SEVA: a framework to dynamically set up and run secure extranet

Pierre VANNEL[1] and Yves ROUDIER[2]
[1]*Gemplus Labs, Parc d'activités de Gémenos, B.P.100, 13881 Gémenos CEDEX, France*
[2]*Institut Eurécom, 2229 route des Crêtes, B.P. 193, 06904 Sophia-Antipolis, France*
E-mail: pierre.vannel@gemplus.com

Abstract. An extranet lets an organisation share part of its information system (e.g. documents, services, computers…etc.) securely over the Internet. In-house data is available to suppliers, customers, or external partners. Security is critical, but it must not impede upon effective business relationships. Exchanges should comply with an agreed security policy, but no generally accepted solution exists to achieve this.
The SEVA framework deals with these issues and this paper describes the SEVA architecture. A typical scenario of operation of a SEVA extranet is provided in this paper.

1. Introduction

Digital information has become a key asset for many corporations, and thus needs to be carefully protected. Information should become the key administrative element in corporate information systems. Another major trait is emerging in today's corporate networks: information needs to be shared with external parties such as suppliers, customers, partners, etc. Security, or more precisely, access control, thus becomes a critical issue. Rollout time is a key factor for businesses, since new relationships often need to be implemented very quickly, and furthermore over very short periods of time.

The SEVA project aims to answer these needs, by providing a framework for dynamically setting up and running secure extranets. The main features of this framework are as follows:

- fine-grained access control to the digital resources
- automatic configuration and operation
- transparent use for the end-user
- strong authentication
- ability to cooperate with intrusion detection systems.

2. Business Rationale

It is illusive to make an exhaustive inventory of the needs to build up extranets. Here are the major motivations of the SEVA project partners:

- *Towards the absolute zero stock*

Reducing the stocks in manufacturing processes is one basic of the production management. However it remains a latency barrier. Breaking it requires interconnecting the information systems between supplier and customer.

- *Collaboration*

Some Open Source developments and multi-partner research projects have demonstrated that collaboration was a valid model in various ways:
- sharing costs of development,
- sharing knowledge,
- spreading technologies,
- etc.

Today's collaboration infrastructures often set up a common information system that is distinct from that of the participants. Implementation is thus a slow and administratively complex process. Certain organisations such as SourceForge.net, are now proposing to host collaborative projects but such solutions will only really work for public projects.

- *Resource Sharing*

Emerging peer-to-peer technologies are appreciated as a way to optimise existing information infrastructures. Sharing computer power and software costs between organisations represents the main interest at this work. Confidentiality and integrity of the exchanged data remain to be properly ensured.

- *Nomadic Accesses*

The underlying objective is to offer to nomadic users the same access to their information system as settled users, at the lowest cost. An isolated branch has the same constraints as a nomadic user. Both they are assumed to be in a hostile environment. A secure communication channel is not sufficient: the nomadic platform could be used as a gateway to access to the user's information system. Intrusion detection system is a necessity.

Increasing the connectivity between organisations must not compromise overall security, yet rollout time remains primordial. Automatic extranet configuration and operation must also be provided for, not to mention end-user convenience. Strong security needs to be implemented without making itself felt on the end-user.

3. Extranet Establishment

3.1 Extranet Agreement

The Extranet Agreement is the basis upon which a SEVA extranet is built. It is composed of four parts:
- general terms,
- administrative interfaces,
- parameters of the naming system of the extranet resources,
- definition of the services.

The general terms define the name of the agreement, its type and its duration. All the parties involved are described: names, addresses, contacts, administrative entry points, public keys, etc. New roles can be specified so that additional parties could easily join the extranet by being appointed to a role. The liabilities of the parties and litigation settlement are defined, allowing an arbitrator to be named.

The agreement presents the administrative interfaces of all the parties. It consists of the definition of a subset of the administrative protocol defined between the parties: publication/cancellation of services, intrusion detection, user revocation, etc. These information must be exchanged over a trusted channel, with an assurance about the authenticity of the public key of each party, and about the integrity of the information sent.

This part of the agreement specifies the network entry points and the security parameters: secure transport protocol, cryptographic parameters ...

