COMPREHENSIVE EMBEDDED SECURITY IN MICROWAVE NETWORKS

EXECUTIVE SUMMARY

The current and ongoing migration toward IP networking on backhaul networks supports rising data volumes, which is increasing the opportunities and motivations for data and call interception. As data volumes rise in wireless networks and their associated microwave backhauls, security has become of greater concern.

Very sensitive data is traversing every backhaul network—not just information critical to the financial system and defense and intelligence agencies but also important, private communications of world figures and just everyday ordinary people. Both institutional and individual users already assume your network protects their data and voice communications end-to-end. Their uncontrolled disclosure could cause exposure to unnecessary legal and PR liabilities.

There is also the issue of securing your physical network from intrusion, manipulation, subterfuge and sabotage. Proof-of-concept exploits on machine-to-machine communications and actual case histories of successful attacks on the wireless infrastructure are in the news more and more often. Equipment either has been compromised or taken over by unauthorized parties for unknown, malevolent purposes. In addition, there is the possibility that low-level but authorized users could gain unauthorized access to radios and unintentionally misconfigure them with higher-level commands through unsecured ports.

Rising numbers of access points in the form of smartphones, netbooks and tablet computers, more end users and increasingly diverse application traffic have heightened these opportunities for network breakins and the overall network threat level. Migration to IP networking perpetuates this scenario of increasing chances for attack and gives motivation to those who would take advantage of the situation.

What's needed is a high level of security for both microwave payload and management traffic.

FEBRUARY 2011

TABLE OF CONTENTS

The word is out. Microwave backhaul security is becoming a higher profile topic. While Wi-Fi and WiMAX connections are encrypted with at least 128-bit algorithms, microwave backhaul systems in many cases send data as plaintext.

COMPREHENSIVE EMBEDDED SECURITY IN MICROWAVE NETWORKS

"Once at the base station, encryption is up to the network operator, who might decide to shave off their microwave backhaul by not bothering to encrypt it at all. Once in the operator's network the call isn't encrypted, and that's where [the] shifty can tap your calls."

— Bill Ray, *The Register*, Sept. 4, 2009

"Any system that traverses an airwave should be encrypted. Look for a system that provides security with over-the-air AES (advanced encryption standard) encryption capabilities. Take a good look at security when using any wireless solution!"

— Leo Wrobel, *InformIT*, July 13, 2007

INTRODUCTION

The word is out. Microwave backhaul security is becoming a higher profile topic. While Wi-Fi and WiMAX connections are encrypted with at least 128-bit algorithms, microwave backhaul systems in many cases send data as plaintext.[1] In addition, the vast majority of microwave backhaul equipment does not provide security as a standard feature or even offer it as an option.

And though microwave communications equipment has some built-in security-like features such as scrambling, narrow beamwidth, proprietary airframe, coding and other factors, it is not very hard to break them, given the proper expertise. Some vendors even openly offer commercial wireless interception systems for "legitimate" monitoring. In today's connected world, the issue of network security can apply to any type of communications network—whether it is fixed, mobile or private.

The Strong Security suite from Aviat Networks offers solutions for high-level wireless protection with options for Secure Management, Payload Encryption and integrated RADIUS capability.

Secure Management offers secure management access to Aviat Eclipse Packet Node radios over unsecured networks. It protects the radio from accidental or intentional misconfiguration and provides centralized access control based on sophisticated permission attributes. Its Security Event Logger feature records all management activity for increased accountability and improved troubleshooting and root cause analysis.

Payload Encryption secures wireless data and in-band and out-of-band management traffic.

Integrated RADIUS capability enables authentication, authorization and accounting of remote user accounts and allows central management of Eclipse user accounts within existing IT infrastructure—using the same method as for PC user account administration.

