



802.11 Wireless LAN Security

Case study in Design Errors

(from *SECURE CODING*, by M.G. Graff & K.R. van Wyk, O'Reilly)



Background

- 802.11 popular (standard of) suite of protocols for wireless LAN
- One of early security requirements: provide security equivalent to wired LAN
- WEP: Wired Equivalence Protocol authentication and encryption mechanisms
 - Data Privacy: prevent eavesdropping
 - Data Integrity: ensure correct data
 - User Authentication: restrict accessibility

2



Background (cont.)

- WEP has no standard key management
- Each entity in the wireless LAN has 4 static WEP keys, with KeyIDs 0,1,2,3, shared by an AP and all stations accessing it
- Designed by committee that did not include cryptographers
- NOT successful for several reasons, one 'operational' and four 'cryptographic'

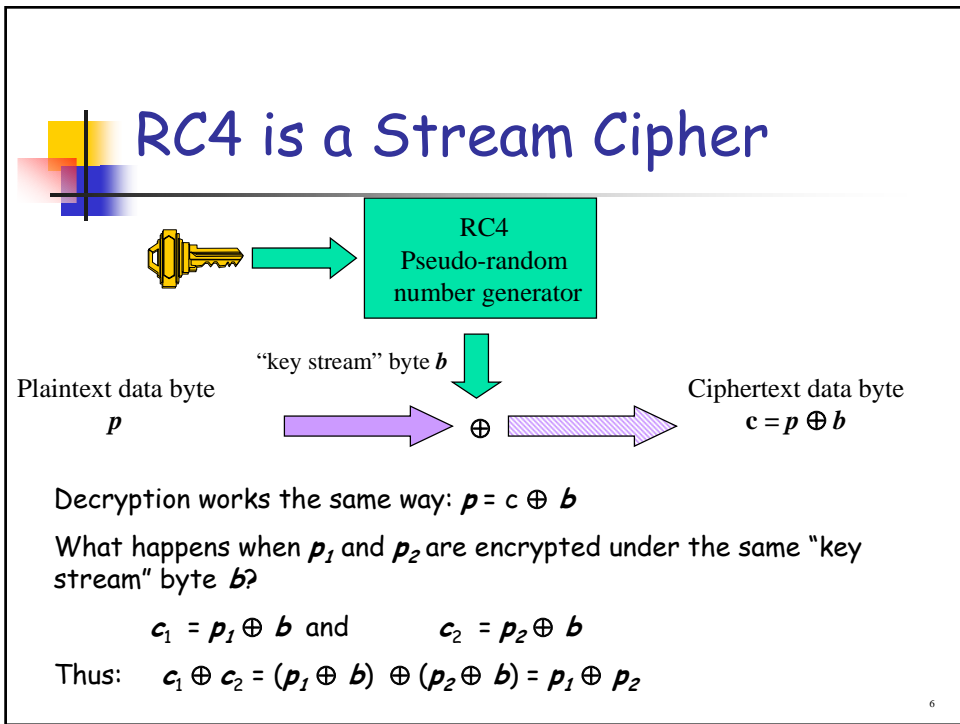
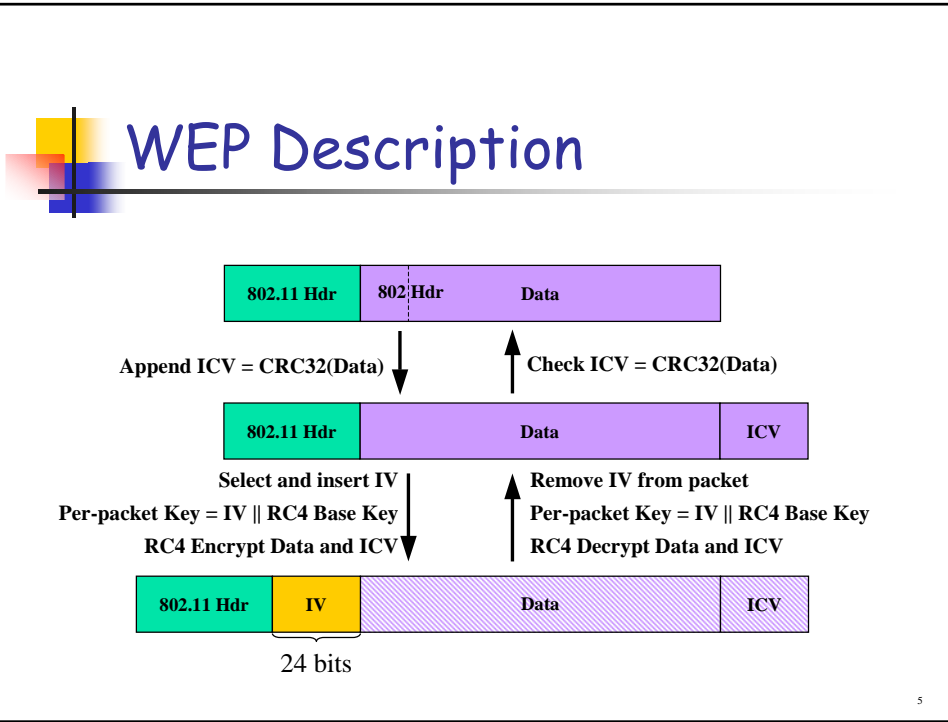
3



