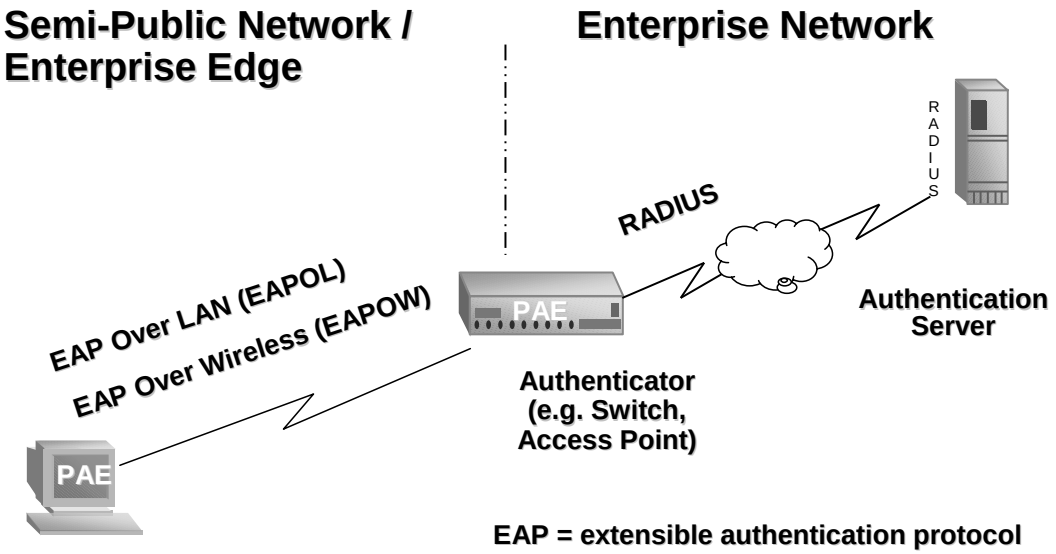
- random=(client_hello.random, server_hello.random)
- PRF1(master secret, "client EAP encryption", random)
- PRF2(" ", "client EAP encryption", random)
- PRF1 is 128 bytes, PRF2 is 64 bytes
- PRF1 is truncated into 4 times 32 bytes : this produces ***encryption keys*** and ***MAC*** for peer-EAP server and EAP server-peer conversations
- PRF2 is trucated into 2 times 32 bytes : this produces the ***Initialization Vectors*** (IV) for both conversations

IEEE 802.1x Defined

Port based network access control

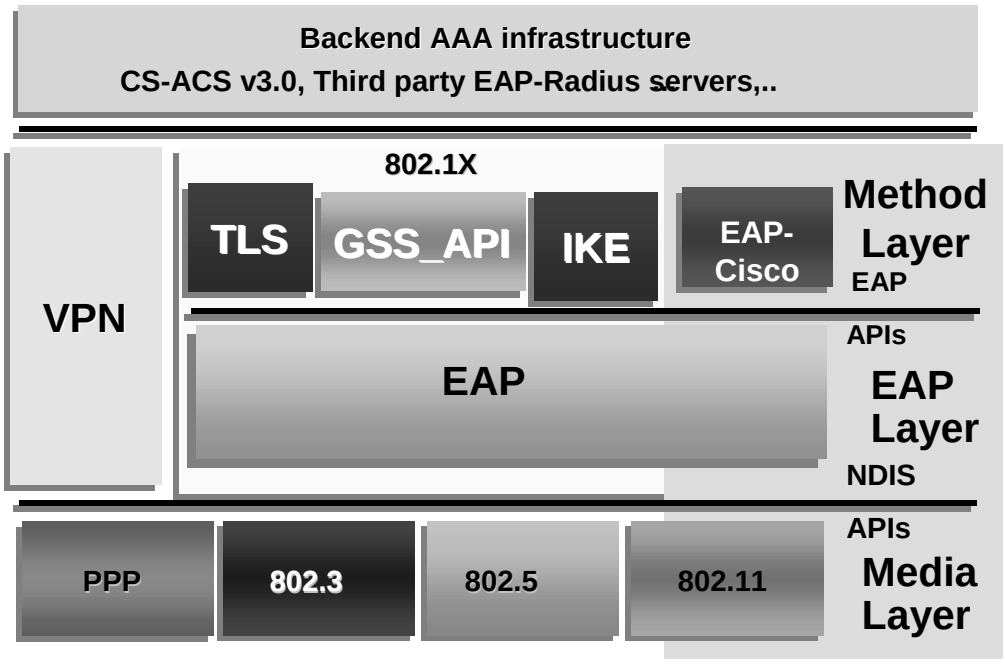
- 802.1x is an IEEE Standard in progress for Port Based Network Access Control, EAP based
- Falls under 802.1 NOT 802.11
- NETWORK standard, not a wireless standard
- Provides Network Authentication, NOT encryption
- Improved authentication: username/password
- Works on 802.3 LAN switch or 802.11b WLAN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

