Network Security (NetSec)

Summer 2015
Chapter 06: Link Level Security
Module 03: Wireless Network Security

SECURE MOBILE NETWORKING

Prof. Dr.-Ing. Matthias Hollick

Technische Universität Darmstadt
Secure Mobile Networking Lab - SEEMOO
Department of Computer Science
Center for Advanced Security Research Darmstadt - CASED

Mornewegstr. 32
D-64293 Darmstadt, Germany
Tel.+49 6151 16-70922, Fax. +49 6151 16-70921
http://seemoo.de or http://www.seemoo.tu-darmstadt.de

Prof. Dr.-Ing. Matthias Hollick
matthias.hollick@seemoo.tu-darmstadt.de

Wireless Security Requirements

Learning Objectives

In-depth discussion of security for wireless links

- Understand challenges of wireless networks
- Recap of basic functionality of wireless local area network
- Understand design flaws of Wired Equivalence Privacy (WEP)
- Solutions to address WEP flaws

- Hands-on session in lecture hall: “attacking” IEEE 802.11 networks …

Overview of this Module

(1) Recap: IEEE 802.11

(2) Wired Equivalent Privacy (WEP)

(3) Weaknesses of WEP

(4) 802.11i

(5) Weaknesses of 802.11i

Chapter 06, Module 03

802.11 - Architecture of an Infrastructure Network

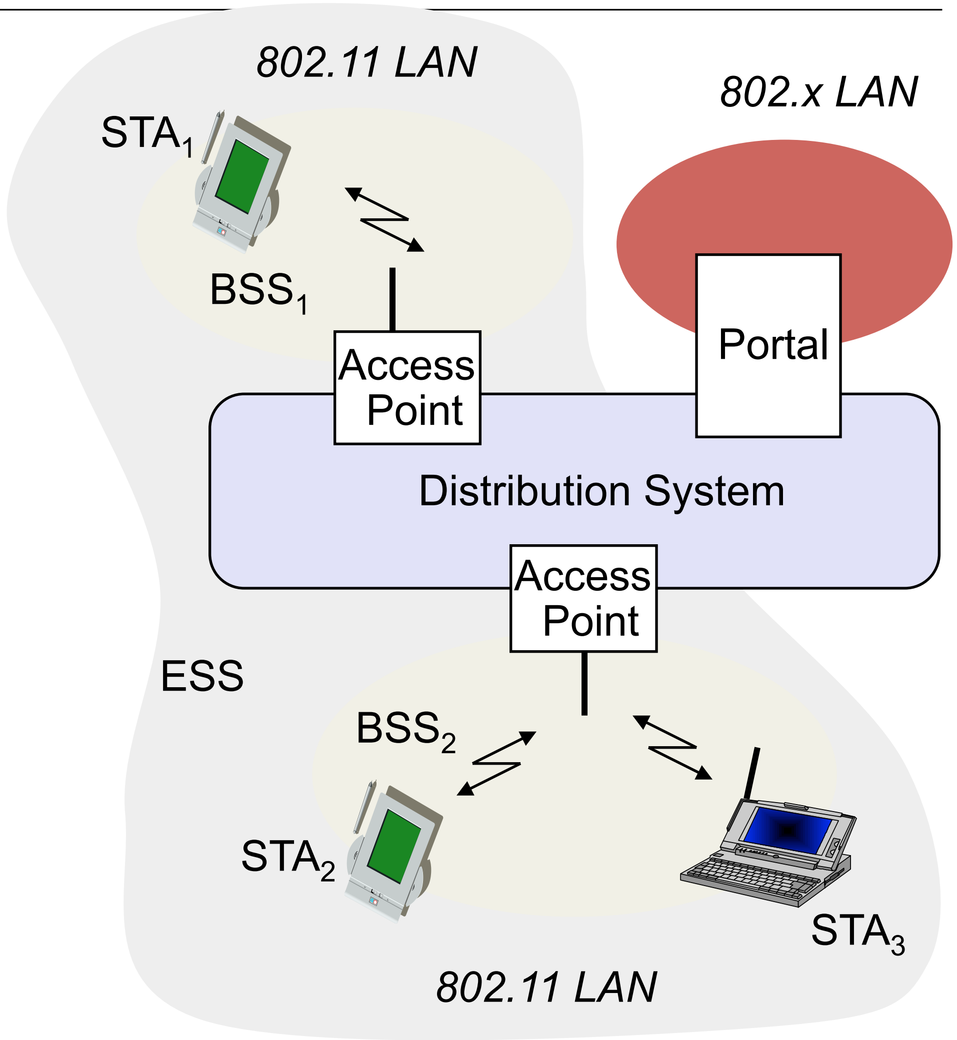
Station (STA):
- Terminal with access mechanisms to the wireless medium and radio contact to the access point

Basic Service Set (BSS):
- Group of stations using the same radio frequency

Access Point:
- Station integrated into the wireless LAN and the distribution system

Portal:
- Bridge to other (wired) networks

Distribution System:
- Interconnection network to form one logical network (extended service set, ESS) based on several BSS



Security Requirements

Confidentiality
- messages sent over wireless links need to be encrypted

Authenticity
- origin of messages received over wireless links needs to be verified
- replay detection: freshness of messages received over wireless links needs to be checked

Integrity
- modifying messages on-the-fly (during radio transmission) is not so easy, but possible …
- integrity of messages received over wireless links needs to be verified

Access control
- access to the network services should be provided only to legitimate entities

Availability
- protection against jamming and Denial-of-Service attacks should be provided

Security Services of Original IEEE 802.11

Security services of IEEE 802.11 are realized by:

- Authentication (Open System/Shared Key)
- Wired Equivalent Privacy (WEP) mechanism
- 802.11i Security Standard

WEP is supposed to provide the following security services:

- Confidentiality
- Data origin authentication / data integrity
- Access control in conjunction with layer management

WEP makes use of the following algorithms:

- The RC4 stream cipher
- The Cyclic Redundancy Code (CRC) checksum for detecting errors

Protected access using WEP

WEP = Wired Equivalent Privacy

- Part of the IEEE 802.11 specification

Objective

- Make the WiFi network at least as secure as a wired LAN (that has no particular protection mechanisms)
- WEP was never intended to achieve strong security
- At the end, it hasn't achieved even weak security

Services

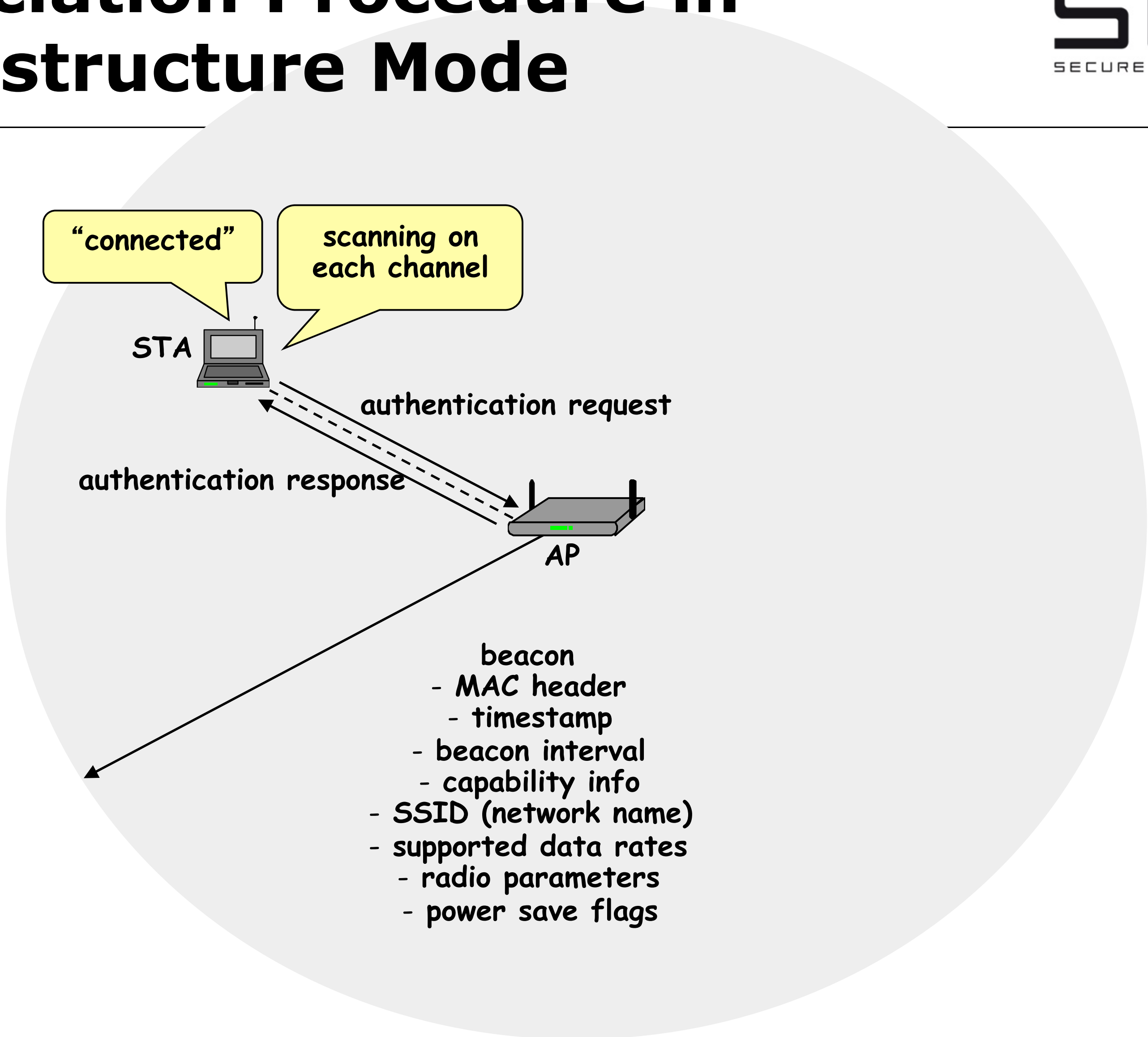
- Message confidentiality
- Message integrity
- Access control to the network

