

WEP Case Study

Information Assurance

Fall 2006

802.11 or Wi-Fi

- IEEE standard for wireless communication
 - Operates at the physical/data link layer
 - Operates at the 2.4 or 5 GHz radio bands
- Wireless Access Point is the radio base station
 - The access point acts as a gateway to a wired network e.g., ethernet
- Laptop with wireless card uses 802.11 to communicate with the Access Point

External Security Mechanisms

- MAC restrictions at the access point
 - Protects servers from unexpected clients
 - Unacceptable in a dynamic environment
 - No identity integrity. You can reprogram your card to pose as an “accepted” MAC.
- IPSec
 - To access point or some IPSec gateway beyond
 - Protects clients from wireless sniffers
 - Used by UIUC wireless networks

Wired Equivalent Privacy (WEP)

- Excellent example of how security system design can go wrong.
 - Flaws widely published in late 2000
 - Unsafe at Any Key Size. Tech. Rep. 00/362
<http://grouper.ieee.org/groups/802/11/Documents/Docu>
 - (In)Security of the WEP algorithm.
<http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>
 - Intercepting Mobile Communications: The Insec
- Took secure elements and put them together poorly

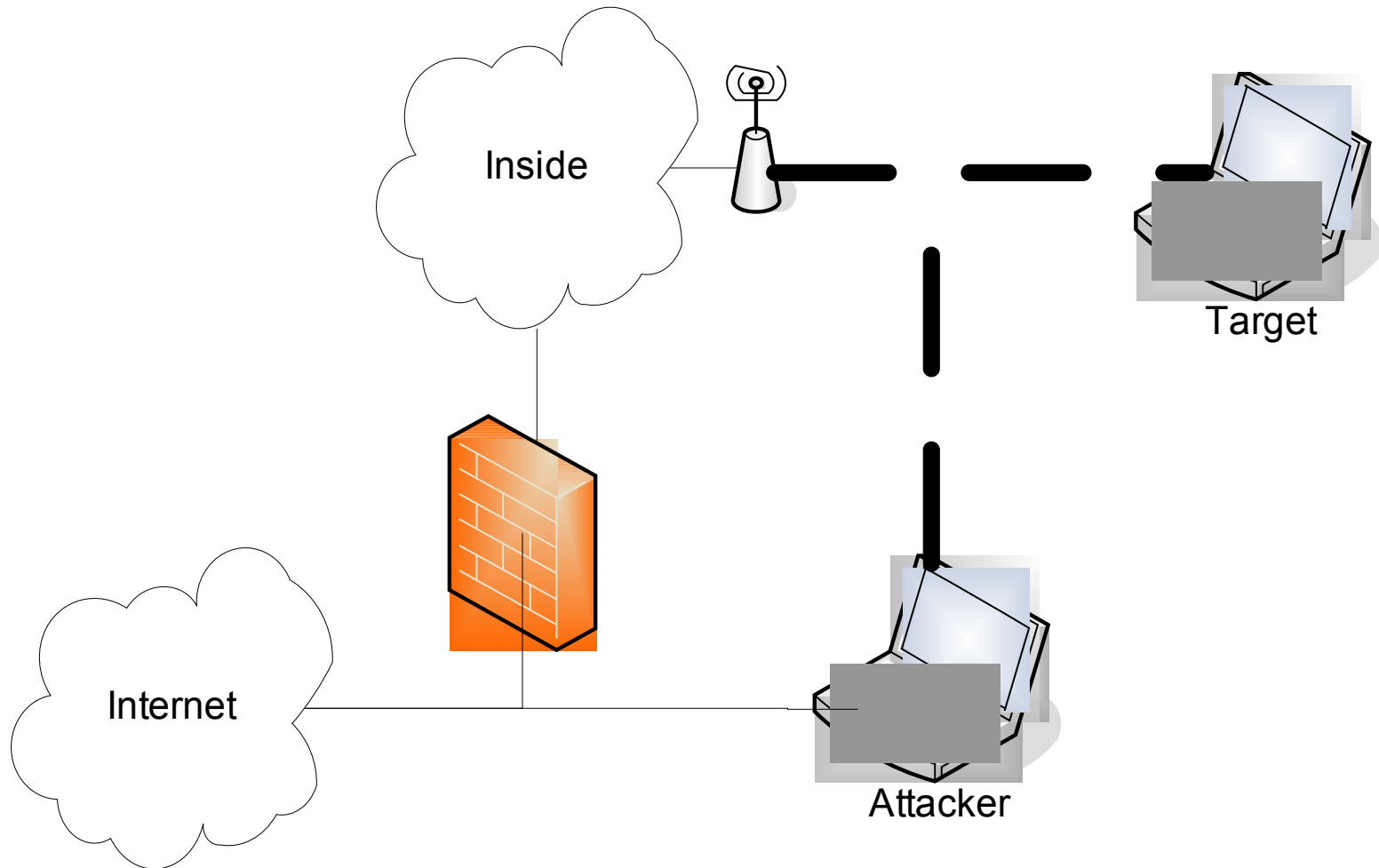
RC4 Stream Cipher

- Takes a key value as input and generates a key stream
 - Key stream is XOR'ed with plaintext to create ciphertext
 - $ci = pi \oplus ki$, for $i = 1, 2, 3$
 - Ciphertext is XOR'ed with key stream to create plaintext,
 - $pi = ci \oplus ki$, for $i = 1, 2, 3$
- Knowing two of key stream, plaintext, and ciphertext lets you easily compute the third
 - Reusing a key value is a really, really bad idea. A well known fact for RC4

