802.11 Security – TKIP

Shambhu Upadhyaya
Wireless Network Security
CSE 566 (Lecture 17)

TKIP

- Temporal Key Integrity Protocol
- Designed as a wrapper around WEP
  - Can be implemented in software
  - Reuses existing WEP hardware
  - Runs WEP as a sub-component
- Quick-fix to the existing WEP problem
- New "procedures" around Legacy WEP
- Components
  - Cryptographic message integrity code
  - Packet sequencing
  - Per-packet key mixing
  - Re-keying mechanism

TKIP Introduction

- Never use the same IV value more than once for any particular session key
  - Prevents key-stream reuse by a system
- Receivers discard any packets whose IV value is less or equal to the last successfully received packet encrypted with the same key
  - Prevents replay attacks
- Regularly generate a new random session key before the IV counter overflows
  - Prevents key-stream reuse
- Provide a more thorough mixing of the IV value and the session key to derive the packet's RC4 key
  - To "fix" the RC4 Key scheduling issues with WEP

Weaknesses of WEP

1	IV value is too short and not protected from reuse
2	The way keys are constructed from IV makes it susceptible to weak key (FMS) attack
3	No effective way to detect message tampering
4	Directly uses master keys with no provision for re-keying
5	No protection against replay attacks

Changes from WEP to TKIP

Purpose	Change	Weakness Addressed
Message Integrity	Adds a message integrity protocol to prevent tampering (one which can be implemented in software using a low power microprocessor)	(3)
IV selection and use	Changes how IV values are selected, uses it as a replay counter	(1) , (3)

Changes from WEP to TKIP

Purpose	Change	Weakness Addressed
Per-Packet Key Mixing	Changes encryption key for every frame	(1),(2),(4)
IV Size	Increases the size of the IV to avoid reusing the same IV	(1),(4)
Key Management	Adds a mechanism to distribute and change keys and derive temporal keys	(4)

Message Integrity

- Essential to security of the message
- WEP uses ICV (Integrity Check Value), but it offers no real protection
- Thus, ICV is not a part of TKIP security
- Basic idea behind computing the MIC (Message Integrity Code) is calculating a checksum over the message bytes so that any modification to the message can be detected
- This MIC is combined with a secret key so that only authorised parties can generate and verify the MIC
- Many available cryptographic methods can be used for the purpose

Message Integrity - Michael

- As WEP is required to work over existing hardware it cannot use computationally intensive cryptographic methods
- Even if the computations are moved to software level in clients, existing Access Points cannot perform heavy computations
- Thus, TKIP uses a method of computing MIC called *Michael*
- *Michael* uses simple shift and add operations instead of multiplications and hence is usable in TKIP

Message Integrity - Michael

- Michael operates on MSDUs (MAC Service Data Unit) rather than individual MPDUs (MAC Protocol Data Unit)
  - Useful as the computation can be performed in the device driver on the computer rather than on the adapter card
  - Also reduces overhead as MIC is not calculated for each MPDU being sent out
- As Michael is computationally simple, it offers a weak form of security
- To counter these drawbacks, it includes a set of *countermeasures* which are used when an attack is detected

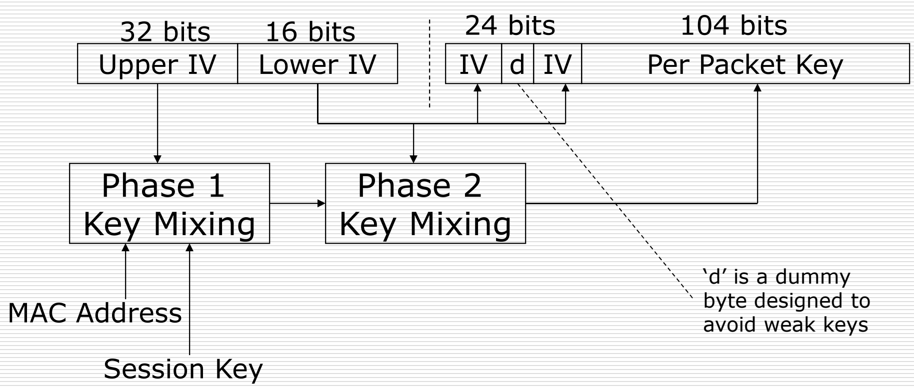
Michael Countermeasures

- Used to reliably detect attacks and shut down communication to the attacked station for a period of one minute
- This is done by disabling keys for a link as soon as the attack is detected
- Also has a blackout period of one minute before the keys are reestablished
- This can be used by the attacker to launch a DoS attack on the network (theoretically)