Reason 1

- WEP was specified to be optional, and manufacturers could ship Access Points with WEP turned OFF by default
- Majority of users never turned ON the WEP option
 - Laziness ?
 - Fear of unknown ?

4

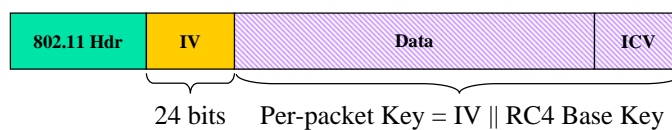


Other four reasons

- Solutions must address all four problems, otherwise attack tools can be developed to exploit the remaining holes
- Need to address *all* of the problems
 - IV Collisions
 - Weak Keys
 - Message Forgery
 - Replay (Defeated by using the IV as a sequence number: receiver discards packets associated with same key and IV value less than previously received packet)

7

IV Collisions



- WEP expands the RC4 Base Key into 2^{24} per-packet keys
- Data can be recovered if IV is ever repeated with same per-packet key
- There are only 2^{24} different IVs
- Probability of two packets sharing the same IV is $> 50\%$ after 4823 packets (!)
- RC4 key *must* be changed at least every 2^{24} packets, otherwise data is exposed when the same IV is used for a second packet
- (To defeat it, expand IV)

8

Weak Key Attacks



Per-packet key = IV || RC4 Base Key, so the first three bytes of the Per-packet Key are always exposed!

- Some RC4 weak keys exist, where patterns in the first three bytes of the key causes a corresponding pattern in first few bytes of the key stream
- The IV identifies the use of potential weak keys
- Known plaintext allows direct computation of start of the key stream, exposing some of the secret RC4 Base Key value
- Iterate over a sequence of packets with different IVs until all the bits in the RC4 base key are found
- (Defeated by computing key from BaseKey + 48-IV + 48-TA)

9

Forgery Attacks

Sample Attack - Attacker has accomplice on the wired network:

1. Recv-Addr, Src-Addr, Dest-Addr are unprotected
2. Record any packet, replace the Dest-Addr with accomplice's address; resend it
3. AP will decrypt data and send it to the accomplice

Also :

The integrity check is a simple CRC-32 checksum, not cryptographically strong (detects simple random bit errors). Individual bits in the encrypted body can be changed without affecting the checksum

$$\text{CRC}(\text{XOR}(A,B)) = \text{XOR}(\text{CRC}(A), \text{CRC}(B))$$

10