Architecting the Next Generation
End-to-End e-Business Trust Infrastructure

STANISLAV MILANOVIC *, NIKOS E. MASTORAKIS #

* WSEAS, Highest Institute of Education, Science and Technology
Haghiou I. Theologou 17
15773, Zographou,
Athens, GREECE

# MILITARY INSTITUTIONS OF UNIVERSITY EDUCATION
HELLENIC NAVAL ACADEMY
Terma Hatzikyriakou, 18539, Piraeus, GREECE.
mastor@ieee.org http://www.hna.gr/index-hna.htm

Abstract: This paper presents an end-to-end architecture for secure e-Business over the Internet spanning corporate sites, remote workers and customers/suppliers/business partners of a global organization. Policy-based PKI (Public Key Infrastructure) and single sign-on enabled IPSec VPNs (Virtual Private Networks), along with incorporated intrusion/misuse detection and response system, could efficiently protect all e-Business environments allowing enterprise to benefit related Return on Investment within only several months. Deployed trustworthy solution is automatically updated to include the latest anti-virus signatures and intrusion policies to guard against malicious attacks.

Key-Words: End-to-end e-business security, IPSec, PKI, Internet-based VPN, Single Sign-On, Intrusion Detection

1 Introduction
e-Business opens the door to millions of end users, exposing Web sites, invaluable corporate information mission-critical business applications, and consumers’ private information to more risk than ever before [1, 2, 3, 4, 5, 6, 7, 8, 9]. To be successful in this environment, organizations must allow access to resources while simultaneously protecting valuable assets and ensuring the privacy of consumers’ confidential information [10]. 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 [11]. Internet-based 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 [12].

![The Threat from the Net](image-url)

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 [13]. 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 [14].

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 [15]. 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 [16]. 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 [17]. 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 (Figure 3) involves performing to a message a one-way hash function such as MD5 (Message Digest Algorithm) or SHA-1 (Secure Hash Algorithm), 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 [18].

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.

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.
After the signed and encrypted message is received, the message is decrypted and its content integrity is verified (Figure 6). 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.

3 Objective
The Goals of Implementing e-Business Trust Infrastructure are the following:
- Protecting the corporate network resources against internal and external threats.
- Providing a cost-effective 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 [19].
- Deploying an efficient enterprise intrusion/misuse detection and response system.
- Delivering reliable Quality of Service (QoS).
- High Availability and load balancing [20].
- Interoperability.
The Next Generation End-to-end Security Architecture for e-Business Environments

An end-to-end architecture for trusted e-Business was based on the Rapidstream appliances (Figure 7) running Check Point Next Generation (NG) software (VPN-1/FireWall-1 Gateway) while deployed in high-availability configuration. Rapidstream appliances were installed in a standalone configuration (single gateways) in which the VPN/FireWall Module and the Management Server (Enterprise Primary Management or Enterprise Secondary Management) were on the same machine (appliance) while the Graphical User Interface Client was installed on a different machine (Management Console) [21]. A Management Server includes an ICA (Internal Certificate Authority), which provides X.509-based certificate services for Check Point components (overseeing the generation, signing and revocation of the certificates [22]).

VPN-1/FireWall-1’s VPN Module encrypts communications to guarantee data privacy and security. The Firewall Module includes the Inspection Module, the Security Servers (which implement Content Security and User Authentication), and the Synchronization feature which is basis for High Availability. The Content Security enable intelligent inspection of communications content and protect users from various hazards, including computer viruses, malicious Java applets and undesirable Web content. The Inspection Module is located in the operating system kernel, below the network layer at the lowest software level. Packets are not processed by any of the higher protocol layers unless Inspection Module verifies that they comply with the enterprise Security Policy. The Inspection Module uses Check Point’s Stateful Inspection technology 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 [23].

Meta IP was integrated with Management Server and defined from the Management Console. It automatically manages enterprise-wide IP addresses and hostnames. Meta IP also delivers transparent single sign-on for network access via User-to-Address mapping (UAM) service by capturing network access login information and dynamically assigning IP addresses. With full authentication information from the UAM server, FireWall-1 does not have to challenge users each time they request a connection through the firewall.

The Security Policy is defined from the Management Console and saved on the Management Server. The Management Server maintains the FireWall-1 databases, including the Security Policy (defined in terms of network objects, user definitions and security rules) and log files for any number of firewall enforcement points while the user information is stored in LDAP-enabled directories. Upon policy update, the Management Server downloads the Security Policy to the distributed Firewall Modules (enforcement points). The connections between the Management Console, Management Server and multiple enforcement points are secured, enabling true remote management. Thus, the GUI Client (Management Console) initiates an SSL based connection with the Management Server. The Management Server verifies that the Client’s IP address belongs to an authorized GUI Client, and sends back its certificate. Any number of Firewall Modules can be set-up, monitored and controlled from a single enterprise Management Console, but there is still only one enterprise-wide Security Policy.

VPN-1 SecureClient establishes secure connectivity for both Remote Access and Intranet VPN clients. It integrates personal firewall and centralized management capabilities, ensuring client systems are securely configured for true end-to-end security. 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.

FloodGate-1 and ConnectControl were installed on Rapidstream appliances. FloodGate-1 is a policy-based enterprise bandwidth management solution providing quality of service for VPN, Private WAN, and Internet links. The ConnectControl module enhances network connectivity through advanced server load balancing.
RealSecure from Internet Security Systems — an automated, real-time intrusion/misuse detection and response system, providing a threat management for entire enterprise network [24]. RealSecure is closely integrated with FireWall-1, using network objects that have already been entered into FireWall-1 and consolidating events into the FireWall-1 log file for simplified event auditing. 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.

6 Conclusion
Deployed end-to-end security solution leverages an Internet-based VPN to enable organization establish secure links with customers/suppliers/partners and extend communications to remote branch offices, regional corporate sites and mobile workforce. An integrated security management system utilizes a centralized mechanism for consistent policy implementation, verification, and enforcement in distributed enterprise network. With employed high-performance appliances, global corporation can reap the benefit of using secure, high-speed IP-based voice, data and multimedia services over the public Internet. The solutions’ openness and extensibility provides the flexibility to leverage existing technologies and adopt new ones as the corporate e-Businesses evolve.
References:


