WHITE PAPER

# SECURITY IN BROADBAND WIRELESS NETWORKS

POWERFUL. VERSATILE. RELIABLE.

redline®
communications

# TABLE OF CONTENTS

## INTRODUCTION

Broadband wireless is an essential part of building out and extending network coverage to all users and applications resulting in the need for increased network security. This paper provides an overview of security threats to broadband wireless networks, describes various counter measures, and how a well-designed system can significantly improve security with minimal burden or overhead on network performance.

## BENEFITS OF WIRELESS

Broadband wireless has proven to be reliable, cost effective, and quick to deploy for mission critical applications and services. Wireless systems are now an essential component of backbone networks for larger private enterprises, and for network build-out and extension for companies in a broad range of sectors including the oil & gas industry, telecom and data service providers, military and government networks, and law enforcement security networks. In many of these deployments, broadband wireless connectivity is superior to wired or fiber based solutions in terms of performance, cost, and serviceability. Additionally broadband wireless systems are the only practical solution in many parts of the world where there are no alternative means of connectivity.

All network technologies need to provide security, however due to the shared nature of any technology based on radio frequencies (RF), wireless systems can be more vulnerable to security issues than wireline deployments. High capacity wireless systems require additional levels of security as these systems are regularly deployed to cover distances ranging from tens of kilometers to more than a hundred kilometers.

Methods that are popular for many private Wi-Fi networks, such as restricting physical access to private areas, reducing RF emission, and site surveys are impractical and ineffective for wireless network that build out the core network or cover wide areas. In these cases, adequate built-in security measures must be included within the system design.

## SECURITY THREATS AND COUNTER MEASURES

System authentication and data privacy are extremely important for wireless systems for the data plane as well as the management and control plane. Broadband wireless systems can face several different types of security threats against these access points. Attacks range in type (passive or active) and severity and specific prevention and counter measures must be included in the wireless system design and deployment scenario.

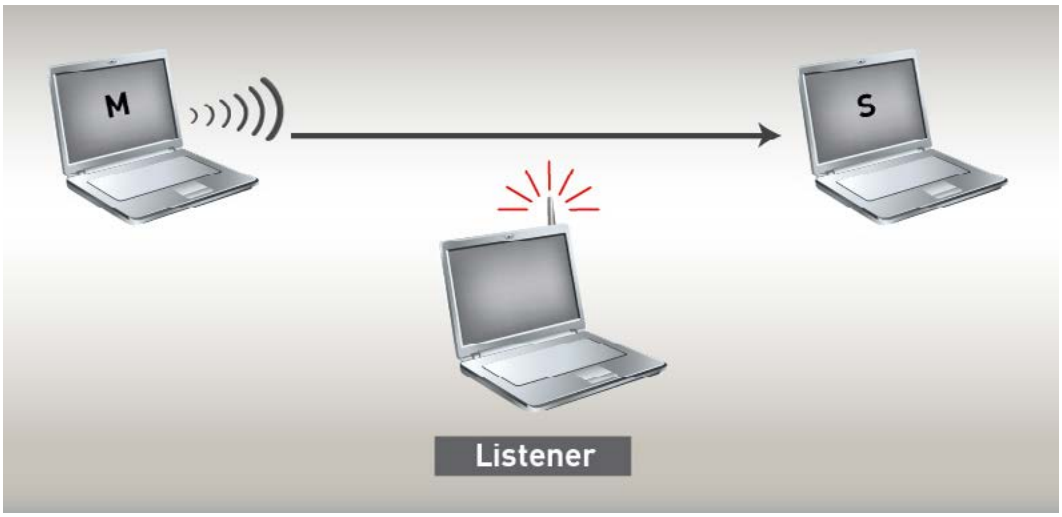
### Passive Attack

In a passive attack scenario, the intruder simply eavesdrops on an active wireless transmission between two or more legitimate wireless systems. The intruder listens passively and captures over-the-air traffic. The intruder then attempts to analyze and decode the data to discover sensitive information and/or prepare for a subsequent active attack.

#### Counter Measure

Strong wireless data encryption and encryption key management can render captured data useless to an eavesdropper. The Advanced Encryption Standard (AES), also known as Rijindale in cryptography, is an example

of a well-known and proven encryption algorithm. AES has been adopted as a standard by the U.S. government and is the basis for National Institute of Standards and Technology's (NIST) Federal Information Processing Standards (FIPS) for use with classified information and services.




Any encryption algorithm is only as secure as its encryption key generation and management. To effectively protect the privacy of the encrypted data, it is vital to employ a secure method for creating, storing, renewing, and exchanging encryption keys among communicating systems. Common methods for achieving initial secure encryption key exchanges include using strong cryptographic protocols such Diffie-Hellman or using a strict security policy and a mechanism for establishing shared keys. After the initial encryption key exchanges, it is equally important to continuously renew and exchange subsequent encryption keys using a method that ensures keys are not repeated or predictable, and that keys are transmitted over an encrypted tunnel between wireless systems.

