Securing the Networked e-Business Throughout an Internet Distributed Organization

STANISLAV MILANOVIC [a], ZORAN PETROVIC [b]

[a] WSEAS, Highest Institute of Education, Science and Technology
Ag.I.Theologou 17-23,
15773, Zographou,
Athens, GREECE.

[b] University of Belgrade, Faculty of Electrical Engineering
Department for Telecommunications
Bulevar Kralja Aleksandra 73, 11000 Belgrade
YUGOSLAVIA

Abstract: - This paper explores an Internet-based VPN solution, built upon IPSec, which combines tunneling with PKI authentication and encryption. To protect the valuable company resources, an efficient intrusion/misuse detection and response system was incorporated into deployed security solution. This approach enabled a large-scale customer provide their global e-business safely. As a result, an integrated policy-based management system and a PKI environment provided enterprise network managers with a scalable and secure network administration.

Key-Words: - e-business, Internet-based VPN, IPSec, PKI, Intrusion/Misuse Detection and Response System, Single Sign-On

1 Introduction

With the constant stream of new technologies, companies are rapidly changing their IT environments to keep a step ahead of their competitors [1, 2, 3, 4, 5]. However, implementing the e-business applications may be impossible without a coherent, consistent approach to e-business security. Failure to protect information assets from external and internal intruders can lead to embarrassing public exposure, loss of customer confidence and financial loss. A company's decision to protect itself isn't just a technology decision. It's a business decision.

Although private networks would appear to offer better security, this has more to do with the users' perception than reality since, whether on private leased lines or the Internet, unsecured data is visible to the Service Providers [6]. Internet-based Virtual Private Networks (VPNs) provide a flexible and cost-effective alternative to private networks for secure wide-area data communications; even companies with 10 or more telecommuters could expect to see a Return on Investment within 6 to 9 months of operation. These cost savings are achieved by paying only for a local connection to the nearest Internet Service Provider (ISP) at each end of the connection. Nevertheless, since most security threats originate inside an organization (Figure 1), security measures such as access control, encryption and user authentication must also be deployed internally [7].

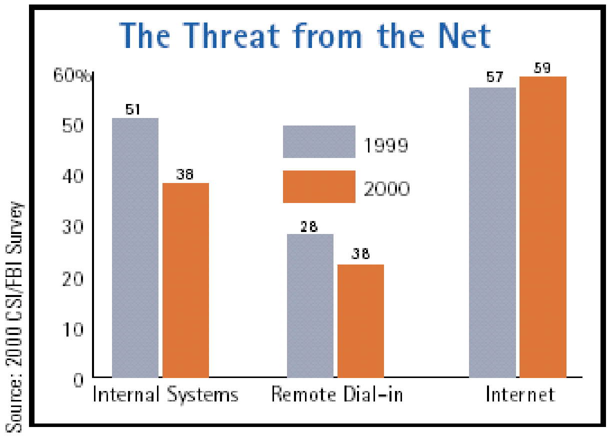

Figure 1. Sources of Computer Attacks

To protect valuable company resources, corporations must be able to automatically detect and respond to network attacks or misuse in a proactive manner. For this purpose, an efficient intrusion/misuse detection and response system must be incorporated into security solution.

2 The Security Technology Overview

Internet-based VPNs are a new way to build secure, private communications infrastructures on top of the Internet. IPSec can be used to create a secure VPN on the fly, on demand and with anyone else using the standard [8]. The Internet Engineering Task Force (IETF) defined IPSec: a set of protocols to support secure exchange of packets at the IP layer. IPSec uses packet headers, called Authentication Headers (AH), to validate users and Encapsulating Security Payloads (ESP) to encrypt data. IPSec specifies 56-bit DES (Data Encryption System) or 168-bit 3DES encryption for data privacy. To keep addresses private while communicating over the Internet, IPSec can be used in tunnel mode: the entire private IP packet — header and payload — is hidden inside a public IP packet "envelope". Tunnel mode is typically employed by security gateways: edge devices like routers and firewalls that relay packets on another system's behalf. But, inside a LAN, to reduce processing overhead and packet length without sacrificing security, the original header can be used on packets exchanged between hosts: in transport mode, ESP hides only the private packet's payload. Transport mode IPSec can be used to efficiently protect data end-to-end between clients and servers, peers in a workgroup, and extranet partners (Figure 2). Transport and tunnel mode can be used in conjunction to secure the total enterprise network by applying each where appropriate: tunnel mode to WAN security, transport mode to LAN security [9].

