MERIT 2004

AN EXAMINATION OF SECURITY ALGORITHM FLAWS IN WIRELESS NETWORKS

Erica Simcoe, Hirsh Goldberg, Mehmet Ucal

Introduction

- Most common standard in wireless devices today is IEEE 802.11b
- Utilizes the Wired Equivalent Privacy (WEP) protocol
  - Data packets encrypted using RC4 algorithm
  - Implementation is critically flawed
  - Vulnerable to a variety of attacks
  - Three main kinds of security (data authentication, confidentiality, and integrity) are compromised.

RC4 Algorithm

Characteristics of RC4 Cipher

Symmetric- Same key is used in encryption and decryption.

Synchronous- Key stream is generated separately from the plaintext

Stream- Data is encrypted one byte at a time

Key Scheduling Algorithm (KSA)- Generates a random 256-value state array S, based on the secret key, K (length *l*)

Pseudo Random Generation Algorithm (PRGA)- Outputs a streaming key based on the KSA array S

```
KSA(K)
Initialization
    For i=0…255
        S[i]=i
        j=0
Scrambling
    For i=0…255
        j=j+S[i]+K[i mod l]
        Swap(S[i], S[j])
```

```
PRGA(K)
Initialization
    For i=0
        j=0
Generation Loop
    For i=i+1
        j=j+S[i]
        Swap(S[i], S[j])
        Output z= S[S[i]+S[j]]
```

Figure 1 - RC4 Algorithm

WEP Algorithm

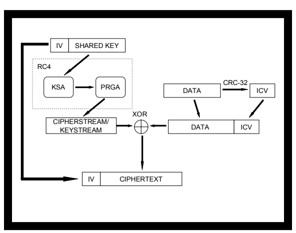

Figure 2 - WEP Encryption

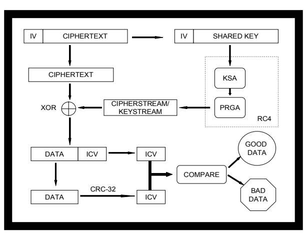

Figure 3 - WEP Decryption

Problems with WEP

- No key management protocol in WEP
  - IV incrementation unregulated
  - Manually entered shared key

Weak IVs

- Weak IVs have the form (B+3, 255, X), where B is the index of the shared key byte and X can be any number.
- Knowing plaintext before it is encrypted allows people to exploit the weak IVs and gain knowledge of the shared key. The SNAP encapsulation header 0xAA is widely known and is almost always the first plaintext byte encrypted.
- There are 9000 known weak IVs and 2000-3000 are needed to crack a 104-bit shared key, which takes a minimum of ~1 million packets.

IV Reuse

- Collisions occur when an IV is used more than once and so the same RC4 key stream is used to encrypt the data.
- IVs are only 24 bits, or 3 bytes long, so there are only 2^{24} unique IVs.
- This seemingly large space can be depleted quickly. On average reuse occurs after ~5 hours.

Simulation Results

This experiment involved the simulation of a wireless network, mysterynet, using an AP and laptop. Traffic was created by ping-flooding the AP. Another unrelated laptop sniffed the traffic and ran it through AirSnort, collecting enough interesting packets to crack WEP. The numerical results are shown below. Cracking a real network would take longer depending on the amount of traffic on the WLAN.

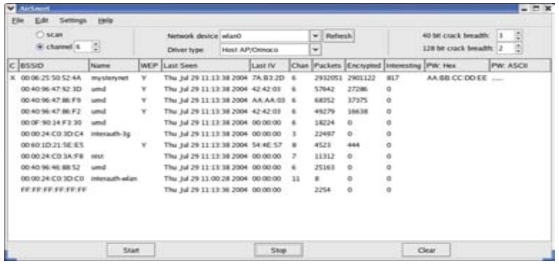

Figure 4 - Successful WEP crack

Simulation Results

- SSID- mysternet
- Encryption- 40-bit WEP
- Key- AA:BB:CC:DD:EE
- Interesting IVs needed- ~800
- Elapsed Time- 2 hours
- Total Packets- ~2 million

Security Solutions

Possible Improvements to WEP

- Hash IV and shared key combination before sending through RC4
- Discard first 256 outputs of RC4 algorithm to reduce correlation between input and output
- Use longer IV

Patches/Upgrades for WEP

- 802.1X
  - Mutual authentication accomplished through a server on network, behind the access point
  - Provides dynamically varying encryption keys
- Temporary Key Integrity Protocol (TKIP)
  - Uses longer IV – reduces IV repetition
  - IV sent encrypted
  - Unique key for each packet
  - Message Integrity Check (MIC) replaces CRC-32

Permanent Replacements for WEP

- Wi-Fi Protected Access (WPA)
  - Combines TKIP encryption scheme with 802.1X/EAP authentication and is still compatible with WEP enabled systems
  - Uses Michael Message Integrity Check (MMIC)
- Advanced Encryption Standard (AES)
  - Uses a mathematical algorithm called Rijndael instead of RC4
  - Various key size choices (128-, 192-, or 256-bits)
  - Not compatible with 802.11a, b, and g standards
- 802.11i (WPA2)
  - Requires AES – but backwards compatible with legacy devices
  - Endorses TKIP encryption over WEP
  - Uses 802.1X/EAP authentication

	WEP	WPA	802.11i
Cipher	RC4	TKIP	AES
Key Length	40/104 bits	128 bits encryption 64 bits authentication	128 bits
Key Life	24-bit IV	48-bit IV	48-bit IV
Packet Key	Concatenated	Mixing Function	Not Needed
Data Integrity	CRC-32	MMIC	CCM
Header Integrity	None	MMIC	CCM
Replay Attack	None	IV Sequence	IV Sequence
Key Management	Statistic	EAP-based	EAP-based

Figure 5 - WEP / WPA / 802.11i Summary

Conclusions

- WEP, as implemented in 802.11b standard, is susceptible to attacks
- Some other means of protection is needed to provide a more secure wireless computing environment
- Increasing IV space does not prevent attack – only prolongs it

Special Acknowledgments: Dr. S. Ulukus, Shabnam Shafiee, Nick Petroni, Jr.