IEEE 802.1X Terminology



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

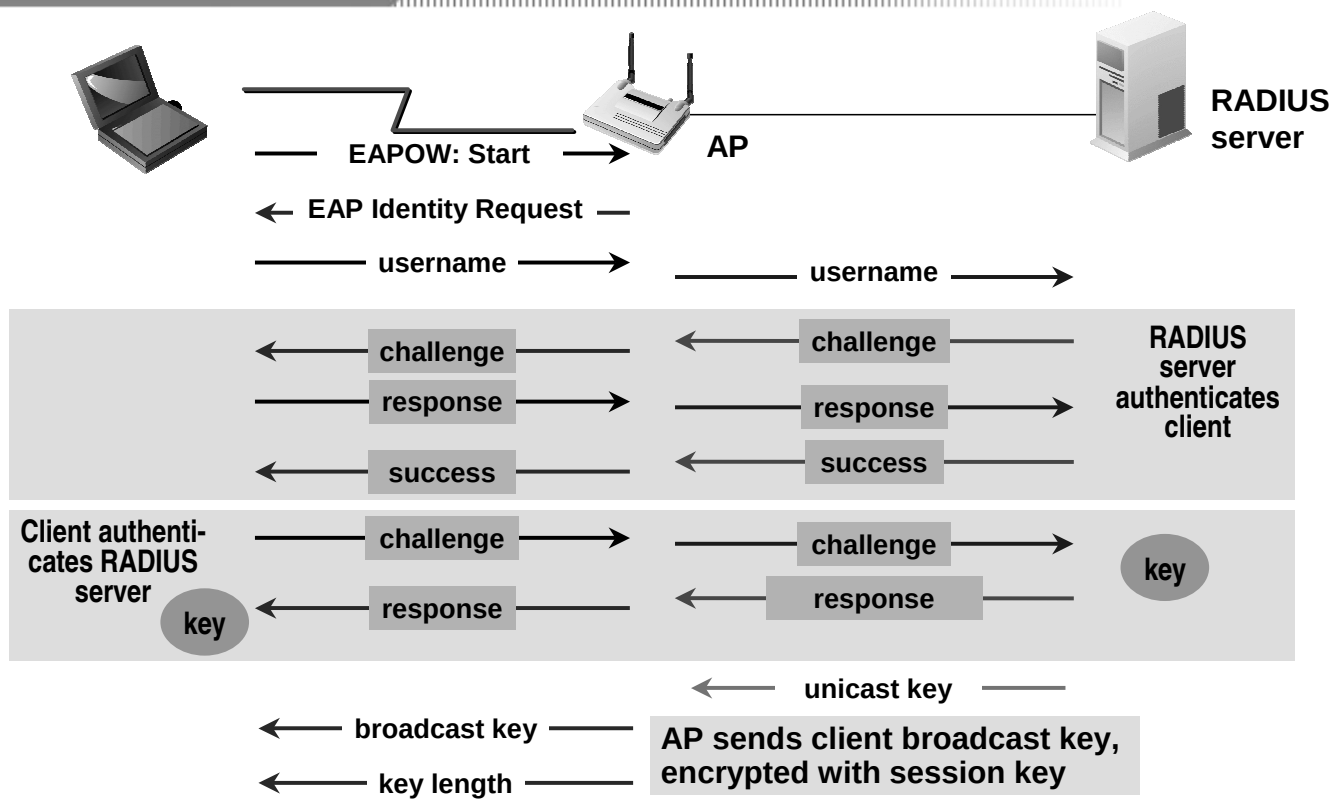
New WLAN Security Framework



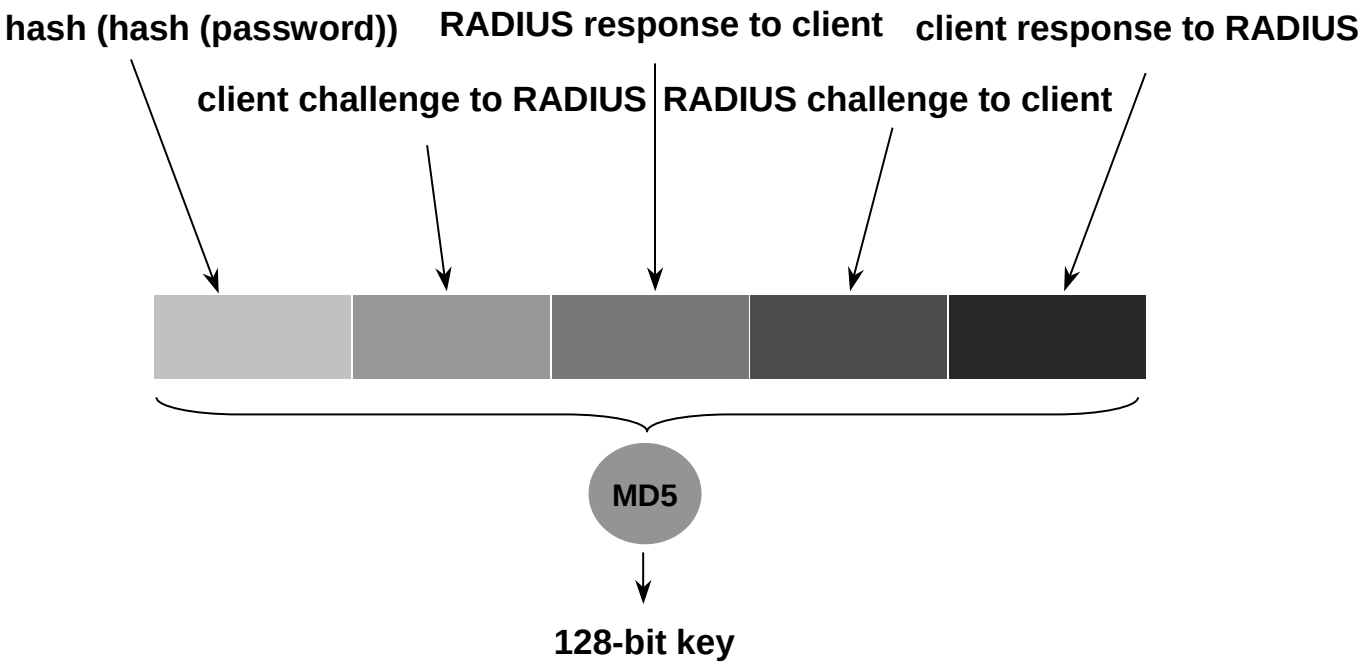
EAP-Cisco Defined

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

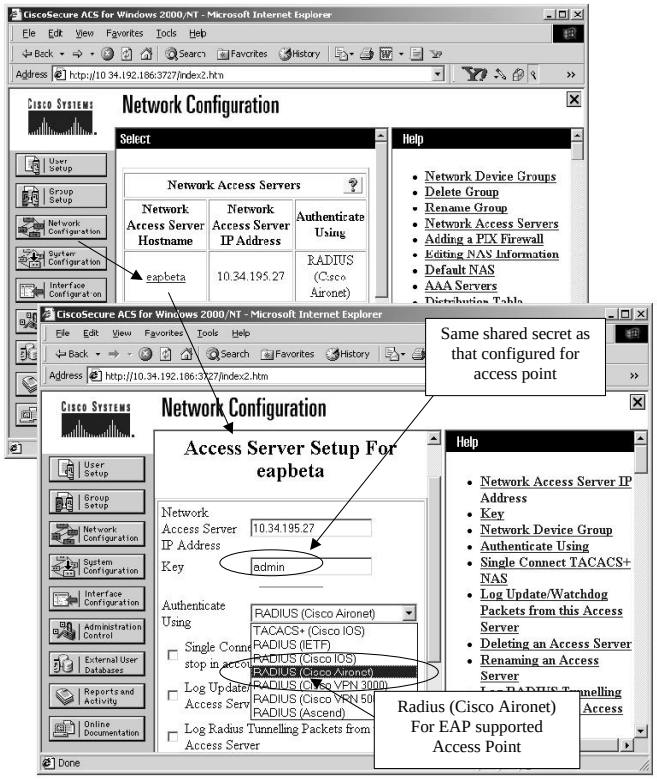
EAP-Cisco Steps: Mutual Authentication



Deriving the Session Key



What Does the RADIUS Server Perform



