WIRELESS SECURITY CONT
Lecture 22

COMPSCI 726
Network Defence and Countermeasures

Nalin Asanka Gamagedara Arachchilage

Slides from Muhammad **Rizwan** Asghar

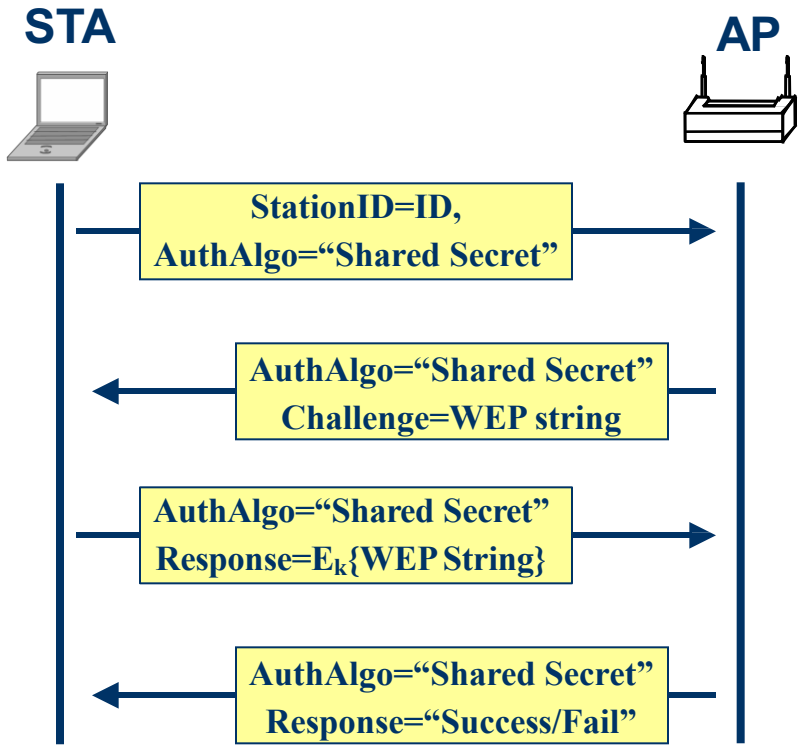
September 20, 2021

Source of some slides: **University of Twente** and **University of Trento**

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

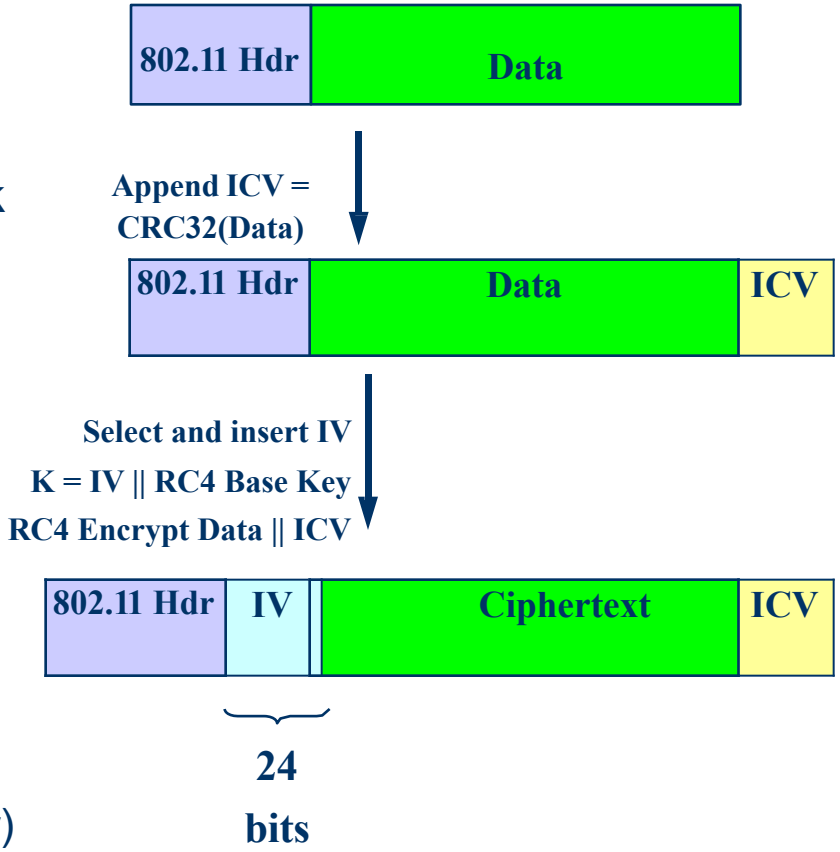
WEP AUTHENTICATION PROTOCOL

- STA proves knowledge of the pre-shared secret key K by encrypting the challenge
  - AP sends challenge to STA
  - STA encrypts challenge with RC4
  - Encrypted challenge is sent to AP
  - AP decrypts received message
  - AP compares decrypted challenge to the transmitted one

