

# Wireless Communications Security

With regards to wireless networks security there are a number of issues that need to be addressed. In particular I study wireless network risks and specially focus on flaws of Wired Equivalent Privacy (WEP) [Borisov 2001] and Denial of Service attacks in Ad Hoc networks [Imad 2004]. Current protocol deficiencies are studied that allow for protocol compliant attacks. Some countermeasures are also discussed and current standards are compared.

## 1. Security Overview

As wireless networks are increasingly used with mobile devices there are a growing number of security and privacy risks. Cryptography is the art of protecting data and there are many techniques available to help encrypt data over public communication networks.

### 1.1 Purpose

The purpose of all security mechanism is to ensure [Kurose 3E]:

1. Confidentiality: Only the sender and receiver can understand the contents of the messages they are exchanging and this is achieved by encryption/decryption using one or more keys
2. Authentication: The sender and receiver are able to confirm the identities of each other and this is essential to prevent an intruder masquerading. It is achieved using public/private keys
3. Integrity and Non-repudiation: The sender and receiver should be able to determine that the message has not be altered during transit and is indeed the message sent and proof is available that the message indeed came from the claimed sender. Further the sender cannot deny having sent the message.
4. Availability and Access Control: The communication should be always available for legitimate users and they should not be denied its use by malicious users

All security systems/protocols attempt to attain these four security goals.

### 1.2 Attacks

Attacks are typically classified as passive or active. In passive attacks there is unauthorized access to the network however there is no modification to any communication. It includes:

1. Eavesdropping: Listening to communications taking place between two entities on the network
2. Traffic Analysis: Monitoring the pattern of communication to asses network assets

In active attacks there is unauthorized access and attempts are made to modify data or disrupt communications. It includes:

1. Denial of Service (DoS): Normal use of network is disrupted by attacker resulting in poor service to legitimate users
2. Masquerading: The attacker gains access by assuming the identity of a trusted user to gain unauthorized access
3. Replay: The attackers monitors traffic and then retransmits selected messages to legitimate users
4. Message Modification: The attacker alters legitimate traffic

Generally *unauthorized users have malicious intent* and therefore maintaining network security is imperative. As we will see many current standards for wireless communication are severely lacking in implementing security.

## 2. Encryption Methods

Encryption basically relies on substituting a known variable such that the substitution method is not known to third parties. For example using a simple Caesar Cipher<sup>1</sup> an A may be represented as a D, a B as E and C as F, such that the word CAB becomes FDE. This is of course a very simple example and there are a number of very complex methods based on sound mathematical theory. There are two basic ways to encrypt data – using symmetric or asymmetric keys.

### 2.1 Symmetric Keys

In this method there is a **single shared private key** that is used to both encrypt and decrypt the message. The main weakness of this method is the issue of exchanging keys. For two parties to communicate they must both have the same private key; however there is no way to communicate this secret key over a public network and be assured that is its safety.

DES, 3DES and BLOWFISH are good examples of popular symmetric key algorithms. See [Schneier 1995] for excellent discussions.

### 2.2 Asymmetric Keys

In this method there are two keys. There is **one private-key and one public key**. As the names imply the private key is known only to one entity while the public key is openly available to everyone. Asymmetric key algorithms rely on the computation infeasibility of one-way functions. These one-way functions are easy to compute however when trying to reverse compute, the computation hardware available would require thousands of years to compute to crack using brute-force.

---

<sup>1</sup> [http://en.wikipedia.org/wiki/Caesar\\_cipher](http://en.wikipedia.org/wiki/Caesar_cipher)

RSA is a good example and the most popular asymmetric algorithm. See [Schneier 1995] for excellent discussions.

### 3. Security Standards and their Weaknesses

IEEE 802.11x provides mechanisms for security, however short of using VPN Tunneling over these protocols security and confidentiality cannot be assured as many flaws have been published. Network security can be easily compromised and a few methods are discussed here.

#### 3.1 Firewalls – MAC Filtering

This is the simplest method to impose restrictions to network access and can be easily configured on all access points. It is based primarily on the hardware MAC address that is unique for all adapters, however it is a very weak form of security as MAC addresses can be easily spoofed by determined hackers and is secure only until the authorized MAC addresses are unknown to third parties. However it adds another level of security and is therefore advisable to use in addition to other methods and it helps prevent unauthorized access to the network.

#### 3.2 Wired Equivalent Privacy (WEP)

In an infrastructure based network there are two steps before communication starts – Association (finding the access point) and Authentication (becoming part of the network). [Mishra 2002] shows these states and their transitions and WEP is used to protect communication from eavesdropping and ensuring “*privacy equivalent to that of wired networks.*”