THE PROBLEM

Traditionally, microwave networks have always been unsecure—unsecure as far as any purpose-built payload encryption or secure management. Until recently, those were deemed essential only for the most confidential microwave communications of financial firms, defense agencies and government, where the law can require them.[2] With the spread of knowledge of microwave security limits via the Internet, ability and awareness to exploit wireless security holes is greater than ever.[3]

MICROWAVE UNDER ATTACK

First, management of microwave networks needs to be secure. Microwave networks are vulnerable to tapping. With most microwave networks commonly managed with IP-based network management systems (NMS), attackers can take advantage by tapping into the NMS channel. Tapping into the

[1]Def.: Plaintext is the "normal" representation of data before any action has been taken to conceal, compress or "digest" it, retrieved from http://en.wikipedia.org/wiki/Plaintext.

[2]Messmer, E., "Secure wireless network brings Wisconsin cities together," *Network World*, 30 August 2007, retrieved from www.networkworld.com.

[3]Lieberman, J., "Vulnerabilities on microwave point-to-point broadcasts," *Tom's Hardware*, 15 August 2005, retrieved from www.tomshardware.com.

A hacker can use a second radio for a "sniffing" attack with its antenna placed inside the airlink beam, tap the NMS channel and gain knowledge of access methods, usernames and passwords. Then the attacker can tap the NMS channel, log onto the radio and any network devices for which usernames and passwords were detected.

management channel can happen anywhere in the public network between the radio and your network operations center (NOC). Even if your network is not truly "public," your enterprise network gives many people the possibility of accessing the radios. Within the telecom industry, preventing unauthorized users from controlling a radio network is a well-known problem that can lead to a range of potentially harmful actions. For example, unauthorized users can tap into the management channel and then change radio frequencies, reconfigure circuitry and drop traffic to kill it or just drop it locally. Payloads could also be rerouted to the next radio, assuming there is access to the cross-connect. They can also download malware onto the radio.

Many government operators and a growing number of private enterprise operators require that their wireless communications solutions comply with FIPS-140-2 for secure management protocol requirements, which can provide for secure software downloading, as an example. External security solutions do not provide a good option as communications can be tapped between the radio and an external security solution before protection can be applied to management traffic. Furthermore, most microwave solutions do not offer any security at all.

Over an unencrypted link, it is possible to intercept the management band. On an over-the-air link, a hacker can use a second radio for a "sniffing" attack with its antenna placed inside the airlink beam and tap the NMS channel. In this way, he can gain knowledge of access methods, usernames and passwords. Then later on, the attacker can tap the NMS channel and log onto the radio and any network devices behind it for which usernames and passwords were detected in the airlink. The attacker will then proceed to obtain ill-gotten information.

Also, depending on factors such as frequency and gain, "sidelobes" can leak out and be picked up by sensing equipment near the microwave transmitter—but not necessarily along the transmission path. Someone wishing to tap into an unsecure microwave network can receive the incoming management commands, modify them and then send out falsified management commands to the receiving end of the link to impair or disable it. This would be the classic "man-in-the-middle" attack (Figure 1).

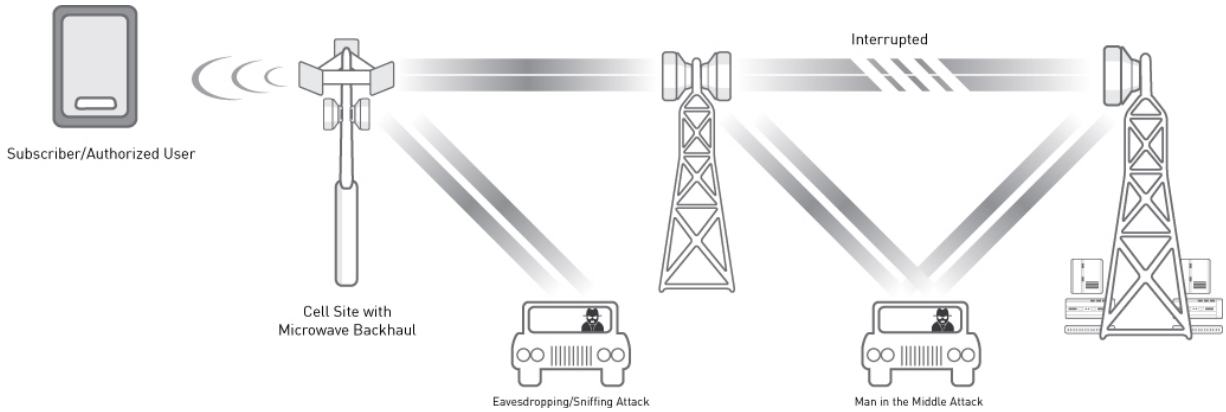

Figure 1. Would-be wireless attackers employ a number of techniques to compromise payload and management traffic on unsecure microwave radio backhaul networks, including "sniffing" and "man in the middle" attacks.

