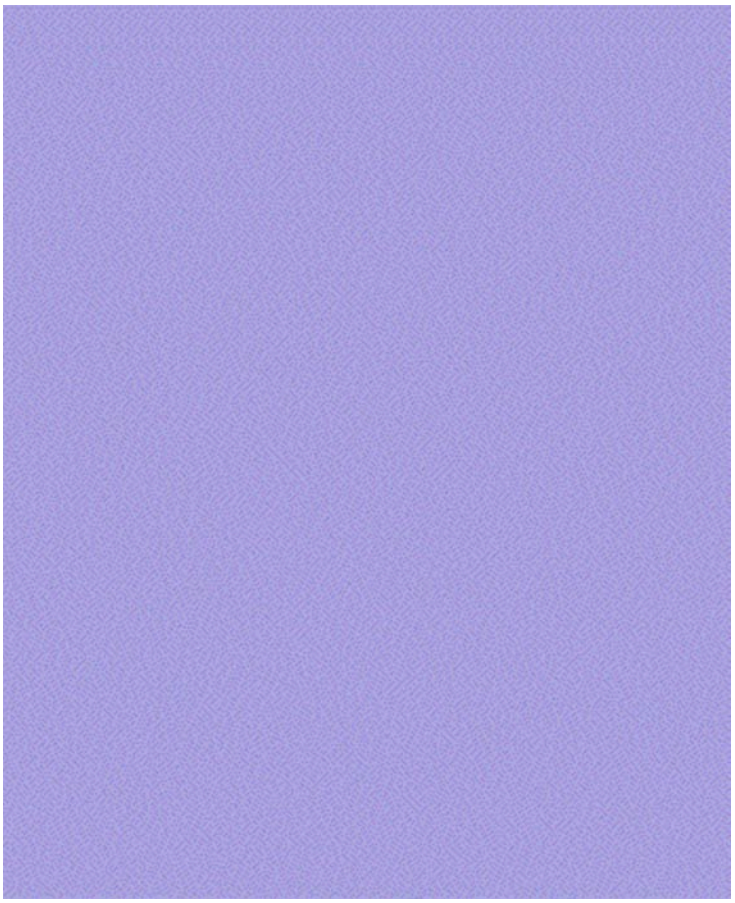
MOTOROLA
intelligence everywhere™



Security and the Motorola Canopy™ Wireless Broadband Platform

(Advanced Security Techniques)

TABLE OF CONTENTS

List of Tables

List of Acronyms

AES.....*Advanced Encryption Standard*

AP.....*Access Point*

BAM.....*Bandwidth and Authentication Manager*

BH.....*Backhaul Module*

CMM.....*Cluster Management Module*

DES.....*Data Encryption Standard*

DHCP.....*Dynamic Host Configuration Protocol*

FIPS.....*Federal Information Processing Standards*

IP.....*Internet Protocol*

LAN.....*Local Area Network*

NAT.....*Network Address Translation*

QoS.....*Quality of Service*

SM.....*Subscriber Module*

SNMP.....*Simple Network Management Protocol*

SQL.....*Structured Queary Language*

TIA.....*Telecommunications Industry Association*

NOTICE

The information in this publication is subject to change without notice. Motorola shall not be liable for technical or editorial errors or omissions nor for any damages resulting from the use of this material.

Each configuration tested or described may or may not be the only available solution. This test is not a determination of product quality or correctness, nor does it ensure compliance with any federal, state or local requirements. Motorola does not warrant products other than its own strictly as stated in Motorola's product warranties.

INTRODUCTION

Until just recently, it would have been unimaginable for medical institutions to exchange high resolution digital imagery over wireless networks. Why, you may ask? Not only were the early wireless systems incapable of transmitting detailed medical images over their seemingly small pipes — originally designed to carry voice conversations — but securing this sensitive data from vulnerabilities such eavesdropping, session hijacking, data alteration and manipulation *(among others)* and ultimately protecting the privacy of the patient seemed an insurmountable challenge.

Over the last 10 years, Motorola has been investigating the use of fixed wireless broadband systems and has brought to the marketplace a product that is capable of not only handling these incredibly large digital medical images with lightning fast speeds but has integrated advanced security measures into the product that transparently, efficiently and effectively safeguard the precious information that is transmitted over Motorola's Canopy™ wireless broadband system. Today, medical institutions have moved far beyond simply imagining the use of wireless broadband systems to actually applying the technology to collaborate and often times performing life saving diagnostics.

