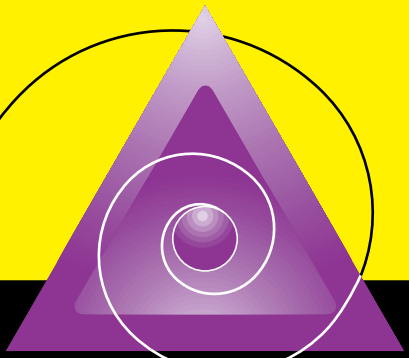
Visit techguide.com

The Technology Guide Series

A Guide to Securing Broadband Cable Networks: DOCSIS Security



This Guide has been sponsored by

RSA SECURITY™

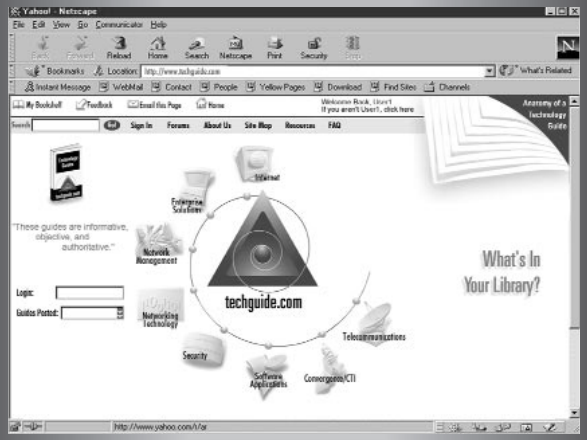


Table of Contents

Editoral Writing Team

ATG's Technology Guides and White Papers are produced according to a structured methodology and proven process. Our editorial writing team has years of experience in IT and communications technologies, and is highly conversant in today's emerging technologies.

209 West Central Street, Suite 301, Natick, MA 01760
Tel: (508) 651-1155, Fax: (508) 651-1171
E-mail: info@techguide.com Web Site: http://www.techguide.com

Introduction

Cable networks are referred to as shared-media networks. All users within the same hybrid fiber-coax (HFC) segment share a common cable line running between their cable modems (CM) and the cable modem termination system (CMTS) servicing that segment. The traffic to and from any user is visible to all other users on the same network segment, and an eavesdropper can view this traffic using a packet-sniffing[1] tool. In the context of cable broadband networks this means that a user can intercept voice and video traffic to and from other users on the same segment.

In addition to loss of privacy, attacks on cable networks may result in service theft and damaging denial-of-service attacks. Many such attacks involve cloning of customer premises equipment (CPE) or network server impersonation, and threaten both consumers and cable operators. Authentication, access control, integrity, confidentiality, and non-repudiation assist in combating these threats.

This Technology Guide is intended to summarize the latest technical specifications outlined by CableLabs, a consortium of cable industry vendors and service providers, addressing security in data over cable standards. It covers the security requirements in:

- Data Over Cable Services Interface Specification (DOCSIS) 1.0 Baseline Privacy Interface (BPI) (SP-BPI-I02-990319).
- DOCSIS 1.1 BPI+ (SP-BPI+-I06-001215).

This Guide is intended to introduce readers to the security specifications outlined within DOCSIS. It is not intended to act as a definitive guide to DOCSIS security, but as a quick reference or starting point.

What are the Security Risks?

Every network has the potential to expose its users to tremendous risks. The following section will describe some of the security vulnerabilities inherent in the broadband cable network which expose subscribers and multiple system operators (MSOs) to unnecessary risks.

Table 1: Security Vulnerabilities in Broadband Cable Networks

SECURITY RISKS	WHO IS AT RISK?	HOW TO PROTECT
Eavesdropping	Subscriber	Data confidentiality using encryption
Network-based attacks • Masquerading attacks • Denial of service attacks • Replay attacks	Subscriber and MSO	Authentication of network devices and traffic encryption
Device Cloning	Subscriber and MSO	Authentication of device using digital certificates and RSA key pairs
Theft of services	Subscriber and MSO	Authentication of device using digital certificates and RSA key pairs
Rogue Software Updates	Subscriber and MSO	Data integrity using digital signatures applied to software updates

Securing Data

Attaching a computer to the Internet is like living in a city. There is much to gain in terms of the wealth of information, however, there are also risks associated with having a direct ramp onto a global information highway.

