Encrypting ATM Firewall

Abstract
This paper explores the mechanics and policies that are necessary to protect information transmitted over an untrusted high speed wide area ATM network. The network model assumes a set of local area networks that are physically secure, interconnected by an untrusted wide area network. The threat model assumes an outsider threat such that security demands strong encryption of the data as well as access control between the untrusted wide area network and trusted local area networks. This paper details the security assumptions and requirements for this type of network. The paper then presents a set of reference networks and discusses the cryptographic requirements necessary to achieve a high level of information privacy, provide access control, scale efficiently as the network grows in size and speed, and operate transparently to the end user.

Introduction

Motivation
The commercialization of the Internet and the advent of broadband networking technologies have ushered in the “Information Revolution.” As with all advances in information exchange, the benefits of rapid communication also carry the liability associated with security for both the information and the information infrastructure.

With the emergence of broadband services such as Asynchronous Transfer Mode (ATM), the same network can be used for voice, video, data, transaction processing, and a host of other integrated services. These network services provide the means for information exchange. For businesses, this information often represents intellectual property, the “family jewels,” which must be protected.

This paper details a cost effective mechanism for protecting information on high speed ATM networks. It starts with the assumption that information privacy and network access control are the most important elements to security of intellectual property. The second assumption is that the inclusion of security into a network needs to be completely transparent to the end user and compatible with existing switched network services. This means that the addition of privacy and access control must be a seamless overlay on the existing network. For these reasons, any approach that requires private lines, fixed point-to-point connections, manual intervention, or any other changes to the existing network infrastructure is unacceptable.
Scope

The concept of network security means a lot of different things to different people; thus it is important to define the terms associated with security. For our purposes, network security specifically refers to the means to assure privacy of data and to control access from untrusted networks. The term privacy means that data transmitted on an untrusted network provides as little information as possible to unauthorized third parties. Privacy is achieved by encryption of data.

Access control refers to the policy of allowing communication between certain entities and disallowing communication between other entities. This means that access control can be used to prohibit network access between untrusted networks and trusted networks. One of the issues associated with access control is identification of the entities that are providing privacy and access control services. These entities are referred to as cryptographic units. Access control is achieved by requiring that connections between hosts over an untrusted network always go through the cryptographic units. The cryptographic units are responsible for establishing a trusted, secure connection for the hosts. This concept of a trusted connection over an untrusted network is referred to as a security context.

This paper does not address issues such as denial-of-service attacks, malicious attacks by an adversary designed to disrupt service. This paper also does not address the issues of physical security. It is assumed that the cryptographic unit is in a physically secure location. Finally, it is outside the scope of this paper to address the issues associated with insider threats.

Assumptions

Before one designs, builds, and deploys a network security system, it is essential to answer the following questions:

- What information are we trying to protect?
- From whom are we seeking protection?

Deciding what is important to protect and why is the first step in defining a “security perimeter.” Security can be thought of as the concentration of trust. The more people and things that have access to sensitive material, the more difficult it is to secure these materials. Thus, an essential aspect of a security system is defining both the people and equipment that can be trusted with sensitive material.

Deciding what constitutes a security threat is the second part of the equation. The method one uses to protect sensitive material is very dependent on the capabilities and intentions of the adversary. One uses different methods for protection depending on

- Where is the risk perceived? Is the risk internal or external to an organization?
- What is the technical capability of the adversary?
- What is the determination of the adversary, i.e., how much cost and effort is the adversary willing to spend to defeat security measures?

This section discusses a threat model and defines the security perimeter for broadband networks. The threat model and the security perimeter concepts are tightly coupled, so a definition of one of these concepts helps to define the other.
**Threat Model**

The basic assumption of this paper is that the threat to networking security is an outsider threat. In other words, any security breach will occur outside the security perimeter. This outside threat is technically sophisticated with access to the best commercially available technology, and is tenacious enough to break weak security procedures. A corporate espionage operation is an example of such a threat.

For network communication there are two major types of security breaches that are applicable for this paper, wire tapping and information mis-routing. Both of these concerns involve a third party gaining access, either accidentally or maliciously, to sensitive information.

