SECURITY FOR NEXT GENERATION ACCESS NETWORKS

Stephen Thomas
Wave7 Optics

Abstract

Broadband access networks—including those built with advanced HFC, wireless, and fiber technologies—have unique network security concerns. This paper analyzes the security threats present in such networks, and it develops a general security threat model for broadband access networks. Significant threats include masquerade and eavesdropping.

The paper then examines cryptographic techniques appropriate for countering these threats, focusing on authentication and encryption. It considers the strengths and costs of various alternatives. The final section discusses practical implementation issues, particularly those that arise because of the potential size of access networks and because of the data rates at which they operate. These characteristics demand security measures that are very scalable and capable of very high speed operation.

Security Threats

Like any other network infrastructure, broadband access networks face an array of threats to their correct operation. Malicious parties may attempt to steal service; they may try to deny service to legitimate users, and they may attempt to compromise the confidentiality of network users. Compounding these traditional security threats, access networks face a unique and challenging problem: customer premise equipment.

Unlike enterprise and backbone networks, significant components of the access network are not under the physical control of the network operator. In fact, customers, who may have easy physical access to these network elements, may well be the most likely attackers. This situation exacerbates two broad security threats, masquerade and eavesdropping.

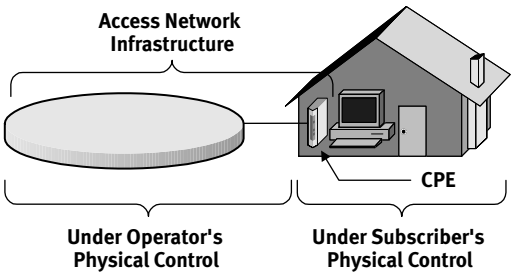

Figure 1 CPE is not controlled by operator.

Masquerade

In most communication networks, especially those provided as a commercial service, the operator must know the identity of its users. Collecting revenue, for example, usually depends on knowing who to bill. When attackers masquerade, they disguise this very information.

> ***masquerade**: The pretense by an entity to be a different entity in order to gain unauthorized access.*[1]

Customer premise equipment can make the threat of masquerade particularly acute. The equipment is sitting inside (or just outside) the potential attacker's home, waiting to be reverse-engineered, modified, or even relocated. Some may find the temptation irresistible. "For instance, right now you can type in 'TiVo hack' on Google, and you'll get a thousand sites of hard drives that are compromised at the user's premises.'[2]

Successful masquerades can have many consequences. Attackers may pirate

service by pretending to be a legitimate user, or they may intercept key exchange messages so as to decipher encrypted communications. Masquerade is also one step in a more wide-scale attack such as device cloning.

Eavesdropping

Customers of communication networks often presume that the information they exchange using those networks remains confidential. Attackers that eavesdrop compromise that confidentiality.

> ***eavesdropping**: The unauthorized interception of information-bearing emanations.*[1]

Access customers are often particularly sensitive about their privacy. Customers have objected strenuously when the network operator has apparently violated their privacy,[3] even to the point of involving senior members of the US Congress.[4] The expected repercussions would be significantly more severe if private information was exposed to an unauthorized third party.

On most access networks, customer premise equipment heightens the threat of eavesdropping. Access networks frequently rely on shared media, where the physical media for information transfer—coaxial cable, fiber optics, or wireless spectrum—is shared by many users. This characteristic means that information transmitted to one user is inherently available for reception by other users. In fact, with early cable modem deployments, it was quite easy to eavesdrop on your neighbor unintentionally.[5]

Countermeasures

Fortunately, the science of cryptography has developed countermeasures to combat these security threats. Authentication protects against masquerade, and encryption can prevent eavesdropping.

Authentication

Authentication protects access networks against masquerade attacks by giving users or devices a way to prove their identity.

> ***authentication**: A security measure designed to protect a communications system against acceptance of a fraudulent transmission or simulation by establishing the validity of a transmission, message, or originator.*[1]

In access networks, authentication allows *untrusted* network elements, such as customer premise equipment, to prove their identities to *trusted* equipment physically controlled by the network operator. Table **1** lists the trusted and untrusted elements for common access network technologies.

Table 1 Parties to Authentication

	Trusted	Untrusted
HFC	CMTS	Cable Modem
802.11	Access Point	Wireless Client
PON	OLT	ONU

To prove their identities, untrusted elements demonstrate their knowledge of a secret value. The most straightforward approach relies on a shared secret such as a password. The trusted element knows the passwords of elements that it must authenticate; the authentication process requires that untrusted elements prove they know the same shared secret.

