Wireless Security

7. Csapat

Ferencz ALBERT
László FÜLEKI
Attila PÉTER
Zsolt SIMON

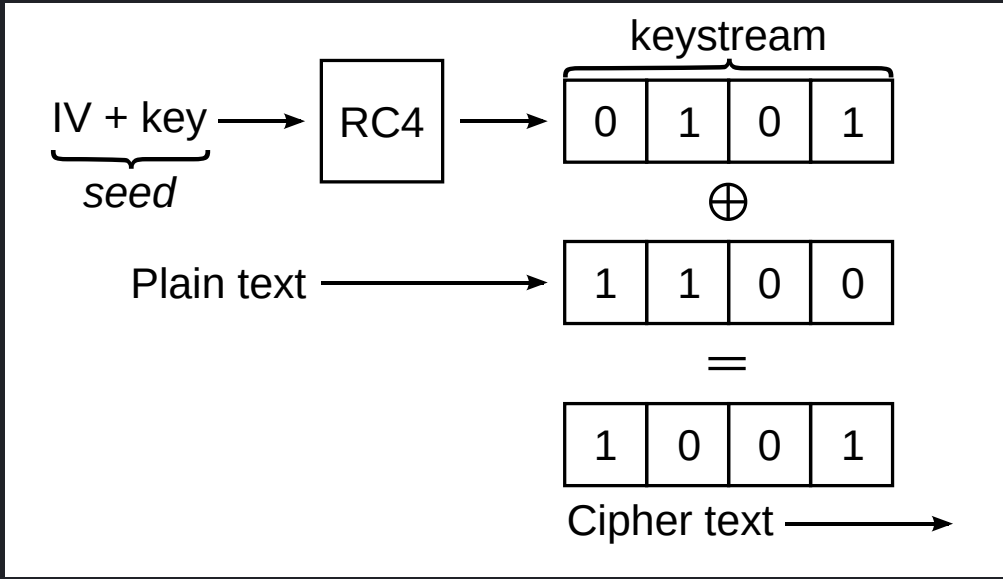
WEP - Wired Equivalent Privacy

1. Security algorithm for IEEE 802.11 wireless networks
2. Was ratified as a security standard in 1999
3. First versions were not particularly strong, the US limited manufacturers to a 64-bit key

WEP - Wired Equivalent Privacy

Encryption Details

1. Stream Cipher RC4 for confidentiality
2. CRC-32 for integrity



RC4 streamcipher and WEP Demo

WEP - Wired Equivalent Privacy

Problems

1. CRC-32 is linear, which means that it is possible to compute the bit difference of two CRCs based on the bit difference of the messages over which they are taken.
2. Initially 64-bit WEP keys, then 128-bit WEP keys
    - IV 24 bits, small space, overlaps fast: 2^24 possible IVs
    - with an average pps of 97.6 (me watching YT) it takes 1 day, 22:36:12 to exhaust the IVs
    - with an average pps of 1000 (hypothetical, while gaming) it takes 4:39:37.21 to exhaust the IVs

WEP - Wired Equivalent Privacy

Attacks

1. Passive Attack to Decrypt Traffic: intercept data, look for overlaps, create statistics
2. Active Attack to Inject Traffic: modify the content of a packet with a know plaintext to inject data into the access point
3. Active Attack from Both Ends: modify packet header, not content, redirect to port, route to victim
4. Aircrack-ng: PTW, FMS/KoreK method
5. Aircrack-ng: Caffe Latte Attack: sending forged ARP messages, generating ARP responses, cracking a 128-bit WEP key in 6 minutes (source)

WEP - Wired Equivalent Privacy

Remedies

1. 802.11i (WPA and WPA2)
2. Implemented non-standard fixes:
    - WEP2: extended both the IV and the key values to 128 bits
    - WEPplus/WEP+: enhances WEP security by avoiding "weak IVs"
    - Dynamic WEP: combination of 802.1x technology and the Extensible Authentication Protocol

WPA - Wi-Fi Protected Access

WPA I

- Remedies WEP by using TKIP
- Was created to quickly work around the problems of WEP
- Introduces WPA-Enterprise which uses 802.1X/EAP with a RADIUS server to authenticate clients

