Conceptualizing and Implementing an Information Security Strategy for Internet Billing Systems

Panagiota Papadopoulou, Nicholas Kolokotronis, Panagiotis Kanellis and Drakoulis Martakos

Abstract—**The decentralized nature of Internet billing systems demands a careful evaluation of the pantheon of security issues in order to avoid the potential occurrence of business risks that could not be easily mitigated. Understanding that Internet security is not merely a local technology issue implemented at each one of the endpoints of the interorganizational application, this paper presents an integrated approach based on a rigorous multi–level and multi–dimensional framework. Through synthesis, the framework evaluates and uses the available tools and techniques in a consistent manner, aiming to aid the implementation of the most effective security strategy possible. Its use and applicability is demonstrated over 'Billing Mall' – an Internet billing system currently being developed for the** *Hellenic Telecommunications Organization* **(OTE).**

Keywords—**Network security, cryptography, information security strategy, Internet billing systems, electronic commerce.**

I. Introduction

The initial response of the market to various commercial applications regarding *Electronic Bill Presentment & Payment* (EBPP)[1] is indicative of the future potential such systems hold in becoming contenders for a permanent place in the worldwide Internet infrastructure. According to industry analysis, within 3–5 years the majority of bills will be presented and paid electronically [7], [12]. In the United States alone it is projected that by taking the 'paper' out of the billing process, EBPP could save billers, customers and other constituents over $2 billions annually by 2002 [21]. In reference [22], it is emphasized that Internet billing must be thought of as a *Servicescape* – the environment within which direct interactions between the customer and the business occur [31]. In other words, such systems must be designed so as to provide the necessary prerequisites for service encounters to take place between buyer and seller.

Internet billing can deliver transactional as well as relationship benefits to the biller. The richness of information about individuals that can be gleaned from the Internet makes it an enormously powerful marketing medium, which encourages relationship building with the customer because of its real time and interactive nature [1]. Thus, such systems should be viewed by the business not only as the means by which bills are delivered and payments are collected, but rather as strategic channels for improving customer acquisition and retention through the provision of new services.

The achievement of such strategic goals such as increasing market share are directly related to the reliability of the network infrastructure of organizations. The adoption of the Internet implies however that the occurrence of business risks is more eminent as the corporate network, processes, and critical business data are now vulnerable to attacks by anyone having Internet access [1], [7], [29], [30]. What it has been observed however is that most organizations treat the Internet simply as a transport medium. The result as [29] noted is that "...Internet security remains a relatively technical, local and distinct issue from the corporate level (information systems) design and management". We advocate that as security is the dependent variable for the success of any EBPP system, any information security strategy should be formed taking into account the business vision and the business strategies adopted to meet this vision. Furthermore, it should not be approached as an afterthought, but rather it has to be designed and evolve concurrently with the development of the system. Any other way to approach this issue could result to badly design payment system where purposive failure "...quickly leads to massive fraud, system failure, and acrimonious lawsuits" [10]. In summary, the definition of any effective information security strategy should thus be a well planned and concentrated effort at the corporate level, and not be seen only as a local technology issue [29], or as an ad hoc mix of particular technical solutions to specific problems.

Taking into consideration the above issues, this paper offers an integrated approach to the development of an information security strategy for EBPP systems based on a rigorous multi–level and multi–dimensional framework that evaluates and uses the available tools and techniques in a systematic manner. In the next section we offer a primer on issues and available mechanisms for securing business transactions over the Internet. The section that follows presents the framework and its building blocks for aiding the implementation of an effective security strategy. Its applicability is demonstrated over an EBPP system currently being developed, and a concluding discussion closes the article.

II. Security Issues – Overview

In this section an overview of the main issues involved in securing business transactions over the Internet is presented. As those constitute the building blocks of any information security strategy, we are including them herein with the purpose of informing the interested reader and to point him to a number of works that cover them in more

The authors are with the Department of Computer Science, National and Kapodistrian University of Athens, Athens, Greece. E-mail: peggy@di.uoa.gr, nkolok@di.uoa.gr, kanellis@di.uoa.gr and martakos@di.uoa.gr.

[1] The terms *Electronic Bill Presentment & Payment* and *Internet Billing Systems* are used interchangeably.

detail.

The key-points an organization's information security strategy is expected to address are *confidentiality*, *integrity*, *authentication*, *access control*, and *availability of service*. When an interorganizational system providing its customers with e-commerce (or financial) solutions is the case, many additional topics have to be considered. These include *non-repudiation* and *time-stamping* techniques [9], mainly used to facilitate dispute resolution.

A. Security Primitives

In terms of cryptography, the building blocks necessary for achieving the previously mentioned security properties are *encryption*, *digital signatures* and *hash functions* [13], [19], [24], [28]. Encryption ensures the confidentiality and integrity of data whereas digital signatures can be used to authenticate the originality of content and to build access control mechanisms. Encryption can be performed by utilizing algorithms, also called *ciphers*, of either *symmetric* or *public key* cryptography.

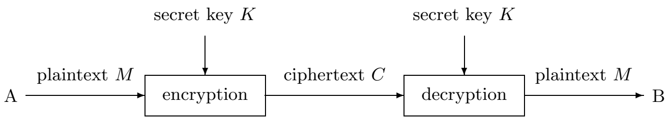


Fig. 1. Encryption/decryption using symmetric cryptography.