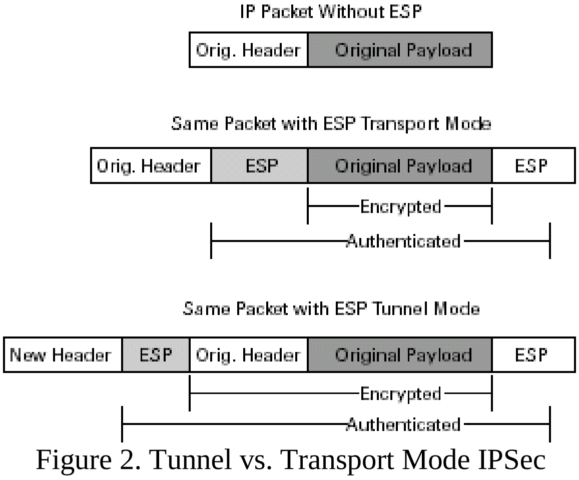

Figure 2. Tunnel vs. Transport Mode IPSec

IPSec parameters between the tunnel endpoints are negotiated with the Internet Key Exchange (IKE) protocol, normally using PKI digital certificates in the authentication and encryption process. PKI (Public Key Infrastructure) is an emerging environment of policies, protocols, and standards, which provides the necessary components for centralized management (e.g. issuing, revoking, validating) of digital certificates [10]. Digital certificate is a set of digital credentials and can contain a variety of information, including the certificate holder's name, public key, activation and expiration date of the certificate, operations the public key can perform (encrypt, decrypt or verify digital signatures), the issuer's (CA's) digital signature, serial number of the certificate and encryption method. The International Telecommunications Union (ITU-T) recommendation X.509 defines a standard format for these certificates. Digital signature is used to ensure data integrity and non-repudiation (the ability to prove that a customer has completed or authorized a specific transaction). A Certification Authority (CA) is a trusted entity responsible for binding a given set of credentials to a subscriber and issuing digital certificates [11]. Digital certificates are trusted because of the CA's digital signature placed on it. CAs run by two differing institutions can be made aware of each other, effectively allowing parties aware of either CA to authenticate users certified by both, by a mechanism known as cross-certification [12]. PKI utilizes a key pair system of asymmetric keys (private key and public key) that are mathematically related to each other and perform opposite functions. What one key encrypts, only the other key can decrypt. Public keys are not secret and can be distributed over non-secured networks, while private keys do not need to be distributed. Since only the owner of a private key needs to have it, the private key can be generated on the machine where it is used and must be protected from compromise. The first step in the signature process involves performing to a message a one-way hash function such as MD5 or SHA-1 (Figure 3), which results in a unique mathematical abstract of the original message (message digest). The message digest is then encrypted with the sender's private key resulting in the digital signature, which gets appended to the original message. The receiver can validate the sender's digital signature using the sender's public key contained in the sender's digital certificate, which can be retrieved from the certificate repository [13].