IEEE 802.11 Entity Authentication

IEEE 802.11 authentication comes in two “flavors”:

- Open System Authentication:
  - “Essentially it is a null authentication algorithm.” (IEEE 802.11, section 8.1.1)
- Shared Key Authentication:
  - “Shared key authentication supports authentication of STAs as either a member of those who know a shared secret key or a member of those who do not.” (IEEE 802.11, section 8.1.2)
  - “The required secret, shared key is presumed to have been delivered to participating STAs via a secure channel that is independent of IEEE 802.11”

Association Procedure in Infrastructure Mode

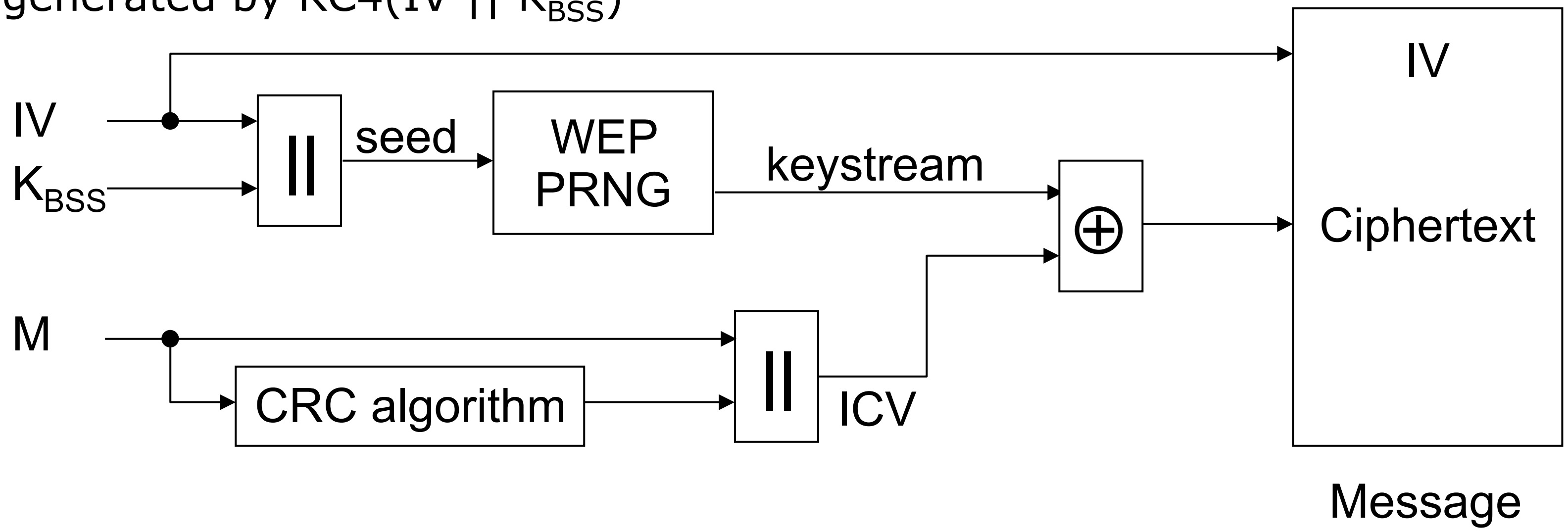


A Short WEP Mechanism Walkthrough

IEEE 802.11's Wired Equivalence Privacy (1)

IEEE 802.11's WEP uses RC4 as a pseudo-random-bit-generator (PRNG):

- For every message M to be protected a 24 bit initialization vector (IV) is concatenated with the shared key K_{BSS} to form the seed of the PRNG
- The integrity check value (ICV) of M is computed with CRC and appended ("||") to the message
- The resulting message (M || ICV) is XORed ("⊕") with the keystream generated by RC4(IV || K_{BSS})



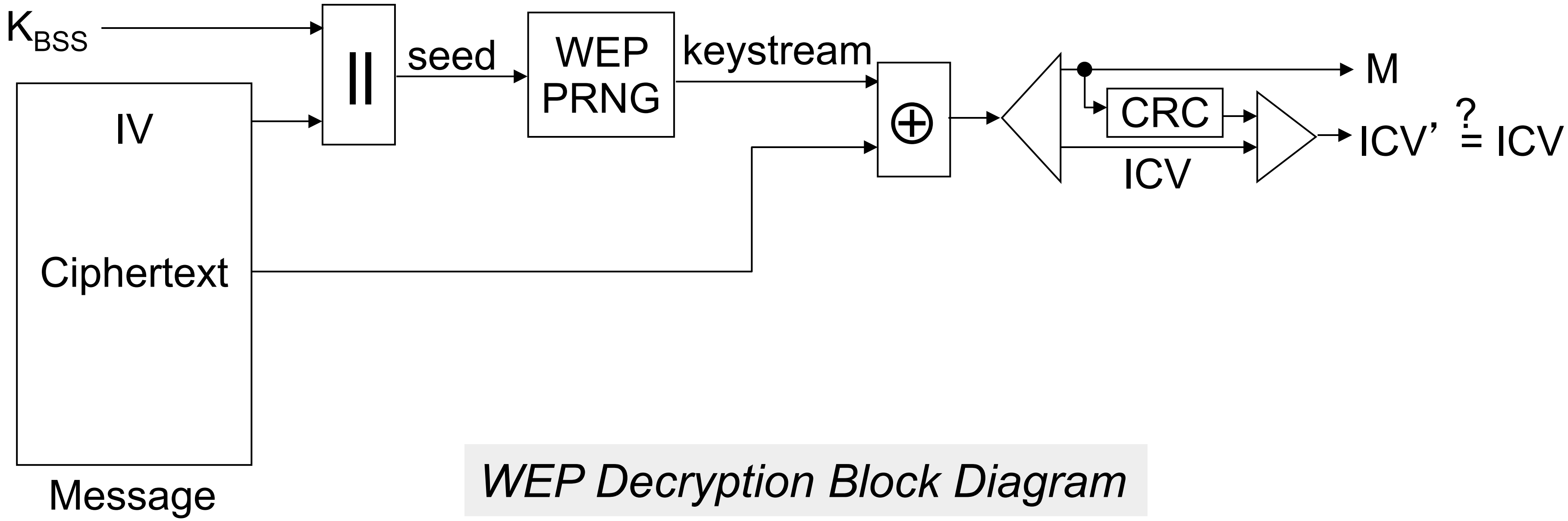
WEP Encryption Block Diagram

IEEE 802.11's Wired Equivalence Privacy (2)

As *IV* is send in clear with every message, every receiver who knows K_{BSS} can produce the appropriate keystream to decrypt a message

- This assures the important *self-synchronization property* of WEP

The decryption process is basically the inverse of encryption:



WEP Decryption Block Diagram

WEP Authentication

user

probe request
(sent on all channels, trying to find AP with matching SSID)

→

response (if in range)

←

auth. request (choosing "best" AP)

→

challenge

←

response

→

auth. decision

←

.... if authentication successful

association request

→

association response

←

user can now send data

→

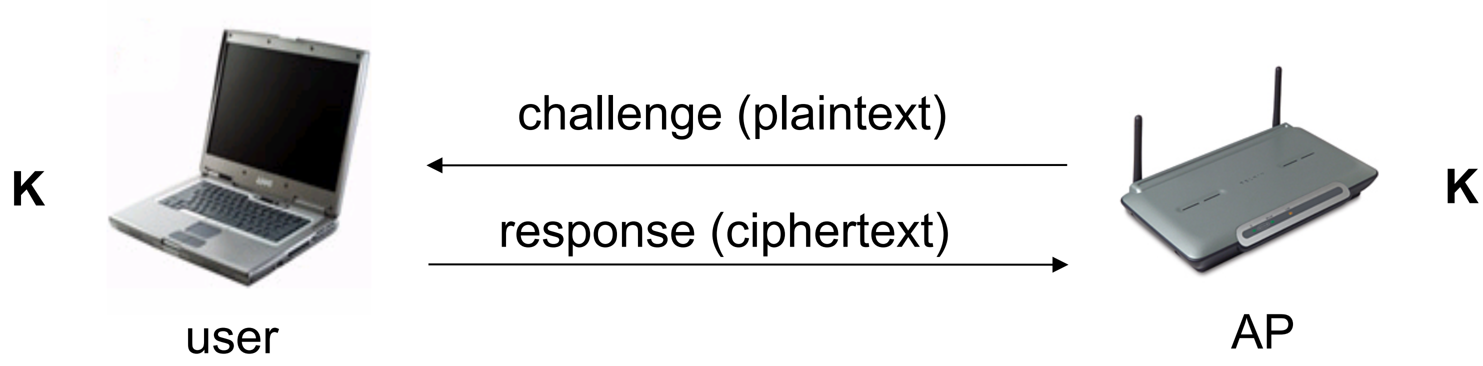
AP

WEP Authentication (1)

Based on a shared key between the station and the AP (40 bit or 104 bit)

- Utilizing the RC4 symmetric stream cipher to solve the challenge

Authentication through a ‘classical’ challenge-response authentication protocol ... using the shared key **K** ...



WEP Authentication (2)

Challenge text sent in payload in cleartext (128 octets), random IV used

Response sent in payload encrypted with the key shared between the AP and the station

Size in octets	2	2	6	6	6	2	0 - 2312	4	
	Frame Control	Duration	Dest Addr	Source Addr	BSSID	Seq #	Frame Body	FCS	Management Frame Format

	Algorithm Number	Seq Num	Status Code	Element ID	Length	Challenge Text	Authentication Frame Format
Size in octets	2	2	2	1	1	128	

After authentication, use shared key for confidentiality protection

IEEE 802.11 WEP's Security Claims

The WEP has been designed to ensure the following security properties:

- Confidentiality:
  - Only stations which possess K_{BSS} can read messages protected with WEP
- Data origin authentication / data integrity:
  - Malicious modifications of WEP protected messages can be detected
- Access control in conjunction with MAC layer management:
  - If set so in the MAC layer management, only WEP protected messages will be accepted by receivers
  - Thus stations that do not know K_{BSS} can not send to such receivers

Unfortunately, none of the above claims holds.

WEP was a security disaster…

WEP Weakness #1: The Keys

SECURE MOBILE NETWORKING

IEEE 802.11 does not specify any key management:

- Manual management is error prone and insecure
- Shared use of one key for all stations of a BSS introduces additional security problems
- As a consequence of manual key management, keys are rarely changed
- As a another consequence, “security” is often even switched off!

Key Length:

- The key length of 40 bit specified in the original standard provides only poor security
- The reason for this was exportability
- However, basically all today's wireless LAN cards offer longer key lengths, i.e., keys of length 104 /128bit

WEP Weakness #2: Confidentiality

Even with well distributed and long keys WEP is insecure

The reason for this is reuse of keystream:

- The encryption is re-synchronized with every message by pre-pending an *IV* of length 24 bit to K_{BSS} and re-initializing the PRNG
- Consider two plaintexts P_1 and P_2 encrypted using the same IV_1:
  - $C_1 = P_1 \oplus \text{RC4}(IV_1, K_{BSS})$
  - $C_2 = P_2 \oplus \text{RC4}(IV_1, K_{BSS})$

  then:
  - $C_1 \oplus C_2 = (P_1 \oplus \text{RC4}(IV_1, K_{BSS})) \oplus (P_2 \oplus \text{RC4}(IV_1, K_{BSS})) = P_1 \oplus P_2$

$\oplus$ operation is associative

- Thus, if an attacker knows, for example, P_1 and C_1 he can recover P_2 from C_2 without knowledge of the key K_{BSS}

How often does reuse of keystream occur?

- In practice quite often, as many implementations choose *IV* poorly ("weak IV")
- Even with optimum choice, as IV's length is 24 bit, a busy base station of a 11 Mbit/s WLAN will exhaust the available space in half a day

WEP Flaws #3: Integrity and Replay Protection

Example:

An attacker can manipulate messages M despite the ICV mechanism and encryption

– CRC is a linear function wrt. to XOR:

$$CRC(X \oplus Y) = CRC(X) \oplus CRC(Y)$$

- attacker observes $(M \,||\, CRC(M)) \oplus K$ where K is the RC4 output
- for any ΔM, the attacker can compute $CRC(\Delta M)$
- hence, the attacker can compute:

$$((M \,||\, CRC(M)) \oplus K) \oplus (\Delta M \,||\, CRC(\Delta M)) =$$
$$((M \oplus \Delta M) \,||\, (CRC(M) \oplus CRC(\Delta M))) \oplus K =$$
$$((M \oplus \Delta M) \,||\, CRC(M \oplus \Delta M)) \oplus K$$

Without knowing the key, the attacker can produce a message that seems authentic.

WEP Weakness #4: Access Control is Insecure

Recall that the integrity function is computed without any key

Consider an attacker who learns a plaintext-ciphertext pair:

1. As the attacker (Trudy) knows M and C = RC4(IV, K_{BSS}) ⊕ (M, CRC(M)), she can compute the keystream used to produce C
2. If Trudy later on wants to send a message M' she can compute C' = RC4(IV, K_{BSS}) ⊕ (M', CRC(M')) and send the message (IV, C')

As the reuse of old IV values is possible without triggering any alarms at the receiver, this constitutes a valid message

- An "application" for this attack is unauthorized use of network resources:
  - The attacker sends IP packets destined for the Internet to the access point which routes them accordingly, giving free Internet access to the attacker

⇒ WEP Access Control can be circumvented with known plaintext

WEP Weakness #5: RC4 Key Scheduling

In early August 2001 a new attack to WEP was discovered

- Complete recovery of a secret key, called Fluhrer, Mantin and Shamir attack (FMS)
- Based on a weakness in the PRNG used to generate the keystream.
- RC4 is vulnerable to deducing bits of a key if:
  - many messages are encrypted with keystream generated from a variable initialization vector and a fixed key, and
  - the initialization vectors and the plaintext of the first two octets are known for the encrypted messages

- The attack is described “Weaknesses in the Key Scheduling Algorithm of RC4”, by FMS
  - R. Rivest comments on this [Riv01a]:

  “Those who are using the RC4-based WEP or WEP2 protocols to provide confidentiality of their 802.11 communications should consider these protocols to be broken [...]”

Conclusions on IEEE 802.11 WEP Deficiencies

IEEE 802.11 WEP does not provide sufficient security:

- Missing key management makes use of the security mechanisms tedious and leads to rarely changed keys or even security switched off
- Entity authentication as well as encryption rely on a key shared by all stations of a basic service set
- Insecure entity authentication protocol
- Reuse of keystream makes known-plaintext attacks possible
- Linear integrity function allows to forge ICVs
- Unkeyed integrity function allows to circumvent access control by creating valid messages from a known plaintext-ciphertext pair
- Weakness in RC4 key scheduling allows to cryptanalyze keys
- Even with IEEE 802.1X and individual keys the protocol remains weak
- The WEP can be broken very fast … recently, a team at TU Darmstadt broke it in under 60 seconds …

IEEE 802.11 Alternative Access Mechanisms

Which unfortunately do more harm than good

Different security “patches” or “recommendations” from industry based on security by obscurity

- Using SSIDs (Service Set Identifier) for authentication and as a secret and hide broadcast of SSID
- MAC filtering & Access Control Lists

→ No security at all …

SSID-based access control

SSID = Service Set IDentifier (network name)

- a 32-character unique identifier
- acts as a “password” when a mobile device tries to connect to the WLAN
- SSID differentiates one WLAN from another
- all devices attempting to connect to a specific WLAN must use the same SSID

Found in the header of every packet

802.11 MAC header

SECURE MOBILE NETWORKING

Addr. 1 = All stations filter on this address.