Cable data services are a public network with each subscriber receiving a fixed IP address. Consequently, subscribers are exposed to typical open network security breaches experienced on public networks like the Internet, or local area networks (LANs). One of the biggest risks is the protection of data. Because the cable network is a

public network made up of data packets being transferred over shared media, unprotected data in transit can easily be exposed. For instance, subscribers using the cable network to access their corporate email can expose important company confidential and proprietary information sitting behind their employer's firewall. The need for virtual private networks (VPN) is paramount.

A VPN is a private network which runs on top of a public network, most commonly the Internet, but a VPN can securely connect any two points on the network by encrypting the traffic flowing between them. Encryption is the first step in data protection. In the cable network, information flowing between the cable modem (CM) and the cable modem termination system (CMTS) can be protected this way. The security standards and protocols in DOCSIS standards enable virtual private networking (VPN) and higher levels of baseline privacy for increased data security protection for subscribers and MSOs.

Protection Against Network Attacks

Hackers need to know the Internet address of the target system before they can launch an attack. If a hacker can obtain the name and address of the targeted host system, he or she can then begin sending network traffic to that host in order to pry it open and gain unauthorized access. DOCSIS standards therefore employ similar policing functions (filtering) available in remote access servers from traditional line network service providers to hide network addresses and protect subscribers. Three of the most common network attacks are the denial of service (DoS), denial of availability (DoA), and man-in-the-middle attacks.

Denial of Service and Denial of Availability Attacks

Information that is unavailable when required is of no use, even if secured. An effective DoS or DoA attack can take out services for a matter of minutes, hours, or days. On the Internet, DoS attacks are highly publicized and many popular online shopping and trading sites like Amazon.com and Yahoo! have been affected. While DoS attacks can be costly to businesses, they also impact consumer confidence. The ramifications for cable networks' subscribers could be disastrous. Subscribers who fear that their cable network services will be easily interrupted will not want to network their PC, Cable/TV, and/or other services or appliances to the cable network. In a DoS attack against an MSO, services like television, Internet access, and even telephone services could be taken down, leaving subscribers helpless.

But, DoA attacks are not inherent only to the Internet. Any computer network is susceptible, even one of the most reliable networks in the world, the US telephone system, or the Public Switched Telephone Network (PSTN). In a publicized case, the AT&T long-distance network began to falter and within minutes on January 15, 1990 more than half of all calls being attempted by AT&T customers were answered by a recorded message informing them that, "All circuits are busy. Please try again later." Not until 11:30 P.M., some nine hours later were services available. The economic consequences were significant. AT&T estimates the company lost $75 million dollars in lost calls alone. And, this is not an isolated case, it is estimated that many others have lost millions of dollars to DoA.

As services like cable, telephone, and Internet begin to merge onto one network and become linked with the networked world of general computer systems, the DoS and DoA attacks could target the MSO or cable subscriber and should be expected if no measure of protection is taken.

Device Cloning and Man-in-the-Middle Attacks

Device cloning and man-in-the-middle attacks occur when an intruder clones another subscriber's modem so that the MSO believes they are the same subscriber. In the digital world this is analogous to stealing someone's identity. Once the modem or CMTS is cloned, the intruder is believed to be something which they are not and can launch an attack such as a DoS or DoA because the other devices on the network trust the rogue device. This could amount to stealing cable services, or stealing information from subscribers who trust a cloned or rogue CM or CMTS.

Stealing Services—Economic Impacts

Fraud and theft of services pose serious economic threats for cable operators and their subscribers. It is estimated that computer crime in general may be costing the economy as much as $50 billion dollars annually. The Computer Security Institute and the Federal Bureau of Investigation polled 273 organizations in 2000 who cumulatively reported financial losses as high as $265 million attributable to computer hackers and unauthorized access into their computer networks. The temptation to steal services is great and the need for data protection and strong authentication of users and networked devices should not be underestimated. These two simple steps combined would deter the majority of the crime and could potentially save industries like the cable industry billions of dollars.

Conclusion

Cable networks need highly reliable security solutions which protect subscribers and MSOs from common network attacks. The incentives to steal services, data and subscribers' identities is great and could be disastrous. Cable security standards like DOCSIS take steps to secure the cable broadband network from the greatest risks posed by the inherent network vulnerabilities that exist today. These security measures should be adopted and implemented quickly.