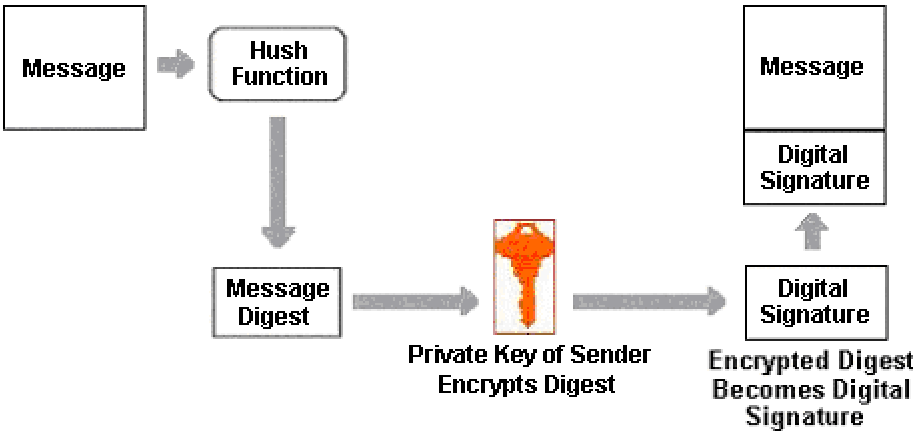
Message
Hush Function
Message Digest
Private Key of Sender Encrypts Digest
Digital Signature
Encrypted Digest Becomes Digital Signature
Message
Digital Signature

Figure 3. Digital Signature Process

The next stage is to encrypt the message and its signature by one-time symmetric key (Figure 4). A symmetric key is a unique key created for a one-time use that is able to both encrypt and decrypt a message. Both the sender and the receiver will need the same symmetric key to encode and decode the message. PKI adds an extra layer of security by encrypting the one-time symmetric key with the receiver's public key so only the receiver can decode the symmetric key with his or her private key. The encrypted one-time symmetric key is appended to the encrypted message and the message is now ready to be sent.

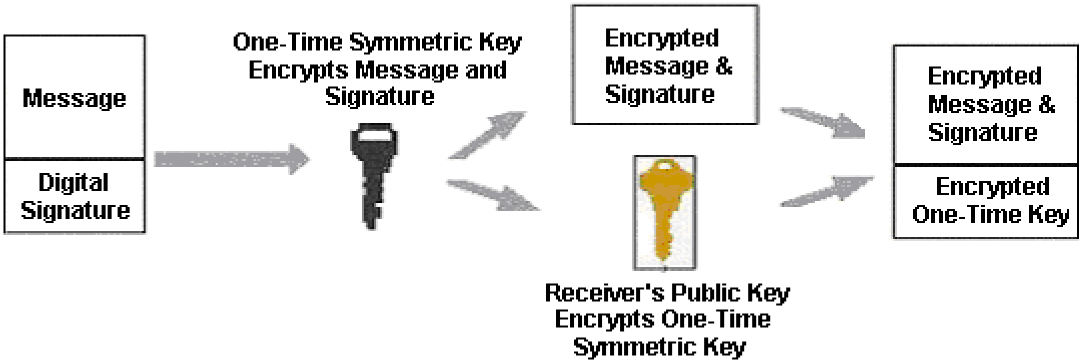
Message
Digital Signature
One-Time Symmetric Key Encrypts Message and Signature
Encrypted Message & Signature
Receiver's Public Key Encrypts One-Time Symmetric Key
Encrypted Message & Signature
Encrypted One-Time Key

Figure 4. The Encryption Process

CA issues in advance its digital certificate (containing CA's public key) to all subscribers, and its public key can be used by the receiver to authenticate the public key in the sender's digital certificate. When the sender's public key has been validated, the receiver can use it to authenticate the sender's digital signature of the message itself. The certification process is as follows (Figure 5):

1. Subscriber applies to CA for digital certificate.
2. CA verifies subscriber's identity and issues certificate digitally signed with CA's private key.
3. CA publishes subscriber's digital certificate to the repository.
4. Subscriber signs message with its private key and sends message to second party.
5. Receiving party verifies digital signature with sender's public key and requests verification of sender's digital certificate from repository.
6. Repository reports status of subscriber's certificate.

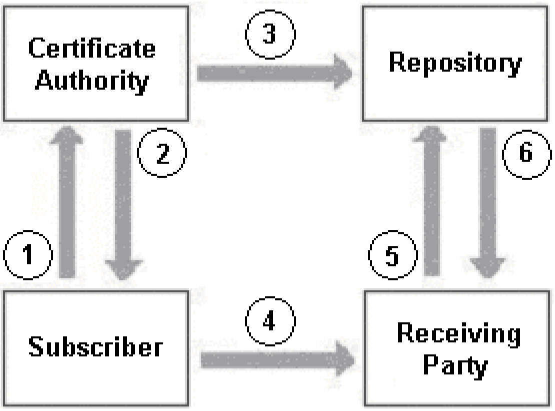

Figure 5. The Certification Process

After the signed and encrypted message is received, the message is decrypted and its content integrity is verified. The one-time symmetric key that was used to encode the message is unscrambled using the receiver's private key.

The symmetric key is then used to decode the encrypted message and signature. Using the public key of the sender, the digital signature is decrypted and the digest for the message is extracted. The decrypted message is checked to see if its contents are exactly as they should be through a repeat of the agreed upon hash function. The result of the hash algorithm is a second message digest. If that second digest perfectly matches the original digest, the message integrity is confirmed and the message has been successfully transmitted (Figure 6).

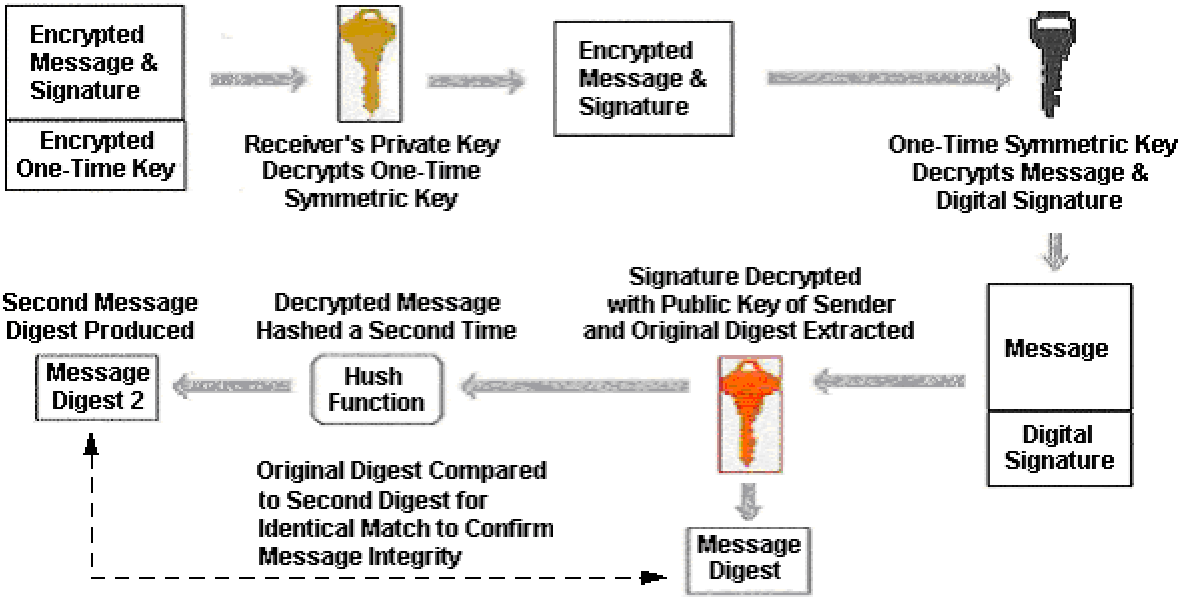
Encrypted Message & Signature
Encrypted One-Time Key
Receiver's Private Key Decrypts One-Time Symmetric Key
Encrypted Message & Signature
One-Time Symmetric Key Decrypts Message & Digital Signature
Message
Digital Signature
Signature Decrypted with Public Key of Sender and Original Digest Extracted
Decrypted Message Hashed a Second Time
Hush Function
Second Message Digest Produced
Message Digest 2
Original Digest Compared to Second Digest for Identical Match to Confirm Message Integrity
Message Digest

Figure 6. Message Decryption and Verification Process

A significant up-front effort is required to determine and establish policies, procedures, and technologies that will lead to a successful enterprise PKI deployment.