The third part concerns the naming system used to identify the resources on the extranet. It describes:

- the extranet central naming service where all the sub-naming authorities of the extranet are referenced.
- The local naming service hosted by each extranet partner.

A naming service description gives the network addresses of the servers and the supported transport protocols. The description provides the administrators' credentials of the local naming service to be registered by the central naming service.

The final part of the agreement specifies the services of the extranet. A service is understood as a collection of resources or other services. A service description defines its deployment into the extranet: resource references, interfaces between the resources, constraints, etc. A service ranges from a simple HTML page to a complex component-based application.

The Extranet Agreement is a key element to set up the extranet.

Every partner with shared resources uses this agreement to generate the access rights for authorised parties. The central naming service uses the agreement to reference the local naming services hosted by the partners. Every partner uses it to configure its firewall and administrators stations and to diffuse the extranet services accross its own organisation; it may even form new added-value services based on original extranet services.

In the search for a human and machine-readable language, XML [1] was selected. It is used to automate processing of the agreement. The core of the agreement definition is based on tpaML [2]. The tpaML syntax expresses the general terms and the administrative interfaces of the Extranet Agreement. The syntax is extended to describe the naming service configuration. The definition of the services is based on academic works about architecture description languages [3] and component-based application [4].

3.2 Service Update

An extranet is a living organisation: new members join, others leave. Rules for an extranet will change over time: liabilities, security parameters…etc. New services are proposed while others are cancelled. Services could be updated: new resources, additional rights, renewal of rights…etc.).

Thanks to the role definition into the Extranet Agreement, the extranet could easily be extended to new participants by assigning a role to a new member. Changing the extranet rules, especially security rules, remains to be solved by the proposed framework.

The administrative protocol manages the diffusion of the updates across the extranet. The corresponding information could be broadcast to all relevant extranet participants or sent to the right member. For example, the joining or the leaving of a member is broadcast to all extranet participants. On the other hand, the renewal of access rights is sent only to the relevant member.

4. Access Control Design

4.1 Fine-grained Access Control

While the sheer volume of information on networks is exponentially growing, it appears that the access control to the computers where this information is stored, is not sufficient. The granularity of the access control should be set at the information level. However, the diverse nature of digital information (e.g. web pages, multimedia documents, applications...) makes it very difficult to implement an universal access-control scheme. Referencing a digital information item on networks represents another challenge.

The Corporation for National Research Initiatives has proposed to the IETF the Handle System as "a general-purpose global name service enabling secure name resolution over the Internet" [5, 6]. They set a unique global namespace for digital resources over the Internet, with a root naming authority, referencing all world-wide sub-naming authorities. An identifier to a digital resource is called a handle. The CNRI also runs a distributed resolution service: the root name service and local name services run by the sub-naming authorities. The resolution service returns to the end-user the handle record corresponding to the handle requested (i.e. the resource identifier). Thanks to this record, the end-user is able to retrieve the resource, using for example its URL.

In essence, an extranet is a private space. The current architecture of the Handle System, with a unique namespace, does not meet the requirements of the SEVA framework. We have modified the Handle System and have used it in the following way in our experimental extranet:

Assumptions

- Every extranet participant runs a Local Handle Service (LHS).
- An organisation could participate to several separate extranets (each comprising several participants).
- Every extranet end-user has a SEVA smart card.
- Various access control systems are in use at a participant site.

Operation

- One extranet participant runs the extranet central authority to reference all naming authorities of the other partners, possibly replicated by other partners. *(New feature).*
- A handle on an extranet resource is only visible to extranet participants. End-users are authenticated thanks to their smart card. *(New feature).*
- The use of the same digital resource by different extranets is allowed thanks to the handle alias mechanism.
- Access control information is added into a handle record. When the end-user asks to the LHS the resolution of a handle, the LHS retrieves the access control information, automatically configures the SEVA firewall to allow to access to the corresponding resource,and possible applicative access control systems. *(New feature).*

The handle system provides an extensible framework for access control, making it perfectly suited for defining multi-application access rights like in the SEVA framework.