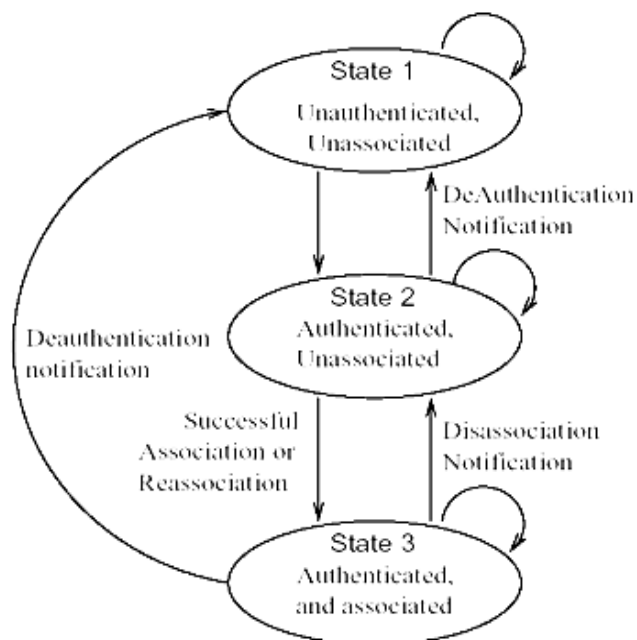
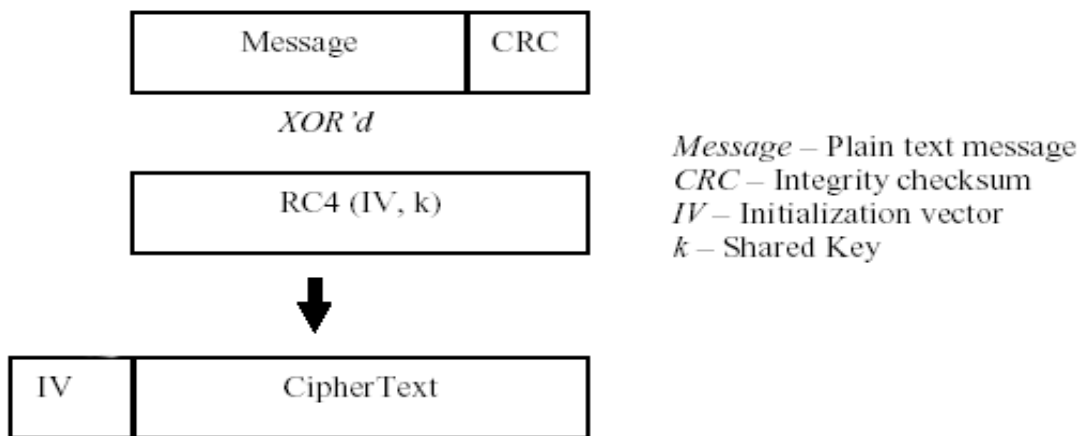


Figure 1: State Transition Diagram for 802.11

The WEP protocol is designed to protect link-level data communication and relies on a secret key  $k$  that is shared between the two parties to encrypt the message  $M$ . The process is as follows:

1. Check-summing: The checksum  $c(M)$  is computed and concatenated with  $M$  to obtain the plaintext  $P$
2. Encryption: Using an initialization vector (IV)  $v$ , and  $k$  a key-stream is generated using the RC4 algorithm as  $RC4(v,k)$ . Then the encrypted cipher-text  $C$  is obtained by XOR of  $P$  and  $RC4(v,k)$ .  $C = P \oplus RC4(v,k)$
3. Transmission: This encrypted message  $C$  is then transmitted along with the IV. At the receiving end this process is reversed.



**Figure 2: WEP Encryption Process**

The use of this single static shared private key (40 or 104 bits) and no way described to enable this exchange securely is a key problem with WEP. Borisov describes the pitfalls of stream ciphers and how encrypted messages can be decrypted and the integrity can be compromised.

RC4 is a stream cipher and relies on the IV and secret key  $k$ , to generate the key-stream that is used to encrypt the message. With stream ciphers it is well known that if two messages are encrypted using the same key-stream then XOR of them effectively negates the encryption (Collision Attacks).

$$C1 = P1 \oplus RC4(v,k)$$

$$C2 = P1 \oplus RC4(v,k)$$

$$C1 \oplus C2 = P1 \oplus P2$$

Therefore it is essential that key-streams are never reused, however this is not as easy to implement. A passive attacker can intercept messages and find instances of reuse of key relatively easily since IVs are transmitted unencrypted and can easily be compared while

the secret key hardly ever changes. The IV field is only 24-bit long so given a busy access point and a patient attacker it is only a matter of few hours before the IV is reused!

Also different implementations may use poor algorithms that reuse IVs earlier, for example certain cards reset the IV to zero every time they are reset. Once this plaintext is discovered it is relatively simple (using frequency analysis or other techniques) to obtain the actual message.

Active attacks for WEP include Modification [Borisov 2001] and Replay Attacks [Walker, Cam-Wignet 2003]. In a replay attack an attacker passively captures frames and then selectively replays relevant frames so as to appear to be a trusted entity. This can allow malicious users to gain access to networks, for example by replaying passwords. Replay attacks are generally prevented by using timestamps and session tokens. 802.11i proposes packet sequencing and mixing to overcome this.

The use of CRC32 to check the integrity of the frame leaves it susceptible to modification and forgery. Modification can occur since CRC and RC4 linearly XOR bits, making it possible to modify the packets maliciously in a controlled manner such that the CRC check still passes. Forgery can occur since checksum does not depend on the key. Once plaintext is known it can be used together with the public IV to create totally new packets. Also since IVs can be reused this can continue to be exploited indefinitely.