3 The Goals of Implementing an e-Business Trust Infrastructure

- Protecting the corporate network resources against internal and external threats.
- Providing a cost-effective world-wide connectivity for mobile and remote employees over the Internet.
- Securely and efficiently managing the network's IP address infrastructure of the company.
- Integration of the Single Sign-On across the enterprise, allowing users to access multiple applications or resources while only having to authenticate once.

4 Requirements

The e-business trust infrastructure had to satisfy the following key requirements:

- Centralized policy management and granular access control to network resources [14].
- Deploying an efficient enterprise intrusion/misuse detection and response system.
- Delivering reliable Quality of Service (QoS)
- High Availability and load balancing [15]
- Interoperability

5 The Solution: Building an Infrastructure for Secure e-Business

Deployed infrastructure for trusted e-business consists of the following components (Figure 7):

- Check Point VPN-1 Gateway, which integrates FireWall-1 and VPN functions into a single enforcement point. VPN-1 Gateway is based upon Stateful Inspection incorporating communication- and application-derived state and context information, which is stored and updated dynamically. Stateful Inspection provides full application-layer awareness without requiring a separate proxy for every service [16]. VPN-1 Gateway enables the establishment of heterogeneous extranets by supporting the simultaneous use of digital certificates from multiple CAs [17].
- FloodGate-1 — a policy based, quality of service solution for private WAN and Internet links.
- ConnectControl module enhances network connectivity through advanced server load balancing.
- The Chrysalis-ITS' Luna VPN — a hardware-based cryptographic accelerator card installed at the VPN-1 Gateway hosts [18].

- High Availability Module is used to configure VPN clusters in which one or more redundant gateways serve as backups to a primary gateway.
- Enterprise Management Console provides a unified interface for defining and managing firewall security, VPN and bandwidth management policies. Whenever a change is made to enterprise security policy, it's automatically distributed to all relevant enforcement points.

