J. Lopez, A. Mana, and J. J. Ortega, "An User Authentication Infrastructure for Extranet Applications", *IEEE International Carnahan Conference on Security Technology*, pp. 354-362, 1999.
NICS Lab. Publications: https://www.nics.uma.es/publications

AN USER AUTHENTICATION INFRASTRUCTURE FOR EXTRANET APPLICATIONS

Javier López, Antonio Maña and Juan J. Ortega
Computer Science Department
E.T.S. Ingeniería Informática. University of Málaga
29071 Málaga. SPAIN
{jlm, amg, juanjose} @lcc.uma.es

An Extranet is used to connect businesses with their suppliers, customers or other businesses that share common goals in a way that automates their administrative interactions using Internet technology. The security of the communications over Internet is considered an essential feature. To guarantee secure operation the aid of some user authentication infrastructure is needed. This paper introduces a Public Key Infrastructure (PKI) and user identification scheme to be used in extranet applications. The flexibility of the system allows it to fit the usual hierarchical organization structure.

INTRODUCTION

There has been a time when companies could allow their Local Area Networks (LANs) to operate as separate, isolated islands. Each branch office might have its own LAN, with its own naming scheme, email system, and even its own network protocol. However, as more companies resources moved to computers, there came a need for these offices to interconnect. This was traditionally done using leased phone lines of varying speeds. The most representative example is *Frame-Relay* service [1][2], which is based on the transfer of information frames between intermediate switching offices. The service, that uses *Permanent Virtual Circuits* (PVCs) through telephone network routers, presents some drawbacks:

- It becomes expensive because connections remain open permanently.
- The architecture creates large latency periods because of the poor connectivity between intermediate routers.
- Full connectivity requires the increment of PVCs and, hence, of intermediate network routers; but the cost of avoiding routing problems in this way is high.
- The number of companies that offer Frame-Relay services is small compared to the number of *Internet Service Providers* (ISPs), so competitiveness is more limited.

Evolution of commercial needs and transference of company resources to computers have forced organizations to interconnect the networks of their branch offices, setting up their own private networks.

On the other hand, open networks, like Internet, offer a more profitable solution than leased lines because they use relatively low-cost, widely available access to public networks to connect remote sites together safely. Rather than using proprietary networks to exchange information, companies can now leverage their investments in Internet Technology, because those new network architectures are inherently more scalable and flexible

than classical WANs, and they allow organizations to add and remove branch offices into their systems in an easy way.

Moreover, today, being able to procure and provide access to information is a defining characteristic of successful companies. And as companies open up their networks to partners and other third-party users to share information, security has become more important than ever. Companies require comprehensive security systems that allow controlled access.

Therefore, a company needs to be able to limit access so that only specified individuals have access to certain resources. This means that traditional encrypted tunnels of, for instance, *Virtual Private Networks* (VPNs), which are fine as long as everyone at both ends is trusted, are inadequate for third-party access. When it comes to sharing information with outsiders, companies need to provide one-way directed access to predefined information.

An *Extranet* is a communication network connecting businesses with their suppliers, customers or other businesses that share common goals in a way that automates their administrative interactions. When properly designed and implemented, extranet systems can be highly effective in improving cross-company information flows, as well reducing the administrative burdens of repetitions inter-company requests. Extranet services use existing Internet interactive infrastructure, including standard servers, email clients and Web browsers. This makes extranets far more economical that the creation and maintenance of a proprietary network. It enables trading partners to form a tight business relationship and a strong communication bond. Hence, companies can use extranets for diverse applications, such as: Order Status Inquiry, Inventory Inquiry, Account Status Inquiry, On-line Catalogs, Order Entry, Warranty Registrations, Customer Service Claims, On-line Discussion Forums, Custom Pricing, etc.

