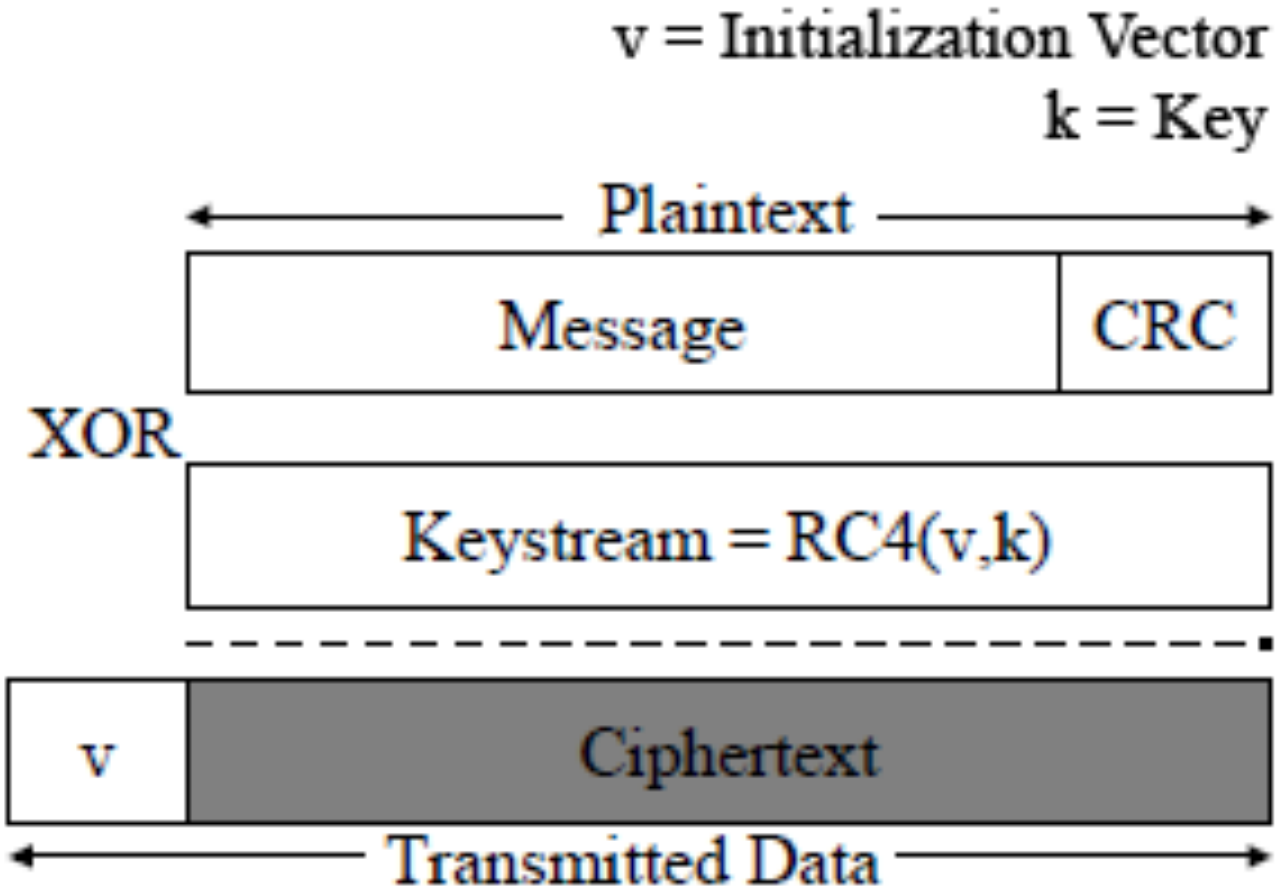
CIS 700/002 : Special Topics : WEP & WPA Attacks

Dagaen Golomb
CIS 700/002: Security of EMBS/CPS/IoT
Department of Computer and Information Science
School of Engineering and Applied Science
University of Pennsylvania

10 February 2017

Wired Equivalent Privacy (WEP)

Lets get this out of the way: DON'T USE IT



The Beginning: FMS Attack

- 2001
- Discovery of a correlation between earlier parts of the key on later parts of the key
- First few bytes (3) are easy to obtain since IV is transmitted plain-text and packet headers are predictable
- Start here and work on next byte of key successively

The Beginning: FMS Attack

$$S_l[1] < l$$

$$S_l[1] + S_l[S_l[1]] = l$$

$$S_l^{-1}[X[0]] \neq 1$$

$$S_l^{-1}[X[0]] \neq S_l[1]$$

$$K = S_l^{-1}[X[0]] - j_l - S_l[l] = S_l^{-1}[S_{l+1}[l]] - j_l - S_l[l]$$

Improvement: KoreK Attack

- 2004
- KoreK is the name of a user on a forum who presented 16 additional correlations similar to the FMS attack
- Using the same approach but with all of these correlations, the number of required packets decreases

Further Improvement: PTW Attack

- Previous correlations required several bytes to have a special relationship, and often not change in successive iterations
- PTW attack presented the first correlation that holds for all packets, with no special preconditions.
  - Even if not as individually predictive, the other attacks only apply to a small number of packets
  - Using all packets allows for fewer packets to decrypt key

Cipher/Design Exploit: Chopchop Attack

- This attack relies on the weak CRC checksum and the specified behavior in the WEP standard
- Decrypt last m bytes of a packet with m*128 packets injected into network
- Does not reveal key! Simply decrypts a packet without the key due to cipher/ standard weaknesses