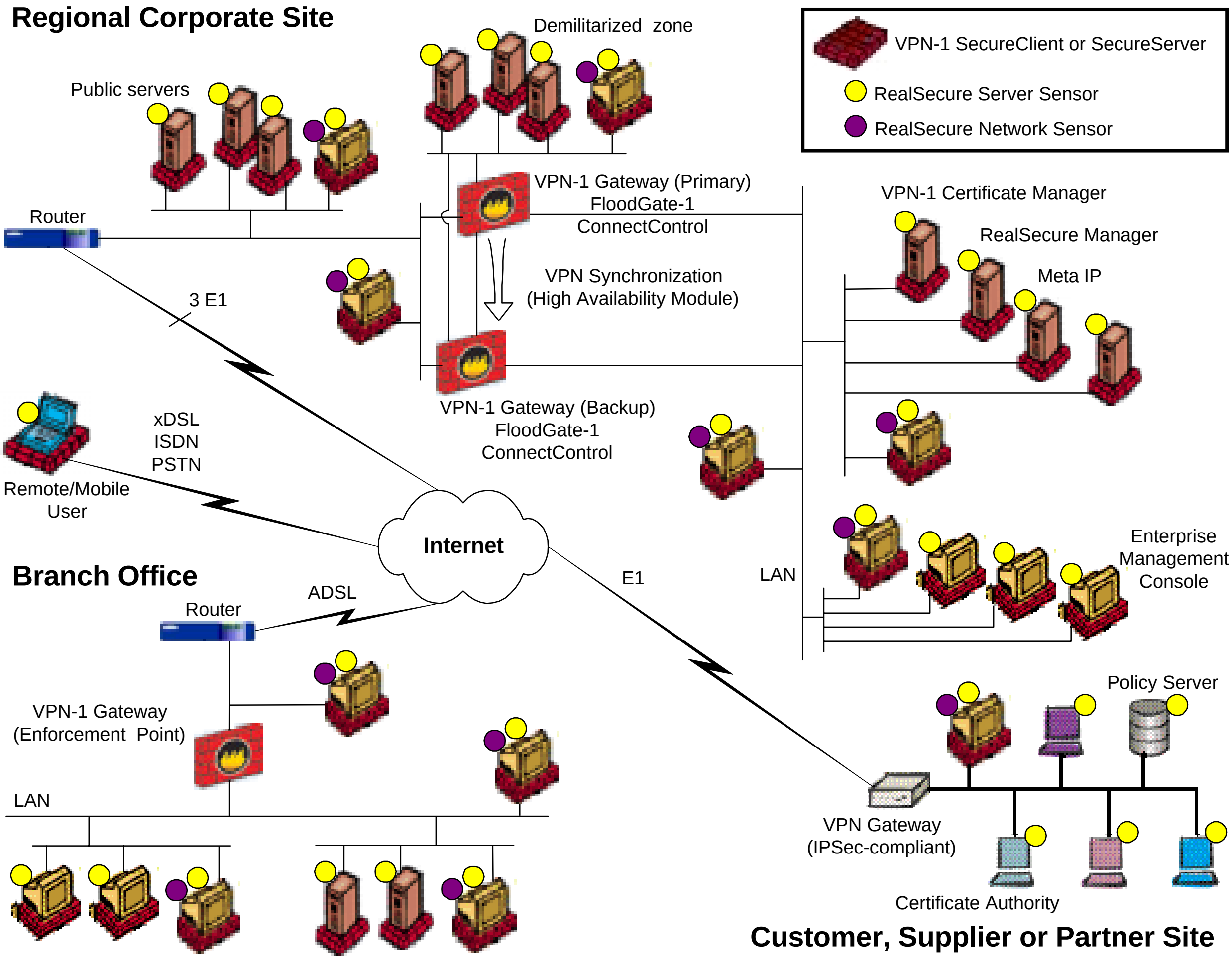

Figure 7. Deployed e-Business Trust Infrastructure

- VPN-1 SecureClient establishes secure connectivity for both Remote Access and Intranet VPN clients. Once a VPN user successfully authenticates, the enterprise desktop security policy is downloaded onto the client machine.
- VPN-1 SecureServer delivers security and VPN connectivity, specifically for a single server running mission-critical applications.
- Meta IP provides centralized management and distributed administration of enterprise-scale IP network infrastructures and also delivers a Single Sign-On service for network resources.
- VPN-1 Certificate Manager — a turnkey PKI solution for Check Point IPSec/IKE-compliant VPNs. VPN-1 Certificate Manager is comprised of the CA (to create/revoke digital certificates), LDAP-compliant directory (for storing/retrieving digital certificates) and account management client (for managing all aspects of the user account lifecycle).
- RealSecure from Internet Security Systems — an automated, real-time intrusion/misuse detection and response system, providing a threat management for entire enterprise network [19]. RealSecure encompasses the following modules:
  - RealSecure Network Sensor runs on dedicated host and monitors traffic of the specified network segment for signs of malicious intent and responds automatically.
  - RealSecure Server Sensor runs on dedicated host and monitors both inbound and outbound network traffic directed at a single host as well as the key system files for indications of malicious intent and responds automatically.

- All RealSecure Network Sensors and RealSecure Server Sensors report to and are configured by the RealSecure Manager.

6 Conclusion

Deployed security solution leverages an Internet-based VPN to enable a world-wide organization establish secure links with customers/suppliers/partners and extend communications to more than 300 branch offices, 27 regional corporate sites and over 5000 mobile workforce. An integrated security management system utilizes a centralized mechanism for consistent policy implementation, verification, and enforcement in distributed enterprise network. Besides controlling access, a prominent industry leader is now able to monitor security events across the enterprise so that suspicious activities can be quickly pinpointed. End-to-end network security with hardware-based encryption offers an optimum balance between security and performance.