But an extranet requires a high degree of security and privacy from competitors. Because extranets are all about letting third-party users into corporate networks, they need to be extremely secure, and access needs to be highly controllable. Access control, authentication, encryption, and filtering, all core elements of a secure extranet, are most effective when tightly integrated into a single comprehensive security and management platform.

Public-key cryptography [DiHe76] seems to be well suited to satisfy the requirements of the Internet, and is fast becoming the foundation for those applications that require security and authentication in an open network. Public-key cryptography is based on the use of *digital certificates*, computer-based records that attest to the connection of public keys to identified subscribers, sometimes providing additional information about them. A digital certificate can be used in three ways:

- First, it allows the owner to sign documents and data transmissions;
- Second, a certificate can be used to send somebody confidential information;
- Third, a certificate can be used to authenticate somebody, just as a username and password can be used for authentication purposes. Authentication means that a certificate could be used to control access to different portions of a Web site, or even different portions of an extranet.

Still, the use of a global scale public-key cryptosystem is not practical unless it is

complemented by an efficient and trustworthy mean to manage and distribute digital certificates. This service is covered by a Public-Key Infrastructure (PKI) that additionally provides confidentiality, integrity, authentication and non-repudiation between parties that do not have an external relation. Up to the moment different infrastructures have been proposed to cover PKI services in the Internet environment, but none has achieved an extensive use.

PUBLIC KEY INFRASTRUCTURES FUNDAMENTALS

Definitions

As mentioned before, the use of a global public-key cryptosystem for extranets requires the operation of a PKI. The reason is that it is impractical and unrealistic to expect that each employee in a company will have a previously established relationship with all other employees in every company included in the extranet. The staff of every company is continuously changing; new employees join the company while others quit, are fired or promoted. In this scenario, it is inefficient and risky for every node to control the access of all external users in the same way it is done in a local area network. The use of digital certificates as a mechanism for identification and authorization can solve this problem.

Issuing of digital certificates is the most important function of a PKI. Within most PKIs, some predetermined entities are responsible for the issuance of certificates; these trusted entities are called *Certification Authorities* (CAs).

Another basic PKI process is certificate *validation*. The information signed by the issuer CA can change over time. The user of a certificate needs to be sure that all the data it contains is trustworthy and up to date. A process closely related to validation is certificate *revocation*. Security of private keys is paramount in public-key cryptography. It is inevitable that someone's key will be lost or compromised, either through carelessness or a successful cryptanalytic attack. In addition, there are circumstances – such as when a company goes out of business, or an employee quits, is fired or transferred to a new position – when a key may no longer be needed or used. Thus, sometimes a certificate needs to be revoked before it expires. The most common solution to revoke certificates is to use a *Certificate Revocation List* (CRL), a database of certificates that have been revoked before their expiration date.

The certification relationships are not limited to parent and children. A CA can certify another CA located in a different branch of the certification graph, producing a *cross-certification*. Its use allows greater flexibility and short certification paths. But problems arise when the number of cross-certificates is high. In that case, this feature does not yield a viable architecture for the PKI.

Proposals

Many proposals have been introduced as PKIs for general use in the Internet, but only a few have achieved an extensive use. Let us briefly summarize their essential features

One of the first ones was *Privacy Enhanced Mail* (PEM) [RFC1422] [RFC1424], based in X.500 standard [ISO88], but one decade later, the solution of the X.500 directory has not reached its global implementation and everything indicates that this is not going to occur. Moreover, the *Internet Architecture*

Board has recently considered PEM as *not useful* [RFC2316].

Based on the work of PEM, the IETF PKIX Working Group has proposed an infrastructure [PKIX97] that covers automatic identification, authentication, access control and authorization functions using the X.509 v3 certificates [ISO96]. The draft papers elaborated by this group have not been adopted as standards yet because some implementation issues are not definitely closed.

The recent extensions to the *Domain Name System* (DNS) [RFC1101] establish another proposal that allows authentication through digital signatures. Its name is Secure-DNS [RFC2065] [RFC2137]. These extensions describe a hierarchic PKI, integrated into the DNS database.

There are some proposals that do not have a fixed PKI structure. In those cases every user can act as a CA, with full autonomy to assign trust. The most important example of this type of unstructured PKIs is Pretty Good Privacy (PGP) [Zimm95], where users build their confidence on other users certificates. Therefore, a *web of trust* is created between users. This is a good option for communication among a closed set of persons as, for example, a group of friends. A very important problem of PGP is that no entity is responsible if (or when) something goes wrong, not even the user. The use of PGP in a commercial situation is difficult and may not adequately protect the business interests involved, as they usually need to be guaranteed in well-defined contracts with accurate responsibilities. There are some problems associated to scalability and key administration too; for instance, revocation process is problematic, since multiple users may sign the same public key.

Other proposals as *Simple Public Key Infrastructure* (SPKI) [SPKI98a], and *Simple Distributed Security Infrastructure* (SDSI) [RiLa97] are similar to the previous one in the sense that no global PKI is used. These proposals introduce a framework for the deployment of a partial PKIs that can interoperate by sharing a common environment composed of a certificate structure and related operating procedures. Both schemes share the idea that every subject must be unequivocally identified by a number, the public key, and not by a common name (contrary to the X.500-based proposals). Actually, both proposals are merging [SPKI98b].

DESCRIPTION OF THE SYSTEM

Design goals

The fundamental principles of the system were defined and summarized in the following basic goals:

- provide secure, flexible and efficient means to identify users in the extranet;
- eliminate problems associated with the revocation procedures, specially those introduced by the use of centralized systems or CRLs;
- use a distributed CA architecture that satisfy the needs of intra-company departmental certification;
- avoid scalability problems associated to both extranet or company expansion; and
- avoid synchronization problems associated to schemes that keep multiple copies of digital certificates.

Structure

Each company has its own structure of departments, divisions, subsidiaries, etc.

And in most cases it would be desirable that the authorization structure could mimic or fit the company structure. The structure of a typical company is shown in Figure 1.

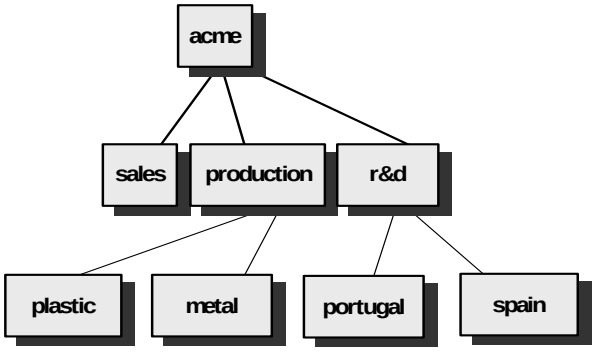

Figure 1. Structure of a Company

Considering that the different organizational structures of companies share hierarchical characteristics, the system proposes a scheme with various managers as CAs that operate independently over different groups of employees, conforming a hierarchy where each node is associated to any division and department email office in the company. The main element in the computer system hierarchy is the *Keys Service Unit* (KSU), which integrates key certification and management functions. Figure 2 shows the resulting KSU hierarchy for the company presented in Figure 1.

As can be deducted from the figure, the KSU hierarchy defined by this system is parallel to the hierarchy of Internet domains. The KSUs are associated to any e-mail office corresponding to an Internet domain (i.e. organization departments and divisions).

