7th INTERNATIONAL MULTIDISCIPLINARY CONFERENCE
Baia Mare, Romania, May 17-18, 2007
ISSN-1224-3264

BUSINESS MODELS AND SECURE WEB LEARNING ON PUBLIC KEY INFRASTUCTURES

Cezar Toader[1], Adrian Petrovan[2], Cristinel Costea[3]
[1]Professor PhD, [2]Assistant, [3]Assistant
North University of Baia Mare, 62/A V.Babeş Street, Baia Mare, RO-430083, Romania

Abstract: *This paper deals with Public Key Infrastructures (PKI) deployment considerations in an enterprise medium. After a presentation of services offered by public-key cryptography, business models secured with this technology are presented. On top of these infrastructures, Web-based learning systems can be implemented and the secure communications between learners and Web-learning servers are assured.*

Keywords: *Network security, business models, Web learning, secure communications, Public Key Infrastructure.*

1. SERVICES OF PUBLIC KEY CRYPTOGRAPHY

After the year 1976 the problem of network security and the cryptography knew interesting new directions. Diffie and Hellman imagined a new security technology in which the key for encryption and the key for decryption were related but different. More, it is possible to made public one of these key without the danger of anyone being able to compute the other. Their concept presented in [2] was radical at the time. Since then, a large number of mathematicians, computer scientists and engineers explored the boundary between theory and practice and tried to understand the difficulty of specific mathematical problems. Since the publication of the classic Diffie-Hellman paper, much progress has been made, but the research in the field of asymmetric ciphers and related subjects continues.

Asymmetric ciphers make use of two related keys. In this key pair, knowing one does not allow derivation or computation of the other even if the enemy can use a lot of computing power. The information encrypted with one key must be decrypted with the other one. This means that one of the keys will be made publicly available, and the other one will be kept private. The idea that one of the keys in this pair can be revealed publicly was so radical and this method became known as public-key cryptography.

The relationship between the keys in a pair is mathematical and may rely on information known only by the key pair creator. In this technology, the security is based on the fact that that is computationally infeasible for anyone than the key pair creator to derive the private key from knowledge of the public key.

Of course, theoretically, the private key can be derived, but the amount of time, memory and computing power necessary to do so is prohibitively high.

The more important and interesting services of public key cryptography are: security of communications between strangers, encryption, digital signatures, data integrity, and key establishment.

The use of public key cryptography make possible to ensure privacy and security of Internet connections between two entities, such as an electronic shop and an unknown client. This technology is the base of Web security, having direct effects in e-commerce, e-business.

The client establishes a connection with the desired website. First step is to accept the download of the public key in order to start a secured communication with that website. At the other end of connection the private key is kept in a very secure place in that operating system. The information send by the electronic shop, for example, to the client is encrypted with the private key and can be decrypted only with the public key. All the information send by the client is encrypted using the public key and can be decrypted only by the owner of the private key, in this case, the electronic shop. Thus, the client can be sure that at the other end of the connection is the right website (institution or business), and the system on the other end (the electronic shop) is sure that nobody can interfere in the communication with the client.

There are many environments where the computation involved in public key cryptography is to slow and impractical. The use of symmetric cryptography would increase the computation speed. Typically what is done is a two-step process, as follows:

- A symmetric key is randomly generated and the data is encrypted with this key.
- The symmetric key is then encrypted using the public key of the intended recipient of data (institution or business).

When the recipient receives the encrypted data a two-step process takes places:

- The recipient decrypts the symmetric key using the private key.
- The actual data is decrypted using that symmetric key.

The two-step processes presented above are typically used rather than data encryption and decryption using the key pair (public and private keys). The processes speed is increased, the processing is kept clear and simple, even the total amount of data is small.

There is a service enabled by the public key cryptography that is not achievable with secret key cryptography (with symmetric ciphers): the digital signature. This is analogous with handwritten signature because a single entity can sign some data, but any number of entities can read that signature and verify his accuracy.

A digital signature relies on the concept of a key pair. There must be a private key known only by the entity (institution or business), named here A, that signs some data. That

encrypted data is uniquely and explicitly tied to the entity A. On the other hand, the public key must be available to a wider group of entities (noted B) so that the signature can be verified and identified to the emitting entity A.

The emitting entity A might compute a Message Authentication Code (MAC) on some data using the symmetric cryptography. But the symmetric key used by A would have to be revealed to any entity B wishing to verify the value of MAC. Details about MAC computation and verification are presented in [3]. After the secret key is revealed to B, this value can no longer be tied with entity A, because it can be used by B to create encrypted data as well. Thus the computation that entity A performs this way cannot be considered a signature.

We can think of the digital signature as a private key operation on data in which the resulting value is the signature. If A is the only entity who knows this private key, then A is the only entity who could sign that data. On the other hand, any entity B, knowing the public key, can verify the signature by doing a public key operation on the signature and checking whether this result corresponds with the original data.

Data to be signed can be of any size, but a private key operation takes a fixed size input and computes a fixed size output. In order to do so, a cryptographic hash function is used (details in [6] and [5]). This hash function has the property that it maps an input of arbitrary size to a fixed size output (suitable for a future private key operation) and it is computationally infeasible to find two different inputs that produce the same hash outputs.

The signing process has two steps:

- The signer uses the hash function to obtain a fixed size value (uniquely related to data).
- The signer does a private key operation on this hash value.

The verification process has also two steps:

- The verifier hashes the data to find the fixed size hash value.
- The verifier examines this value, the received signature and the public key of signing entity. If the signature matches the key and the hash value, then the signature is considered verified, otherwise the verification fails. Details in [8].

A digital signature provides both data origin authentication (who originated the data) and data integrity (data has not been altered in any way). Any alteration of data will lead to a different hash value, which cause a failure in signature verification. If the signature verification is successful, then the verifier is confident that data integrity has been preserved.

2. PKI – PUBLIC KEY INFRASTRUCTURE

A PKI is the basis of a security infrastructure whose services are implemented and delivered using concepts and techniques based on public key cryptography. The fundamental

premise in the original formulation of public key cryptography was that two strangers should be able to communicate securely. In order to use digital certification on a large scale, several concepts have been formulated and analyzed: certification authority, certificate repository, certificate revocation, key backup and recovery, certificate lifetime and automatic key update, key history, cross-certification, non-repudiation, time stamping. Details on [1].

A PKI is generally considered to be associated with three primary core services:

- *Authentication* – is the assurance to one entity that another entity is who he/she/it claims to be.
- *Integrity* – is the assurance to an entity that data has not been altered in any way.
- *Confidentiality* – is the assurance to an entity that no one can read a particular piece of data, except the receiver explicitly intended.

There are several mechanisms used to enable the PKI services of authentication, integrity and confidentiality. Details in [4], [7], [RFC2104], [RFC2144]. Based on the PKI core services offered, new PKI enabled services can be defined:

- Secure communication.
- Secure time stamping.
- Non-repudiation.
- Privacy.

Secure communication means the transmission of data from a sender to a receiver with one or more of the properties of authenticity, integrity and confidentiality. Examples: secure e-mail, secure Web server accessing, and secure VPN – Virtual Private Networks.

These PKI-enabled services are described in many books [1], papers and Internet Requests for Comments: [RFC2311], [RFC2312], [RFC2246], and [RFC2410].

3. PKI DEPLOYMENT AND BUSINESS MODELS

A PKI is a comprehensive security infrastructure and not many point solution. PKI offers a single security infrastructure that can be used across multiple applications in different environments. Specifically, a PKI can be used to enable confidentiality, integrity, authentication and non-repudiation services in numerous contexts: secure e-mail, secure electronic data interchange, secure electronic forms, secure desktop and remote access, secure intranets, secure extranets, secure Web applications, and object signing.

The benefits realized from these services are extensive, but in many cases hard to quantify.

From a corporate-security perspective, the overall goal is to provide cost-effective, usable security that is commensurate with the perceived level of risk.

Considering the internal communications business model, the business needs a particular security solution from the following areas:

- Enhanced authentication and accountability.
- Secure e-mail.
- Secure desktop and remote access.
- Secure internal (intranet) and external (extranet) communications.
- Paper reduction through adoption of secure electronic forms.

The external communications business models are treated from two perspectives: *business-to-business* (B2B) and *business-to-consumer* (B2C)

The main goal in B2B communications is to provide secure and cost-effective interorganizational communications. A given business may want to communicate with external sources for a variety of reasons: payment transfer, purchase-order exchange, collaborative research, preauthorization of financial transactions, correspondence, supply chain management, secure document exchange.

Today's B2C e-commerce would not be possible without the Internet and Web. There are two prevalent business models when it comes to provide B2C electronic commerce.

The first model is *user-centric*. Individual users obtain their own certificates from a third-party service provider or they generate their own certificates. In many cases they use standard Web technology to do business. This model is unstructured and uncontrolled, in which the most basic certificate is simply unavailable. In this model, e-commerce is based on SSL or TLS protocol (see RFC 2246), which provides a confidential tunnel between the Web server and the browser. However, the use of SSL/TLS is criticized due to a lack of "persistent" confidentiality. When the server decrypts data, if it does nothing to protect that data, it is vulnerable to attack. In addition, SSL/TLS does not support digital signatures over the data, so there is no way to preserve a persistent digital signature in association with a given transaction, which is a serious limitation in applications based on transactions.