In symmetric cryptography, two users (e.g. user-A and user-B) must share the same *secret key* in order to communicate securely. This key K, is used to perform both encryption and decryption (*see* figure 1). Furthermore, symmetric algorithms are subdivided into the classes of *block ciphers* and *stream ciphers* [27]. Stream ciphers are much faster than block ciphers, but are less secure. Research is conducted towards the area of finding stream ciphers satisfying certain cryptographic criteria [14]. The well-known DES algorithm [17], [18] belongs to the class of block ciphers.

Public key cryptography makes use of two different keys, the *private* and the *public* key, which are denoted by K_1 and K_2 respectively. The public key should be made available to other users if someone wishes to receive encrypted messages. Then, the decryption of an encrypted message is done by using the corresponding private key. This procedure is depicted in figure 2, where the public key of user-B is assumed to be known to user-A. In subsequent sections we will refer to some of the ways by which user-A could have obtained the public key of user-B, and their importance in establishing a secure e-commerce environment.

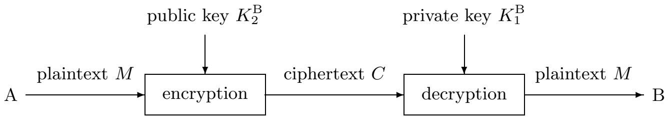


Fig. 2. Encryption/decryption using public key cryptography.

Encryption of plaintext with the private key results in the generation of a digital signature. Since digital signature algorithms operate on fixed-size blocks of data, and a plaintext can be of arbitrary size, an algorithm for calculating a representative of the plaintext with a suitable block length, is needed. This representative is almost[2] unique and is called the *hash value* of the plaintext. Consequently, a digital signature algorithm operates on a message's hash value, denoted by the letter H, and not on the message itself (*see* figure 3).

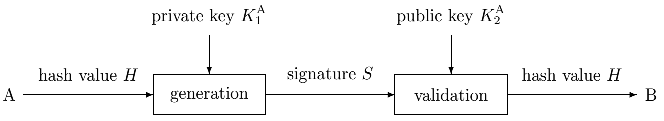


Fig. 3. Generation/validation of a digital signature using public key cryptography.

Note that in the generation step of a digital signature the private key is used, while in the validation step the public key is used. For this reason we say that generation is analogous to decryption and validation to encryption [28]. Let E, D denote the encryption and decryption algorithms respectively. According to the above, if user-A wishes to send an encrypted and digitally signed document M to user-B, he should send him

$$\{C,S\} = \{E_{K_2^B}(M), D_{K_1^A}(H)\} \ . \tag{1}$$

On the other hand, the original document M can be obtained from user-B by decrypting C with his private key. The authenticity of M can be proved by encrypting S with user-A's public key, and comparing the result with the hash value of M, i.e. H. This is illustrated next

$$M = D_{K_1^B}(E_{K_2^B}(M)) \quad \text{and} \quad H = E_{K_2^A}(D_{K_1^A}(H)) \ . \tag{2}$$

Their agreement is a verification that document M is indeed sent by the person whose public key is K_2^A, possibly user-A. The trust that should be placed in the public key depends entirely on the source that provided it.

B. Certification Authorities and Trusted Third Parties

Among other things, *Certification Authorities* (CAs) solve the problem of public key distribution. For this purpose, the CA issues a certificate for all its registered users. This certificate creates a tight coupling between a public key and its holder's identity. Moreover, the certificate is digitally signed with the CA's private key. Not only the authenticity of the certificate is assured, but any attempt of modification is detected when validating the CA's signature. Consequently, users have strong confidence about the correctness of the certificate's information.

Many ways exist for distributing the public key certificates to the interested parties. The first method consists of implementing and maintaining a certificate directory [19]. The directory services offered can be based on either X.500 or the *Lightweight Directory Access Protocol* (LDAP). In

[2] The probability of any two messages having the same hash value is negligible but nonzero.

this case, the query services supported by X.500 are a valuable tool for retrieving a certificate. This scheme requires that CA be an entity trusted by both communicating parties. If not, a *Public Key Infrastructure* (PKI), i.e. a hierarchy[3] of CAs, must be established. The second method rests on the user to send his public key certificate attached to every outgoing e-mail.

In the electronic environment, non-repudiation and time-stamping services are of great importance in protecting the rights of legal users against any malicious acts. Specifically, non-repudiation is of two types: non-repudiation of origin and non-repudiation of delivery. Expanding the capabilities of CAs to support these functions lead to the notion of *Trusted Third Parties* (TTPs).

Technical aspects of TTPs are addressed in subsequent sections where an approach for defining and implementing an information security strategy is presented.

C. Firewalls

Historically, firewalls have been the main mechanism used for protecting a corporate network and data from external attacks. A firewall is a software application preventing unwanted and unauthorized communication into or out of a network, allowing an organization to enforce a network security strategy on traffic flowing between its internal network and the Internet [20]. The main advantage of using a firewall is that only a single point, in an organization's network, has to be carefully configured for preventing security threats. The model described is seen below.

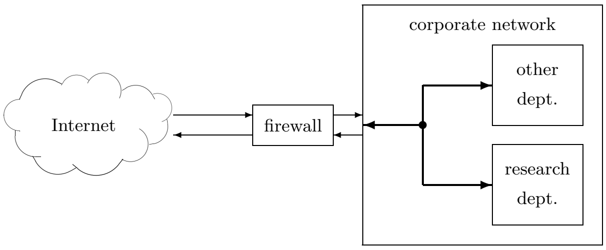


Fig. 4. An example scheme for safeguarding a corporate network.

The firewall depicted in figure 4, actually defines a *security perimeter* which may be considered as the first line of defense against possible attacks. A well configured firewall will intercept almost all suspicious packets arriving from the Internet. This security model may be characterized as being *single-dimensional* [2], due to its lack of employing alternative security methods for dealing with successful attacks.

If the users inside the corporate network are considered to be trustworthy then no problem is ever likely to occur. However, surveys indicate that most unauthorized activities are perpetrated by internal users, i.e. the company's employees. In order to protect the company's sensitive data from disclosure, multiple lines of defense may be put in place. For example, an internal firewall could control access to the research department of an organization (*see* figure 5). Despite the multiple lines of defense used to protect critical information, firewalls are usually combined with other security mechanisms to create a comprehensive security system. This is sometimes called a *multi-dimensional* security model [2].

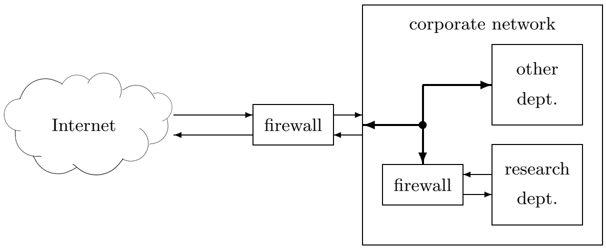


Fig. 5. Employing a two lines of defense security model.

Keeping an organization's network and data secure means that not only technical solutions are applied, but also that every employee conforms to the organization's security strategy requirements. These might include extra security tools running independently on each personal computer (e.g. virus utilities, etc). Such methods are not discussed in this paper.

The services offered by firewalls are often enriched by cryptographic functions. This is particularly helpful in cases were an organization's departments are located in different geographic areas and thus building a private network is not considered feasible for a variety of reasons. However, a *Virtual Private Network* (VPN) can be established since all information traveling through the network can be appropriately encrypted [15]. This case is shown in figure 6.

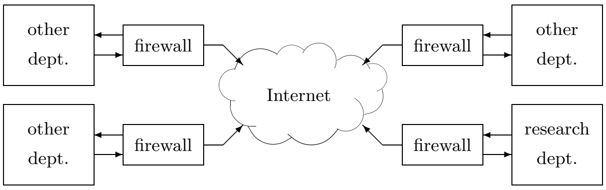


Fig. 6. The corporate's Virtual Private Network.

Due to the growth and the relatively low cost of the Internet, corporations now consider VPNs as an alternative infrastructure option to *Value Added Networks* (VANs). There is a growing trend for interorganizational systems taking advantage of VPN techniques in order to provide a secure environment for electronic business transactions. With the demise of the centralized computing model where business risks could be easily managed and alleviated, and the advent of distributed systems, increased at the same time the difficulty of security management. As a result, the need for an effective information security strategy has climbed to the top of the corporate IT agenda. In the next section we offer an integrated approach to the development of a corporate security strategy based on a multi-level and multi-dimensional framework.

[3] This term is used generically to contain all known Certification Authority interrelationship structures (*see* [9] for more details).

III. An Information Security Strategy Framework

The framework which is depicted in figure 7, portrays the process of designing and deploying an information security strategy through a cyclic iterative model comprising of the different stages or successive steps that have to be taken. The stages identified, namely *business needs analysis*, *risk analysis*, *security strategy implementation*, and *monitoring, research & analysis*, are analyzed in the following paragraphs.

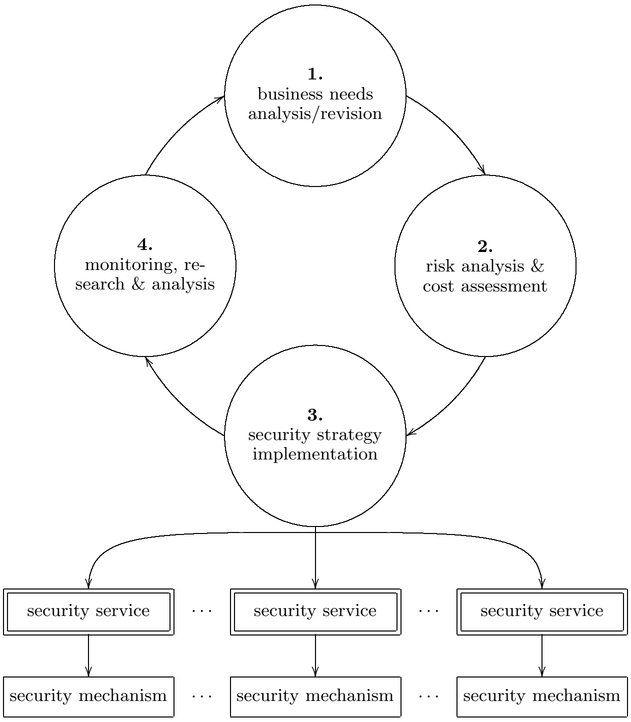
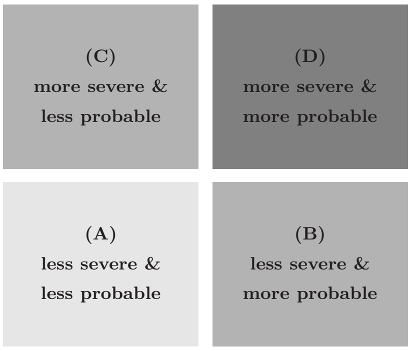


Fig. 7. The life cycle of a system's security strategy.

As already mentioned, security should not be treated in isolation from an organization's vision and strategy, but should be viewed as an integral part of the overall strategic and tactical organizational plan. Thus, any approach to security should start with business needs analysis, in order to provide a solid foundation for setting a strategy. Understanding business objectives and organizational as well as interorganizational requirements is fundamental for identifying the security needs of an Internet billing system. Since such a system surpasses the traditional IS boundaries and extends across multiple organizational entities, a profound understanding of business goals at strategic level is deemed necessary to enable a clear estimation of the demanded security. Moreover, since the information owned by an organization is of critical importance, the information resources that are to be protected, in terms of their value to the business goals, their ownership and physical location should be identified. In addition, it has to be specified from whom the previously defined organizational assets should be protected from. All these issues should be considered in conjunction with the cost of deploying the security strategy. Cost assessment will also determine the provision of management support, an essential part for developing the strategy and a prerequisite for its future application [29].

Having completed the analysis of business needs, the next step is to conduct a risk analysis. Risk analysis constitutes an assessment of the potential vulnerabilities, risks and threats an Internet billing system is facing across all organizational levels. Amongst others, typical business risks include the theft and alteration of data, unauthorized access to sensitive information, inability to meet customer needs quickly and the loss of business. Hence, the purpose of risk analysis is to facilitate decision–making about the desired level of security as well as the methods that should be adopted for preventing risks. The distributed nature of Internet billing systems imply the existence of a multitude of vulnerabilities and threats which have to be thoroughly examined to guarantee a secure environment for Web–enabled commercial transactions. Potential risks should be identified at all levels of the corporate information system, including vulnerabilities and threats associated with network services, architecture, operating systems and applications. The probability of these threats materializing should also be estimated to provide a comprehensive view of the weak points, in a system, that could be exploited accidentally or intentionally and jeopardize its operation. Moreover, risk quantification should include a cost assessment of the possible damage caused by each threat, over against the cost for preventing the threat in terms of time, expenses and resources. The identified risks should then be categorized according to their probability and the severity of their impacts (*see* figure 8), and prioritized with respect to the cost needed for their elimination. Certainly, one needs to consider first those threats resulting in greater losses (classes D and C), but still not to ignore threats, of less financial impact, occurring more frequently (class B). Following the above steps a complete analysis of risks is produced, which will be used proactively to mitigate the number of potential threats compromising the security of an Internet billing system.



(C) more severe & less probable	**(D)** more severe & more probable
(A) less severe & less probable	**(B)** less severe & more probable

Fig. 8. Risk classification according to their severity and probability of occurrence.

When risk analysis is completed, the next step is to implement the organization's security strategy. Undoubtedly, this is the most difficult part of the security strategy development plan, since this step involves the identification of the security services needed to be offered in order to protect the organization's information assets from known and unknown threats. Not all security services are used for the protection of all kinds of information resources, since different classes of data require different levels of security. For example, credit card information, when delivered through a communication channel, requires a high level of confidentiality than that of a still image's data, traveling through the same communication channel, and simply making use of authentication services. Next, the specific mechanism(s) that will be used for applying the security services are examined. For example, many communication protocols exist that provide the aforementioned property of confidentiality (*see* table I), but different protocols may best fit under different conditions and assumptions.

As mentioned in section II, classes of security services include *integrity*, *confidentiality*, *authentication*, *accountability & auditing*, *authorization*, *availability* and *non-repudiation*. In order to provide these security services to an Internet billing system, the following two cases must be considered:

1. the security mechanisms offered for data in transit, and
2. the security mechanisms offered for data in storage,

which are illustrated in tables I and II respectively. What follows is a description of the security mechanisms whose purpose is either to prevent or to detect security incidents, inside and outside a corporate's internal network, is given. This should be of special importance to those faced with the challenge of building a thorough information security strategy.

When data in transit is considered, protocols offering security services are divided into three main categories depending on the *Open Systems Interconnection* (OSI) layer they operate, namely the *network*, *transport* and the *application* layer. Furthermore, the application layer security mechanisms are subdivided into those targeting on data of a specific structure and those targeting on data of specific nature (financial data).