One obvious way to authenticate using shared secrets is for the untrusted element to simply send the password to the trusted element, as in figure 2. A disadvantage to this approach is that the shared secret is transmitted, in the clear, across the access network. If an adversary can intercept those communications, the adversary can learn the shared secret and impersonate the untrusted element.

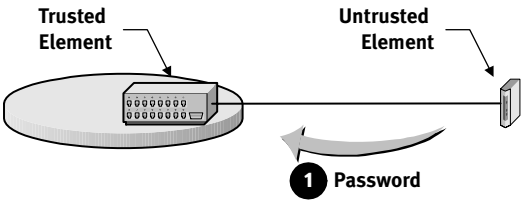

Figure 2 Simple password authentication.

Fortunately, there are simple cryptographic techniques that can significantly improve the security of shared secret authentication. A common approach relies on special mathematical functions known as *hash functions* or *message digests*. A message digest is a one-way function: it is easy to compute but extremely difficult to reverse. For example, figure 3 shows the result of computing the Secure Hash Algorithm[6] on a block of input data. The mathematical properties of the algorithm are such that, given only the output from figure 3, an adversary cannot deduce any information about the original input.

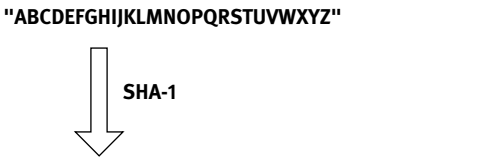

Figure 3 A message digest algorithm.

Figure 4 illustrates how message digests improve the security of authentication exchanges. Both the trusted and untrusted elements share a secret, but the value of that secret never crosses the access network. Instead, the trusted element sends the untrusted element a *challenge*. The untrusted element combines that challenge with the shared secret and computes the message digest of the combination. It only sends the result of this digest computation across the network. Even if an adversary is able to intercept this message, the adversary will not be able to derive the shared secret.

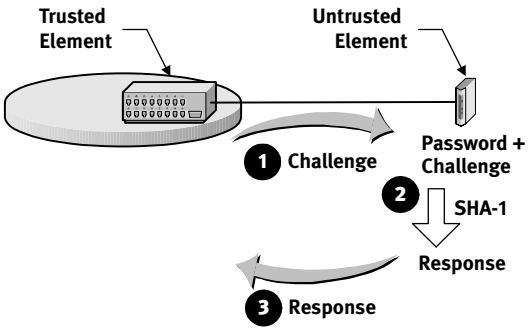

Figure 4 Digest authentication.

Although message digests solve many of the technical security problems with shared secrets, they can't eliminate the operational burden that shared secrets impose. A Hybrid Fiber-Coax (HFC) network serving 100,000 subscribers, for example, would require that the operator maintain 100,000 different shared secrets, provisioning the appropriate values in each Cable Modem Termination System (CMTS), managing additions and deletions, protecting their values from theft, and so on.

Some technologies minimize the operational burden by adopting a common shared secret for all network elements.[7] Although this approach may make operational issues more manageable, it provides substantially less security. With a common secret, the trusted network element cannot verify the individual identity of an untrusted element; *all* the untrusted elements know the secret value. For access networks, this vulnerability may allow one subscriber to impersonate another, an unacceptable deficiency in many environments.

For a more secure approach to the operational problems of shared secrets, access networks can use asymmetric encryption. Asymmetric encryption relies on a pair of related keys. One key, known as the *public key*, can be made public, even to potential attackers. The other *private key* is known by only one party. Asymmetric encryption algorithms use the mathe-

matical properties of these keys so that information enciphered with a public key can only be deciphered with the corresponding private key, and vice versa.

Figure 5 shows a typical authentication sequence based on asymmetric encryption. The very first step is the critical one. In that step the untrusted network element sends its public key to the trusted element. This communication can safely take place even if adversaries are able to intercept it; there is no danger in having an attacker learn a public key.

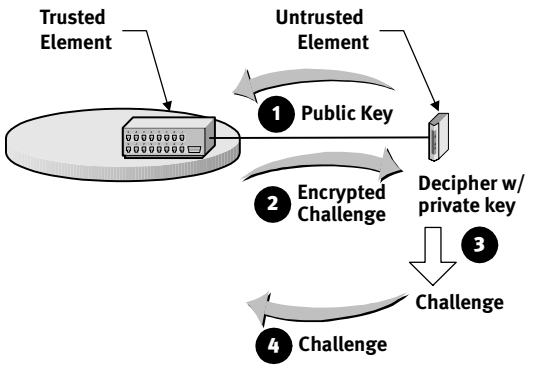

Figure 5 Authentication with public keys.