DOCSIS 1.0 and 1.1 Overview

Using the latest in Public Key Infrastructure (PKI) techniques and technologies, the DOCSIS standards protect subscribers and MSOs against common network security vulnerabilities by creating the foundation for virtual private networks (VPN). This is accomplished by:

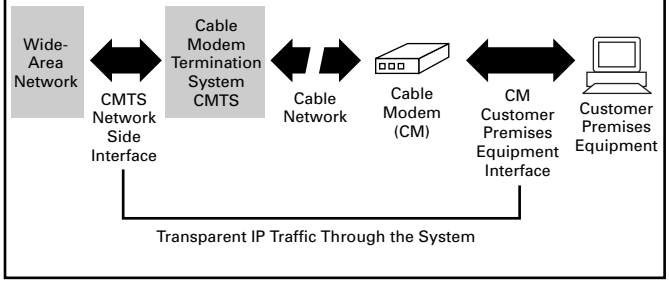
- Securing the transmission of data flowing across the public cable network.
- Authenticating the cable modem that attaches to the public cable network.

Both VPNs and PKIs are common to securing computer networks like the Internet. The following sections will summarize how the DOCSIS 1.0 and DOCSIS 1.1 standards protect cable networks using the same principles that have been developed to secure electronic commerce and remote access over untrusted, public networks.

DOCSIS 1.0 Securing Data on the Cable Network

DOCSIS 1.0 data transport security provides cable modem subscribers with data privacy across the cable network by encrypting the traffic flowing between the CM and the CMTS, essentially creating a VPN.

Figure 1: DOCSIS Security Architecture



In addition, DOCSIS security begins to protect cable operators from theft of service by adding authentication protocols using encryption keys directly in the modem. This way the cable operator knows the subscriber is legitimate. However, this approach is still susceptible to "device cloning," since there is nothing binding the authentication information to the encryption keys.

Therefore, the DOCSIS standard:

1. Prevents unauthorized access to data transport services by enforcing encryption of traffic across the cable network.
2. Addresses theft of service concerns by authenticating each cable modem and thereby binds the cable modem to a paying subscriber who is authorized to access particular services.

DOCSIS 1.0 data transport security protocol has two components:

- An encapsulation protocol for encrypting packet data across the cable network.
- A key management protocol for providing the secure distribution of keys between the CMTS and client CMs.

The encapsulation protocol defines the frame format for carrying encrypted packet data within DOCSIS Media Access Control (MAC) frames, the set of supported data encryption and authentication algorithms and rules for applying the cryptographic algorithms to a DOCSIS MAC frame's packet data. DOCSIS 1.0 employs the Cipher Block Chaining (CBC) mode of the US Data Encryption Standard (DES) to encrypt a DOCSIS MAC Frame's packet data.

The Baseline Privacy Key Management (BPKM) protocol running between the CM and CMTS allows the CM to obtain authorization and traffic keying material from the CMTS. BPKM uses public-key encryption to securely transmit keying material between the CMTS and CM. Each cable modem must contain a key pair specifically for this purpose.

DOCSIS 1.0 data transport security provides a level of privacy across the shared-medium cable network equal to or better than that provided by dedicated-line network access services (e.g. telephone, ISDN or DSL). It should be noted, however, that these security services apply only to the access network. Once traffic makes its way from the access network onto the Internet backbone it will be subject to privacy threats common to all traffic traveling across the Internet, regardless of how it got onto the Internet.

A DOCSIS 1.0 compliant CMTS authenticates a cable modem using the IEEE MAC address associated with that cable modem. The current DOCSIS 1.1 BPI+ specification considers this to be a weak authentication scheme.

DOCSIS 1.1—Technical Requirements for a PKI

DOCSIS 1.1 BPI+ improves the encryption and authentication mechanisms present in DOCSIS 1.0. BPI+ mandates the use of triple-DES, in lieu of DES, for significantly stronger traffic encryption. BPI+ was also designed with extensibility in mind, and may be extended to support different encryption ciphers like the Advanced Encryption Standard (AES) without a redesign.

DOCSIS 1.0 BPI provides limited authentication of a cable modem to a CMTS (based on the CM's

IEEE MAC address). DOCSIS 1.1 BPI+, on the other hand, strengthens the authentication process by adding digital-certificate-based authentication to its Baseline Privacy Key Management (BPKM) protocol. A BPI+ CMTS requires each CM to provide a unique X.509 certificate with every initial authorization request. The CMTS distributes keying material (i.e., an authorization key) based on successful verification of the CMs certificate. Once the CM certificate has been verified, the CMTS encrypts the authorization key using the corresponding public key, and returns it to the requesting CM. CM certificates are never renewed, and must have a validity period longer than the anticipated lifetime of the cable modem.

According to DOCSIS 1.1 BPI+, each cable modem must contain a 1,024-bit key pair along with a properly signed X.509 digital certificate. The manufacturer is given the following options:

1. Install the key pair and certificate during the manufacturing process, or
2. Generate the key pair and request a certificate after deployment of the cable modem into the field.

The second option requires the cable modem to contain all the necessary algorithms for key pair generation and certificate request creation. In practice, the key pair and certificate are most frequently installed during manufacturing to eliminate the need for additional algorithm support on the cable modem and to improve the security of the certification process.

Included in DOCSIS 1.1, but absent in DOCSIS 1.0, is a true certificate hierarchy for implementing PKI. The three-level hierarchy consists of a DOCSIS Root Certification Authority (CA) belonging to CableLabs, subordinate manufacturer CAs, and CM certificates. The DOCSIS Root CA uses its certificate to sign each manufacturer's CA certificate. These manufacturer CA certificates are then used to sign the certificates for each CM produced by that manufacturer, completing the trust chain.

The final security feature added by DOCSIS 1.1 is the use of secure software upgrades. Each manufacturer and MSO can digitally sign code updates destined for subscriber cable modems. A cable modem will not install a code update unless it can verify the signature, and trusts the manufacturer and/or MSO. This capability provides dramatic cost savings to the MSOs & manufacturers and ease of use benefits to the consumers, since installing new software in the cable modem can now be securely handled automatically and controlled remotely.

Requirements—DOCSIS 1.0 and DOCSIS 1.1

The following section outlines the security requirements in DOCSIS 1.0 and DOCSIS 1.1 to serve as a quick reference guide for modem manufacturers needing:

- To become DOCSIS 1.0 compliant
- To become DOCSIS 1.1 compliant
- To upgrade from DOCSIS 1.0 to DOCSIS 1.1

It also illustrates the DOCSIS 1.1 features required of MSOs.

The following tables divide DOCSIS security requirements into the following categories:

General Security Requirements for Cable Modem and CMTS Manufacturers

DOCSIS 1.0 and DOCSIS 1.1 security algorithms and protocols associated with the CM and/or CMTS

- Encryption algorithms
- Message authentication algorithms
- Authentication

DOCSIS 1.1 security algorithms and protocols associated with the CM

- Secure Code Updates
- Federal Information Processing Standard (FIPS) 140-1 compliance

General Security Requirements for CM and CMTS Manufacturers and MSOs:

DOCSIS 1.1 requirements:

- Public Key Infrastructure (PKI)
- Secure Code Updates

Table 2: General Security Requirements Cable Modem and CMTS Manufactures

SECURITY REQUIREMENTS	DOCSIS 1.0	DOCSIS 1.1
Security Protocols		
Encryption Algorithms	Key Encryption Key (KEK) is a DES encryption key used by a CMTS to encrypt Traffic Encryption Keys (TEKs) sent to a CM from a CMTS.	Key Encryption Key (KEK) is two-key triple DES encryption key used by CMTS to encrypt Traffic Encryption Keys (TEKs) sent to a modem from a CMTS.
	TEK in key reply is DES (Electronic Codebook or ECB mode) encrypted using a KEK.	TEK in key reply is triple DES (encrypt-decrypt-encrypt or EDE mode) encrypted using a KEK.
	Supports only 40- and 56-bit DES encryption algorithms with no data authentication algorithm	Adds security capabilities selection (Section 4.1.1.2 of BPI+ specification). CM passes supported cryptographic suites (data encryption and authentication algorithm) to CMTS during the BPI+ authorization exchange. The CMTS chooses the preferred suite, and identifies this suite in an Authorization Reply. Although only 40- and 56-bit DES are currently supported in the specification, this leaves room to support future enhancements.
Message Authentication Algorithms[2]	(Section 4.1.1.2 of BPI+ xskeyed HMAC digest for Key Requests. CMTS—HMAC-MD5 and HMAC-SHA1	No change.
Key Length	Contains key pair with 768-bit modulus.	Contains key pair with 1024-bit modulus.
Authentication	Weak cable modem authentication using IEEE-MAC address of CM. CM sends MAC address and public key to CMTS in an Authorization Request messages.	Strong authentication within key management protocol uses X.509 v3 digital certificates. All Authentication Requests sent from CM to CMTS contain the CM's X.509 certificate. The certificate is issued by a manufacturer CA during production, and contains the public key of the CM along with other identifying information (CM MAC address, serial number, and manufacturer ID).
FIPS 140-1 Security Level 1	No formal support for physical protection of keys within CM and CMTS.	Use of FIPS-140-1 for physical protection of keys within CM and CMTS—deters physical access to key pair.
Secure Code Updates		
	CM capable of receiving code updates. However, there is no authentication of the source of the code update.	Signed code updates—both manufacturer and MSO may sign updates; CM must have support for PKCS#7 to unwrap and verify the signature attached to the PKCS#7 message containing