This paper *Security and the Motorola Canopy Broadband Wireless Platform* offers a snapshot of some of the security issues being faced by the wireless broadband industry as well as the safeguards that Motorola is employing in the Canopy platform to ensure the security and integrity of this advanced system for our customers.

WHY ARE SECURITY MEASURES NECESSARY?

When the Internet was first introduced, there was little concern about security measures. The specifications for the Internet Protocol (IP) did not take into account the fact that operators may actually need to protect the data that they were transmitting. Obviously a great deal has changed since that time. Seemingly harmless attacks have wreaked havoc on computer networks with wireless adding a new dimension of vulnerability. The first step in understanding how these attacks can be prevented is in analyzing the basic weaknesses in a typical IP system.

CLEAR TEXT TRANSMISSIONS

When data is transmitted over an IP network, all information is relayed as clear text. That is to say, the data is not scrambled or rearranged and is transmitted purely in its raw form. This information includes both the data and authentication streams of information and is referred to as *transmitting in the clear.* When transmitting clear text transmissions, login name, user identifications, passwords, electronic mail (from a POP3 mail client), websites visited, downloaded information — *everything* — is open to the prying eyes of anyone with a network analyzer.

PASSIVE MONITORING

As mentioned previously, it is relatively easy to monitor clear text transmissions over an IP network. Unfortunately, most of the time invaders are not easily detected. This is because monitoring of the traffic is performed using passive devices that do not transmit any data of their own. Therefore, they can't be easily detected. In addition, attackers do not require physical access to any particular facility to conduct these passive monitoring sessions.

END-TO-END SECURITY

While hackers don't require physical access to monitor *(hack)* a network, they can be easily connected by placing a probe or analyzer anywhere along the transmission path — *from system initialization to destination*. Since vulnerabilities can exist anywhere along the IP transmission path, complete system security can only be achieved by applying end-to-end security measures. The security measures built into the Canopy system architecture are designed to cover only the wireless portions of the network. These include:

- Access Point (AP)
- Subscriber Module (SM)
- Backhaul (BH) Module
- Cluster Management Module (CMM)
- Bandwidth and Authentication Manager (BAM)

The Canopy system security does not include elements outside of the wireless transport, such as:

- Client (Computer)
- Wireless Modems
- Local Area Networks
- Routers
- Printers
- Servers
- Various Network Peripheral Equipment

Protecting equipment outside of the Canopy system from security invasions can be accomplished using software, devices and security techniques from various manufacturers and should be included as part of an end-to-end system design.

SECURITY FEATURES WITHIN CANOPY SYSTEM

Privacy and integrity of data are key considerations for both broadband network subscribers and operators. Security and authentication to prevent unwanted access to critical data or services are necessary for the effective operation of any broadband network. Applications such as medical, remote surveillance, safety, security and homeland defense would not be possible without incorporating advanced security features into the fixed wireless network. Gone are the days when it wasn't necessary to be concerned with security as a fundamental building block.

Today, the Canopy system incorporates a flexible security model that supports a wide variety of system configurations ranging from a fully open system to an authenticated/encrypted air link with dynamic session key assignment. The Canopy system uses industry proven authentication and encryption technologies to ensure that the service provider maintains control of the network. The system comes with Data Encryption Standard (DES) to protect against eavesdropping and Advanced Encryption Standard (AES) is available as an option for customers requiring the most secure network available. The following paragraphs highlight each of these advanced features in further detail.

CANOPY'S PROPRIETARY PROTOCOL

Canopy's proprietary air interface provides a strong foundation against attacks by invaders. First of all, because the Canopy system is based on a proprietary protocol, there are no published specifications for the product by which sniffer radios could be built. In addition, a sniffer would require the proprietary Canopy chip set that is not readily available. Second, the MAC protocol for packet assembly, disassembly and retransmission is not published. Third, data transmitted over the air is scrambled into 64-byte data packages thus providing an additional obstacle to unauthorized decoding. Finally, the directionality of the Canopy system transmissions impedes eavesdropping. In other words, the proprietary air interface presents a major hurdle for unauthorized parties. Of course, the Canopy system's security is not based merely on secrecy of its air interface.

AUTHENTICATION

Clearly it is inadvisable to transmit information that one assumes is secure using clear text as it can be easily monitored. Unlike many fixed wireless broadband products, the Canopy system does not use clear text transmissions but rather a proprietary protocol for transmissions. When this protocol is combined with the Canopy Bandwidth and Authentication Manager (BAM), an added level of security is achieved for the operator and the network.

The BAM controls access to a Canopy system, and each AP module can be configured to require secure SM authentication prior to providing network access. Each SM must be authenticated by the BAM before entering the network. SMs are authenticated and keys are managed individually. The authentication process also takes into account the electronic serial number unique to each transceiver along with a 128-bit secret key that is unique to each SM and is known only to the network operator. The eight step authentication process is shown in Table 1.

Table 1. The Authentication Process

Step	*Description of Task*
1	When an SM attempts to enter the Canopy network it sends a registration request to the AP.
2	The AP then sends an authentication request to the BAM.
3	The BAM generates a 128 bit random number that is sent to the SM as a challenge.
4	The SM calculates a response using either its factory set key or the Authorization key it has been assigned by the network operator.
5	This challenge response is sent to the BAM through the AP.
6	The BAM compares the challenge response to what it calculated using the same random number and the Authentication key from the BAM SQL database.
7	If the results agree, the BAM sends the AP a message authenticating the SM and sends the SM and AP QoS information.
8	If the results do not agree or the SM is not in the database the BAM sends the AP a message denying authentication and the AP sends the SM a message to lock itself out from that AP for 15 minutes before retrying.

KEY MANAGEMENT

The Canopy system uses an ESN, two keys and a random number for authentication. Table 2 details the functionality of each of these along with the random number.

Table 2. Canopy Key Management

Key/Number	*Description*
Electronic Serial Number	Each Canopy SM has a factory set ESN that cannot be changed. The ESN is the identifier which is being authenticated and is 48 bits in length.
Authentication Key (Authorization key or Skey)	This key is set by the network operator in the BAM SQL database and by either the network operator or by the subscriber in the SM. This key can be seen in the BAM SQL database by the network operator; it can't be displayed in the SM Configuration web page by subscriber. It is 128 bits in length.

Key/Number	*Description*
Session Key	The session key is calculated separately by the SM and the BAM, using the Authentication Key, the ESN, and the random number. This key is sent to the AP by the BAM – like the other keys, it never goes over the air. The network operator or the subscriber never sees this key. This key is either 56 bits (DES) or 128 bits (AES) in length.
Random Number	A random number is generated by the BAM and used during each attempt by an SM to register and authenticate. The subscriber or network operator never sees this number. This is a 128 bit number.

Of the three numbers presented in Table 2, only the Authentication Key is settable by the network operator and it must be set both in the BAM and in the SM. Further information about Canopy's authentication process is detailed in *Bandwidth and Authentication (BAM) User Guide.*

ENCRYPTION

The Canopy system also has provisions for the industry-accepted DES with key management via the Telecommunications Industry Association (TIA) standard BRAID cryptosystem. In addition, the Canopy system provides for AES for customers who require the most secure networks available. These encryption techniques are transparent to network firewalls, Dynamic Host Configuration Protocol (DHCP) servers and Network Address Translation (NAT) devices.

Data Encryption Standard (DES)

DES is an encryption standard that uses an encryption technique developed in the mid 1970s by IBM and then adopted by the Federal government as a federal standard in 1977 for protecting sensitive, but not classified data. DES was designed so that even if someone knows some of the plain text data and the corresponding ciphertext, there is no way to determine the key without trying all possible keys. The strength of DES encryption based security rests on the size of the key and the proper protection of the key.[1] The following paragraphs discuss details of DES from the document entitled, *Federal Information Processing Standards (FIPS) PUB 46-3 Data Encryption Standard (DES):*

> The Data Encryption Standard (DES) specifies two Federal Information Processing Standards (FIPS) approved cryptographic algorithms as required by FIPS 140-1. Encrypting data converts it to an unintelligible form called cipher.

[1] *Security Complete*, Adapted from *Active Defense,* by Chris Brenton with Cameron Hunt.

Decrypting cipher converts the data back to its original form called plain text. The algorithms for DES described in the DES standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

A DES key consists of 64 binary digits ("0"s or "1"s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, may be used for error detection. The 8 error detecting bits are set to make the parity of each 8-bit byte of the key odd, i.e., there is an odd number of "1"s in each 8-bit byte[2]. Authorized users of encrypted computer data must have the key that was used to encipher the data in order to decrypt it. The encryption algorithms specified in the standard are commonly known among those using the standard. The cryptographic security of the data depends on the security provided for the key used to encipher and decipher the data.