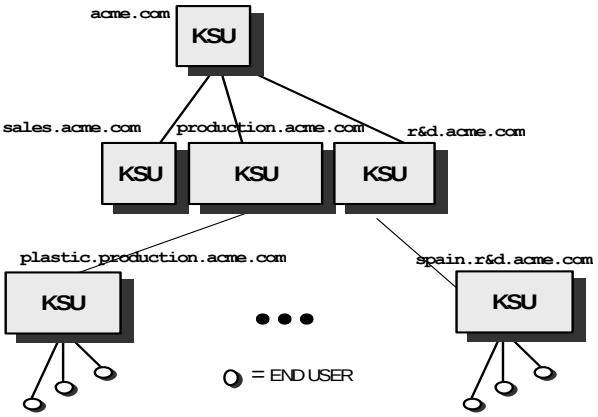

Figure 2. Hierarchy of KSUs

Every KSU is managed by a CA (division/department manager) as Figure 3 illustrates. Additionally, it contains a database to store the certified keys of its users. It must be emphasized that each user's certificate is stored exclusively in the database of his/her KSU. The third component is the key server, which receives requests and delivers the certificates.

The figure shows that the database is solely managed by the corresponding CA; therefore, updating and revocation of certificates are local operations that do not affect the rest of the system. It must be emphasized that CRLs are not needed in the system.

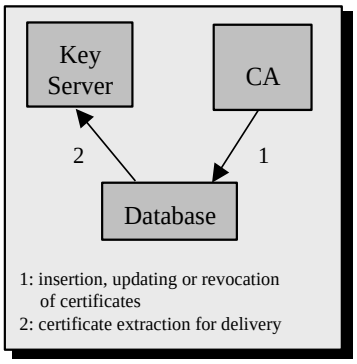

Figure 3. KSU Components

System Operation

The scheme defines a special user called *CA@<domain>* (*CA@x.y.z* in the example

shown in) in every KSU that denotes the correspondent CA. The certificate of any CA is stored in the database of its parent KSU (*y.z*). Finally, the keys of the root CAs, the CAs located in the top-level domains (.*z*), are cross certified to establish the extranet.

We review now the certificate request process. The only information needed to request a key is the e-mail address of the key owner. Figure 4a shows the information flow produced when user *Bob* (*bob@r.s.t*) requests the key of user *Alice* (*alice@x.y.z*).

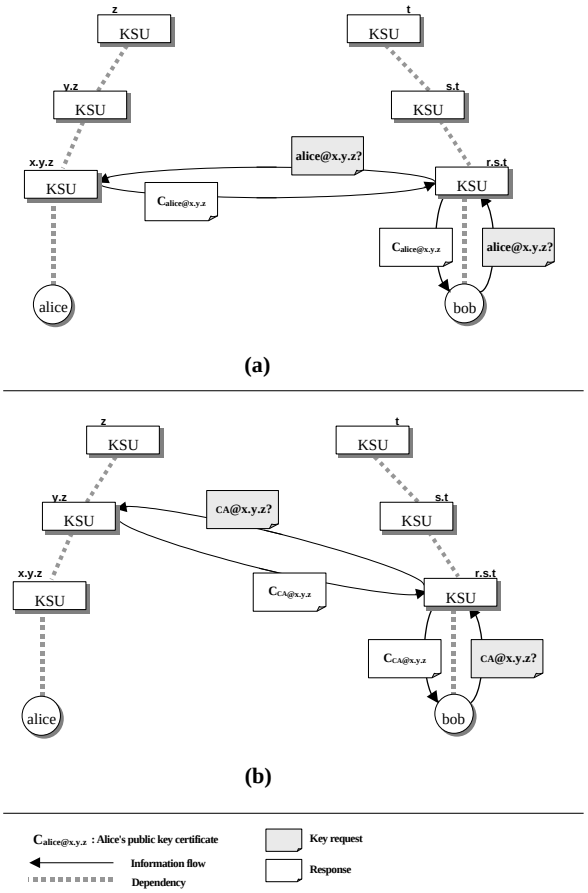

Figure 4 a) Certificate Request
b) Certificate Verification

As shown in the figure, Bob requests Alice's key from his own KSU (step 1) and this one directs the request to the KSU located at the *x.y.z* node (step 2). The response from the addressee's KSU (step 3) is then forwarded to Bob (step 4). Bob must request the key from his KSU due to the access restrictions that other KSUs set, and also to take advantage of the proxy of his KSU.