Table 3: General Security Requirements for Manufacturers and MSOs

SECURITY REQUIREMENTS	DOCSIS 1.0	DOCSIS 1.1
PKI Infrastructure		
	No PKI support.	Full PKI hierarchy and use of X.509 v3 certificates. • DOCSIS Root CA signs manufacturer CA certificate; manufacturer signs each CM certificate. • CMTS parses and verifies CM certificate.
Certificate Authority		
		Certificate issued by DOCSIS Root must contain a signature with a key modulus length of at least 1024-bit and no larger than 2048-bit.
Secure Code Updates		
	No formal security requirements for code updates	Requires use of signed code updates. A manufacturer must sign all code updates distributed to MSOs or directly to CMs. An MSO may optionally sign the code update before pushing the software to subscribers' CMs.

Options for the Modem Manufacturer

Modem manufactures want DOCSIS services that make securing the modem a simple, cost-effective task, so that modems are DOCSIS-compliant quickly with little impact to modem development schedules.

To meet DOCSIS standards, modem manufacturers will need to implement:

- Strong encryption
- Public key cryptography
- Digital certificate management

They will also need to generate a large number of cryptographic keys and corresponding digital certificates and "burn" these credentials directly into the write-once flash memory of cable modem devices on the assembly line. The certificates embedded in the modem must be able to chain up to the DOCSIS "Root CA" at the top of the DOCSIS trust hierarchy to ensure compatibility with multiple DOCSIS cable system vendors. In addition, certificates must conform to the DOCSIS-mandated 20-year certificate life span which frees manufacturers from needing to deal with certificate renewals.

Currently, there are three ways for the cable modem manufacturer to achieve this:

- Buy some or all of the security software needed to become DOCSIS-compliant.
- Outsource some or all of the security software to third parties and then embed these components into the modem.
- Build their own versions of DOCSIS security software.

In this section, we explore these options and outline the important factors the modem manufacturer must consider to become DOCSIS-compliant quickly, easily and cost-effectively. These factors are summarized in Table 4.

Table 4: Options for the Manufacturer

OPTIONS	COSTS AND SECURITY RISKS	BENEFITS
OPTION ONE: License DOCSIS security from a provider: • Security software • In-house CA	• License fees, royalties, and maintenance fees on software. • Cost to adapt and integrate software into modem • Cost to maintain system and network for CA server (minimal).	• Usually most competitive pricing in terms of TCO. • More control over security—manufacturer controls key generation. • More secure—no transport across networks (private keys should never be far away from their "owners"—in this case, the modems). • Products often customized to particular manufacturing environment. • Easier to port to the modem manufacturer's unique micro-processing environment. • Allows engineers to focus on core expertise. • Eliminates the risks and difficulty of implementing cryptography to secure PKI and VPNs at the network level.
OPTION TWO: Outsource to a third party • License security software • Outsourced CA	• Most expensive, priced a-la carte. • License fees, royalties on software. • Cost to adapt and integrate software into modem. • Cost to purchase keys and certificates • Cost to house keys and certificates in internal database for later use. • Less secure (third party generates keys and transports certificates over public network). • Less control of security in manufacturing environment. • Process is owned by the third party vendor, not the manufacturer—may be more time-consuming and less secure. • Often only a short-term solution.	• Frees manufacturer from having to manage their own equipment and software. • Maintenance fees of CA included in price. • Responsibility and accountability for compliance is managed by the third party.
OPTION THREE: Build your own DOCSIS security	• Time-consuming and difficult for modem manufacturers without PKI or cryptography expertise. • Takes engineers away from their core competencies. • Often requires manufacturer to rely on open-source where the code is difficult to embed in devices, difficult to port, insecure & untrusted and unsupported. • All accountability resides with the manufacturer in terms of schedules, quality, support, and ongoing maintenance.	• No licensing or royalty fees.