The second model is *organization-centric* and it was adopted by many organizations. This model is more controlled and more secure than the first model. In this model, an organization has a Certification Authority. The certificates are issued for the constituents of that organization for a specific purpose. This model may also include the use of special-purpose software, typically issued from the organization to the individual user, in order to offer more comprehensive certificate management and more secure communications. It also enables the organization to easily control the purpose and scope of the certificates it issues.

The second model seems to be adequate to organization oriented to Web learning, where the teaching materials and also the results must be secured and the users access to that data must be kept under control (see figure below). In order to support Web learning activity, the network must fulfill several requirements:

- Regular users must have the possibility to connect to Web-learning servers any time from a special designated subnet within the organization or from a remote location (from their home) and this connection must be secure (usually using SSL/TLS).
- Teachers must be able to connect to servers and send data or modify existing data. They often need to create teaching materials or modify them. Also, they need to access the exam results (for this, special designated reporting services must be functional).
- Administrators must have full access to the servers and powerful authentication systems are necessary. Their connections must be secure. For login to servers from a remote computer, SSH (Secure Shell) systems must be implemented. Details on SSH protocol in Internet Request for Comments RFC 4250, 4251 … 4256.

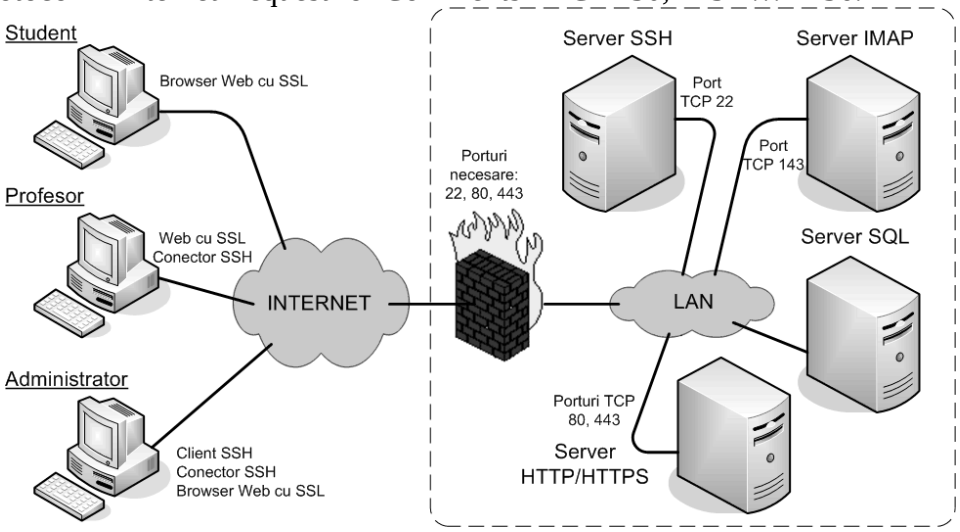

Fig.1. *Sketch of secure network adequate for Web-learning*

REFERENCES

1. Adams, C., Lloyd, S., *Understanding PKI: Concepts, Standards and Deployment Considerations*, 2nd ed., Addison-Wesley, Pearson Education, 2003.
2. Diffie, H., Hellman, M., *New Directions in Cryptography*, IEEE Transactions on Information Theory 22, 1976.
3. Federal Information Processing Standards Publication 113, *Computer Data Authentication*, Springfield, US Department of Commerce, National Bureau of Standards, 1977.
4. Menezes,A., Oorschot, P.van, Vanstone, S., *Handbook of Applied Cryptography*, CRC, 1997.
5. Preneel, B., Govaerts, R., Vandewalle, J., *Information Authentication: Hash Functions and Digital Signatures*, Computer Security and Industrial Cryptography: State of the Art and Evolution, Springer-Verlag, Berlin, 1993.
6. Preneel, B., *Analysis and Design of Cryptographic Hash Functions*, PhD diss., Katholieke Universiteit Leuven, Belgium, 1993.
7. Rivest, R., Shamir, A., Adleman, L., *A Method for Obtaining Digital Signatures and Public-Key Infrastructures*, Communications of the ACM 21, 1978.
8. Stallings, W., *Cryptography and Network Security: Principles and Practice*, 2nd ed., Prentice Hall, 1999.
9. [RFC2104] – HMAC – Keyed Hashing for Message Authentication, 1997.
10. [RFC2144] – The CAST-128 Encryption Algorithm, 1997.
11. [RFC2246] – The TLS Protocol version 1.0, 1999.
12. [RFC2311] – S/MIME version 2 Message Specification, 1998.
13. [RFC2312] – S/MIME version 2 Certificate Handling, 1998.
14. [RFC2410] – IP Security Document Roadmap, 1998.
15. [RFC 4251] – The Secure Shell (SSH) Protocol Architecture, 2006.
16. [RFC 4252] – The Secure Shell (SSH) Authentication Protocol, 2006.
17. [RFC 4254] – The Secure Shell (SSH) Connection Protocol, 2006.