Addr. 2 = Transmitter Address (TA).

Addr. 3 = Dependent on To and From DS bits.

DATA

Bytes:								
2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration ID	Addr 1	Addr 2	Addr 3	Sequence Control	Addr 4	Frame Body	CRC

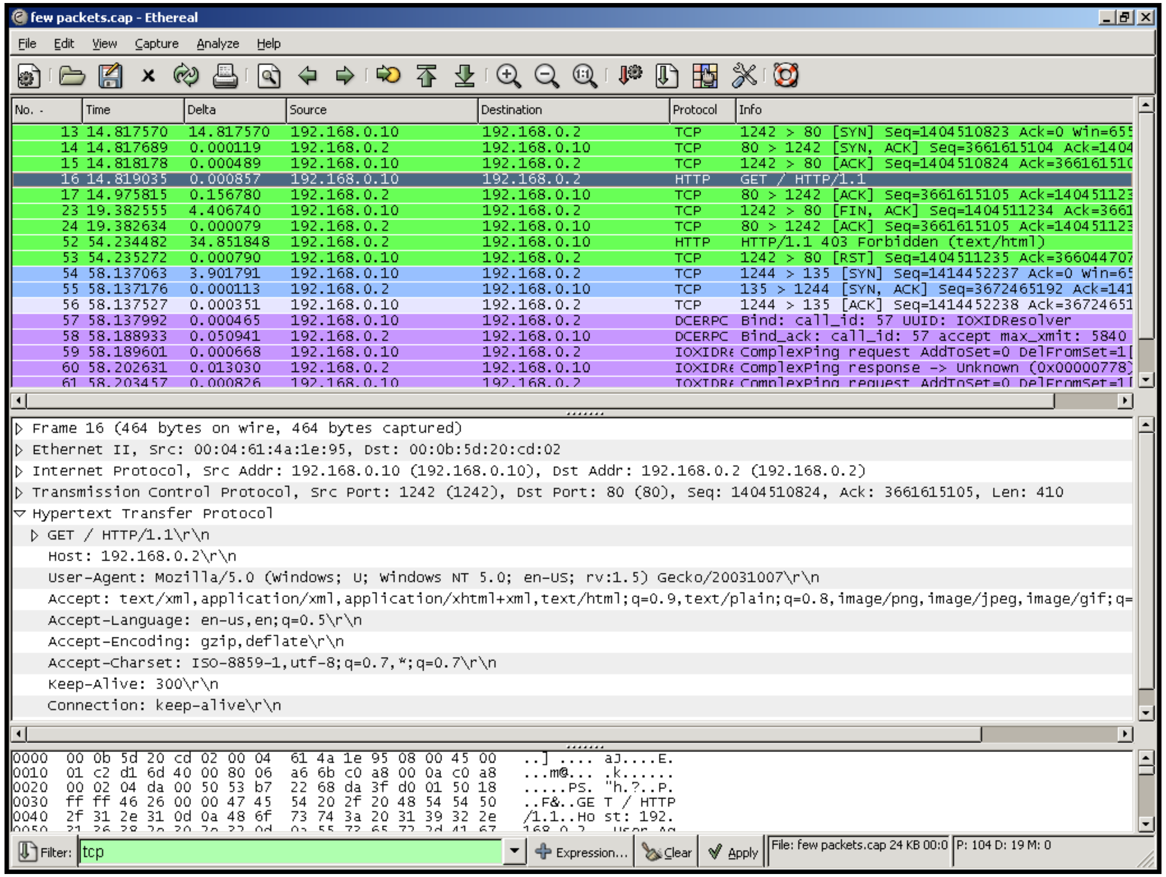
Frame Control Field

Bits: 2	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	SubType	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Rsvd

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

3 simple steps for overcoming MAC filtering

1. Put your card in promiscuous mode (accepts all packets).
2. Sniff the traffic and find out which MAC addresses are accepted by the AP
3. Change your MAC address (need a card that can do that)




```
# ifconfig ath0 hw ether <mac address of C>
```

A Life After WEP: IEEE 802.11i

After the collapse of WEP, IEEE started to develop a new security architecture aka 802.11i

Main novelties in 802.11i wrt to WEP

- Authentication and access control model is based on 802.1X and EAP
- Different functions (encryption, integrity) use different keys derived from the session key using a one-way function
- Integrity protection is improved
- Encryption function is improved

802.11i is also called RSN Robust Security Network

IEEE 802.11i Security vs. Performance Tradeoff:

- WiFi Protected Access (WPA) TKIP + RC4
- WiFi Protected Access 2 (WPA2): AES-CCMP

Fixing WLAN Security: IEEE 802.11 Task Group *i*

Objective:

- Enhance the 802.11 Security
- Defining the interaction between 802.1X and 802.11 standards
- Draft standard was ratified on 24. June 2004 (IEEE 802.11i)

802.11i defines two classes of security algorithms:

- Pre-RSN security Network (→ WEP)
- Robust Security Network (RSN)

RSN security consists of two basic subsystems:

- Security association/authentication management:
  - 802.1X authentication - replacing 802.11 authentication
- Data privacy mechanisms:
  - TKIP - rapid re-keying to patch WEP for minimum privacy (recommended only as patch for Pre-RSN equipment)
  - AES encryption - robust data privacy for long term (CCMP)

An Intermediate Solution: Temporal Key Integrity Protocol

SECURE MOBILE NETWORKING

Design Goals:

- Quick fix to the existing WEP problem, runs WEP as a sub-component
- Can be implemented in software, reuses existing WEP hardware
- Requirements on existing AP hardware:
  - 33 or 25 MHz ARM7 or i486 already running at 90% CPU utilization before TKIP
  - Software / firmware upgrade only

Main concepts:

- Message Integrity Code (MIC)
- Sequence counter
- Dynamic key management (re-keying)
- Key mixing

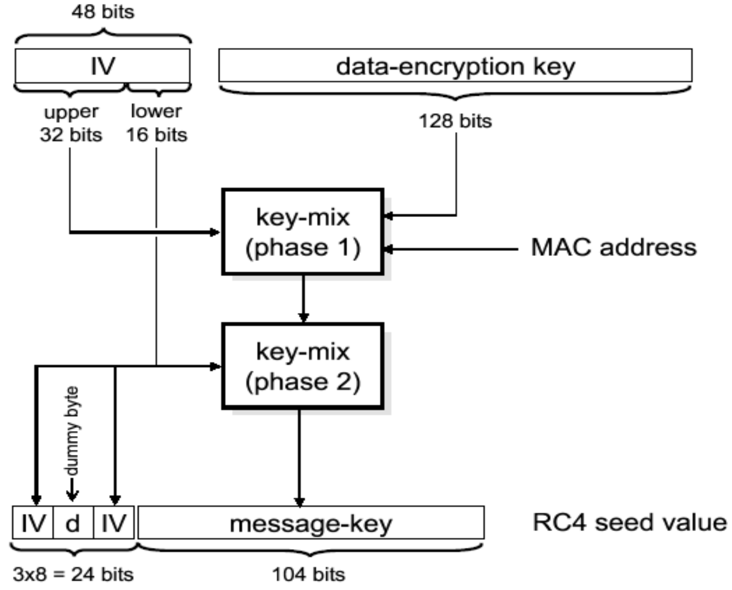
TKIP Design: Replay Protection and RC4 Key Scheduling