Ensuring the security of corporate assets is a continuous and dynamic process, rather than an item on a checklist that can be forgotten once it is set up [20]. The solutions' openness and extensibility gives to a global communications company the flexibility to leverage existing technologies and adopt new ones as its e-businesses evolve.

References:

[1] Stanislav Milanovic, Zoran Petrovic, "Deploying IP-based Virtual Private Network Across the Global Corporation", Communications World, pp. 13-17, WSES Press, 2001, http://www.wseas.org , Proceedings of WSES/IEEE CSCC 2001, pp.CD-ROM, July8-15, 2001, Crete, Greece, http://www.wseas.org

[2] Stanislav Milanovic, Zoran Petrovic, "A Practical Solution for Delivering Voice over IP". Proceedings of IEEE ICN'01, July9-13, 2001, Colmar, France, http://iutsun1.colmar.uha.fr/pgmICN01.html; Lecture Notes in Computer Science #2094, Part II, pp. 717-725, Springer-Verlag GmbH & Co. KG., http://link.springer.de/link/service/series/0558/tocs/t2094.htm

[3] Stanislav Milanovic, Zoran Petrovic, "Building the Enterprise-wide Storage Area Network", Proceedings of IEEE EUROCON 2001, Vol. 1, pp.136-139, July 5-7, 2001, Bratislava, Slovakia, http://www.ktl.elf.stuba.sk/EUROCON/program.htm

[4] Stanislav Milanovic, "At the Front End in Migrating to Gigabit Ethernet". Proceedings of IEEE SoftCOM 2000, Vol.1, pp. 369-378, October 10-14, 2000, Split, Rijeka (Croatia), Trieste, Venice (Italy), http://www.fesb.hr/SoftCOM/2000/IE/Network_Architectures.htm

[5] Stanislav Milanovic, Alessandro Maglianella, "ATM over ADSL Probe in Telecom Italia Environment", Computer Networks, Vol.34, No.6, pp.965-980, Elsevier Science, November 2000, http://www.elsevier.com/inca/publications/store/5/0/5/6/0/6/index.htt .Proceedings of TERENA Networking Conference 2000, pp. CD-ROM, 22-25 May 2000, Lisbon, Portugal, http://www.terena.nl/tnc2000/proceedings/10A/10a3.pdf

[6] "IPSec White Paper", Information Resource Engineering Inc., 2001.

[7] "An Introduction to Network Security – Ensuring the Safety of your Network", Enterprise Management Associates, Inc., 2000.

[8] "PKI and VPNs — Enabling Security in an Increasingly Networked World", Alcatel, 2001.

[9] "How to Build Secure LANs with IPSec", The Technology Guide Series, The Applied Technologies Group, Inc., 2001.

[10] "Public Key Infrastructure — Securing the Future of Communication", PKI White Paper, Rainbow Technologies, Inc., October, 2000.

[11] "An Introduction to Enterprise Public Key Infrastructure (PKI)", METASeS, Inc., February 2001.

[12] Jim Turnbull, "Cross-Certification and PKI Policy Networking", White Paper, Entrust Technologies Inc., August 2000.

[13] "Enhancing Enterprise Security - An Overview of Network Security Issues and Technologies", Technical Paper, 3Com Corporation, 1999.

[14] "Secure Virtual Network Architecture", Check Point Software Technologies Ltd., 2000

[15] "Top 10 Challenges to Securing Your Network", White Paper, Check Point Software Technologies Ltd., May 2000.

[16] "Check Point FireWall-1 — Technical Overview", Check Point Software Technologies Ltd., October 2000.

[17] "VPN-1 Gateway", White Paper, Check Point Software Technologies Ltd., 2000.

[18] "Luna VPN — Ultimate Trust Cryptographic Accelerator", Luna VPN Datasheet, Chrysalis-ITS, 2001

[19] "RealSecure", White Paper, Internet Security Systems, Inc., 2001.

[20] "Securing E-Business", White Paper, The Technology Guide, The Applied Technologies Group, Inc., 2001.