In terms of technology and tenacity it is assumed that the adversary:

- can physically access and monitor information passing through the untrusted network,
- can store and analyze the information passing through the untrusted network,
- can communicate on the untrusted network and attempt to gain access to the trusted network via standard network protocols,
- has the means, desire, and resources to break weakly secured communication, and
- can isolate specific or sensitive information from other information.

**Security Perimeter**

In terms of networking security, it is important to decide whom can be trusted with what type of information and what should be the access control strategy. The security perimeter is the boundary between those people and equipment that can be trusted and the rest of the world. An encrypting firewall between the trusted network and the untrusted network is one approach to providing this security perimeter. In general, the smaller the security perimeter, the more expensive it is to achieve security per user since it requires an encrypting firewall for each security perimeter. However, the information security for the overall network is improved. The larger the security perimeter, the lower the cost per user, but at the liability of needing to trust a larger number of people and equipment.

This paper presents a set of examples to illustrate methods to define the security perimeter for various network configurations and security requirements using the encrypting firewall security model. The basic model assumes that groups sharing common infrastructure such as a LAN or a building constitute a trusted set of users. This basic model attempts to balance risk against cost and complexity.

**Requirements for an Encrypting ATM Firewall**

Before discussing how to deploy security within a network, it makes sense to define the requirements for an Encrypting ATM Firewall (referred to as a cryptographic unit). The following items compose the functions necessary for a cryptographic unit to operate as an encrypting firewall:

- Ensure privacy of the data.
- Provide access control to the trusted network.
- Be transparent to the network and users.
- Communicate with a certificate authority for credential and policy information.
- Provide Operations, Administrations, Maintenance, and Provisioning (OAMP) functions.
Privacy

The most important function for an encrypting security device is to provide privacy for the data in transit over the untrusted network. This means that the data must be scrambled with a sufficiently robust cryptographic algorithm, such that no information is available to a potential adversary other than the existence of a message and possibly its length. This means that the payload of every cell transiting the untrusted network must be encrypted with a strong cryptographic algorithm. Furthermore, the algorithm should ensure that patterns in the plain text do not show up as patterns in the encrypted text, also referred to as cipher text.

Another aspect of privacy is the generation and distribution of session keys. Each active VC must have a unique encryption key (or set of keys). This ensures that a compromise of one session does not affect the security of any other active session. Encryption keys should be established between the cryptographic units during call setup. This ensures that each call has a unique security context with a limited lifetime. Additionally, the encryption keys must be easily changeable during the lifetime of the call. Changing of the keys is necessary for certain types of encryption feedback modes, and ensures that an encryption key has a limited lifetime and is used to protect only a limited amount of data. Finally, a cryptographic unit must be able to support a large number of unique virtual circuits concurrently. This is necessary to meet the transparency requirement for access to the switched public network.

Access Control

The second major function of an encrypting firewall is to provide access control between the trusted network and the untrusted network. The amount of access control is a policy issue dictated by the security administrator. The most restrictive (and secure) access control policy is to allow connections between trusted networks via the untrusted network only if that connection is part of an authenticated security context.

One method to administer access control is to require the establishment of a security context on a per-Virtual Circuit (VC) basis is during call setup. When a host-to-host connection request is first made across the untrusted network, the cryptographic units must first set up a security context before the connection is allowed to be completed between the hosts. The security context establishes the identity of the cryptographic units and sets up the necessary session keys for encrypting the particular VC. This approach also permits security for Point-to-Multipoint (PMP) connection.

Transparency

The third major requirement for a cryptographic firewall is transparency, with respect to the end-user and the network. In short, for users within trusted networks the existence of the cryptographic firewall should not be visible. The cryptographic firewall must be compatible with the ATM standards with respect to user cells and signaling channels. For user cells, only the payload of the cell is encrypted. This means the ATM header information remains in the clear and thus the encryption does not affect transit of the cell through the untrusted network. For signaling channels, the cryptographic firewall is responsible for intercepting call setup messages from the trusted network to the untrusted network. The cryptographic firewall must then comply with the signaling standards in order to interoperate seamlessly between the trusted network and the untrusted network.

Certificate Authority

A Certificate Authority is generally used to vouch for the authenticity of a public key and its association with other identifying information. In the context of a network security system, it can also play a critical role in vouching for the identity of cryptographic units and other
entities. As part of establishing a security context, cryptographic units need to exchange certificates signed by a trusted certificate authority. A security context between cryptographic units is only valid if both cryptographic units can validate the credentials of the other cryptographic unit.

**Security Policies**

It is anticipated that security policies will be administered through existing network management protocols. The certificate authority may also play a role in authenticating management agents, policy changes, and so forth. Some of policy issues that are relevant to a network security system include:

- time limits on session keys,
- revocation of certificates,
- certificate lifetimes,
- distribution of public keys associated with a cryptographic unit,
- access between hosts on trusted networks and hosts on untrusted networks,
- audits and response to unusual events, and
- policies concerning establishment of Permanent Virtual Circuits (PVCs) and Permanent Virtual Paths (PVPs).

**Reference Network Architecture**

This section illustrates the mechanism of defining a security perimeter for networks. These networks are referred to as reference networks and represent typical configurations for deploying security. As part of defining these reference networks it is necessary to discuss the particular components that make up the security system and how each of these components fits into a network based security system.

**Components of the security system**

The basic components of a network based security system are the cryptographic unit and the certificate authority. The cryptographic unit performs the following functions

- Encryption and decryption of ATM cell payload on a per-cell basis;
- Access control based on call setup within a switched virtual circuit network;
- Enforcement of policies and confirmation of credentials for each secure session.

The certificate authority is responsible for providing proof of credentials and distribution of certain security policies (such as revocation lists and certificate lifetimes).

ATM traffic generally consists of a large number of virtual circuits (VCs) that traverse the same physical link at high rates of speed. For security purposes each virtual circuit is dynamically assigned its own unique encryption key during the call setup procedure. When a cell arrives at the cryptographic unit, the unit must associate the cell VC with its unique encryption key. That key is then used to encrypt the payload of the cell; the header is left in the clear.

None of the network architecture issues discussed in this paper are dependent on the algorithm chosen. Whatever algorithm is to be used must be cryptographically strong, computationally fast, and provide recovery from errors. An example of an encryption algorithm that meets the requirements for data privacy is triple-DES. However, single DES is not strong enough to allow for good privacy. It is also necessary to provide some type of
chaining in order to effectively hide patterns in the clear text. For this reason, Electronic Code Book (ECB) encryption is not recommended. Both Cipher Block Chaining (CBC) and Counter Mode encryption provide the necessary chaining to meet the privacy requirements. If Counter Mode is chosen a mechanism must be established to recover from lost cells, since Counter Mode is not a self-recovering encryption mode (a loss of data causes all subsequent data to be corrupted). The ATM Forum Security Working Group has established a set of recommendations for the use of Counter Mode, including recovery from lost cells.

A basic requirement of a security firewall is that it fit seamlessly into a switched virtual circuit network. The mechanism used to provide access control and establish privacy in an SVC network is based on establishing a security context during call setup. The reference network shown in Figure 1 is used to illustrate steps for call setup and key exchange.

![Figure 1. Reference Network](image)

According to the criteria for trusted networks, the security overlay must be transparent. In order to talk to Host B across the untrusted network, Host A simply attempts to establish a call using standard ATM signaling. The cryptographic units transparently establish a security context through the untrusted network according to the following steps.

1) Host A sends a call setup message to the network to establish a call with Host B. Cryptographic Unit A intercepts the call setup message.

2) Cryptographic Unit A then forwards the call setup message to Host B, where it is intercepted by Cryptographic Unit B. As part of establishing a security context, Cryptographic Unit A may alter the original call setup message to include additional security information or to ensure that policies are enforced. Cryptographic Unit B then completes the connection with Cryptographic Unit A to establish a virtual circuit across the untrusted network.