Afterwards, in case Bob needs to be more confident in the received certificate, he can request the certificate of *CA@x.y.z* from the KSU located at *y.z*, obtaining a new certificate (Figure 4b).

This procedure guarantees Bob that Alice's CA was not impersonated. If desired, the ascending verification process can continue until the top-level node of the company is reached. If no KSU is present at certain node, say *y.z*, the certificate of *CA@x.y.z* is automatically requested from the parent node, that is, *z*. This allows that a company uses an incomplete structure without loss of functionality. For example, the employees of the division of *sales* at *Málaga* of the *Acme Company* can be registered in the KSU installed at *malaga.sales.acme.com* while all the other people in *Cádiz* and *Granada* (where a KSU is not installed) are registered in *sales.acme.com*.

User identification based on the e-mail address

It must be pointed out that many of the identity certificates presently used are based exclusively in a contact through Internet between the user and the CA. This is clearly unsatisfactory because the acceptor of a certificate will usually require some proof of the link between the identity of the user in the real world and his name in the Internet world. Therefore, in these certificates, trust is mislead from the start. In our system, a CA will only certify the keys of those users that are close to it; that is, the manager (CA) will only certify the employees (users) belonging to the division/department

There are two common criticisms about the use of e-mail addresses as distinguished names. Firstly, it is claimed that the relationship between a person in the real world and an electronic mail address is not univocal because a user can have several e-mail accounts and different aliases. Besides, there are certain e-mail addresses that don't represent a single user but a group of them. Secondly, it is also claimed that, in some cases, the alias file can be modified without *administrator* or *root* permissions. Our scheme is not exposed to these disadvantages because it makes no distinction between an e-mail account and an alias, therefore the translation between the e-mail address and the real-world identity will always success.

Regarding the second criticism, although a malicious user could change, under some circumstances, the address that is represented by an alias, no problem arises unless the registered user of the alias gives up his private key to the malicious one. It is evident that this malicious user will not be able to certify and insert the new key in the KSU database.

Additional Features

One of the advantages of the system is that, in case the private key is compromised or lost, the associated public key can be revoked or replaced without the knowledge of the private one. This is possible because there is a manager responsible for the maintenance of the database of certificates, which can identify the real-world employee. Opposed to other systems that require that the user generates a "suicidal note" to be used in case the key is compromised or lost or designates an “authorized revoker” for that cases, users of this system do not need to take any prevention measures for this circumstance.

The need to access CRLs to check for certificate revocations becomes a performance handicap. Frequently, systems that use CRLs or similar mechanisms (e.g., On-line Certificate Status Protocol [PKIX98], or Suicidal Bureaus [Rive98]) as a tool to invalidate certificates incorporate solutions to minimize the number of accesses needed to verify a certificate, but these solutions are sometimes artificial and not efficient. Therefore, avoiding the use of CRLs has been considered one of our priority goals.

To achieve a design that does not expose the mentioned problems of the use of CRLs, we impose the following restrictions:

- All the information related to the certification of a specific user must be located and managed at the corresponding KSU.
- Users must not distribute their certificates. On the contrary, the certificates must be kept in the database of the corresponding department and distributed by their KSU.

When a user certificate needs to be invalidated (because his/her key has been lost or compromised, or because the CA has to cease certifying the user) the CA simply deletes the certificate from its database. This procedure is simple, immediate and requires no communication.

Our approach shares some ideas with the Secure-DNS proposal. Both use the Internet domain name hierarchy to find the location where a particular key is stored, but the Secure-DNS uses the Name Server files while we use the e-mail offices. This choice is based on the following reasons:

- Frequently, DNSs are not closely related to users because several

domains can share the same DNS. Oppositely, e-mail offices are tightly coupled with the users.