The AES standard has provision for three different key lengths — 128-bit, 192-bit, and 256-bit. The design and strength of all three AES algorithm key lengths are considered sufficient to protect classified information up to the 'Secret' level, while 192-bit or 256-bit key lengths are required for 'Top Secret' information.

Redline's broadband wireless systems such as the AN-80i and RDL-3000 employ a high performance hardware-based AES cipher block for its wireless data transmission. The cipher block supports all three AES key length options. The encryption engine along with the encryption key establishment and management are designed to fully comply with and exceed the NIST FIPS140-2 standards.

### Active Attack

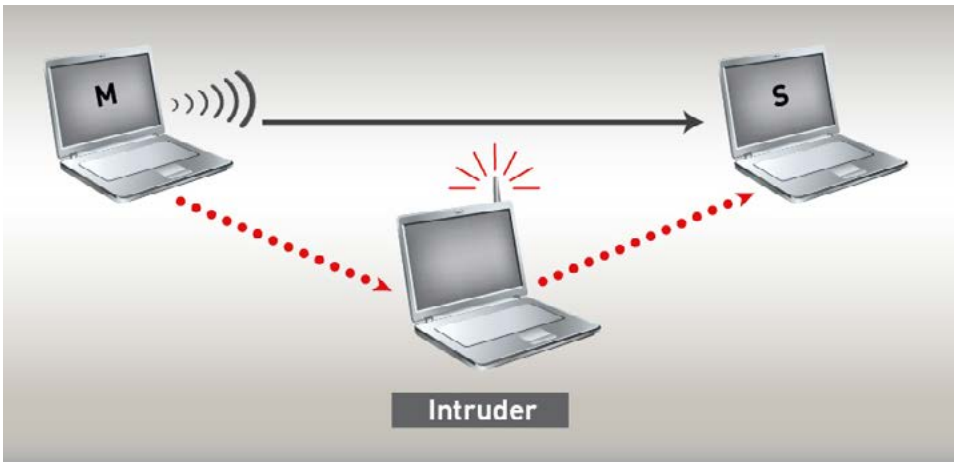
Security intrusions may also be active attacks. There are different types of active attacks:

I. Man-in-the-Middle

II. Replay Attack

Each requires a different set of counter measures designed into the wireless system.

*Man-in-the-middle*




A Wireless Man-in-the-Middle (MITM) attack is a form of active eavesdropping where the intruder makes independent connections with unsuspecting end systems and relays messages between them. The end connections will believe they are talking directly to each other over a private connection, when in fact the intruder is controlling the entire conversation. The intruder may simply attempt to gain access to the data transmission, or the data may be modified before retransmission.

Due to the technical challenges, intercepting and changing wireless transmissions at the physical RF level and at the logical data level make this type of attack on a wireless system less likely but not impossible. If these technical challenges are overcome, and an RF link is established, the only line of defense is to make impersonating the legitimate end systems impossible for the intruder.

### Counter Measure

A commonly used method to defend against MITM attacks is to use strong node level authentication mechanisms such as private or secret keys. The key is used for encryption/decryption and is known only to the end systems that exchange protected messages. In traditional private key cryptography, a key is shared by the legitimate end systems so that each can encrypt and decrypt messages.

The risk with private or secret keys is the possibility that it may be lost or stolen. A more robust alternative is to use a 'digital certificate' within a public key infrastructure (PKI). The PKI system provides for a digital certificate that can be used to authenticate the identity of the message sender. Each certificate associates a private key that is known only by the system for which the certificate was generated. Everything encrypted with the public key can only be decrypted using the associated private key, and everything encrypted with the private key can only be decrypted with the associated public key.

Each certificate contains:

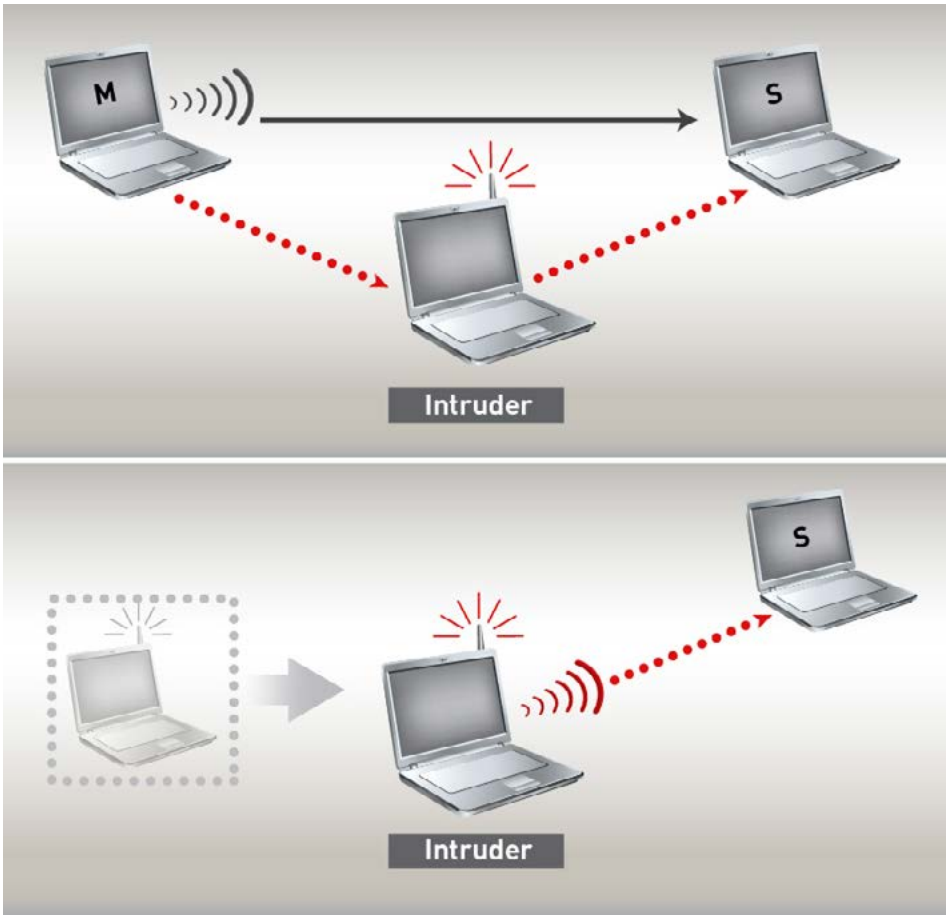
- Information about the unit for which it was generated (e.g., unit MAC address).
- Information about the entity generating the certificate.

- Information about the algorithms for which this certificate applies (e.g. RSA, DH, SSL/TLS).
- Information about the hash function used to generate the signature attached to certificate and its strength.
- The public key associated with this certificate.
- A digital signature.

An end system attempting to authenticate itself must use a private key to digitally sign a random number challenge issued by the verifying entity. This random number is a time variant parameter unique to the authentication exchange. Only after the verifier confirms the signed response using the claimant's public key can the claimant be successfully authenticated. This authentication mechanism ensures that a legitimate end system can instantly detect and reject an MITM attack.

Redline solutions employ the X.509 standards based digital certificate format and provides secure protection for its wireless transmission against even the most elaborate MITM attack schemes.

***Replay Attack***




A Replay Attack is a combination of a passive and active attack. The intruder first listens and records messages exchanged between two legitimate communicating end systems. The intruder then retransmits the recorded

messages to the second end system in an attempt to trick that system into performing unauthorized operations, giving additional responses for further attacks, or to overload that system to achieve a denial of service (DoS) attack.

### Counter Measure

The most effective method to avoid a replay attack is to employ entropy based session tokens in system authentication challenges and subsequent data exchanges. The use of entropy based random number generation (RNG) for the session tokens during the system authentication phase can render a replayed message invalid. Without successful authentication, the receiving system will not open a data channel for communications with an attacking system.

In addition to authentication phase protection, subsequent contiguous system authentication can be achieved through message level validation. For example, the message Integrity Check Values (ICV) in the AES data structure of every wireless packet may be encoded with non-repeating time sensitive information. The receiving system will perform regular ICV checks, and can recognize and discard any replayed messages.

Redline solutions incorporate system level authentication and contiguous data transmission validation based on the principle described above to detect and report on replay attacks. Control data for establishing link and data channels, as well as encrypted user and management data are verified in real-time. Any replayed data is immediately detected and discarded as 'outdated' eliminating the possibility of this type of attack.

## Management and Control Plane Attack

The management and control plane is another critical security area. Risks associated with passive attacks and active attacks on the data plane described earlier in this paper are equally applicable to the management plane. Intrusions may also originate from a connected wireline network.

### Counter Measure

Secure tunnels for management traffic and node level authentication mechanisms are a necessary and effective counter measure to prevent attacks to the management and control plane. PKI based encryption and authentication provides secure management channels and effectively prevents passive and active attack attempts, without affecting authorized users. Password based access control over secured channels provides the necessary means of authenticating legitimate access.