Each mechanism is characterized by its own advantages and disadvantages, e.g. host–to–host authentication is performed by network layer protocols compared to transport layer protocols which provide process–to–process authentication. However, some protocols (like SSL) can also authenticate the user's identity if its public–key certificate is used in the protocol's authentication part (SSL handshake subprotocol). For an excellent survey about the security services provided by the mechanisms of table I, the reader is referred to [20]. The relatively new OFX specification [4], provides support for a wide range of financial activities such as fund transfers, bank & credit card statement downloads, and bill presentment & payment, between a wide range of financial institutions such as banks, merchants, and brokerage houses. OFX is an emerging standard for Internet billing systems due to its advantages of extensibility, robustness, and platform independence, and because it gives a specification for presenting financial data. It provides a framework for building secure online financial services, since both transport–level and application–level security features are incorporated.

TABLE I
MECHANISMS USED TO ENFORCE THE SECURITY STRATEGY FOR DATA IN TRANSIT.

Layer	**Protection**	**Mechanisms**
network/ Internet	host–to–host	IP security protocol (IPSEC), IP authentication header (AH), IP encapsulating security payload (ESP), network layer security protocol (NLSP), point–to–point tunneling protocol (PPTP).
transport/ session	process–to–process	secure sockets layer (SSL), transport layer security (TLS), open financial exchange (OFX).
application	data structure–specific	secure hypertext transfer protocol (S-HTTP), pretty good privacy (PGP), privacy enhanced mail (PEM), secure multipurpose Internet mail extensions (S/MIME).
	data nature–specific	secure electronic transactions (SET), open financial exchange (OFX).

In general, it is easier to protect a corporate's assets from third parties outside the corporate network, than from its employees who intentionally or accidentally may cause severe security incidents. Thus, it is of crucial importance to ensure that everyone inside the corporate network comply with the corporate's security strategy guidelines, which means that security not only depends on the technology used, but also on the proper administration of systems, as well as the observance of related business procedures, physical access controls, and audit functions. Not all business requirements and objectives are identical. Consequently, security mechanisms for data in storage are not absolute – there is not one standard that will fit all businesses and industries. In table II, we present the mechanisms (hardware and software oriented), currently used by many organizations, for safeguarding their critical information. We consider necessary to separate software–based security solutions into the areas of *operating systems*, *database management systems* (DBMS) and other *commercial applications*.

It is evident that one of the most critical elements in protecting the organizational information assets, excluding firewalls and other similar devices, is the security offered by the operating system itself. Operating systems, such as Windows NT and UNIX have implemented controls on who can view, modify or delete information, along with a number of other features for managing these security services. These controls are implemented using ACLs – a form of role–based access control mechanism [6], in addition to SIDs which play a prominent role in providing the system with monitoring capabilities. User authentication is performed by the most widely used mechanism; this of user–name and password, in which case features are provided against password guessability [16], whilst for distributed applications, Kerberos–based authentication is

TABLE II
Mechanisms used to enforce the security strategy for data in storage.

Type		**Solutions**
hardware		smart cards (PVC, EMV), other tamper–proof devices, screening routers.
software	operating system level (Windows NT and UNIX)	password–based authentication, password expiration and filtering, kerberos–based distributed authentication, access control lists (ACL), security identifiers (SID), cryptographic application programming interface (CAPI).
	database management system level	password expiration, password standard's enforcement, break–in detection and evasion, dormant user ID identification, centralized security administration, comprehensive report generation, maintenance of audit logs.
	application level	anti–virus software, audit log analyzers, various commercial products, firewalls, backup utilities.

used. In order to enhance the overall security, the Windows NT operating system for example also provides the feature of storing user–name and password information in smart cards, and a number of other utilities for managing user accounts and recording security–related events.

So far, database management systems have relied upon the security services provided by the underlying operating system, or the user–name and password mechanism, in order to control access to stored data. From this perspective, the entire database is just another file system and therefore internal access control mechanisms could not be easily implemented. In the newer client/server environment, access to databases can be obtained by using a vast number of different applications, query tools and database utilities [3], [11]. This increases the level of security provided, in case when the operating system security controls, if misconfigured, are bypassed by an intruder. Incomplete security functionality and the lack of security management tools at the database level increases an organizations exposure to unauthorized modification, erasure and theft of mission-critical data. The results caused by such attacks are decreased productivity, loss of competitive position and customer confidence. Currently, modern database management systems offer sophisticated tools for implementing an information security strategy at database level. System administrators can take advantage of these tools to control user access in a more granular basis on almost every database object, even to tables or attributes. Features like password expiration & filtering, centralized administration and security report generation, traditionally found in operating systems, have become a common place in the DBMS scene.

The last but equally important type of security mechanisms are those provided by software vendors, and among others they include firewalls, backup & anti–virus utilities and audit log analyzers. These tools implement a complementary security framework to the one established by the previous two types of mechanisms, and they provide administrators with valuable information about the security status of their system (*see* step 4 in figure 7). This information indicates possible weaknesses of the currently deployed security strategy, and may in turn constitute the starting point for radical changes in the organization's strategic plan and/or needs.

In this section we provided a comprehensive framework for aiding the definition and deployment of an information security strategy at the corporate level. What follows is a description of how this framework was used to define the security strategy of an Internet billing system currently being developed for OTE.