After the first step, the process is very similar to figure 4. The trusted element generates a random challenge, enciphers that challenge using the public key, and sends the result to the untrusted element. The untrusted element must then decipher the communications to recover the original challenge. Since the untrusted element is the only party that knows the private key, it is the only element that can recover the original challenge. By doing so, and by returning that challenge to the trusted element, it proves possession of that private key.

Even though authentication using asymmetric encryption resembles authentication with message digests, the extra step at the beginning is very significant. With asymmetric encryption the trusted element does not have to know the secret value, it simply learns the public key directly from the element it is authenticating.

Asymmetric encryption does introduce one additional factor in the authentication process. Figure 5 shows how a trusted element can verify that an untrusted element possesses a specific private key (the one corresponding to the exchanged public key). But how does the trusted element ensure that the keys are the right ones? Certificate authorities provide that assurance.

A certificate authority (CA) vouches for the authenticity of a public key. It creates a digital certificate that includes the public key, a distinguishing feature of the party possessing the public key, and the certificate authority's digital signature. As long as the trusted element in the access network believes the CA, it can verify the untrusted element's public key.

Encryption

Although cryptography is often critical to authentication, its more glamorous function is encryption.

> ***encrypt:*** *To convert plain text into unintelligible forms by means of a cryptosystem.* [1]

In access networks, encryption protects against eavesdropping. An attacker may be able to intercept a network's communications, especially if the network relies on a shared media. But if that communications is encrypted, the information content will remain unintelligible to the attacker.

The effectiveness of encryption as a security measure depends on several factors, including the particular cipher algorithm, its implementation, the size of cryptographic keys, and their generation and management. The most common measure of encryption strength is key

size, as measured in bits. Key size allows objective comparisons between different encryption approaches.

In July of 1998, the Electronic Frontier Foundation demonstrated a special-purpose (but relatively inexpensive) hardware system that could exhaustively search for the cryptographic key used to encipher given ciphertext. To demonstrate its effectiveness, the EFF was able to discover a 56-bit key in 56 hours, although a full search of all possible keys would have taken 9 days.[8] Table 2 shows how long that same (1998) technology would take to exhaustively search the key space for various key sizes.

Table 2 Strength of Key Sizes

Key Size	Network	Search Time
24 bits	APON	180 microseconds
40 bits	802.11	12 seconds
56 bits	DOCSIS	9 days
128 bits	*future*	116×10^{18} years

Despite the popular focus on key sizes, most deployed encryption systems are actually broken because of implementation flaws. Those flaws have included poor random number generation,[9] poorly designed algorithms,[10] weakness in how keys are scheduled for use,[11] and weaknesses in how keys are derived.[12] Unfortunately, there is no simple way to assess the strength of these factors in an encryption system prior to actual deployment.

The utility of encryption in an access network link is sometimes questioned because the access network is typically only part of an end-to-end communication path. Users that desire real security will have to adopt their own measures to protect the end-to-end path, and these security measures could potentially make access network encryption redundant. This argument is false. However, because it does not consider all the information that can be obtained through eavesdropping.

Figure 6 shows a typical use of end-to-end encryption: the user is accessing a Web site with the Secure Sockets Layer (SSL) protocol.[13] If the user purchases an item from the Web site, SSL encrypts the contents of the transaction to protect the user's credit card number. The SSL protocol, however, does not obscure the identity of the Web site. The eavesdropper may not be able to intercept the credit card number, but he can certainly discover that the user made some purchase from a specific Web server. Most users would consider that to be a violation of their privacy, and only link encryption within the access network itself can prevent it.

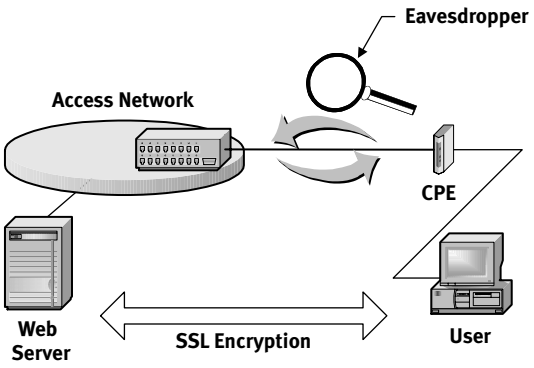

Figure 6 End-to-End Encryption.