Option One: Own DOCSIS Security Components

Many modem manufacturers want to own their own security components. Because modem manufacturers are working in extremely competitive situations, many are not looking to re-invent the wheel. They want products and solutions from experienced vendors with expertise in embedding security in constrained devices and unique manufacturing environments. They are looking for security solutions which give them a competitive advantage.

Option one allows the cable modem manufactures to embed DOCSIS security directly into modems within their own manufacturing environment so that the modem manufacturer can:

- Embed DOCSIS 1.1 security software into the CM or CMTS.
- Run their own Certification Authority (CA) so that manufacturers can build trust in at the point of manufacture and complete the DOCSIS trust chain.
- License the source code for the security components for easy integration into the manufacturer's unique environment and porting to the specific micro-processing environment.
- Have more control over security since keys are generated directly at the modem.

While each modem manufacturer has different skill sets and requirements, licensing third party DOCSIS security components allows manufacturers to focus on their value-add, differentiation and benefit from the competitive advantage of getting to market faster. It also places the burden on someone other than the manufacturer to ensure timeliness, quality and support.

Option Two: Outsource Security to a Third Party

Option two is really a hybrid solution in which the modem manufacturer must rely on a trusted PKI provider with the capability to securely create key pairs and certificates and distribute them to the manufacturer. The manufacturer must then maintain a database of these key pairs and certificates and deploy software to embed them into the modem. Here is a scenario of how this commonly works:

1. The modem manufacturer creates a MAC address file, containing the necessary identifying information about the cable modems requiring certificates.
2. The modem manufacturer then sends the MAC file to a PKI service provider.
3. The PKI service provider generates key pairs and certificates using a bulk-generation system and inserts the certificates and their private keys into batch file.
4. The batch file is encrypted, usually with a single key, for all certificates.
5. The modem manufacturer downloads the batch file of certificates.
6. The modem manufacturer decrypts the batch file and loads the keys and certificates into a local database for retrieval later during modem manufacture.
7. The modem manufacturer's manufacturing system retrieves the certificates and private keys from the database and inserts them into the cable modems as they are manufactured.

Outsourcing is often an appealing solution for companies with little experience building-in key security features like digital certificate management, PKI, or implementing DOCSIS-compliant encryption technologies like 3DES. Often, however, outsourcing is only a short-term solution for manufacturers who realize that it is not flexible enough to their manufacturing environment and much more costly than managing the key security functionality themselves. It is also subject to the availabilities, response times, rules, and quality characteristics of the outsourcers.

When outsourcing, manufacturers must take greater steps to ensure that the certificates and keys they receive are indeed from a trusted third party and have not been compromised and are indeed interoperable in a multiple CA environment. Since the private keys are generated far away from their owners (the cable modems themselves) and must go through several network hops before arriving at the modem, they are also more susceptible to compromise than when they are created in-house at the manufacturing station.

Option Three: Build Your Own DOCSIS Security

While in the minority, some modem manufacturers attempt to build their own DOCSIS compliant security features. This option is often risky and time-consuming and always incurs hidden costs in delayed development cycles and long-term commitments to maintenance updates. Modem manufacturers who are considering the building of their own DOCSIS security systems should be aware of the complexities and costs of network security. Unfortunately, it is often the complexity, level of difficulty, and unnecessary risk involved which is overlooked when a manufacturer takes the build option.

How important is the security implementation?

A recent example of a build-it-yourself security disaster is the recent hole exposed in the IEEE 802.11b network. IEEE 802.11b is a networking protocol for wireless LAN operation allowing laptops to communicate wirelessly to base stations within a 150 ft radius. The networking issues in IEEE 802.11b are analogous to the security concerns of the cable broadband network, however, implemented with different security protocols.

In Feb 8, 2001, The Industry Standard and other publications broke a story exposing the hole in the IEEE 802.11b Wireless LAN protocol stating:

"The engineers who designed the security for this type of wireless network considered the risks, say the Berkley researchers, but they didn't implement the encryption correctly. The protocol's problems are a result of misunderstanding of some cryptographic primitives and therefore combining them in insecure ways'. In other words they should have checked with the experts".

This hole in the IEEE 802.11b protocol is a result of the researchers breaking the WEP (Wired Equivalent Privacy) algorithm which can now be exposed with inexpensive off-the-shelf equipment.