Unauthorized users can tap into the microwave network management channel and then change radio frequencies, reconfigure circuitry and drop traffic to kill it or just drop it locally.

MUST PROTECT THE NETWORK

Microwave networks must be protected against intentional and accidental misconfiguration. All radio ports must be secured on a logical basis. All backdoors must be disabled. Those seeking access to the network could possibly find and exploit management backdoors. It is even possible that low-level but authorized users could gain unauthorized radio access via telnet using a craft interface tool or an NMS terminal and unintentionally misconfigure radios with high-level commands through unsecure ports.

Next, the data payload of microwave networks has to be secured. Microwave eavesdropping has to be prevented. For example, the U.S. federal government requires a minimum standard of encryption for sensitive data during transmission in compliance with FIPS-197 security criteria.

Finally, all management activity must be tracked. For microwave management to be as secure as possible, all radio management activity has to be logged. Any event that can affect traffic, user accounts, login, logout or security needs to be documented. User account activity and IP addresses have to be recorded to account properly for all these events. These are only a few examples of what can be tracked.

Aviat Networks offers an integrated, embedded, standards-based security solution for Eclipse microwave networks. This standards-based solution allows you to define your own security policies.

THE SOLUTION

Aviat Networks offers an integrated, embedded, standards-based security solution for Eclipse microwave networks. Eclipse Packet Node can be protected with secure management, payload encryption and integrated RADIUS capability for remote user authentication, authorization and accounting with Strong Security built into the Eclipse Packet Node INU (intelligent node unit).

STANDARDS-BASED SECURITY, YOUR SECURITY POLICY

Aviat Networks' Secure Management supports secure management interfaces and protocols validated against FIPS-140-2 requirements. With Secure Management, Aviat Networks is the only microwave radio provider to offer a complete security solution with FIPS-140-2-validated secure management. To qualify for use by U.S. government and other operators concerned about security, Secure Management uses a FIPS-140-2 validated algorithm. Furthermore, this standards-based solution allows you to define your own security policies. With any combination of four groups of user access privileges, you can specify the precise user profiles that work best with your security policies. Secure Management can provide access control based on fine granularity of more sophisticated configurable user permission attributes to customize a profile for each authorized user. It can be defined to match your own internal security policy. Management access to Eclipse can be made razor sharp based on each user account being able to be assigned any combination of four groups of privileges[4]:

- View only—access to view status and alarms
- Engineer—access to set controls (except security controls), upgrade software and set configuration objects (except user account and security objects)
- Admin—access to view and set user account configuration objects and controls
- Crypto—access to view and set configuration objects and controls (e.g., configure encryption and authentication algorithms)

KEEPING TRACK

The Security Event Tracker feature tracks all Eclipse management activity. The username and IP address for each login attempt are tracked. In this way, an audit trail of which users were supposedly at what management access point in the network is created and retrievable in the event of a network breakin. This audit trail can be examined to resolve discrepancies and determine if the illegal management activity is the work of an insider or an external hacking attempt that succeeded.

SECURE TUNNELING

Using the Portal craft interface tool for configuration and maintenance, the Eclipse radio can be securely managed via TLS v1.2 tunneling. By utilizing this protocol, Eclipse radio software, stored configuration information and hardware components are protected from unauthorized modification, destruction or disclosure. Portal supports Secure Management between the management terminal and the Eclipse radio for both local and remote access.

The username and IP address for each login attempt are tracked. In this way, an audit trail of which users were supposedly at what management access point in the network is created and retrievable in the event of a network breakin.

[4]Each group of privileges is independent, and for each user any combination of up to all four groups can be selected. Note that each group DOES NOT include all the functionality that each lower group offers.