3) After a connection is established between Cryptographic Unit A and Cryptographic Unit B, session keys for the particular connection between Host A and Host B are exchanged. These keys are encrypted and signed by the cryptographic units, and the credentials of the cryptographic units are exchanged. These credentials are ultimately provided by a Certificate Authority. (NOTE: The mechanism for the exchange of cryptographic unit credentials is implementation dependent and may not need to occur on a per-call basis.)
4) Once a security context has been established between the two cryptographic units, the connection between the Host A and Cryptographic Unit A, and Host B and Cryptographic Unit B respectively is allowed to complete.

5) Once the call setup is complete, a virtual circuit is established between Host A and Host B via the two cryptographic units. The cell payload of each cell is encrypted as it passes through the local cryptographic unit and decrypted on the other side of the network.

Since the cryptographic units are part of the call setup procedure, they also act as access control firewalls. According to policies, the cryptographic units can deny access from the network for any call that does not have a security context that is signed, authenticated, and ultimately verifiable by a Certificate Authority. A signed and authenticated security context means that each cryptographic unit has independently verified the identity of the other unit based on information supplied as part of the call setup message. Part of this information includes a certificate provided by a trusted certificate authority.

**Trusted LAN Reference Network**

The basic deployment of a security firewall as a network overlay calls for a trusted Local Area Network connected to an untrusted Wide Area Network by means of a high speed ATM link. The security perimeter is then at the Point-of-Presence (POP) between the untrusted wide area network and the trusted local area network. This section presents two basic configurations for a trusted local area network interconnection to the wide area network.

![Figure 2. Trusted Local Area ATM Network connected to an Untrusted Wide Area ATM Network](image)

The first configuration, shown in Figure 2, assumes a local ATM environment where all end-users are interconnected locally via ATM switches. The security perimeter is between the local root ATM switch and the untrusted wide area network. This configuration assumes that the local network is trusted and the wide area network is untrusted. All local traffic in this configuration would remain in the clear. Traffic entering or leaving the security perimeter would be subject to encryption and access control policies. This configuration represents both a cost effective and security effective solution that scales well with the requirements of the local area network.

©2003 SafeNet, Inc.  August 2003
This configuration is security effective because typically the local area network would represent a building or campus environment that is trusted. Therefore, the security perimeter encompasses the entire building or local campus. Security of the local area network is accomplished by physical security of the networking equipment and cryptographic units.

This configuration is cost effective since only the links from the trusted network to the untrusted network require encryption devices. We assume that the wide area network links are procured from the public carriers and that users will seek to minimize this expense. The cryptographic unit can be matched to the performance of this external link without impacting internal network performance.

Finally, this approach scales well since the local area trusted network can grow in nodes without a significant impact on the need for access to the untrusted wide area network. This model assumes that much of the traffic is local and only a small fraction of the total traffic is external. As the local network grows the requirements for access to the untrusted wide area network will also grow but at a much slower rate.

![Figure 3. Trusted Local Area Legacy Network connected to an Untrusted Wide Area ATM Network](image)

The second configuration, shown in Figure 3, is very similar to the first configuration but allows for backward compatibility with existing legacy networks. In the case, the trusted local network is IP-based, supporting many different network types. (Note that this is strictly a private IP network which is not connected to the Internet.) The IP router with ATM capability provides the interface between IP traffic on the legacy networks and the ATM network. The ATM link between the IP router and the wide area network contains the cryptographic unit that provides encryption of the ATM cell payload (and therefore IP datagrams). This configuration is cost effective, security effective, and scalable in the same manner as the first configuration.
**Trusted LANs within an Untrusted WAN**

The two configurations illustrated in the previous section represent building blocks for developing security within a Wide Area Network. The basic idea for security over a wide area network is that security perimeters are established at the interface between local area networks and the wide area network according to Figures 2 and 3. These local area networks then become “trusted islands.” The assumption is that there is no requirement for trust within the untrusted network. Thus, even if the untrusted network is compromised, there is no compromise to the privacy of the data nor can there be unauthorized access to the trusted ATM networks. This is because all data between the trusted islands is encrypted and access control is accomplished at the point-of-presence to the wide area network.