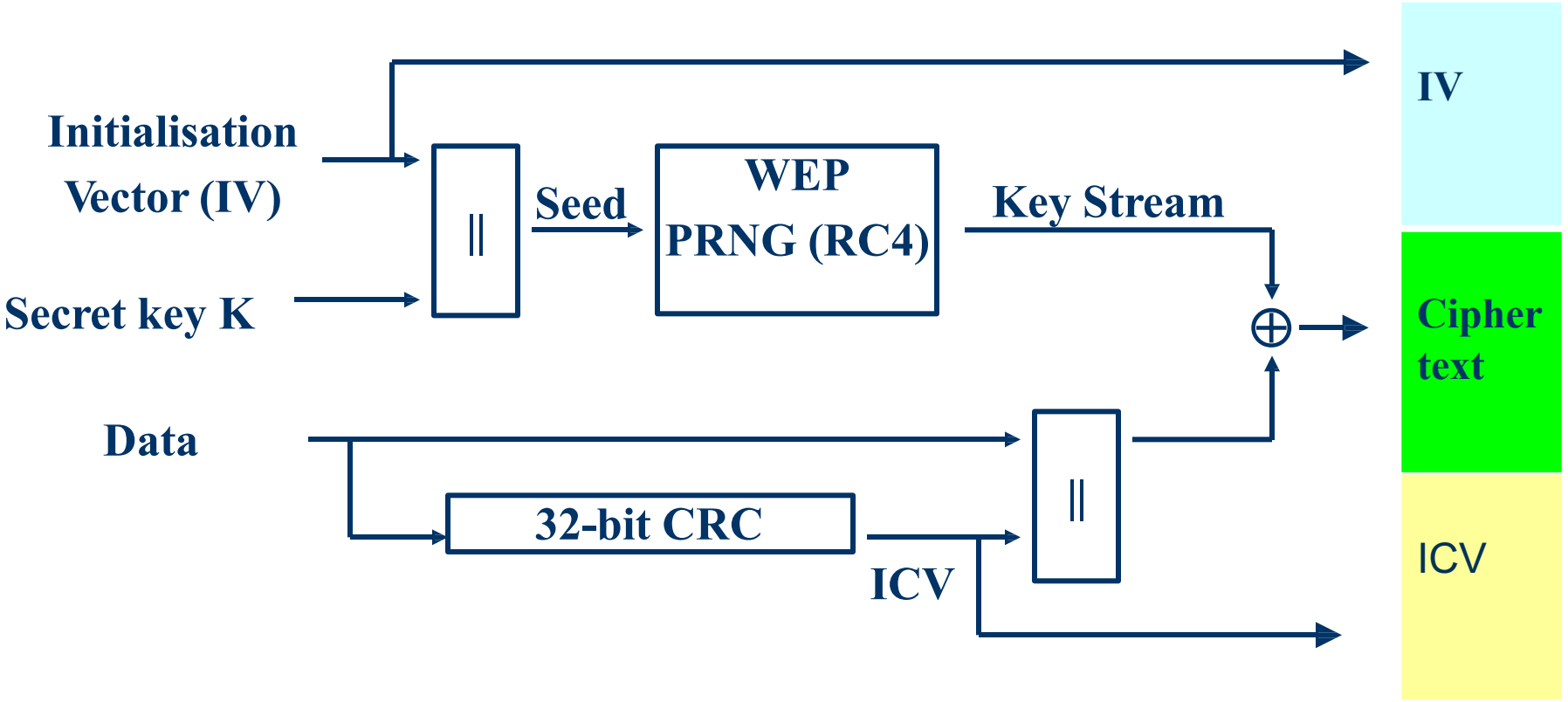


WEP SENDER

- Compute Integrity Check Vector (ICV)
  - Provides **integrity**
  - 32-bit Cyclic Redundancy Check (CRC)
  - CRC appended to message
- Data encrypted via RC4
  - Provides **confidentiality**
  - Data XORed with long key stream of pseudo random bits
  - Key stream is function of
    - 40 or 104-bit secret key
    - 24-bit IV (Initialisation vector)
- Ciphertext is transmitted

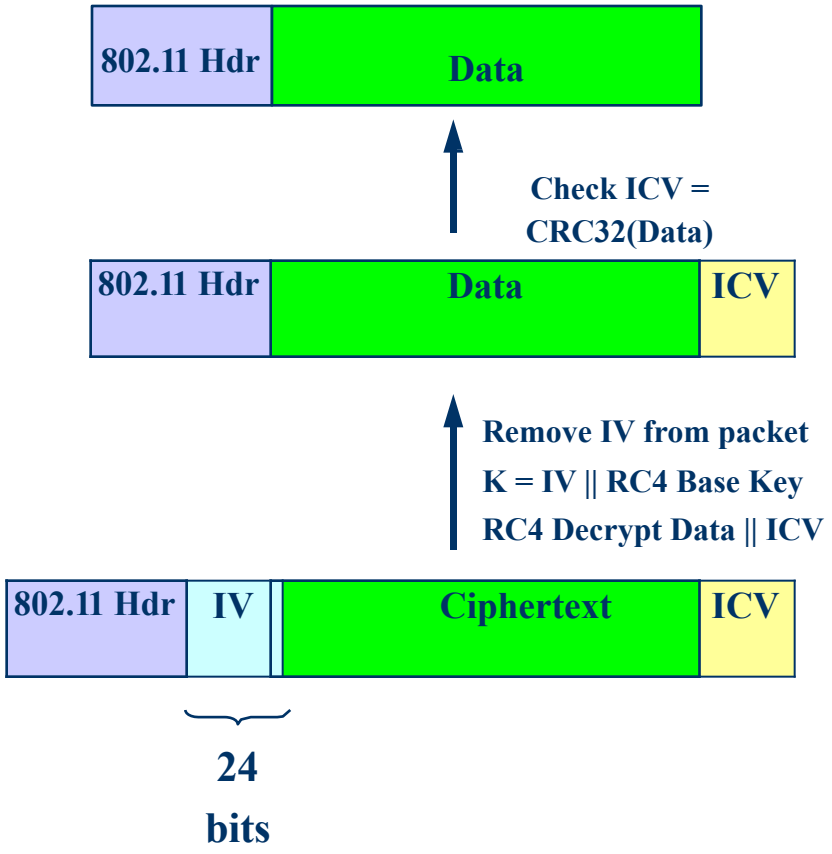


WEP ENCRYPTION



WEP RECEIVER

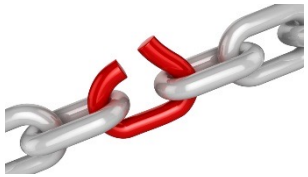
- Ciphertext is received
- Ciphertext decrypted via RC4
  - Ciphertext XORed with long key stream of pseudo random bits
  - Key stream is function of
    - 40 or 104-bit secret key
    - 24-bit IV
- Check ICV
  - Separate ICV from message
  - Compute ICV for message
  - Compare with received ICV



INITIALISATION VECTOR (IV)

- IV must be different for every message transmitted
- 802.11 standard does not specify how IV is calculated
  - It recommends to change IV for each packet
- Wireless cards use several methods
  - Some use a simple ascending counter for each message
  - Some switch between alternate ascending and descending counters
  - Some use a pseudo random IV generator

IV WEAKNESS



- WEP exposes part of PRNG input
  - IV is transmitted with message
  - IV is too small, only 24-bit
- Initial keystream can be derived
  - TCP/IP has fixed structure at start of packets
  - When two IVs collide, they generate the same keystream
- Passive attack

SAME KEYSTREAM

- Two plaintext p_1 and p_2 encrypted under the same "key stream" b:

$$c_1 = p_1 \oplus b$$
$$c_2 = p_2 \oplus b$$
$$c_1 \oplus c_2 = (p_1 \oplus b) \oplus (p_2 \oplus b) = p_1 \oplus p_2$$

- If p_1 is known, it is possible to know p_2
- If multiple messages have been codified with the same keystream, it is easier to obtain the original messages!