IV. Strategy Implementation

'Billing Mall' is an integrated system offering facilities for EBPP, Customer Application Processing and Personalized Marketing (*see* figure 9). EBPP provides electronic delivery of bills to customers through the presentment of bill information, in both summarized and detailed form, and secure electronic payment of a single or multiple bills upon customer request. Customer Application Processing provides the means to the customers who wish to order a new product or service that are available by OTE. Finally, Personalized Marketing provides the necessary functionality and support needed for the effective promotion of products and services based on customer's identified needs and characteristics.

The architectural model of the system has been based on the *Open Internet Billing* (OIB) model, which is currently the predominant model for Internet billing systems. According to OIB, a central service provider, the Consolidator, collects and stores electronic summary bills from registered billers. While offering a single point of access for viewing and paying bills it provides the customer with the option to have access to the biller's web site for detailed bill information. When the customer visits the web site requesting to see a detailed bill, he/she is presented with informative messages regarding products and services available by the Biller's company. The customer is also provided with a facility for placing orders for the advertised products and/or services.

An evaluation of the critical success factors for the deployment of the intended system imposed the need for the parallel development of a comprehensive security strategy. Aiming to guarantee an integrated approach to the multilateral issue of security, the framework described in the previous section has served as the basis for the design and implementation of the system's security strategy. Following the stages prescribed by the framework, a business needs analysis has been conducted first, providing the foundation of the security strategy. In this context, a clear conception of the desired business goals has been formed, indicating the need for a system guaranteeing secure electronic transactions associated with all types of offered services. A rigorous examination of this issue denoted the security re-

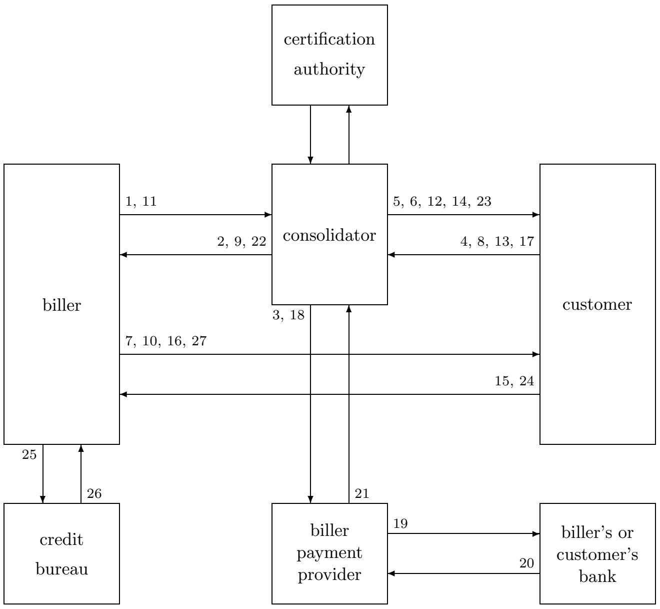


Fig. 9. The 'Billing Mall' Internet bill presentment and payment system. The steps followed are: 1. biller enrolls to consolidator to offer services, 2. biller's certificate from CA, 3. biller payment provider's certificate from CA, 4. customer enrolls to consolidator and selects billers, 5. customer's certificate from CA and login account, 6. announcement of new biller participating in EBPP service, 7. announcement of new biller providing EBPP service, 8. request for receiving and paying bills from the new biller, 9. request for including the new biller in EBPP service is forwarded to biller, 10. notification of EBPP service becoming active for customer, 11. bill summary is made available to consolidator, 12. notification of a new bill made available for viewing and paying, 13. Customer logs in, 14. bill summary is accessed by customer, 15. request for accessing detailed bill information, 16. detailed bill information and personalized marketing, 17. customer initiates bill payment, 18. payment request is forwarded to BPP, 19. payment execution is originated, 20. payment execution is completed, 21. notification for payment completion, 22. notification for bill payment execution and remittance information, 23. notification for successful execution of bill payment, 24. order submission for biller's products and/or services, 25. request for information about risk of crediting customer for purchase of ordered products and services, 26. information about risk of crediting customer, 27. notification about acceptance or rejection of submitted order.

quirements that had to be satisfied in order for the system to be trusted and adopted by the intended customers. To this end, the resources that should be protected were identified at both organizational and interorganizational level, in terms of the information stored, the applications and the hardware used and the underlying network infrastructure. These corporate assets were deemed necessary to be protected from internal as well as external attacks, either intentional or accidental. Finally, in order to mitigate the cost of deploying a secure communication mechanism for financial transactions between the Consolidator and the banks, it was decided that the existing infrastructure currently used for fund transfer between financial institutions should be employed. This implied the need for including an additional entity to the OIB model, the *Biller Payment Provider* (BPP), serving as an intermediary between the Consolidator and the banks.