TKIP

- Was designed to run on WEP hardware, intentionally as a transition, or stopgap, protocol
- Is a preprocessing step before WEP encryption
- RC4 is still the encryption algorithm, and the WEP CRC-32 could not be eliminated
- Adds features into the selection of the per-frame key, and introduces a new MIC to sit beside the CRC-32 and provide better integrity

WPA - Wi-Fi Protected Access

WPA & TKIP - Changes

- IV is expanded to `6 bytes = 48 bits = 2^48` space, much larger, less overlaps
- IV is now a `sequence counter`
- A per connection key is used which is negotiated at the beggining of a new connection `PTK = Pairwise Temporal Key` using the four-way handshake over cleartext communication:
  - **AP -> C**: AP sends the security settings (RSN IE) and a nonce (randomly generated)
  - **C -> AP**: C sends its own security settings and the nonce generated by it, also creating the PTK, by mixing the two nonces, the address of the client and AP and the PMK (`PMK = Pairwise Master Key` , eg, the password chosen by the user). The client signs the message with a MIC
  - **AP -> C**: Same message as the first, but signed with the MIC by the AP
  - **C -> AP**: Response to Message 4
- TSC is used (updated on message count basis)
- MIC is used
- Detecting an ongoing attack

WPA - Wi-Fi Protected Access

WPA & TKIP - Problems & Attacks

- Weak password: brute force of four-way handshake
- Lack of forward secrecy
- If the attacker is on the network, it is possible to forge packets
- WPS PIN recovery

WPA - Wi-Fi Protected Access

WPA2

- Introduces a new encryption algorithm - AES - Advanced Encryption Standard
- AES: a non-linear block cypher
- Uses Counter mode
- MIC is also updated
- (CCMP) Counter Mode with Cipher Block Chaining Message Authentication Code replaces TKIP

WPA - Wi-Fi Protected Access

WPA2 - AES

- Computerphile - AES Explained
  - Uses 128-, 192- 256-bit keys
  - Key expansion
  - Plaintext data is chunked into `4byte x 4byte` matrices
  - Finite fields
  - Substitute:
    1. SubBytes - no fixed points
  - Permutate:
    1. ShiftRows - rotate right in row by value
    2. MixCols - multiply columns with predefined 4x4 matrices
  - Add round key
  - Perform above process multiple rounds, depending on keylength
  - There are AES insturctions in the CPU

WPA - Wi-Fi Protected Access

WPA2 - Attacks

- Computerphile - Krack Attacks
  - Man in the middle
  - Attacks the four-way handshake by exploiting message 3 and 4
  - Man in the middle causes the loss of message 4
  - Nonce is reset, same message with different encrypted data is sent twice

Bluetooth

- Managed by the Bluetooth Special Interest Group (Bluetooth SIG)
- Initially there were two implementations Bluetooth Low Energy and Bluetooth Classic
- Bluetooth 4.0 combines the two, and LE Privacy is born
- Bluetooth is using a protocol stack
- L4 is L2CAP (Logical Link Control and Adaptation Protocol)
- L5 is SMP (Security Manager Protocol)
    1. Pairing
    2. Encryption
    3. Signing

Bluetooth

Bluetooth Security Modes

- Security Levels
  1. Security Level 1 - communication w/o any security
  2. Security Level 2 - AES-CMAC for communication between unpaired devices
  3. Security Level 3 - Support encryption, paring is needed
  4. Security Level 4 - Everything above + ECDHE of AES-CMAC
- Security Modes
  1. Security Mode 1 - no data signing
  2. Security Mode 2 - all data is signed
  3. Mixed Security Mode - includes both above
- Mixing is possible
  - Secure Connection Only Mode - SM1 + SL4

Bluetooth

Attacks

- BlueSmack attack
  1. DOS Attack
  2. L2PING to calculate RTT
  3. Transfers an oversized packet over the L2CAP layer
- BlueJacking
  1. Sending unsolicited contacts over bluetooth
- Bluesnarfing Attack
  1. Only works when the device is discoverable
  2. Exploits the OBEX protocol
  3. Permits copy of data
- Bluebugging Attack
  1. Only works after pairing
  2. Permits installing a backdoor