Relying exclusively on end-to-end encryption also places a considerable burden on the access network's users. Not only must they employ appropriate security measures themselves, they have to recognize when those measures are needed. The need for security may be obvious in applications such as Web browsing, but it may be quite obscure for services such as the transport of PBX traffic to the operator's central office.

Implementation Issues

The science of cryptography has provided network designers the principle tools required to make access networks secure: authentication and encryption. Ef-

fective engineering of access network security requires applying this cryptographic theory to practical systems. Most implementations rely on combinations of public key based authentication, shared secret authentication, and traditional cryptographic ciphers.

Authentication with Public Keys

Because of the operational burdens that shared secrets impose, authentication based on asymmetric encryption is generally considered the most effective, practical technique for authenticating access devices. Creative attempts to use shared secrets in an access network, including common secrets (e.g. IEEE 802.11) and automatically learned passwords (e.g. ITU G.983[14]) have proven to be ineffective.[11][12]

When implementing public key authentication, network designers must chose an appropriate public key infrastructure (PKI). The important components of a PKI include the particular asymmetric encryption algorithm, the format of public key certificates, and the certificate hierarchy.

The asymmetric encryption algorithm of choice for most applications is the RSA cipher invented by Rivest, Shamir, and Adleman.[15] RSA is the algorithm of choice for Web security[13] and for the Cable Labs Data-Over-Cable Service Interface Specifications (DOCSIS).[16]

Opposition to RSA based on intellectual property concerns were addressed in September of 2000 when RSA Security, Inc. released the technology to the public domain (a few days before their US patents would have expired).[17] The technical merits of other algorithms, such as those based on elliptic curve cryptography (ECC),[18] appear to be limited to special environments not typical to access network. (ECC calculations require substantially fewer computational resources than RSA for equivalent levels of security, but, because authentication in access networks is generally very infrequent, the occasional requirement for lengthy calculations is not normally a problem.)

Public key certificates are almost exclusively formatted according to the ITU's X.509 standard.[19] Most of the recent work on enhancing and extending X.509 has taken place within the Internet Engineering Task Force.[20]

Shared Secret Authentication

One domain in which public key authentication is not effective is authenticating humans. Most people find it very difficult to remember lengthy random numbers, and very few are able to perform the complex calculations of asymmetric encryption. Despite their weakness, passwords have proven to be the most effective authentication tool for human users.

Access networks that need to authenticate individual users as well as customer premise equipment, may use both public key and shared secret authentication. Figure 7, for example, shows a CPE that includes an embedded 802.11 wireless access point.

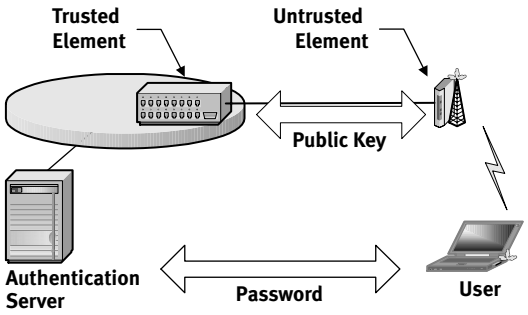

Figure 7 Combined authentication.

The network may use asymmetric encryption to authenticate the CPE and a password to authenticate individual wireless clients that attempt to connect to the access point. Note that the initial version of the IEEE 802 protocol for password-

based authentication, IEEE 802.1.x,[21] has been shown to have significant vulnerabilities.[22]

Ciphers

One of the more interesting challenges facing developers of next generation access networks is the selection of an appropriate encryption algorithm. Clearly, as table 2 demonstrates, the algorithm must be capable of support 128-bit keys, but there are many competent ciphers with that capability. The challenge lies in finding a cipher that can be implemented economically and still operate at the high speeds demanded by next generation networks.

Much of the private sector research into encryption ciphers has focused on algorithms that can be efficiently implemented in software. The data rates of next generation access networks, however, will likely require hardware implementations. Considering the large number of subscribers that a single trusted element may support, efficient hardware implementation is critical for economically viable products.

This problem has led some network technologies to create their own confidentiality algorithms, without the benefit of cryptographic professionals. The results have been predictably poor.[12]

Fortunately, recent cryptographic research has begun to consider hardware implementation efficiency. Table 3, partially adapted from material presented as part of the National Institute for Standards and Technology's competition for the Advanced Encryption Standard,[23] lists representative hardware implementations for a few important ciphers.