- **WEP key is calculated by the RADIUS server, only after the authentication is completed**
- **The key is passed to an 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

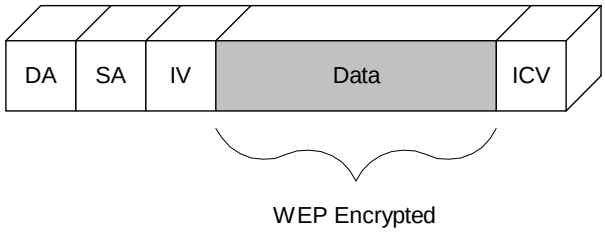
- Every time a client roams to a new AP, it will go through the same authentication and get new WEP session key
- RADIUS server will also require a new authentication / key at a pre-defined time interval (Attribute 027, Session -Timeout)
- This provides different and totally unique WEP key to each client

Security Enhancements for RC4 Based WEP

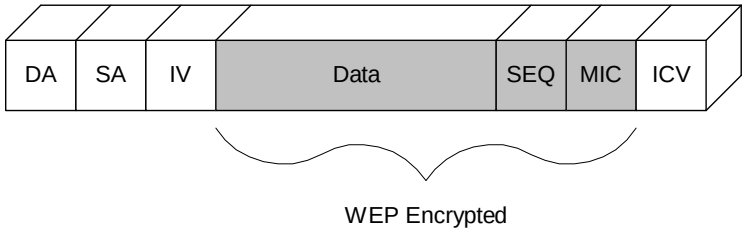
- Security Enhancements to Strengthen RC4-Based WEP Keys
  - Message Integrity Check (MIC)
  - Key Hashing or Temporal Key (TK) of TKIP
  - Linear Initialization Vector (IV) Sequencing
  - Broadcast Key rotation