Problems reusing a key

- Assume you know two ciphers use the same key
 - $C1 = P1 \text{ xor } K$
 - $C2 = P2 \text{ xor } K$
 - $C1 \text{ xor } C2 = P1 \text{ xor } P2 \text{ xor } K \text{ xor } K = P1 \text{ xor } P2$
- If you have more Cx using K , get more variations of XOR plaintexts

Key Use Attack Architecture



Key Reuse Active Attacks

- Insert known plaintext
 - Send email (probably forged or anonymized) to someone on the access point and sniff the stream
 - Knowing both plain and ciphertext getting the key stream for that key is just an XOR
- Sniff both the wireless stream and the wire after the access point
 - Correlate the two streams to get plain and ciphertext pairs

Key Reuse Passive Attacks

- Many packets contain well known fields at well known locations
 - E.g. IP header fields
 - Use knowledge about IP headers to get partial key recovery for all packets
- Analyze the plaintext xor's directly
 - Knowing how plaintext streams differ can help in the analysis
 - Use natural language facts to determine the likely plain text

WEP's Key Reuse

- RC4 40 bit seed is created by concatenating a shared secret with a 24 bit initialization vector (IV)
 - Frames can be lost and stream ciphers do not deal with missing bits, so the stream must be reset with each packet.
 - Therefore, a new IV is sent in the clear with each packet
- A family of 2^{24} keys for each shared secret
- Keys are cycled for each packet

WEP's Key Reuse

- IV is only 24 bits, the time to repeat IV's (and thus keys) with high probability is very short
 - By birthday paradox, 50% probability of getting some IV reuse after using 4,096 IV's.
 - 99% likely that you get IV re-use after 12,430 frames or 1 or 2 seconds of operation at 11 Mbps.
- Build table of cipher text keyed by IV

No Rekeying

- One key used between an Access Point and all clients
- WEP defines no automatic means of updating the shared key
 - In practice folks do not frequently update WEP keys
 - Ideally should be changing shared key after 6 frames to keep low probability of IV collision (99.999% probability of no IV reuse)

RC4 Weak Keys

- RC4 has weak keys
 - Use of weak keys greatly aid crypto analysis
 - 1 of 256 keys are weak
 - There are standard techniques to avoid the weak keys but WEP does not employ these techniques.
- Aircrack-ng and wepcrack tools leverage weak keys
 - Weakness in the Key Scheduling Algorithm of RC4
http://www.drizzle.com/%7Eaboba/IEEE/rc4_ksaproc.p

WEP CRC Problems

- We encrypt the CRC, so it is secure, right?
- Wrong. CRC is linear
 - Flipping bits in the ciphertext can be fixed up in the CRC even if the CRC is RC4 encrypted
- This means that an attacker can change the cipher text and fix up the CRC
 - $CRC1 \text{ xor } \Delta = CRC2$
 - $C = CRC1 \text{ xor } K$
 - $C \text{ xor } \Delta = C'$

SSL uses RC4 Safely

- Over a reliable data stream so the 128 bit key does not need to be reset with each packet
- Would need to capture 2^{64} streams rather than 2^{12} streams to get key reuse with 50% probability
- New keys potentially change all bits not just the bottom 24 bits.
- Rekeying algorithm
- Uses strong crypto hash for MAC
 - HMAC-SHA and HMAC-MD5

IPSec Secures Over Unreliable Protocol

- Uses separate keys in each direction
- Uses 64 bit (for 3DES) or 128 bit (for AES) IV's
- Uses the IV as a salt not as part of the key
- Forces a rekey after at most 2^{32} packets
- Uses strong crypto hash for MAC
 - HMAC-SHA and HMAC-MD5

802.11i

- IEEE effort to improve security of the 802.11 spec
 - Using 802.1X for authentication
 - 802.1X is a general L2 protocol
- Wi-Fi Alliance promoting interim standards
 - WPA, a shorter term solution that uses existing hardware
 - WPA2, an implementation of the full 802.11i standard

Wi-Fi Protected Access (WPA)

- Interim solution to run on existing wireless hardware
- Uses Temporal Key Integrity Protocol (TKIP) for data encryption and confidentiality
 - Still uses RC4, 128 bits for encryption
 - Provisions for changing base keys
 - Avoids weak keys
- Includes Michael a Message Integrity Code (MIC)
 - 64 bits
 - Replaces the CRC
 - Observer cannot create new MIC to mask changes to data
- Increases IV from 24 bits to 48
- Mixes the IV and the base key

WPA2

- Uses AES, specifically Counter-Mode/CBC-MAC Protocol (CCMP)
 - Too computationally intensive in SW for wireless hardware deployed at the time of WEP
- Uses 128 bit key
- Provides data confidentiality by using AES in counter mode
- Provides message authentication using Cipher Block Chaining Message Authentication Code (CBC-MAC)
 - The MAC also covers the packet source and destination

802.11i Summary

| | <u>WEP</u> | <u>TKIP</u> | <u>CCMP</u> |
|-------------------|-----------------|--|-------------|
| <i>Cipher</i> | RC4 | RC4 | AES |
| <i>Key Size</i> | 40 or 104 bits | 128 bits encryption, 64 bit auth | 128 bits |
| <i>Key Life</i> | 24-bit IV, wrap | 48-bit IV | 48-bit IV |
| <i>Packet Key</i> | Concat. | Mixing Fnc | Not Needed |
| <i>Integrity</i> | | | |
| <i>Data</i> | CRC-32 | Michael | CCM |
| <i>Header</i> | None | Michael | CCM |
| <i>Replay</i> | None | Use IV | Use IV |
| <i>Key Mgmt.</i> | None | EAP-based | EAP-based |