The next step towards the implementation of the security strategy was to conduct a risk analysis as a proactive diagnosis of the vulnerabilities and threats that could possibly hinder the proper operation of the system. A number of entity-centric and cross-organizational risks were identified and categorized according to the classification scheme described in the framework. In proportion to the probability and severity of their impacts the risk for denial-of-service attacks, and impersonation, in the form of IP spoofing or misrepresentation were prioritized in category D, while data tampering, eavesdropping, and password sniffing were classified as category C risks. Class B included the risk for repudiation of transactions and customer insolvency, and finally class A contained risks related to software, administration and user activity. The results of this process suggested that the potential vulnerabilities and threats should be effectively addressed by carefully selecting and applying risk prevention, detection and response methods. In addition, the analysis of risks revealed that the OIB model was not adequate to provide the anticipated level of security and reliability that is essential for the networked business processes. Thus, it was decided that it had to be extended in order to accommodate for the establishment of a Certification Authority issuing and disseminating digital certificates to the customers. Furthermore, as a means for addressing the risk of insolvent customers, issuing payment transactions that could not be completed due to insufficient credit, a Credit Bureau entity was added to the architectural model of the system. The functional role of this entity is the provision of information related to the credit limit of the customers, eliminating the possibility of financial damage.

In section III, a brief analysis of the mechanisms usually employed for protecting a corporate's mission–critical data, either being transmitted through some communication channel or stored in some magnetic medium, was given. Based on that analysis and on the results of the first two steps of the framework, an information security strategy was implemented.

Since 'Billing Mall' requires the exchange of large amounts of financial information, the first task was to evaluate the security features of existing protocols in the field. Between OFX and SET, the former was found more appropriate because of the following reasons amongst others:

1. it is based on cryptographic protocols[4] known for their strength,
2. it supports the use of channel–level as well as application–level security, and
3. its security architecture is extendible & customizable.

The SSL protocol met the requirements defined by the deliverables of the first two steps of the framework for ensuring the confidentiality and the integrity of data in transit. However, some constrains had to be put into practice concerning the cryptographic algorithms used, as well as the size of the session key. In contradiction to the OFX specification [4], both server and client side certificate–based authentication is required in the channel–level security in

[4] The SSL protocol is used for implementing channel–level security.

order to eliminate security risks. Thus, password encryption is not required as the specification dictates for authenticating the user, who is provided with the additional capability of encrypting vital information inside the OFX message, such as credit card number and/or bank account data, with the OFX server's public key.

Obviously, it is of primary importance that both communicating parties trust each other's certificate. For this reason only one entity, satisfying the requirements imposed by the European Community's 1999/93/EC directive [8], was decided to play the role of the certification authority. The certificates issued by the CA are based on the PKCS #6 extended–certificate syntax standard [25], because of its flexibility in defining new PKCS #9 selected attribute types [26], and its compatibility with applications requiring the use of X.509 certificates[5]. In order to facilitate certificate & key management, from the Customer's point of view, smart card technology was decided to be a basic part of the overall model. As far as 'Billing Mall' is concerned, a defensive policy is enforced regarding the amount for which a certificate is allowed to be used. This limit, which is interpreted as the amount that the user is willing to risk per transaction, is determined by the user and is accepted or not by the CA and the Credit Bureau. Topics such as certificate issuance, renewal, revocation and suspension are fully described in the *Certificate Practice Statement* (CPS), generated by the corresponding *Policy Creation Authority* (PCA) and approved by the *Policy Approving Authority* (PAA).

Firewalls, as expected, are the first line of defense in all entities[6] participating in the 'Billing Mall' system. Particularly, it is suggested that important information only be accepted from and delivered to servers with a specific IP address, which means that any network package sent by an unknown IP address is automatically rejected. Example procedures taking advantage of this feature are the following:

1. the Consolidator only accepts bill summary information from a small set of IP addresses in the Biller's domain,
2. the Consolidator only forwards Customer's payment requests to the specific BPP's IP address.

This technique allows some degree of resistance against attacks such as the denial of service attack and IP spoofing.

In order to facilitate dispute resolution, the Consolidator[7] holds a complete record of all security–related events occurring within its site, such as Customer's login time/date, Customer's bill payment request, and biller's descriptive bill information delegation. In addition to this feature, every time the Customer initiates a bill payment procedure, he gets back a notification indicating success or failure of the payment process. This notification is, in fact, a message digitally signed with the Consolidator's private key which contains the information returned to the Consolidator by the BPP.

As previously mentioned, smart cards are employed for storing the Customer's certificate and private key. Other mechanisms used for protecting information stored locally, according to the analysis presented in section III, are based on the standard security features offered by the Windows NT operating system and the Microsoft SQL Server.

V. Conclusions

Conducted at the corporate level, the aim of an information security strategy should be to offer a foundation which ensures that business risks to a company's critical information in storage or in transit do not effect in any way the realization of business strategy objectives. Such a security strategy should aid in defining the steps to be undertaken, the ways that these are enforced and the mechanisms available for security management.

In this paper we presented an integrated approach to the development of an information security strategy based on a rigorous framework that helps in the evaluation and use of the available tools and techniques in a systematic manner. Our position that any security strategy must evolve concurrently with the design of the system and not be approached as an afterthought is reflected in the framework which follows closely the phases of a *Systems Development Life Cycle* (SDLC). In addition, the structure of the framework enforces the view that any security strategy must be conducted at the corporate level and not be seen merely as a local technology issue.

Without doubt we believe that the approach presented herein could be further refined and enhanced. 'Waterproof' security of large interorganizational systems is an issue of immense complexity but we believe that we have at least made the necessary first steps towards meeting this challenge.