- DNS are intended to store information about *domains*, not about users. As a consequence, there is a registration procedure for a new domain but not for a new user of one of the registered domains. In fact, there's no need that a final user ever interacts with the DNS to get access to Internet, but users are obliged to interact with e-mail offices to set up an email account.
- DNSs use caching and lifetime mechanisms that could yield inaccurate or false information in some situations; this feature can be used to attack the system;
- The CA of a DNS may not have direct knowledge of the users' identities and, therefore, it is more vulnerable to impersonation.

Conclusions

An Extranet connects an organization with other organizations that share common goals in a way that automates their administrative interactions. However, an extranet requires a high degree of security and privacy from other companies that are not partners. They need to be extremely secure, and access needs to be highly controllable. Public-key cryptography can be used as a basis to achieve this goal, but the widespread use of a public-key cryptosystem requires Public Key Infrastructures as means to manage digital certificates.

This paper has introduced a new key management and certification system that proposes a scheme of KSUs operating independently over different groups of employees, conforming a hierarchy that reproduces the organization structure. The scheme provides secure means to identify users and distribute their certificates; it eliminates problems associated with the revocation procedures, especially those introduced by the use of CRLs, and simplifies the validation of certificates.

REFERENCES

[DiHe76] Diffie, W.; Hellman, M. *New Directions in Cryptography*. IEEE Transactions on Information Theory. IT-22, n. 6. 1976, pp. 644-654.

[Ilpf97] Ilpf Working Group on Certification Authority Practices. *The Role of Certification Authorities in Consumer Transactions*. Internet Law and Policy Forum, 1997.

[ISO88] ISO International Standard 9594. *Information Technology - Open Systems Interconnection Reference Model: The Directory*, 1988.

[ISO96] ISO/IEC JTC1/SC 21. *Draft Amendments DAM 4 to ISO/IEC 9594-2, DAM 2 to ISO/IEC 9594-6, DAM 1 to ISO/IEC 9594-7, and DAM 1 to ISO/IEC 9594-8 on Certificate Extensions*, 1996.

[ITU97] International Telecommunication Union, *Itu-t recommendation x.509. Information technology – Open Systems Interconnection – The Directory: Authentication framework*, 1997.

[PKIX97] PKIX Working Group Internet Draft. *Internet Public Key Infrastructure Certificate Policy and Certification Practices Framework*, 1997.

[PKIX98] PKIX Working Group Internet Draft. *X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP*, 1998.

[RFC1101] Mockapetris, P.V. *DNS Encoding of Network Names and Other Types*, 1989.

[RFC1421] Linn, J., *Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures*, 1993.

[RFC1422] Kent, S. *Privacy Enhancement for Internet Electronic Mail. Part II: Certificate-Based Key Management*, 1993.

[RFC1423] Balenson, D., *Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers*, 1993.

[RFC1424] Kaliski, B. *Privacy Enhancement for Internet Electronic Mail. Part IV: Key Certification and Related Services*, 1993.

[RFC 1510] Kohl, J.; Neuman, B.C. *The Kerberos Network Authentication Service (V5)*. 1993.

[RFC2065] Eastlake, D.; Kaufman, C. *Domain Name System Security Extensions*, 1997.

[RFC2137] Eastlake, D. *Secure Domain Name System Dynamic Update*, 1997.

[RFC2316] Bellovin, S. *Report of the IAB Security Architecture Workshop*, 1998.

[RiLa96] Rivest, R.; Lampson, B. *SDSI – A Simple Distributed Security Infrastructure*, 1996.

[Rive98] Rivest, R. *Can we Eliminate Revocation Lists?*. Financial Cryptography 1998.

[SPKI98a] SPKI Working Group Internet Draft. *Simple Public Key Certificate*, 1998.

[SPKI98b] SPKI Working Group Internet Draft. *SPKI Certificate Theory*, 1998.

[Zimm95] Zimmerman, P. *The Official PGP User's Guide*. MIT Press, 1995.