Redline systems employs proven protocols such as SSH for its secured CLI management interface and SSL/TLS for its secured HTTP web management interface. Factory or operator loaded certificates can be used for node level authentication and to eliminate the possibility of MITM attacks on the management plane. Redline systems also support multiple levels of password protected administrator and user level management accounts.

## Physical Security Attack

In standards based wireless systems such as a Wi-Fi or WiMAX, it is possible for an intruder to modify or 'enhance' test equipment or third party products for use in an attack.

Vendors of high performance broadband wireless systems typically design their own proprietary wireless protocol to achieve optimum functionality and performance. In this case, third party products or standard test

equipment could not be used for analyzing and decoding traffic, or for encoding wireless traffic that could interoperate with the proprietary system.

For proprietary systems intruders will have a strong interest in gaining physical access to the wireless system to analyze or modify the system. Special tamper proof seals and system logging functions are effective means to deter and detect these attacks. To ensure the product design is not copied or modified, additional provision can be made to include programmable hardware devices that are fully protected from the time they are soldered onto the printed circuit board in the factory.

Redline systems such as the AN-80i and RDL-3000 utilize all of these techniques and are the industry leader in the deterrence, detection, and prevention against physical security attacks.

### Certification

Certification is an important factor to consider when selecting any networking gear that will be used to create secure communications environments. A product can be compliant — meaning that the manufacturer believes that the product meets the requirements, or it can be certified — meaning that the manufacturer had the product independently tested by a third party to a set of security requirements.

The Federal Information Processing Standard (FIPS) 140-2 publication is a joint effort by the National Institute of Standards and Technology (NIST) in the United States, and the Communications Security Establishment (CSEC) for the Canadian government. FIPS 140-2 describes the requirements to ensure secure transmission of classified information and services over a network.

The process of achieving FIPS 140-2 certification is managed through the Cryptographic Module Validation Program (CMVP), headed by NIST. Products must undergo a detailed set of rigorous tests to certify that modules meet FIPS 140-2. This process provides stringent third-party assurance of FIPS 140-2 compliance and gives the buyer assurance that they are getting the security they paid for.  Additionally, FIPS 140-2 certification is a mandatory security requirement for all US Federal and Canadian Federal government agency purchases including the military.

Not only was Redline the first vendor to achieve FIP 140-2 certification for broadband wireless systems, Redline has built-in security features above and beyond what's required for certification.

## CONCLUSIONS

The shared nature of wireless systems and deployment scenarios can leave broadband wireless systems vulnerable to a variety of malicious attacks if security measures are not given priority in the network planning stage. Advance planning is crucial as it is extremely difficult to apply patch solutions to a deployed product and achieve the level of protection necessary for defending against these attacks. Successful broadband wireless security implementations depend on:

- Selecting manufacturers who have considered security measures early in the product design phase.
- Working with vendors who have a track record of architecting and deploying secure broadband wireless networks.

Redline has provided over 100,000 broadband wireless systems to government agencies, the oil & gas industry, the military and to large enterprise customers in over 130 countries. By working closely with its customers and with security standards, Redline has developed a range of broadband wireless solutions that deliver the highest level security in the industry. Redline's comprehensive approach to security protects wireless data and the management plane against security threats such as passive and active attacks and against physical tampering. As a result Redline solutions are trusted by some of the most security conscious organizations for mission critical backhaul and high-speed access applications.

## GLOSSARY OF TERMS

| | |
|---|---|
| **CLI** | A command-line interface (CLI) is a mechanism for a user to interact with equipment by typing text only commands to perform specific tasks. |
| **Diffie-Hellman** | Diffie-Hellam (or DH) is a specific method of exchanging keys. It allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. |
| **RSA** | RSA refers to an algorithm for public-key cryptography. It stands for Rivest, Shamir and Adleman, the group who first publicly described it. |
| **TLS / SSL** | Transport Layer Security (TLS) and Secure Sockets Layer (SSL), are cryptographic protocols that provide communication security over the Internet. TLS and SSL encrypt the segments of network connections above the Transport Layer, using asymmetric cryptography for key exchange, symmetric encryption for privacy, and message authentication codes for message integrity. |
| **X.509** | In cryptography, X.509 is an ITU-T standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI). X.509 specifies, among other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm. |

## ABOUT REDLINE COMMUNICATIONS

Redline Communications (www.rdlcom.com) is the creator of powerful wide-area wireless networks for the world's most challenging applications and locations. Used by oil and gas companies, militaries, municipalities and telecom service providers, Redline's powerful and versatile networks securely and reliably deliver M2M, voice, data and video communications.

302 Town Centre Blvd.
Toronto, ON L3R 0E8 Canada

**w** rdlcom.com **t** +1.905.479.8344
**e** info@rdlcom.com **tf** +1.866.633.6669