Supervise all Eclipse links—and OEM equipment—on your network securely over unsecured LANs, WANs or other management access points in the "cloud."

CENTRALIZED MONITORING

For centralized monitoring from a NOC, Eclipse can be securely accessed through any NMS supporting SNMP v3 (Figure 2). Secure Management is compatible with any NMS capable of SNMP v3. This lets you supervise all Eclipse links—and OEM equipment—on your network securely over unsecured LANs, WANs or other management access points in the "cloud." By using SNMP v3 and closing all unsecured ports on Eclipse, wireless management commands get a very high level of protection.

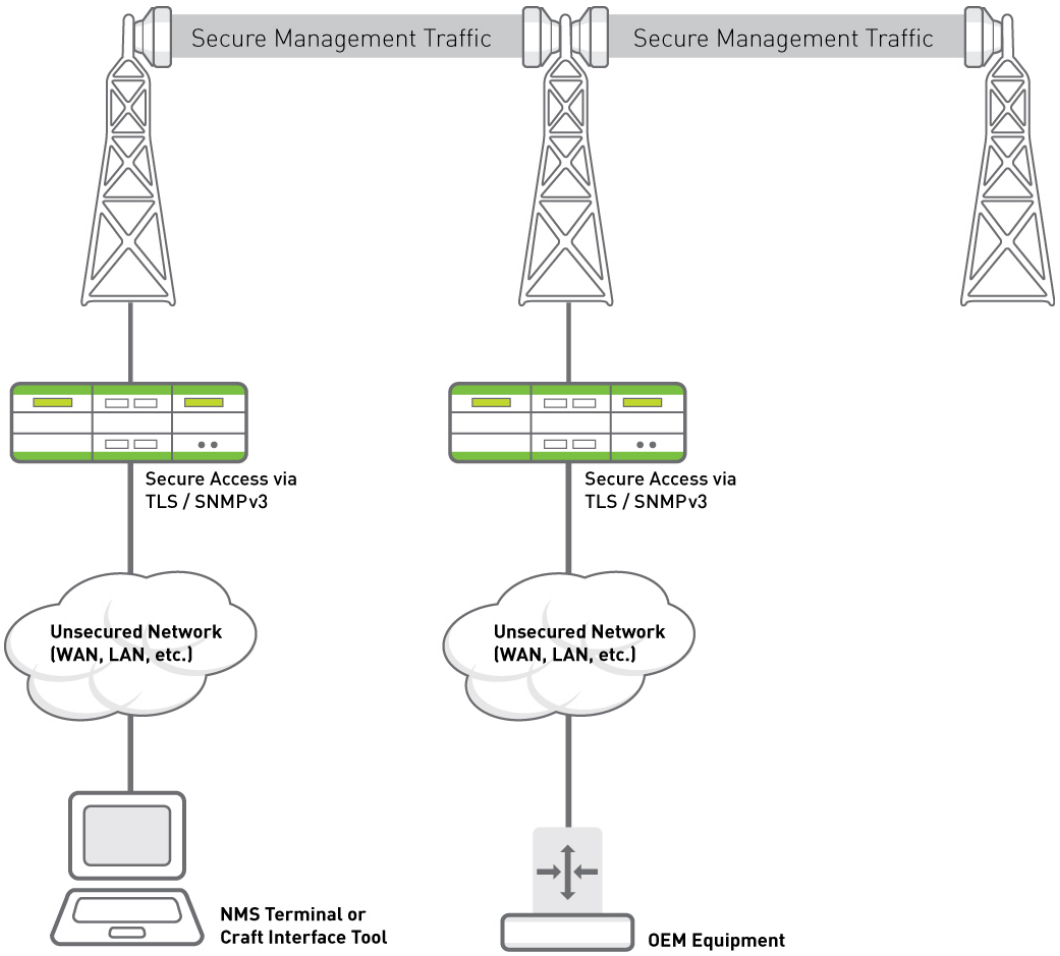

Figure 2. Strong Security on Eclipse Packet Node supports Secure Management functionality via TLS v1.2 tunneling with a craft interface tool or SNMP v3 through a compatible NMS. Note: Data payload traffic and HTTPS protocol support for secure software download present but not shown.