Message Integrity Check

WEP Frame - No MIC



WEP Frame - MIC

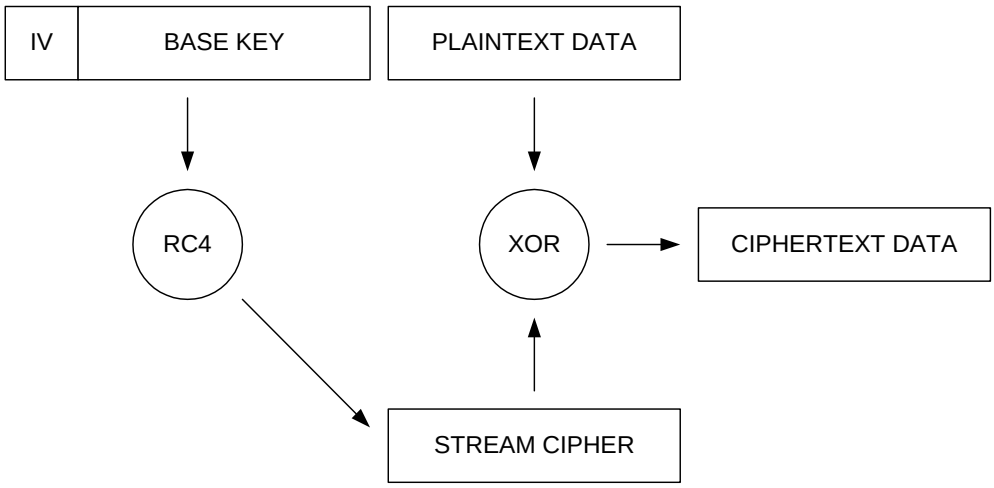


Message Integrity Check

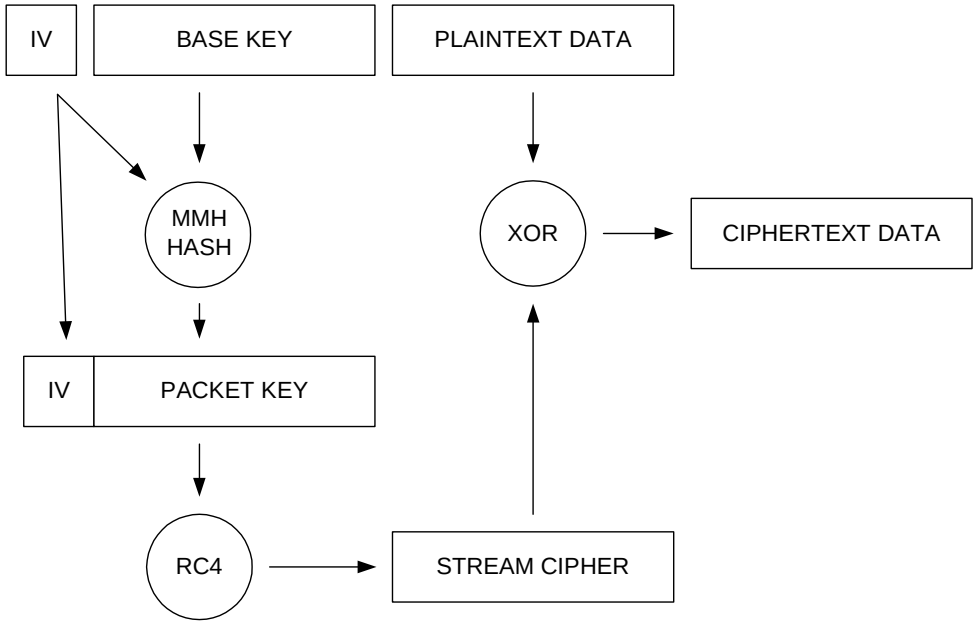
- **The MIC will protect WEP frames from being tampered with and being replayed.**
- **The MIC is based on Seed value, Source and Destination MAC address and payload.**

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

The WEP Encryption Process



WEP Key Hashing



Linear IV Sequencing

- **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**

Broadcast Key Rotation

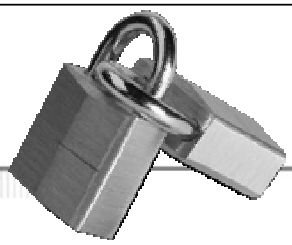
- **Static Broadcast Key is vulnerable to FMS attack over time**

  Similar to static WEP Keys
- **Using Broadcast Key rotation will prevent static WEP users from functioning correctly.**
- **Broadcast Key = Hash (seed, ap_mac_addr, #boots)**

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

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	✗	✓				

IEEE 802.11i Security



- **Passed 1st letter ballot (Draft currently at version 1.6)**

  Fixes to WEP (Software)

  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.

  New AES proposals (Requires Hardware Changes)

- grouper.ieee.org/groups/802/11/Reports/tgi_update.htm

Additional References

- **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
- **IEEE 802.1X:** grouper.ieee.org/groups/802/1/pages/802.1x.html
- **EAP:** www.ietf.org/rfc/rfc2284.txt
- **TLS:** www.ietf.org/rfc/rfc2246.txt
- **EAP TLS:** www.ietf.org/rfc/rfc2716.txt
- **EAP TTLS:** draft-ietf-pppext-eap-ttls-01.txt
- **PEAP :** draft-josefsson-pppext-eap-tls-eap-02.txt

Questions?

Thank You!

Security Enhancements to Strengthen RC4-Based WEP Static Keys

Franjo Majstor
K.U.Leuven, Dept. of Computer Science, DistriNet

franjo.majstor@student.kuleuven.ac.be
franjo@cisco.com