Data can be recovered from cipher only by using exactly the same key used to encipher it. Unauthorized recipients of the cipher who know the algorithm but do not have the correct key cannot derive the original data algorithmically. However, it may be feasible to determine the key by a brute force "exhaustion attack." Also, anyone who does have the key and the algorithm can easily decipher the cipher and obtain the original data. A standard algorithm based on a secure key thus provides a basis for exchanging encrypted computer data by issuing the key used to encipher it to those authorized to have the data.

Data that is considered sensitive by the responsible authority, data that has a high value, or data that represents a high value should be cryptographically protected if it is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage."

Advanced Encryption Standard (AES)

AES Standard is the follow-up to DES and is the result of an exhaustive evaluation by the National Institute of Standards and Technology that began in 1997 with a notice soliciting an unclassified, publicly disclosed encryption algorithm that would be available royalty-free worldwide. Following the submission of 15 candidate algorithms and three publicly held conferences to discuss and analyze the candidates, the field was narrowed to five candidates. NIST continued to study all available information and analyses about the candidate algorithms, and selected one of the algorithms, the Rijndael algorithm, to propose for the AES. The Rijndael algorithm is a variable length block cipher, but its implementation in AES is 128 bits. In decimal terms, this means that there are approximately:

3.4×10^{38} possible 128-bit keys;

[2] Sometimes keys are generated in an encrypted form. A random 64-bit number is generated and defined to be the cipher formed by the encryption of a key using a key encrypting key. In this case the parity bits of the encrypted key cannot be set until after the key is decrypted.

.

In comparison, DES keys are 56 bits long, which means there are approximately 7.2 x 10^{16} possible DES keys. Thus, there are on the order of 10^{21} times more AES 128-bit keys than DES 56-bit keys.

In the late 1990s, specialized "DES Cracker" machines were built that could recover a DES key after a few hours. In other words, by trying possible key values, the hardware could determine which key was used to encrypt a message. Assuming that one could build a machine that could recover a DES key in a second (i.e., try 2^{55} keys per second), then it would take that machine approximately 149 thousand-billion (149 trillion) years to crack a 128-bit AES key. To put that into perspective, the universe is believed to be less than 20 billion years old.[3] Table 3 details the different methods of encryption and their associated keys.

Table 3. Methods of Encryption and Their Associated Keys[4]

Encryption	Bits in Key	Number of Possible Keys
DES	56	2^{56} = 72,057,594,037,927,900
AES	128	2^{128} = 340,282,366,920,938,000,000,000,000,000,000,000

According to NIST, the Rijndael algorithm was chosen for the following reasons:

> "When considered together, Rijndael's combination of security, performance, efficiency, ease of implementation and flexibility make it an appropriate selection for the AES.
>
> Specifically, Rijndael appears to be consistently a very good performer in both hardware and software across a wide range of computing environments regardless of its use in feedback or non-feedback modes. Its key setup time is excellent, and its key agility is good. Rijndael's very low memory requirements make it very well suited for restricted-space environments, in which it also demonstrates excellent performance. Rijndael's operations are among the easiest to defend against power and timing attacks.
>
> Additionally, it appears that some defense can be provided against such attacks without significantly impacting Rijndael's performance. Rijndael is designed with some flexibility in terms of block and key sizes, and the algorithm can accommodate alterations in the number of rounds, although these features would require further study and are not being considered at this time. Finally, Rijndael's

[3] *Advanced Encryption Standard Fact Sheet*, Computer Security Division, National Institute of Standards & Technology, January 19, 2001.
[4] Security Complete, Adapted from *Active Defense,* by Chris Brenton with Cameron Hunt.

internal round structure appears to have good potential to benefit from instruction-level parallelism."[5]

AES is commercially available as an option to the Canopy system and can be very effectively used with the BAM.

SUMMARY

The wireless broadband industry has made significant advancements in the last several years both in terms of capabilities and market acceptance. For this trend to continue, however, these wireless networks must embody the types of security provisions outlined in this paper.

Motorola has taken a very proactive stance on the issues of security and offers a wide range of alternatives to its customers ranging from a fully open system to an authenticated/encrypted air link with dynamic session key assignment. Together, authentication, a proprietary protocol and DES or AES techniques form a powerful bond for protecting the Canopy system and the information that is transmitted over the platform. Already, it is making way for powerful new sets of applications for security focused users. We anticipate that as the platform continues to proliferate these types of applications will be the basis for continued growth of wireless broadband solutions.

Additional product information is located at the Canopy website at www.motorola.com/canopy.

[5] National Institute of Standards & Technology.

Motorola Canopy
50 E Commerce Drive
Schaumburg, IL 60173
www.motorola.com/canopy

1/290503