The final algorithm in the table, W7, is a byte-wise stream cipher developed specifically for hardware implementation in high speed access networks. It has been published as an Internet Draft.[24]

Table 3 Hardware Implementations

Algorithm	Throughput	Area (gates)
3DES	407 Mbps	148,147
Rijndael	1.95 Gbps	612,834
W7	2 Gbps	20,375

Conclusions

As in all commercial data networks, security is a critical component of next generation access networks. Security for access networks, however, is particularly challenging because of customer premise equipment. The fact that elements of the network may be physically located on the premises of potential attackers requires that network designers take great care in the security of their designs. In particular, access networks must protect against masquerade and eavesdropping attacks. Fortunately, modern cryptography provides the tools necessary to defeat these attacks. Strong authentication, typically based on asymmetric encryption, assures operators of the identity of communicating network elements, and advanced encryption, particularly using ciphers optimized for high speed operation in hardware, prevents eavesdropping.

References

[1] *Telecom Glossary 2000*. American National Standard T1.523-2001.

[2] Michael Lee, Vice President and General Manager of Interactive Services for Rogers Communications, as quoted by James Careless in "Rogers, Bell Canada Square Off," *CED Magazine*, September 2001.

[3] John Rendleman. "Comcast Backs Down Over Privacy Concerns," *Information Week*, 18 February 2002.

[4] Edward J. Markey, Ranking Democrat on the House Subcommittee on Telecommunications and the Internet, in a 13 February 2002 letter to Brian

Roberts, President of Comcast Corporation.

[5] Steve Bass. "Opinion: What Life with a Cable Modem is Really Like." *PC World*, 30 April 1999.

[6] *Secure Hash Standard*. Federal Information Processing Standards Publication 180-1, 17 April 1995.

[7] *IEEE Standard for* Information *Technology—Telecommunications and Information Exchange between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. ANSI/IEEE Standard 802.11, 1999 Edition.

[8] Michael Fitzgerald. "EFF quickly cracks Data Encryption Standard." *PC Week*, 17 July 1998.

[9] Ian Goldberg and David Wagner. "Randomness and the Netscape Browser." Dr. Dobb's Journal, January 1996.

[10] Alex Biryukov, Adi Shamir, and David Wagner. "Real Time Cryptanalysis of A5/1 on a PC." Fast Software Encryption Workshop, April 2000.

[11] Nikita Borisov, Ian Goldberg, and David Wagner. "Intercepting Mobile Communications: The Insecurity of 802.11." *ACM Conference on Mobile Computing and Networking*, July 2001.

[12] Stephen Thomas and David Wagner. "Insecurity in ATM-based Passive Optical networks." *IEEE International Conference on Communications*, April 2002.

[13] Stephen Thomas. *SSL and TLS Essentials: Securing the Web*. John Wiley & Sons, 2000.

[14] *Digital transmission systems —Digital sections and digital line system — Optical line systems for local and access networks — Broadband optical access systems based on Passive Optical Networks (PON)*. ITU specification G.983.1, October 1998.

[15] R. Rivest, A. Shamir, and L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." *Communications of the ACM*, February 1978.

[16] *Data-Over-Cable Service Interface Specifications — Baseline Privacy Plus Interface Specification*. Cable Labs Interim Specification SP-BPI+-I07-010829, 29 August 2001.

[17] George V. Hulme. "RSA's Patent Release will Fuel Security Competition." *Information Week*, 11 September 2000.

[18] A. Menezes. *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, 1993.

[19] *Information Technology — Open Systems Interconnection — The Directory: Authentication Framework*. The International Telecommunications Union Recommendation X.509, August 1997.

[20] http://www.ietf.org/html.charters/pkix-charter.html

[21] *IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control*. IEEE Standard 802.1X-2001.

[22] Arunesh Mishra and William A. Arbaugh. "An Initial Security Analysis of the IEEE 802.1X Standard." University of Maryland Technical Report UMLACS-TR-2002-10, 6 February 2002.

[23] Tetsuya Ichikawa, Tomomi Kasuya, and Mitsuru Matsui. "Hardware Evaluation of the AES Finalists." *Third*

AES Candidate Conference. April 2000.

[24] S. Thomas, D. Anthony, T. Berson, and G. Gong. "The W7 Stream Cipher Algorithm." [draft-thomas-w7cipher-00.txt] October 2001.

Stephen Thomas is the Chief Architect for Wave7 Optics. He can be reached at stephen.thomas@wave7optics.com.