There are many other attack methods using the basic techniques already discussed and essentially all security features of WEP have been compromised, using off the shelf equipment and software.

### **3.3 Protocol compliant Denial of Service (DoS) in Ad Hoc Networks**

Mobile Ad Hoc Networks (MANET) are more vulnerable since there is no one central coordinating node and the topology changes very often, therefore mutual cooperation among nodes is essential for good service. JellyFish (JF) and Black Hole attacks [Imad 2004] that result in Denial of Service are difficult to detect since they are protocol compliant and constant network monitoring would be required which is not possible given the ad hoc nature of the network.

JF nodes reduce the network throughput to near zero by mainly exploiting TCP flow and congestion control methods and similar variants on UDP also. There are three variants of JF. The first uses packet reordering, deliberately sending packets in the wrong order, and TCP cannot recover from persistent reordering since all TCP variants are designed for brief periods of such network failure. The second drops packets periodically. This period of time is carefully chosen so as to force the exponentially back-off at link layer and close to the timeout period, causing multiple packet losses and reducing the throughput. The third method periodically delays packets. The delay is chosen so that a timeout occurs for every transmission, and this also disrupts the congestion control mechanisms of TCP. This complies with IP, as IP does not guarantee in-order delivery, loss-free delivery or a time-bound delivery.

Black Hole attacks on a host work by first establishing network routes through them and then deliberately dropping packets. The key difference between JF and Black Hole attacks is that JF affects closed-loop networks (that use protocols that infer network state) while Black Hole affects open-loop networks.

Experiments by [Imad 2004] conclusively demonstrate the adverse affect on the network performance due to these attacks in various scenarios. These attacks severely compromise network availability. Cryptographic techniques are proposed to authenticate all nodes in the ad hoc network to prevent abuse of the network. Key management is of particular interest since a CA is difficult to find due to the ad hoc nature of the network.

### **3.4 Wi-Fi Protected Access (WPA) and 802.11i**

WPA and WPA2 try to address the limitations of WEP by adding authentication and stronger encryption using PPP Extensible Authentication Protocol (EAP) [RFC 2284] and Temporal Key Integrity Protocol (TKIP). It makes use of Dynamic keys with a RADIUS authentication server for stronger protection. 802.11i addresses security concerns while being compatible with existing 802.11a/b/g hardware. It has a new alternative to WEP using Advanced Encryption Standard (AES) and encrypts the complete 802.11 packet. This standard was ratified in September 2004 and vendors are expected to provide firmware upgrades soon.

Key Management is a very important lesson learnt from WEP and EAP/EAPOL plays an important. According to [Changhua 2004] even 802.11i is susceptible to DoS attack during its 4-way handshake.

## **4. Countermeasures and Comparisons**

Many lessons are learnt by protocol designers once weaknesses are discovered and these need to be taken into account for future protocols. WEP weakness can be addressed by considering the 802.11 LAN as a network segment outside the trusted zone and therefore requiring VPN access. This successfully takes care of the security however introduces much administrative and computational overhead required by VPN.

In MANETs victims can respond JF and Black Hole nodes by trying to find new routes. However due to the protocol compliant nature of the attack it is difficult to know if the failure is intentional or genuine. Multi-path routing and establishing “backup routes” are possible ways to counter DoS attacks however there are sufficient delays involved in recognizing and responding to these attacks. This also leads to network portioning that leads to an increase of capacity of the network on unaffected nodes since JF and Black Hole nodes are “black listed” and other routes used. This is also undesirable as fairness and the number of hops is affected. These are important performance metrics along with throughput that we have considered so far.

The following table briefly summarizes the current technologies and while new technologies may seem secure for now, they probably have some hidden weak link.

<b>Table 1: WEP, WPA and 802.11i Comparison</b>			
	<b>WEP</b>	<b>WPA</b>	<b>802.11i</b>
Cipher	RC4	RC4	AES
Cipher Strength	40/104 bits	128 bits encryption, 64 bit authentication	128 bits
Initialization Vector	24 bits	48 bits	48 bits
Packet Key	Concatenated	Mixing Function	NA
Data Integrity Check	CRC32	Michael	CCM
Header Integrity Check	NA	Michael	CCM
Key Management	Static	EAP	EAP
<i>Note:</i> CCM: Counter with CBC-MAC (Cipher Block Chaining-Message Authentication Code)			

It is advisable to use to multiple layers of protection – using MAC filters, WEP, disabling SSID broadcast and using VPN. Encryption at packet level including that for management and control frames is required. Using multiple security technologies can mitigate the risk of yet undiscovered flaws in popular standards today. Also continuous monitoring of the network is required for unusual network usage patterns and this can enable administrators to stop an attack before the network is rendered useless. Wireless networks should become more secure as new technologies are discovered however there are no guarantees when it comes to computer security and staying ahead of hackers in technology is the only solution.

## **5. Security for Mobile Thin-Client Internet Applications**

These are discussed in the section on mobile application architecture.