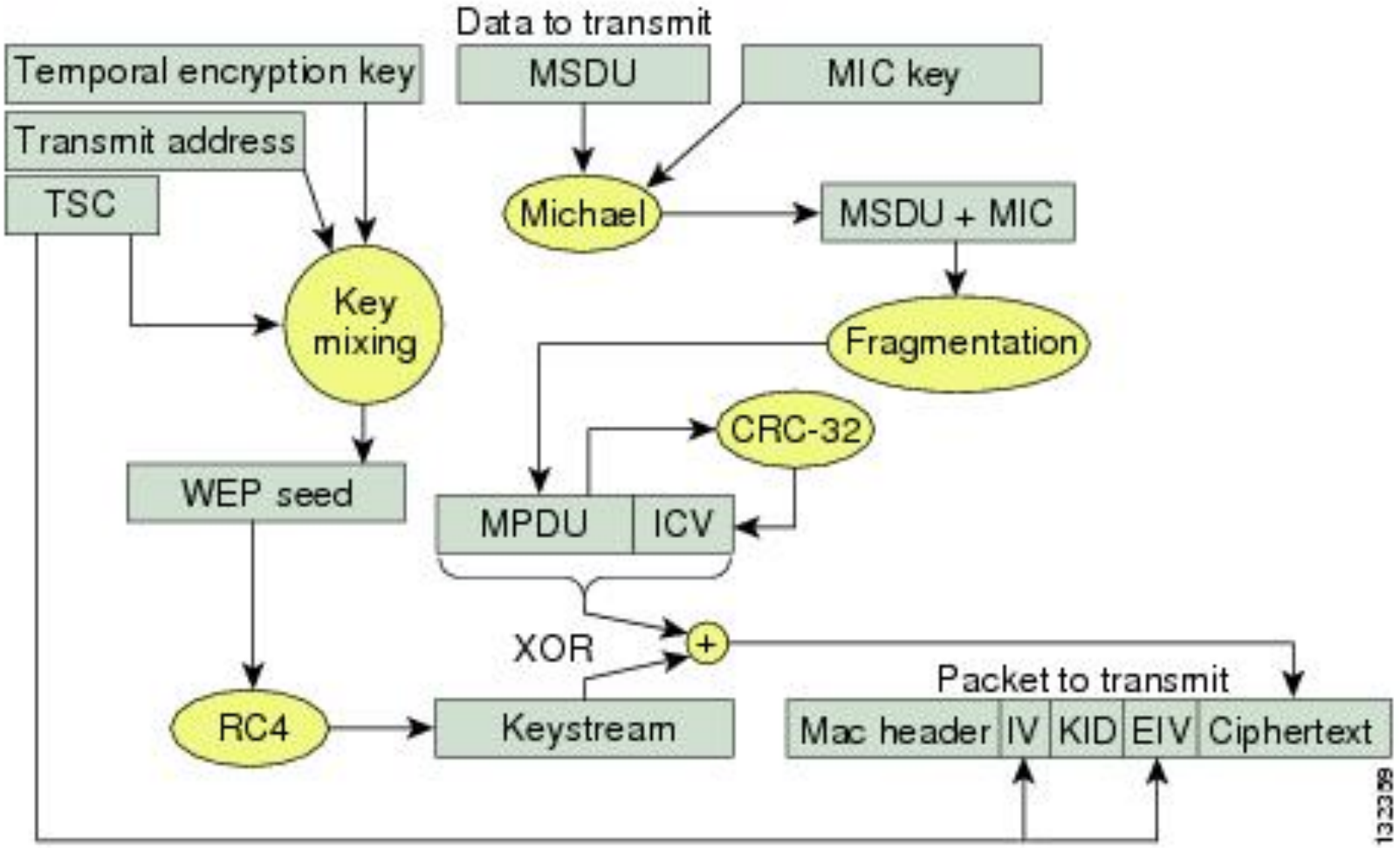
Presented Improvement

- Authors were able to rewrite KoreK correlations into the same general [summation-type] correlation used in PTW
  - With a few exceptions
- They then perform a PTW-like attack using these added correlations

WPA-TKIP

- Intended to be firmware-upgradable by WEP hardware, so uses a similar RC4 based scheme
- Adds some additional protections
  - Better MIC instead of attackable CRC32 checksum
  - Sequence number (TSC) prevents replay attacks
  - Hashing function is more complicated (every byte depends on entire key instead of XOR byte-by-byte dependence which allowed for the WEP correlation attacks

WPA-TKIP


Data to transmit
Temporal encryption key
MSDU
MIC key
Transmit address
TSC
Michael
MSDU + MIC
Key mixing
Fragmentation
CRC-32
WEP seed
MPDU
ICV
XOR
+
Packet to transmit
RC4
Keystream
Mac header
IV
KID
EIV
Ciphertext
132389

First WPA Exploit

- Uses same idea as WEP chopchop attack
- TKIP has some attack mitigations
  - Correct packets increment TSC counter and correct packets with lower-than-current TSC are discarded
  - Incorrect ICV → packet discarded
  - Correct ICV but incorrect MIC → client issues MIC failure frame to inform AP. 2 such packets within 60 seconds shuts down AP for 60 seconds and keys are renegotiated

Countermeasures

- WEP – Don't use it!
  - WPA-TKIP is designed specifically to be compatible with WEP hardware with firmware upgrade
- WPA
  - Use CCMP (or WPA2) instead of TKIP
  - If TKIP must be used, use short key renewal times (120 seconds or less)
  - Disable MIC failure report from clients