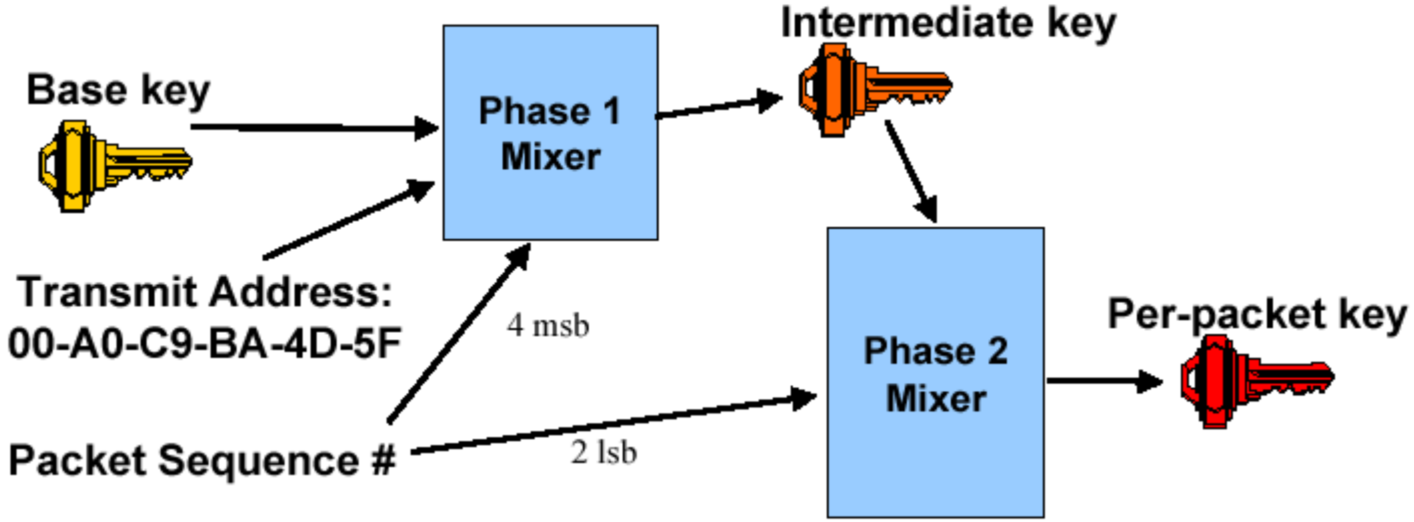
Avoid WEP's encryption weaknesses:

- Build a better per-packet encryption key
  attacks and decorrelating WEP IV and pe

Replay protection:

- Reset packet sequence# to 0 on rekey
- Increment sequence# by 1 on each pac
- Drop any packet received out of sequenc

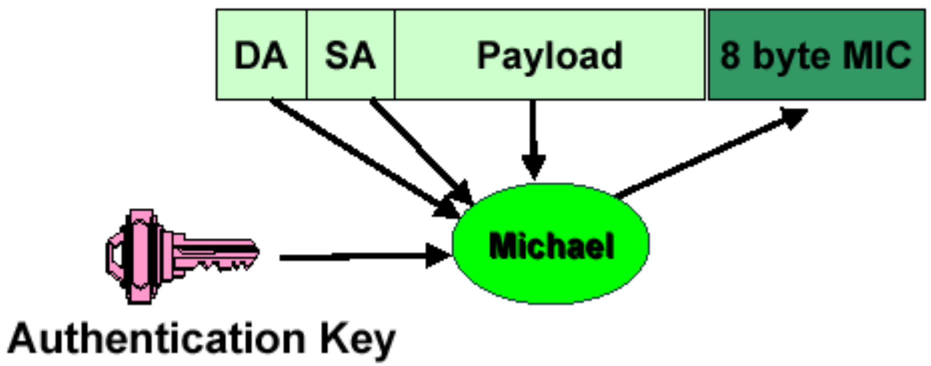




TKIP Design: Message Integrity Code Function “Michael”

Protect against forgeries:

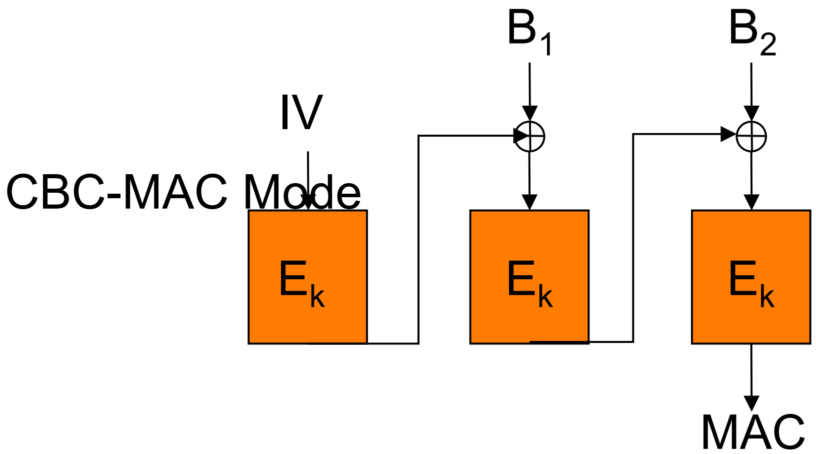
- Must be cheap: CPU budget 5 instructions / byte
- The Michael algorithm designed to provide only 20 bits of security due to the limited power of legacy devices
  - Attacker can guess the right MIC in ca. 219 attempts
  - Countermeasures on detecting forgery attempt (limiting the rate of forgery attempts)
  - If two MIC failures are detected within 60 seconds, AP will block transmission for 60 seconds



The Long Term Solution: AES in WLAN

Counter Mode with Cipher Block Chaining Message Authentication (CCMP)

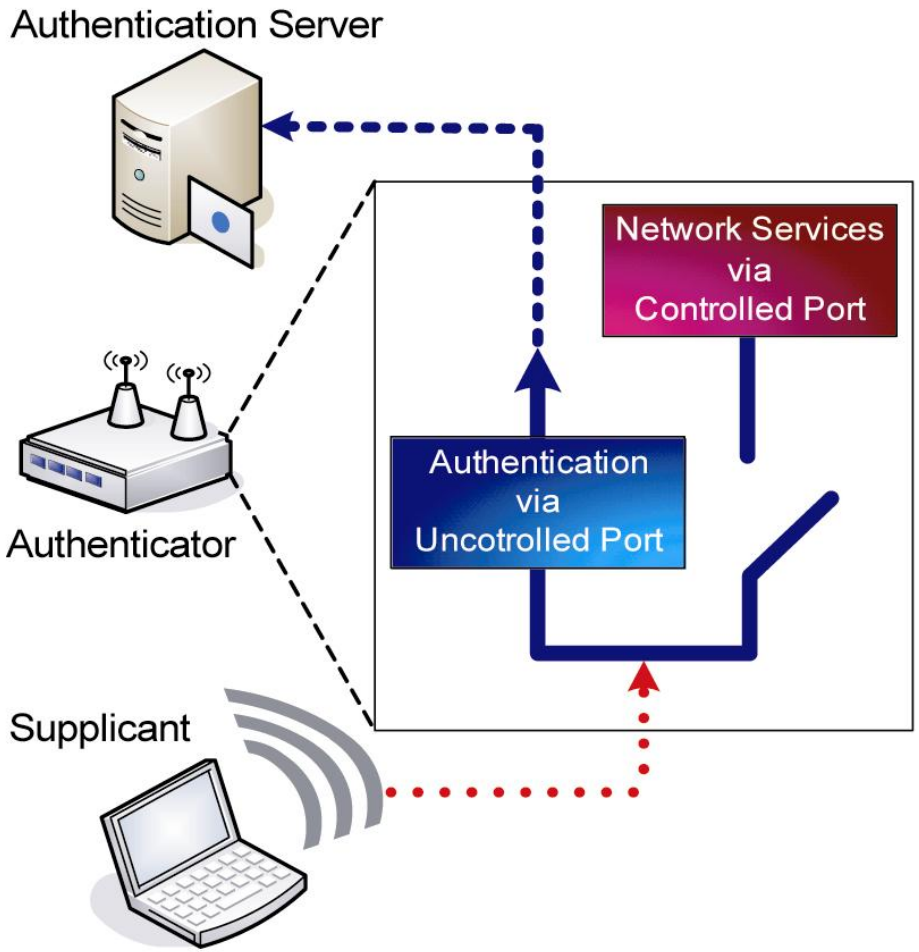
- Mandatory to implement: the long-term solution
- New protocol with no similarity to WEP
- Provides: data confidentiality, data origin authentication, replay protection
- Based on AES in Counter Mode Encryption with CBC-MAC (CCM)
  - Use CBC-MAC to compute a MIC on the plaintext header, length of the plaintext header, and the payload
  - Use CTR mode to encrypt the payload with counter values 1, 2, 3, …



IEEE 802.11i: Authentication

IEEE 802.1X

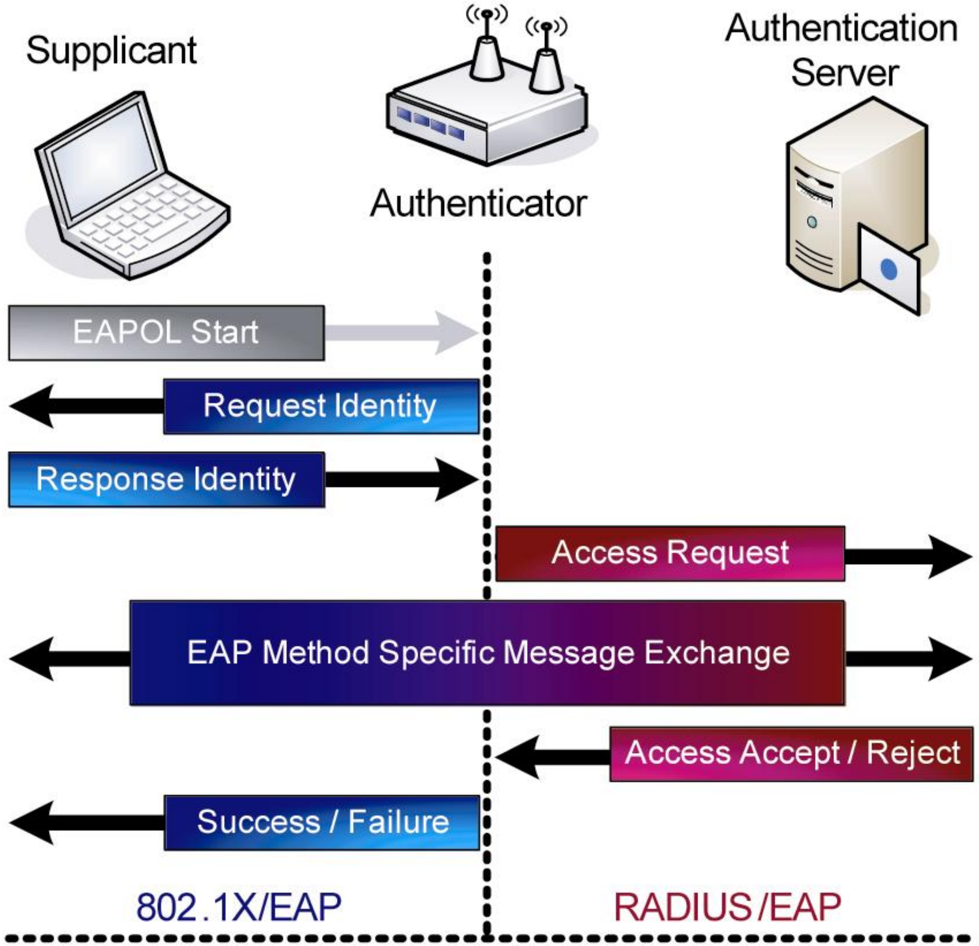
- Port-based network access control
- Authentication and authorization of devices attached to LAN
- Only EAP traffic allowed before authentication
  - "ports" are closed
- Roles:
  - Supplicant (STA), Authenticator (AP),
  - Authentication Server (AS)
  - Remote Access Dial-In User Service (RADIUS)



IEEE 802.11i: Authentication

EAP

- Extensible Authentication Protocol
- Authentication Framework
- Different authentication methods
  - EAP-TLS, EAP-MD5, EAP-Smartcard, many more



IEEE 802.11i: Key Hierarchy

PSK: *Pre-Shared Key*

MSK: *Master Session Key*

- MSK/PSK known only to STA and AS

PMK: *Pairwise Master Key*

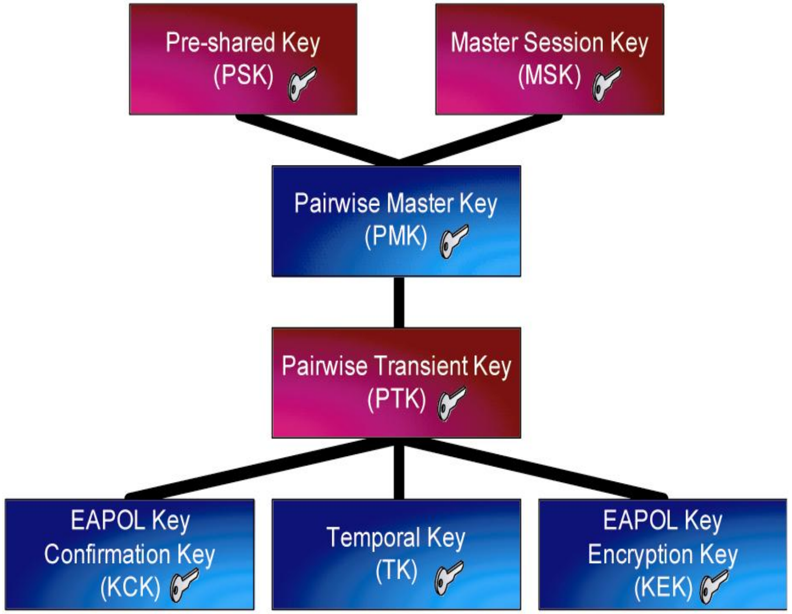
- Key derived from the EAP-TLS (MSK) or any other authentication method (e.g. pre-shared secret (PSK))
- Installed on AP

PTK: *Pairwise Transient Key*

- Collection of operational keys
  - KCK: used to prove the possession of PMK
  - KEK: distribution of group transient key (GTK)
  - TK: used for encryption (cipher specific)

GTK: *Group Transient Key*

- Shared among all supplicants connected to the same authenticator



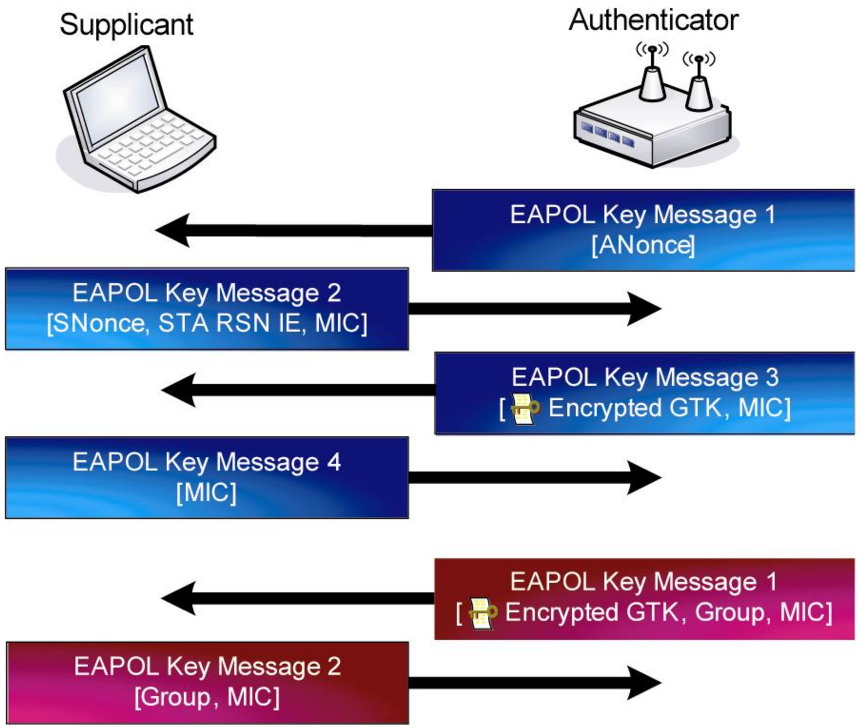
IEEE 802.11i: 4-Way Handshake

IEEE 802.1X: no key management

- Provides only MSK

4-Way Handshake

- Derivation and installation of fresh session keys from PMK
- Binding of keys to MAC addresses
- Verification of the PMK (by MIC)
- Verification of security configuration (by RSN IE)
- Indication that integrity protection and encryption are ready
- Encrypted distribution of GTK