WEP ISSUES

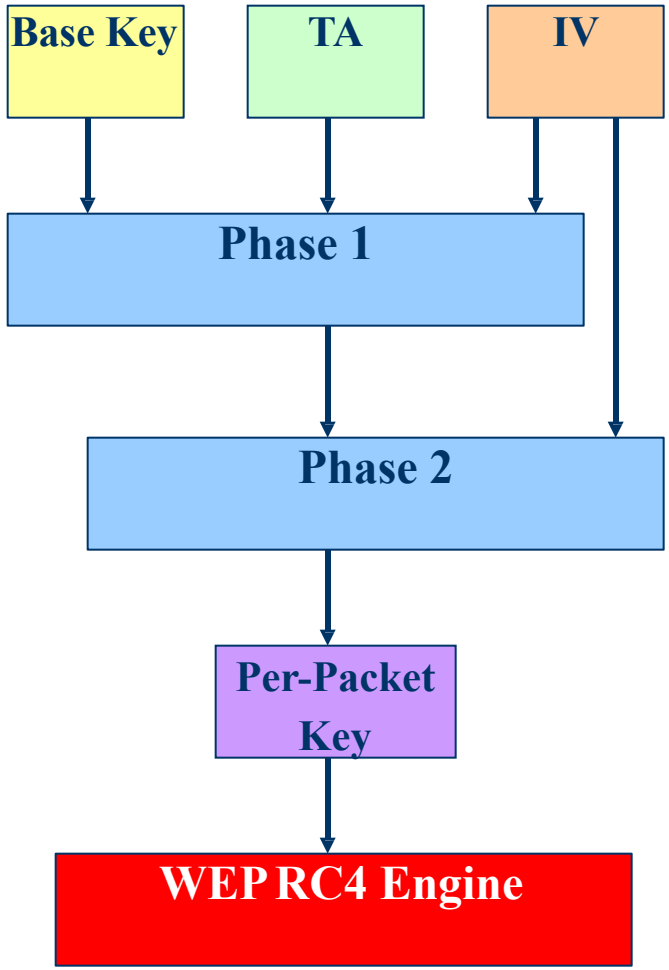
- Flawed design, easily broken
  - IV reuse causes problems
  - Tools to break WEP available on the Internet
  - Increasing key length does not help much
    - Linear complexity
- Offers very little security
- WEP vulnerabilities discovered, WEP broken!
  - Walker (Oct 2000), Borisov et al. (Jan 2001), Fluhrer-Mantin-Shamir (Aug 2001)

WIFI PROTECTED ACCESS (WPA)

- WPA fixes issues in WEP
- WPA uses Temporal Key Integrity Protocol (TKIP)
- TKIP was designed by the IEEE 802.11i task group
- TKIP is based on RC4 stream cipher algorithm
- An interim solution to replace WEP without requiring the replacement of legacy hardware