VI. Acknowledgement

We greatfully acknowledge the *Greek Secreteriat for Research and Technology* (GSRT) for financing the 'Billing Mall' project. We would also like to thank the partners involved in the project: Athens University of Economics and Business, Cyberce Consultants, Datamedia, Sysware, Teiresias, and the University of Crete.

References

[1] A. Abela and J. R. Sacconaghi, "Value exchange: The secret of building customer relationships on line," *The McKinsey Quarterly*, no. 2, pp. 216–219, 1997.

[2] F. M. Avolio, "A multi-dimensional approach to internet security," *Networker*, pp. 15–22, Apr/May 1998.

[3] BrainTree Security Software Inc., *Client/Server Database Security*, 1999. White Paper.

[4] CheckFree Corp., Intuit Inc. and Microsoft Corp., *Open Financial Exchange*, Nov 1998. Specification 1.5.1.

[5] S.-K. Chin, "High-confidence design for security: don't trust – verify," *Communications of the ACM*, vol. 42, pp. 33–37, Jul 1999.

[6] Coopers & Lybrand L.L.P., *Microsoft Windows NT Server: Security Features and Future Direction*, 1997. White Paper.

[7] Derivion Corp., *Internet Billing and the Mid-Tier Biller: Enjoying the Benefits of Electronic Bill Presentment and Payment*

[5] An X.509 certificate is actually contained in a PKCS #6 certificate.

[6] This does not include the Customer.

[7] The Consolidator is an intermediary or a trusted third party.

without Operational Compromise, 1999. Available at http://www.derivion.com/index_9.html.

[8] European Parliament and the Council of the European Union, *on a Community Framework for Electronic Signatures*, Dec 1999. Directive 1999/93/EC.

[9] W. Ford and M. S. Baum, *Secure electronic commerce: building the infrastructure for digital signatures and encryption*. Prentice Hall, 1997.

[10] E. Hughes, "A long-term perspective on electronic commerce," *Networker*, pp. 38–50, Nov/Dec 1997.

[11] Internet Security Systems Inc., *Securing Database Servers*, 1999. White Paper.

[12] Just In Time Solutions Corp., *The Value of Internet Billing*, 1999. Available at http://www.justintime.com/internetbilling/index.html.

[13] C. Kaufman, R. Perlman, and M. Speciner, *Network security: private communication in a public world*. Series in Computer Networking and Distributed Systems, Prentice Hall, 1995.

[14] N. Kolokotronis and N. Kalouptsidis, "On the linear complexity of binary sequences generated by LFSRs with nonlinear combining functions," *under review in IEEE Transactions on Information Theory*, Jul 1999.

[15] C. E. Landwehr and D. M. Goldschlag, "Security issues in networks with internet access," in *Proceedings of the IEEE*, vol. 85, pp. 2034–2051, Dec 1997.

[16] Microsoft Corporation, *Meeting Enterprise Security Needs: Windows NT and UNIX*, 1998. White Paper.

[17] National Institute of Standards and Technology, "Data encryption standard," Federal Information Processing Standards Publication 46-2, U.S. Department of Commerce, Dec 1993.

[18] National Institute of Standards and Technology, "Des modes of operation," Federal Information Processing Standards Publication 81, U.S. Department of Commerce, Dec 1980.

[19] R. K. Nichols, *ICSA guide to cryptography*. McGraw-Hill, 1999.

[20] R. Oppliger, "Internet security: firewalls and beyond," *Communications of the ACM*, vol. 40, pp. 92–102, May 1997.

[21] J. Ouren, M. Singer, J. Stephenson, and A. L. Weinberg, "Electronic bill presentment and payment," *The McKinsey Quarterly*, no. 4, pp. 98–106, 1998.

[22] P. Papadopoulou, A. Triantafillakis, P. Kanellis, and D. Martakos, "A generic framework for the deployment of an internet billing servicescape," in *Proceedings of the 1st World Congress of Electronic Commerce*, Jan 2000.

[23] P.-A. Pays and F. de Comarmond, "An intermediation and payment system technology," *Computer Networks and ISDN Systems*, vol. 28, pp. 1197–1206, 1996.

[24] M. Y. Rhee, *Cryptography and secure communications*. McGraw-Hill, 1994.

[25] RSA Data Security Inc., *PKCS #6: Extended–Certificate Syntax Standard*, Nov 1993. version 1.5.

[26] RSA Data Security Inc., *PKCS #9: Selected Attribute Types*, Nov 1993. version 1.1.

[27] R. A. Rueppel, *Analysis and Design of Stream Ciphers*. Communications and Control Engineering Series, Springer-Verlag, 1986.

[28] B. Schneier, *Applied cryptography: protocols, algorithms and source code in C*. John Wiley & Sons Inc., 2nd ed., 1996.

[29] A. Segev, J. Porra, and M. Roldan, "Internet security and the case of bank of america," *Communications of the ACM*, vol. 41, pp. 81–87, Oct 1998.

[30] K. M. Walker and L. C. Cavanaugh, *Computer security policies and SunScreen firewalls*. Sun Microsystems Press, Prentice Hall Title, 1998.

[31] L. Wanninger, C. Anderson, and R. Hansen, *Designing Servicescapes for Electronic Commerce: An Evolutionary Approach*, 1997. Available at http://www.misrc.umn.edu/wpaper/default.asp.