IV Selection and Use

- TKIP has the following major changes in the way IVs are used as compared to WEP
  - IV Size is increased from 24 to 48 bits
  - IV has a secondary role as a sequence counter to avoid replay attacks
  - IVs are constructed so as to avoid certain 'weak keys'
  - Instead of directly appending it with the secret key, IVs are used to generate mixed keys

IV Use in TKIP



Creating the RC4 Encryption Key

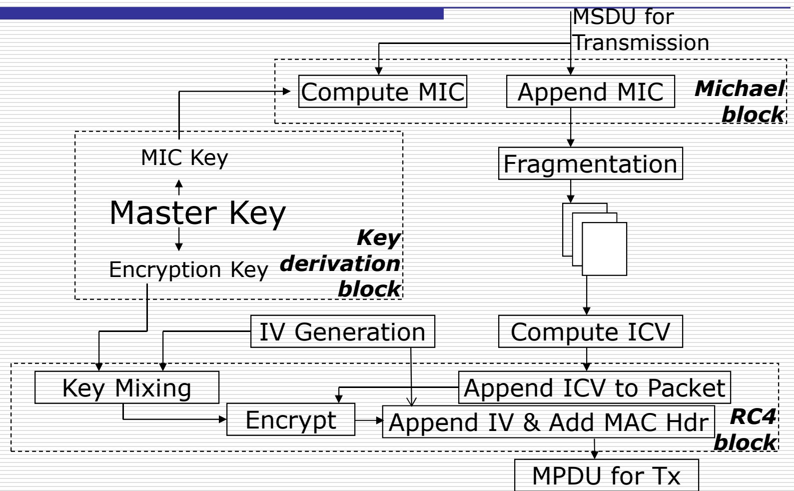
TSC (TKIP Sequence Counter)

- WEP has no protection against replay attacks
- In TKIP IV doubles up as a sequence counter to prevent replay attacks
- TKIP uses the concept of *replay window* to implement the counters
  - The receiver keeps track of the highest TSC and the last 16 TSC values
  - When a new frame arrives it checks and classifies it as one of the following types
    - ACCEPT: TSC is larger than the largest seen so far
    - REJECT: TSC is less than the value of the largest - 16
    - WINDOW: TSC is less than the largest, but more than the lower limit

Per–Packet Key Mixing

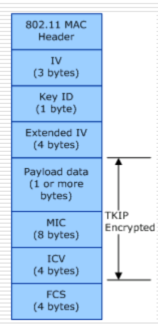
- Uses the session keys which are derived from the master keys
- Per Packet key mixing mechanism further derives a separate unrelated key for each packet from the session key
- To save computation key mixing is divided into two phases
  - Phase 1 involves data that is relatively static like secret session key, higher order 32 bits of IV, MAC address etc. so that this computation is done infrequently
  - Phase 2 is quicker to compute and is done for each packet – and used the lower 16 bits of the IV (which increases monotonically with each packet)

TKIP Role in Transmission

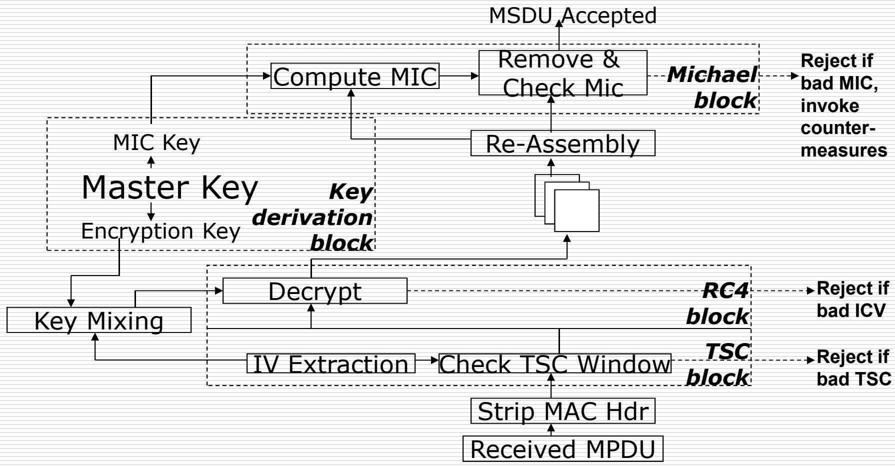


TKIP MPDU Frame

- Initialization Vector (IV)
- Key Identifier (ID)
- Extended IV
- Payload Data
  - MPDU data
- MIC
  - The MIC value is computed using the Michael algorithm over the entire payload data of the MSDU
- Integrity Check Value (ICV)
  - The checksum value computed over the unencrypted payload data
- Frame Check Sequence (FCS)
  - (CRC) computed over all fields of the MPDU



TKIP Role in Reception



References

- Jon Edney and William Arbaugh, Real 802.11 Security, Addison-Wesley, 2004