Strong Security on Eclipse Packet Node supports Secure Management functionality via TLS v1.2 tunneling with a craft interface tool or SNMP v3 through a compatible NMS.

Furthermore, Aviat Networks' Payload Encryption supports encryption of radio management commands based on a module algorithm validated against FIPS-140-2 requirements. In part, this helps fulfill the comprehensive security requirements for sensitive data invoked by FIPS-140-2, corresponding to the Advanced Encryption Standard (AES). Payload Encryption supports AES-128 and AES-256 as well as other cipher suites. Many private operators are becoming aware of higher microwave security and specifying FIPS-140-2 security for their networks.

With embedded Strong Security on Eclipse Packet Node, payload and management traffic get a high level of security against interception (i.e., sniffing) with the Payload Encryption feature.

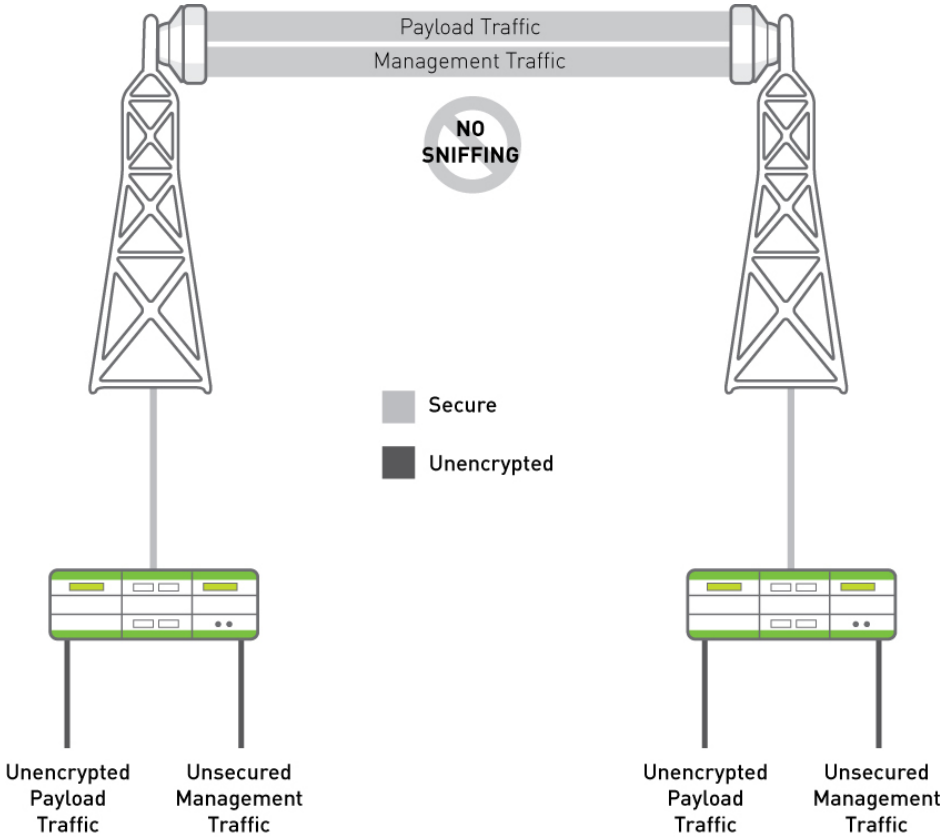

Figure 3. With embedded Strong Security on Eclipse Packet Node, payload and management traffic get a high level of security against interception (i.e., sniffing) with the Payload Encryption feature.

NO EAVESDROPPING POSSIBLE

In addition, Payload Encryption prevents wireless communications from being intercepted (Figure 3). Any eavesdropping equipment, or sniffers, along the transmission path between links or in the transmitter's vicinity will only receive a garbled transmission. With AES encryption and 128-, 192- or 256-bit symmetric keys, a randomly generated encryption combination protects each wireless link pair. Combinations are created and negotiated between links using the industry-standard Diffie-Hellman Key agreement method, which supports groups with modulo of at least 2048 bits. Given this level of support, no encryption combination will be repeated in 835 years. Payload Encryption is fully compatible with AES and complies with FIPS-197, which defines AES encryption.