4.2 Access Rights

Initial access rights to a resource are anonymously defined at a company level. The organisation holding the resource assigns the access rights to the visiting company, which then delegates access rights to end-users. When end-users from the visiting company want to access to a resource, they provide the authorisation chain so that the host organisation can verify authorisation and allow access. Such a scheme is suitable for small organisations seeking to supply services to large companies without to set up a dedicated infrastructure to register and check all the authorised users. Another advantage is to keep the users management to the organisation they are attached: the organisation is in charge of necessary revocations of the granted rights.

The IETF Simple Public Key Infrastructure (SPKI) [7] defines authorisation certificates allowing an efficient implementation of the access rights in the SEVA extranet. Moreover SPKI includes a delegation mechanism that corresponds to the visiting company administrator’s intervention.

How do we use SPKI? The host company issues an authorisation certificate on a public key of the visiting organisation about a resource handle or a set of resource handles. The visiting organisation is then able to issue authorisation certificates for its users by signing them with the private key corresponding to the public key certified by the host company. The issued authorisation certificates must be compliant with the original authorisation certificate exchanged between the two partners: the access rights could only be restricted.

4.3 Access Control Enforcement

Once the access rights have been established by sending certificates, actual traffic can be exchanged between the two intranets. Access control has to be enforced on this traffic to make it compliant with the access rights previously determined.

Keeping application servers unmodified and application clients with as little modifications as possible is an important guideline for the design of the SEVA framework. Transparency for the user is another important guideline. We thus chose to enforce access control by ticketing user traffic transparently on the client side and verifying tickets on the other intranet's firewall, which provides a convenient and centralized checkpoint.

Traffic ticketing

Ticketing is enabled for TCP connections through a modification of the client workstation socket implementation. This modified stack intercepts any communication that is directed towards another SEVA intranet. All such intranets are kept in a list updated on each workstation each time an extranet agreement is established.

The buffer to transmit is encapsulated and marked with a cryptographic ticket. The ticket establishes a link with the user: it simply consists of the HMAC of the data and a session key established beforehand, and based on the user's secret key. TCP packets format is thus altered to a specific SEVA traffic format, comprising the data, the cryptographic ticket, and some additional information like the destination address and port.

The smartcard is used here as a real-world key to the SEVA extranet: it keeps the secret key that does not reside on the workstation itself and can generate the session key using a Javacard applet. No traffic with another partner can take place on the extranet if the smartcard is withdrawn.

Ticket verification

The purpose of traffic ticketing is to ensure that the packets transmitted were sent by an entity owning the secret key of the user. This has two important consequences: the traffic is strongly authenticated; a user can be logged and identified via his public key, although his nominative identity remains unknown.

The ticket verification is performed on the firewall with a generic proxy. This proxy verifies that the ticket was constructed correctly. The proxy also decapsulates the incoming SEVA traffic before passing it to one of the specific application proxies. This second proxy can then check if the user's access is in conformance with his access rights.

Finally, an intrusion detection system can monitor the behavior of each user. In case of a malicious operation, an alarm can be sent to the firewall and to the intrusion detection systems of the extranet partners. The might trigger the suppression of the granted access rights for the user.

4.4 Smart Card Role

The SEVA smart card is a portable and personal wallet to access extranet services. It is used for secure storage of cryptographic keys as well as the references of the services. The SEVA smart card is a multi-application smart card i.e. a JavaCard. It holds a cryptographic card applet and of an embedded secure LDAP-like server [8] where the service references are stored. The cryptographic card applet is a part of the access control scheme as described above.

Two kinds of entries are stored into the embedded LDAP-like server: the service entry and the resource entry. The service entry describes the service: resources or services composing it, connectors between resources, properties. The resource entry contains the identifier of the extranet it belongs to and the reference of the SPKI authorisation certificate. The resource identifier is the handle of the resource. The memory of current smart cards is still limited: only a few tens of kilobytes to store programs and data. The smart card is adequate to store secret cryptographic keys and to protect the cardholder’s privacy. We thus chose to store only the reference to the certificate: the real certificate is stored in a LDAP server inside the user’s company intranet.