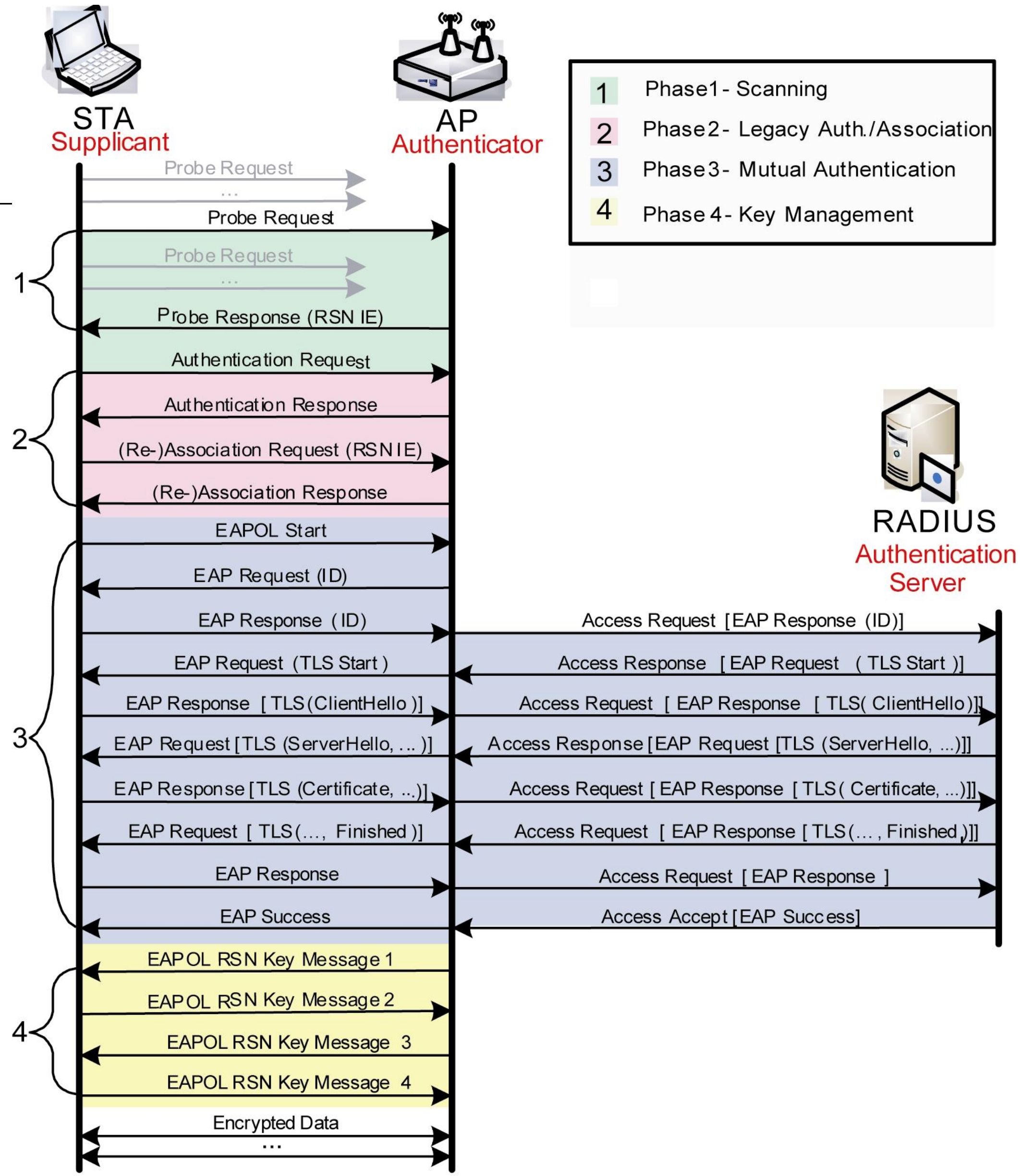
IEEE 802.11i: RSN Overview

Phase 1:
- Network and security capability discovery
- Active/passive scanning

Phase 2:
- 802.11 Open System authentication and association
- Backward compatibility
- 802.1X Ports blocked

Phase 3:
- EAP/802.1X/RADIUS
- E.g. EAP-TLS
- Derivation of MSK and PMK

Phase 4:
- 4-Way handshake
- Installation/verification of PTK, GTK
- 802.1X ports unblocked



Comparison of WEP, TKIP, and CCMP

	WEP	TKIP	CCMP
Cipher	RC4	RC4	AES
Key Size	40 or 104 bits	128 bits	128 bits encrypt, 64 bit auth.
Key Life	24-bit IV, wrap	48-bit IV	48-bit IV
Packet Key	Concat.	Mixing Fnc.	Not Needed
Integrity			
Data	CRC-32	Michael	CCM
Header	None	Michael	CCM
Replay	None	Use IV	Use IV
Key Mgmt.	None	EAP-based	EAP-based

Attacks & Countermeasures on IEEE 802.11i (1)

Early days of IEEE 802.11's security very tragic (→ WEP)

- WepOff, Aircrack, AirSnort, WEPCrack, KisMAC, …

Availability was never primary security objective within IEEE 802.11

- Frequency jamming
- CSMA/CA protocol manipulation
- → hard to protect

Management and control frames still not authenticated

Attacks on availability can be used to start attacks on other security objectives

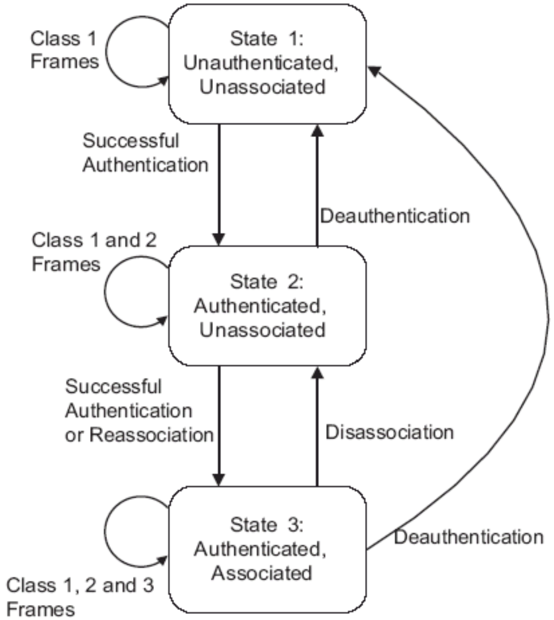
IEEE 802.11w

- Protected management frames standard; status: ratified in 2009
- Solves part of security puzzle by protectiong auth/de-auth/assoc/de-assoc frames (and certain other mgmt. frames)

Attacks on IEEE 802.11i (2)

Inherited attacks:

- De-authentication, De-association, PS-poll, NAV, …



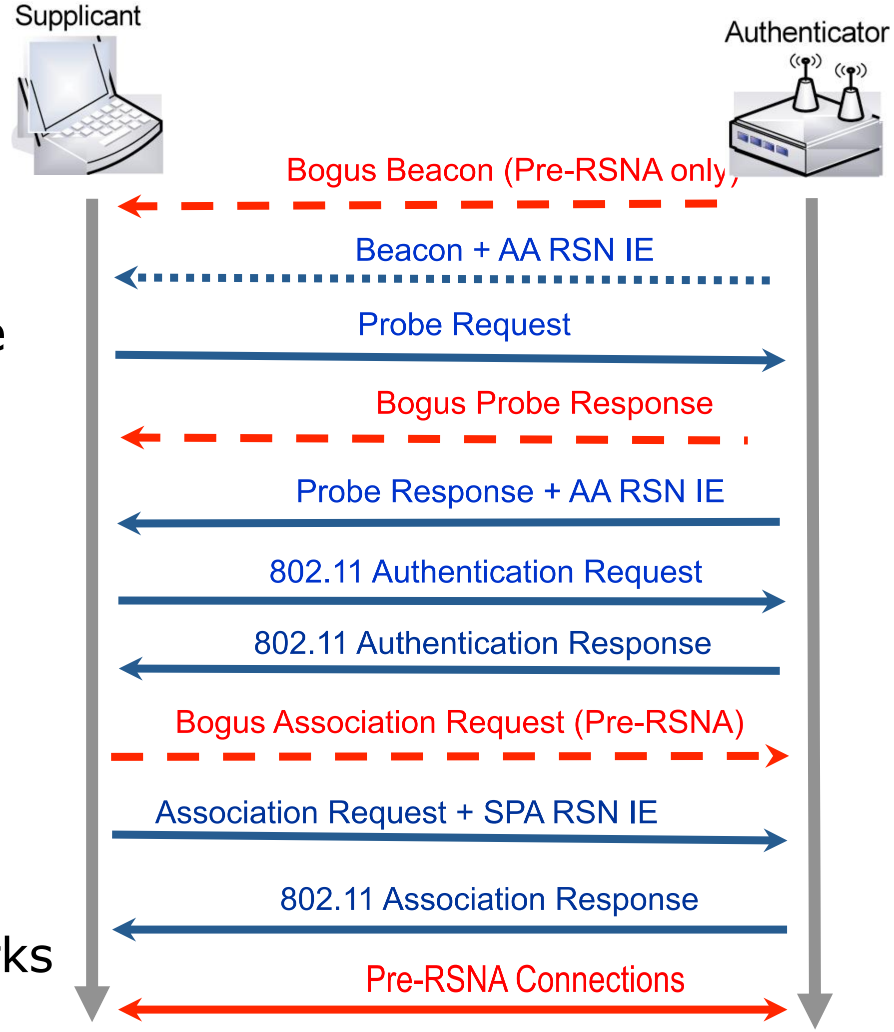
	Control Frames (CF)	Management Frames	Data Frames
Class 1	Request to Send (RTS), Clear to Send(CTS), Acknowledgement(ACK), CF-End, CF-End+CF-Ack	Beacon, Probe Req. / Resp., Authentication Req. / Resp., Deauthentication, Announcement Traffic Indication Message (TIM)	None (infrastructure BSS)
Class 2	None	Association Req. / Resp., Reassociacion Req. / Resp., Disassociation	None
Class 3	Power-Save Poll (PS-Poll)	Deauthentication	All frames