From the perspective of the user within a trusted island, there is no difference in security between communication within a trusted island and communication between trusted islands. Essentially, the cryptographic units have connected each of the distinct islands into one trusted virtual network. The following diagram illustrates the physical interconnection between the trusted islands and the wide area network.

![Diagram of trusted LANs within an untrusted WAN](image-url)

**Figure 4. Interconnection between Trusted ATM networks and an Untrusted Wide Area Network**

The point-of-presence of the untrusted wide area network is typically an Add/Drop multiplexor that connects the local area network to a high bandwidth local loop that goes to the central office of the local carrier. Within the untrusted wide area network, traffic will be switched through a hierarchy of switches starting with the local central office and then (possibly) through the Inter-exchange Carriers (IEC). A customer has no control over the switching or security of switched traffic within the untrusted network. Therefore, it is on the trusted network side of the point-of-presence that a security firewall must be installed.

With cryptographic firewalls on both sides of each connection, all communication between the trusted networks is encrypted prior to entering the untrusted network. All communication from the untrusted network to the trusted network is controlled by means of access control at the cryptographic firewall. Depending on the policy, this may mean that only connections between trusted networks are permitted. The decision to accept connections from the outside world are made at the boundary of the trusted ATM network.

In the network pictured above, there must exist at least one certificate authority. In general the certificate authority is attached to the public (untrusted) network. As part of installation, cryptographic units must be registered with each certificate authority. This registration process provides both routing and identification information such that the cryptographic units may contact the certificate authority.
Conclusion

This paper explored the mechanisms and policies that are necessary to protect information transmitted over an untrusted high speed wide area ATM network. One basic assumption for establishing a trusted network is the development of a threat model. The model chosen is an outsider threat, technically capable and properly motivated such that strong encryption and access control are necessary to protect the security of the data. The second basic assumption is that the local area network is physically secure and trusted. Thus, it makes sense from a security as well as economic standpoint to provide encryption and access control at the point-of-presence to the untrusted wide area network.

The requirements for the cryptographic units include the need to operate at very high rates of speed, support large number of simultaneous virtual circuits, seamlessly interconnect to a switched wide area network and provide strong access control. To ensure privacy of the data the use of counter mode triple DES for encryption has been advocated. To ensure access control, a security context between cryptographic units is established at call setup time for each VC. This security context provides strong authentication of cryptographic units based on credentials supplied by a certificate authority as well as dynamic session keys for encryption. To ensure transparency, the requirements call for the cryptographic units to support a large number of simultaneous virtual circuits. Transparency also requires the support of ATM signaling standards to establish a security context as part of call setup for each VC.

The reference networks illustrate the interconnection between trusted local area networks via the untrusted wide area network. The idea is to develop a trusted virtual network by interconnecting trusted network islands. The use of switched virtual circuits within the wide area network ensures transparency and interoperability with the local and inter-exchange carriers.

Bibliography


About SafeNet, Inc.
SafeNet, Inc. (Nasdaq: SFNT), a leading provider of private and public network security solutions, has set the industry standard for VPN technology and secure business communications and offers the only encryption platform for both WAN and VPN networks. With more than 20 years experience in developing, deploying, and managing network security systems for the most security-conscious government, financial institutions, and large enterprise organizations around the world, SafeNet’s proven technology has emerged as the de facto industry standard for VPNs. SafeNet is the single-source vendor for WAN and VPN security solutions teamed with an easy and low-cost migration path to a broad range of VPN products. SafeNet security solutions, based on SecureIP Technology™ and part of the CGX Security Platform, have become the products of choice for leading Internet infrastructure manufacturers, service providers, and security vendors.

Corporate Headquarters
Phone USA and Canada (800) 533-3958
Phone Other Countries (410) 931-7500
Fax (410) 931-7524
E-mail info@safenet-inc.com
Website www.safenet-inc.com

©2003 SafeNet, Inc. This document contains information that is proprietary to SafeNet, Inc. No part of this document may be reproduced in any form without prior written approval by SafeNet. SafeNet shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretation thereof. The opinions expressed herein are subject to change without notice.