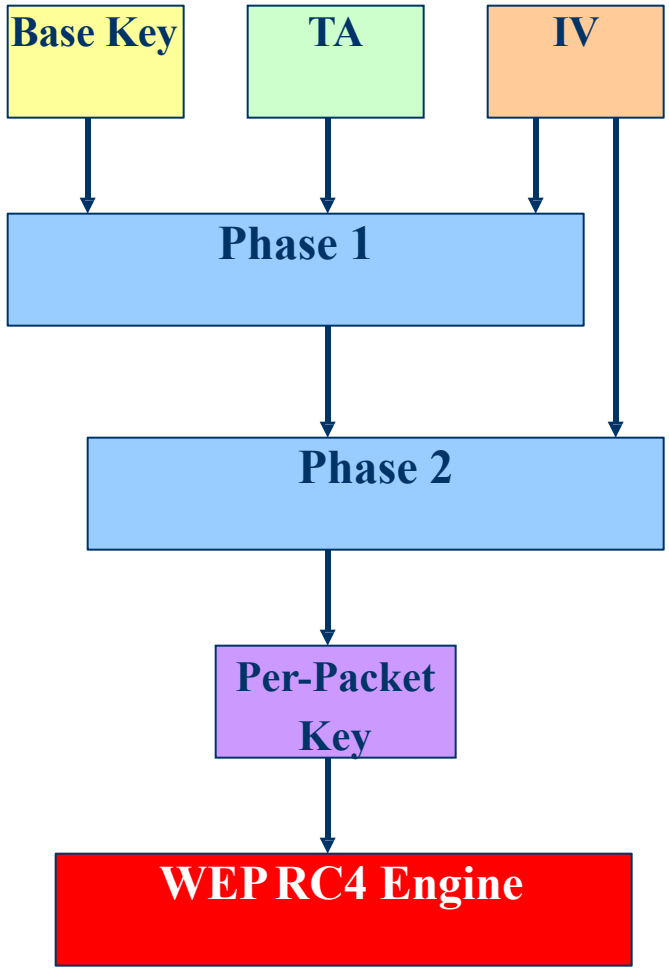
TKIP

- 128-bit base key
- Extended 48-bit Initialisation Vector (IV), which is never fed directly to RC4
- New per-packet key mixing function
- 48-bit Transmitter Address (TA) – keys derived for both directions will be different
- A Message Integrity Check (MIC) – “Michael”, ensures data integrity



TKIP PHASES

- Phase 1
  - Key mix 1 (128-bit base key, 48-bit TA and 48-bit IV)
  - 128-bit result
- Phase 2
  - Key mix 2 (phase 1 result and IV)
  - The result is 128-bit per-packet key
    - **Incrementing IV ensures unique key for each packet!**
  - Keystream = RC4(128-bit per-packet key)



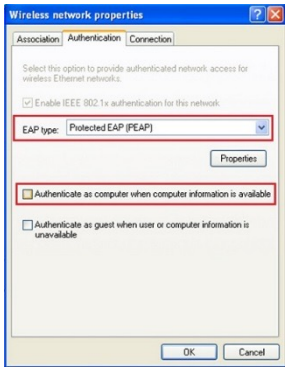
ABOUT WPA

- Per-packet key, a sequence counter and broadcast key rotation discourage many attacks
- The key mixing function also eliminates the WEP key recovery attacks
- TKIP is vulnerable to similar attacks as WEP
  - It uses the same underlying mechanism

WPA2

- WPA2 replaces WPA
- It supports CCMP (CCM Protocol)
  - CCM is a mode of operation for cryptographic block ciphers
    - CCM stands for Counter with CBC-MAC
    - Designed to provide both authentication and confidentiality
- CCMP is an AES-based encryption mode with stronger security
- Issue: WPA2 may not work with some older network cards

EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)



- EAP is an authentication framework used in wireless networks
- Defined in RFC 3748, updated by RFC 5247
- Used for generating keying material
- EAP supports many authentication mechanisms, e.g.,
  - EAP-PSK
  - EAP-MD5
  - EAP-TLS
  - EAP-IKE
  - …

AAA PROTOCOLS

- Authentication, authorisation and accounting processes are needed when user tries to access and use Internet
  - **Authentication:** Act of verifying identity of entity
  - **Authorisation:** Act of determining whether requesting entity is allowed access to a resource
  - **Accounting:** Act of collecting info on resource usage for the purpose of capacity planning, auditing, billing or cost allocation
- Example usage: AAA can be used in combination with IEEE 802.1x for WLAN authentication and authorisation
- AP can communicate with **AAA** servers including RADIUS (typically uses UDP) and DIAMETER (uses TCP or SCTP)
- Both RADIUS and DIAMETER **can encapsulate EAP** messages

WLAN SECURITY SUMMARY

Types	WEP	WPA	WPA2
Cipher Algorithm	RC4	RC4 (TKIP)	AES-CCMP
Encryption Key	40-bit	128-bit	128-bit
Initialisation Vector	24-bit	48-bit	48-bit
Authentication Key	None	64-bit	128-bit
Integrity Check	CRC-32	Michael	CCM
Key Distribution	Manual	802.1X (EAP)	802.1X (EAP)
Key Unique To	Network	Packet, Session	Packet, Session
Key Hierarchy	No	Derived from 802.1X	Derived from 802.1X
Ad-hoc Security	No	No	Yes (IBSS)

GENERAL COUNTERMEASURES

- Use WPA2
- Block your SSID from being broadcasted
- Change the default access point password
- Place the access point in the middle of the building/house

RESOURCES

- Read Chapter 6 of
  Network Security Essentials – Applications and Standards
  Fourth Edition
  William Stallings
  Prentice Hall
  ISBN 0-13-706792-5

- **An Overview of 802.11 Wireless Network Security Standards & Mechanisms**, https://www.sans.org/reading-room/whitepapers/wireless/overview-80211-wireless-network-security-standards-mechanisms-1530

Questions?

Thanks for your attention!