- [Bellardo03] John Bellardo and Stefan Savage (UCSD): 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions, 12th USENIX Security Symposium, pages 15-28, 2003

IEEE 802.11i: Attacks on RSN (3)

Security Level Rollback Attack

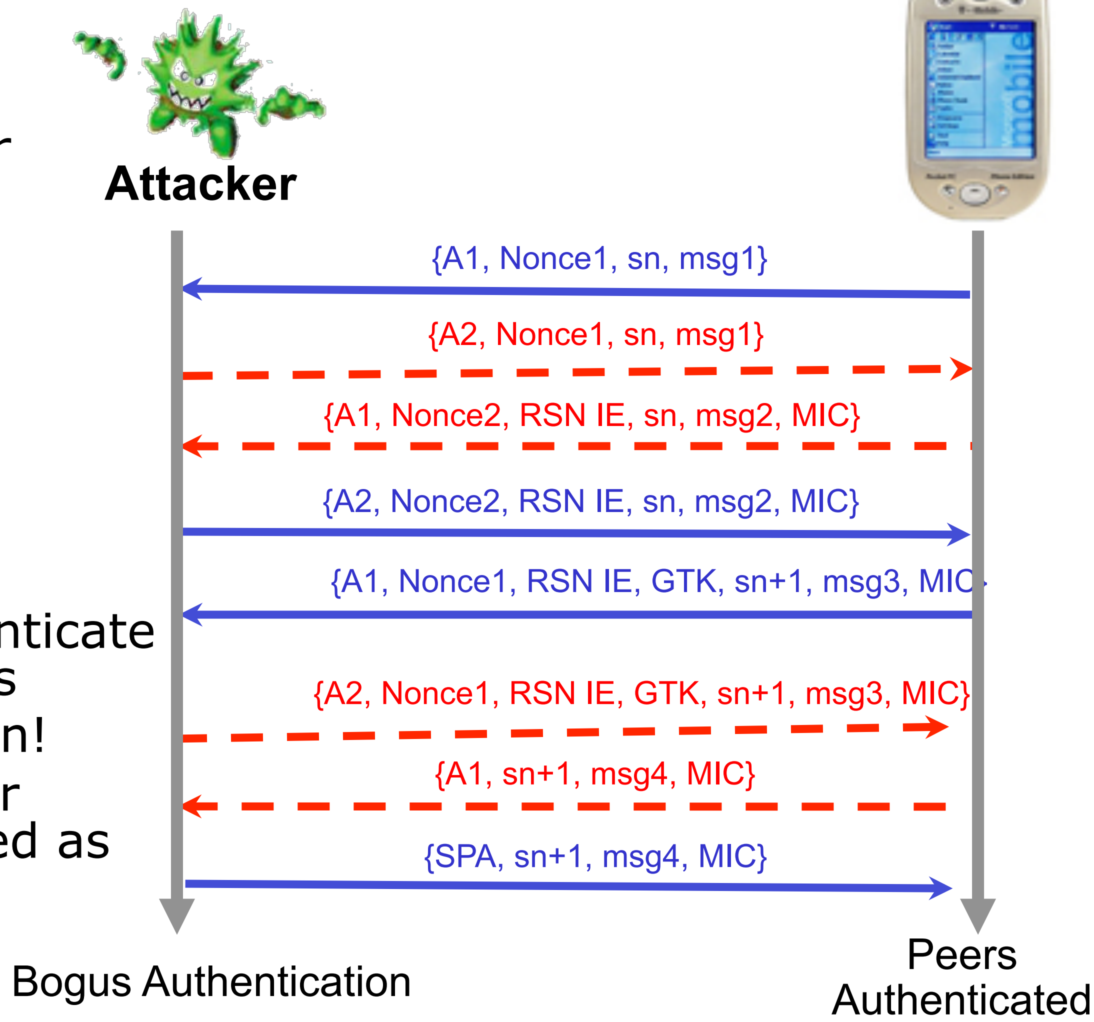
- Attack on authentication
- Both supplicant and authenticator
  - RSNA enabled
  - Pre-RSNA enabled
  - Some RSN implementations enable both Pre-RSN and RSN to support migration
- Goal
  - Rolling back the security level
  - Impersonate supplicant or authenticator and provide only Pre-RSN (→WEP)
  - Impersonate supplicant to request Pre-RSN security
- This attack only likely on Transient Security Networks (TSNs)
  - Pre-RSN together with RSN networks



IEEE 802.11i: Attacks on RSN (4)

Reflection attack

- One device used as both supplicant and authenticator
- Same PMK
- Attacker:
  - 4-Way Handshake as supplicant
  - 4-Way Handshake as authenticator
  - Collects responses from victim
  - Use victim's data to authenticate again or for offline analysis
- Mutual authentication broken!
- Supplicant and authenticator should never be implemented as single device (or have same PMK)



IEEE 802.11i: Attacks on RSN (5)

Attacks on availability (Denial of Service)

- Since the management and control frames are still unprotected, forging and impersonating frames remains most effective DoS attack
  - De-Authentication attack
  - De-Association attack
  - …and many more…(see [Bellardo03] for a nice overview)
- Flooding attack [Disco07-1]
  - Authentication/Association requests floods
  - Some APs crash or exhibit high delays and high losses
  - DoS can serve as catalyser for more sophisticated attacks
- New attacks [He05]
  - Flooding by EAP-Request messages (Identifier space = 8 bit)
  - Sending fake EAP-Failure messages
  - RSN Information Element (IE) poisoning
  - 4-Way Handshake Blocking (first message of 4WH is not authenticated!)

IEEE 802.11i - Conclusion

802.11i provides

- Satisfactory data confidentiality & integrity with CCMP
- Satisfactory mutual authentication & key management

Some implementation mistakes can result in vulnerabilities

- Security Level Rollback Attack in TSN
- Reflection Attack on the 4-Way Handshake

Availability is still a problem

- Simple policies can make 802.11i robust to some known DoS
  - But, till management and control frames are not authentication simple attacks can still disrupt the whole 802.11 network
- Possible attack on Michael Countermeasures in TKIP
- RSN IE Poisoning/Spoofing
- 4-Way Handshake Blocking

Additional References

[IEEE97a] IEEE. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std 802.11-1997, The Institute of Electrical and Electronics Engineers (IEEE), 1997.

- And also the later versions of the standard

[BELLARDO03] J. Bellardo and S. Savage, “802.11 Denial of service attacks: real vulnerabilities and practical solutions,” in Proceedings of the 12th USENIX Security Symposium, Washington, DC, USA, August 2003.

[DISCO07-1] Ivan Martinovic, Frank A. Zdarsky, Adam Bachorek, Christian Jung, and Jens B. Schmitt. *Phishing in the Wireless: Implementation and Analysis.* In Proceedings of the 22nd IFIP International Information Security Conference (SEC 2007), Sandton Johannesburg, South Africa. Springer, May 2007.

[HE05] C. He and J. C. Mitchell, “Security analysis and improvements for IEEE 802.11i,” in Proceedings of the 12th Annual Network and Distributed System Security Symposium (NDSS '05), San Diego, Calif, USA, February 2005.

Acks & Recommended Reading

Selected slides of this chapter courtesy of

- Ivan Martinovic, TU Kaiserslautern
- Some other slides courtesy of G. Schäfer (TU Ilmenau) with changes of J. Schmitt (TU Kaiserslautern) and myself incorporated
- Yet some other slides courtesy of L. Buttyan (ETHZ)

Recommended reading

- [KaPeSp2002] Charlie Kaufman, Radia Perlman, Mike Speciner: Network Security – Private Communication in a Public World, 2nd Edition, Prentice Hall, 2002, ISBN: 978-0-13-046019-6
- [Stallings2015] William Stallings, Network Security Essentials, 4th Edition, Prentice Hall, 2015, ISBN: 978-0-136-10805-4
- [Schäfer2003] G. Schäfer. Netzsicherheit - Algorithmische Grundlagen und Protokolle. dpunkt.verlag, 2003.

Copyright Notice

Contact

Prof. Dr.-Ing. Matthias Hollick
Department of Computer Science

SEEMOO
Mornewegstr. 32
64293 Darmstadt/Germany
matthias.hollick@seemoo.tu-darmstadt.de

Phone +49 6151 16-70920
Fax +49 6151 16-70921
www.seemoo.tu-darmstadt.de