Conclusion

Because millions of DOCSIS compliant cable modems will soon be manufactured, the costs of outsourcing this function may not be effective to many modem manufacturers. Outsourcing also has inherent security vulnerabilities insofar as the private keys are not kept closely with the modems. In addition, outsourcing subjects the manufacturer to the discretion of the outsourcer for critical operational requirements. CM manufacturers should also be advised of the risks of building their own security systems in an effort to comply with the DOCSIS standards. The advantages of self-built security very rarely outweigh the risks and/or the costs.

Many manufacturers are currently looking for ways to in-source and manage DOCSIS security as a way of reducing per modem costs. They are also interested in maintaining their own security systems, provided by expert vendors, because of the competitive advantages offered.

Broadband Security Solutions

Cable modem manufacturers face a unique set of challenges in adhering to the security requirements of DOCSIS 1.1 and require end-to-end security solutions, which allow them to scale to DOCSIS standards quickly and cost-effectively. Today, there are commercially available products that are available for modem manufacturers needing to comply with the security requirements found in the DOCSIS 1.1 standard.

Table 5 outlines some of the needs of the modem manufacturers as they begin to "lock-down" modems against the serious security vulnerabilities that put both cable subscribers and MSOs at risk.

Figure 2: Headend or Distribution Hub

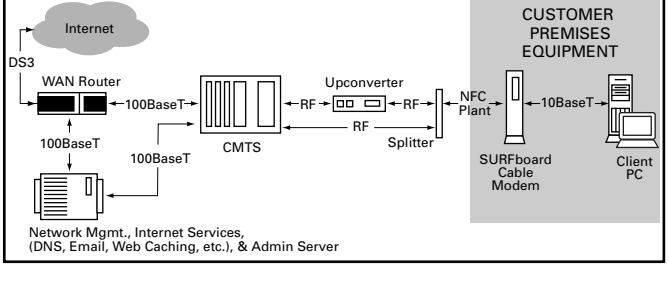


Table 5: Commercially Available Security Products

SECURITY RISKS	HOW TO PROTECT WITH OFF-THE-SHELF PRODUCTS	NEEDS OF THE MODEM MANUFACTURER
Device Cloning Stealing services IP attacks: Man-in-the middle Denial of Service attacks Data Protection	Software Development Kit that provides the strong cryptography certificate handling required by DOCSIS 1.1 standard	• All crypto and PKI functionality designed for modem manufacturers to meet DOCSIS 1.1 standards • High performing crypotography • Security software that fits into embedded devices with small memory and low code footprint • "Bullet-proof security": established track record of impenetrable security tools • Ability to cost-effectively add DOCSIS 1.1 security to modems
	DOCSIS CA	• Flexible and designed to meet the authentication needs of the modem manufacturer • Scalable—manufacturer owns CA, complete control of security • Increase production of modems with lower marginal cost per certificate
Rogue software updates	PKCS#7 Signing Software	• Fast, secure and cost-effective ways to distribute code updates to authenticated subscribers

DOCSIS 1.1 Security Protocols and Secure Code Updates

Manufacturers are looking for software products that deliver everything their developers needs to embed DOCSIS 1.1 security protocols into the cable modem or cable modem termination station (CMTS). Manufacturers should look for security products that have a reputation for providing "bullet-proof" security solutions, interoperable and customized to the needs of the broadband cable industry. Products built on open standards will be more accommodating and allow faster compliance to future cable industry developments.

Why are manufacturers buying DOCSIS 1.1 solutions?

- Enabling compliance by reducing risk in development
- DOCSIS 1.1 solutions work whether the manufacturers need to in-source or outsource security
- Industry participation to develop cable security standards for the future

DOCSIS Compliant Certificate Authority (CA)

Manufacturers need secure ways to generate keys within their manufacturing facility so that key pairs and certificates can be embedded directly into the modem. However, they should also look for CA certificates that are interoperable, or able to chain up to the CableLabs DOCSIS root CA, so that trust domains are created which interoperate across the entire cable industry.

Conclusion

Manufacturers need quick and easy ways to become DOCSIS 1.1 compliant today, as well as have the flexibility to evolve to new data cable standards. Manufacturers should look for product and service offerings, which allow them to reduce the costs of producing secure modems without sacrificing quality or security. Today, security software products allowing manufacturers to own their own security components will allow manufacturers to reduce the cost of DOCSIS 1.1-compliant modems and upgrade to future specifications quickly.