Aviat Networks' implementation of the Payload Encryption feature on Eclipse Packet Node radios provides the strength of security recommended by the U.S. National Institute of Standards and Technology (NIST) for data that must be protected until the year 2030.[5] With this amount of encryption, NIST does not anticipate it will be practicable that data so encoded could be made unsecure until that time, given today's level of computing power.

Aviat Networks' Payload Encryption feature on Eclipse Packet Node radios provides the strength of security recommended by NIST.

RADIUS: PROTECTION FROM UNAUTHORIZED ACCESS

Eclipse is protected against intentional or accidental misconfiguration. Users can only access management functions of the radio for which they are granted permission in advance. All users can be remotely authenticated by a centralized Authentication, Authorization and Accounting (AAA) domain through Remote Authentication Dial In User Service (RADIUS) capability, which Eclipse integrates.

[5]Barker, E., et al, *Recommendation for Key Management — Part 1: General (Revised),* National Institute of Standards and Technology, Washington, D.C., March 2007, p 66, retrieved from http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf.

Strong Security on Eclipse Packet Node offers a high level of microwave communications security. It is integrated and embedded into Eclipse—not "added on." Thus, security cannot be bypassed easily.

RADIUS capability makes it simple to administer user network access. For example, a user profile can be removed from the AAA domain, which removes all access to all radios on the network simultaneously. It also allows you to integrate radios into your existing IT infrastructure and manage Eclipse user accounts from a central location—the same way you manage PC user accounts. This will eliminate manually maintaining user accounts on large numbers of radios.

And RADIUS capability helps protect logins. Users need to create login passwords with at least one letter and one number from eight to 32 characters for additional password complexity. It also supports special characters such as underscore or asterisk and uppercase and lowercase letters. In these ways, RADIUS capability increases password complexity to prevent "dictionary" attacks that break security by guessing logical alphanumeric password combinations based on people's propensity to pick passwords that follow predictable patterns.

Also, RADIUS capability helps protect against security exploits such as "mechanized" attacks where an unauthorized user programs a computer to try a random combination of usernames and passwords on a rapid basis in an attempt to find a valid login. If too many invalid combinations are attempted in a given period, through use of AAA domain capability via RADIUS protocol, users not already logged in will be locked out from trying to log on for a specified period. You can determine the number of logins that can be attempted in a given time frame before users are locked out for your chosen interval.

If RADIUS is unavailable for any reason, a fallback position allows cached credentials to be used to log in. If RADIUS is not accessible for extended periods, local user accounts may be used.

CONCLUSION

In conclusion, Strong Security on Eclipse Packet Node offers a high level of microwave communications security. It is integrated and embedded into Eclipse—not "added on." Thus, security cannot be bypassed easily.

For the best wireless security, you can use Payload Encryption in conjunction with Secure Management and integrated RADIUS capability. Secure Management over unsecured networks is supported through use of standards-based secure protocols validated against FIPS-140-2 requirements. Payload Encryption of data communications is compliant with FIPS-197, qualifying it for use by U.S. government agencies and others that need security for sensitive data and other levels of data classification. Integrated RADIUS and centralized AAA domain capabilities are supported for remote authentication, authorization and accounting for an extra level of wireless security by verifying user identities, providing more control over user access and privileges.

Strong Security will bring the protection level of your wireless network to par with the precautions that exist in Wi-Fi and WiMAX networks. Terminal support for payload encryption will prevent interception.

Knowledge is spreading of the security vulnerabilities of microwave networks. Other "links" in the wireless chain already implement high levels of security (e.g., Wi-Fi, WiMAX). Backhaul networks do not enjoy a similar, widely defined high level of security. However, many government and related organizations—as well as enterprises—are demanding strong security to protect their network communications and data. Find out how Strong Security on Eclipse Packet Node can protect your network—including payload and management traffic—by contacting your Aviat Networks representative.

WWW.AVIATNETWORKS.COM

_w_StrongSecurity_EcliPktNd_UNIV_15Feb11

Aviat NETWORKS