Coresma

Coresma, a developer of technologies designed to enhance broadband communications over multiple network environments, is dedicated to introducing innovative new products that provide consumers with "always on" modem service. To accomplish this, Coresma needed to closely follow the CableLabs Certified Cable Modem specification (formerly known as DOCSIS), which defines interface requirements for cable modems involved in high-speed data distribution over cable television system networks.

The Problem: Cost-Effectively Staying Abreast of Market Specifications

In adhering to the CableLabs specification, Coresma needed not only to follow stringent security guidelines, but also to introduce an open-standards solution to the market. In exchange, CableLabs would provide Coresma's products with their highly coveted seal of approval.

However, the company was faced with a second compelling factor, the ability to implement a high degree of security at a reasonable cost. This was imperative since Coresma's products are targeted at consumers and the company's intent is to reach the price-conscious consumer market on a mass scale.

Enabling Innovative Technology

Coresma's mission was to provide innovative modem solutions that will make a significant impact on the consumer cable market. As part of this objective, the company needed to incorporate industry-leading security into its products. By leveraging the best security technology available, Coresma would be in a position to gain instant credibility with its products' encryption and decryption capabilities. As a result, Coresma selected to partner with RSA Security and employ its RSA BSAFE software.

The Solution: Secured Host-Based Modems

By partnering with RSA Security, Coresma was able to meet all of its specifications and introduced the Coresma CICM 6001RD, one of the industry's first host-based cable modems. Designed for makers of set-top boxes, home-gateways, and Internet-appliances, this solution was ideal for a range of consumer services, including fast, continuous Internet access.

> *"We are pleased to partner with RSA Security, and believe strongly that our joint dedication to innovation and quality will play an important role in furthering CableLabs compliance to enable cable industry expansion. We will continue to work closely with RSA Security, and look forward to offering our customers with RSA Security's certificate capabilities."*
>
> Marius Gafen, Director of Product Management at Coresma.

Built around its own chipset with a minimal number of additional components, the CICM 6001RD was launched as a fully operational, host-based, internal CableLabs 1.1-based cable modem. This reference design proved the Coresma 6001's capability as the main component for building low-cost, high-performance CableLabs-based devices.

In addition, because Coresma' 6001 modem relied on a host processor for real-time functions it was designed for low-cost implementations. It also boasted a high-performance architecture that used typically less than 1/2 percent of the host processor computing resources.

Critical to this low-cost and high-functionality is security. In today's demanding environment, consumers will accept nothing less than the most stringent protection. RSA Security software provided Coresma with instant credibility with its original equipment manufacturer partners. As a result, Coresma is able to more easily promote its new

business model for Internet communication.

RSA Security software allows Coresma's manufacturer customers to offer cable companies all of the encryption and certificate-based security they require to prevent fraud or tampering. At the same time, cable companies can offer host modems at a low cost—from $99 to $149—without tapping into company revenue.

Helping to Enable Cable Industry Expansion

Introducing innovative new solutions requires careful attention to detail, as well as a strong commitment to quality and reliability. Coresma worked hard to combine the perfect combination of resources—its own technical vision and expertise with the leader in security software. This partnership adds up to a highly flexible and unique solution—that is completely safe from tampering or fraud. It also provides manufactures with a low cost, reliable solution that is ideal for targeting the consumer market.

1. Sniffing is the process of capturing data packets as they pass across a network adapter interface. Captured data is usually stored for offline analysis. Typically this is how an attacker would eavesdrop on the communication of other users within the same network segment.

2. Message authentication algorithms are used to establish data integrity.

This Technology Guide is one in an ongoing series of over 100 solutions-focused Guides. These Guides assist IT professionals in making informed business decisions about specific aspects of technology development and strategic deployment.

The Technology Guide Series® offers a broad array of titles, each presenting objective information and practical guidance in a non-biased, "easy-to-understand" style and tone. Our editorial writing team has many years of experience in IT and communications technologies, and is highly conversant in today's emerging technologies.

The Technology Guide Series and techguide.com are supported by a consortium of leading technology providers. The Sponsor has lent its support to produce and publish this Guide.

This Guide, as well as the entire Technology Guide Series, is made available to view and print at no charge by visiting techguide.com.

Over 100 Technology Guides in the following categories:

- Software Applications
- Network Management
- Enterprise Solutions
- Network Technology
- Telecommunications
- Convergence/CTI
- Internet
- Security

produced and published by

techguide.com