6. Deployment Scenario

In this description, we limit the extranet to two companies, while, in our experimentation, four organisations are involved.

There are two companies: the Visiting company (Company V) accessing to resources of the Host company (Company H).

6.1 Agreement Phase

First of all, V and H have to conclude an agreement defining the extranet: public key exchange, PKI interfaces, protocols, accessible resources, agreement duration, etc. In this agreement, company H issues SPKI certificates on the enterprise V public key, defining the authorisations on the accessible resources.

6.2 Providing Users with Access Rights

Company V accredits the end-users by diffusing to them the accessible resources references and issuing the corresponding certificates from the certificates granted by H, thanks to the SPKI delegation mechanism.

6.3 Accessing a Resource

When end-users want to access to a resource, they ask the SEVA Handle Service to resolve a given resource reference (i.e. a handle). They then authenticate themselves and provides the corresponding authorisation certificates. The SEVA Handle Service returns the resource handle values (e.g. an URL) with an encrypted session key to be used to access to the resource. Simultaneously, the SEVA Handle Service has configured the security equipments (firewalls, IDS) of H. Then the end-user accesses to the resource of the company H.

7. Conclusion

With the Handle System, the CNRI has paved the way for an overhaul of the Internet, placing the information at the heart of the system. However, the present Handle System is suitable only for resources on the Internet global name space. The SEVA framework completes this system by managing private name spaces for extranets (or even intranets) and by adding a generic and extensible access control scheme. The SEVA framework is currently under development. As we explained above, this framework will enable the deployment of extranets with following facilities:

- an extranet agreement model based on XML,
- a resource management system offering a uniform and fine-grained definition of the digital resources through a naming system.
- an access control system to manage the access to shared resources by configuring corporate security equipment dynamically and automatically,
- a PKI infrastructure based on SPKI to manage and to distribute access rights between extranet participants. Smart cards are used as a part of the PKI infrastructure. A smart card stores the resource references accessible to the cardholder. It provides highly secure services allowing secure access to the shared resources from various devices.

We expect major benefits from our extranet approach: the focus will be on resources and how to access them, and not on network issues as it is currently the case (IP spoofing, etc.). Modifications of client applications will be minor at worse and servers will not be modified by the deployment of the SEVA system. Although it provides strong authentication for end-users, the SEVA system does not threaten end-user privacy. Finally, it goes nearly unnoticed to the user.

We plan to contribute to standardisation by proposing some extensions to the Handle System and an XML description of an extranet agreement.

8. Acknowledgements

The SEVA project is supported by the French Ministry of Economy, Finances and Industry within the Réseau National de Recherche en Télécommunications (RNRT) framework. The partners of the SEVA project are ATOS, Electricité de France, Institut Eurécom, and Gemplus.

References

[1] Word Wide Web Consortium. Extensible Markup Language (XML) 1.0. W3C Recommandation. http://www.w3.org/TR/2000/REC-xml-200010061 .

[2] IBM. Electronic Trading-partner Agreement for E-Commerce. ebXML proposed specification, version 1.06. http://www.ebxml.org/project_teams/trade_partner/tpaml106.zip .

[3] D. Garlan, R. T. Monroe, D. Wile. Acme: An Architecture Description Interchange Language. Proceedings of CASCON 97, November 1997, pp 169-183.

[4] M-C. Pellegrini, O. Potonniée, R. Marvie. Smart Cards: A System Support for Service Accessibility from Heterogeneous Devices. Proceedings of 9th ACM SIGOPS European Workshop, September 2000, Kolding, Denmark.

[5] S.X. Sun, L. Lannom. Handle System Overview. IETF Draft. http://search.ietf.org/internet-drafts/draft-sun-handle-system-06.txt

[6] S.X. Sun, S. Reilly, L. Lannom. Handle System Namespace and Service Definition. IETF Draft. http://search.ietf.org/internet-drafts/draft-sun-handle-system-def-04.txt

[7] C. Ellison and al. SPKI Certificate Theory. IETF RFC 2693. http://www.ietf.org/rfc/rfc2693.txt

[8] A. Macaire. An Open Terminal Infrastructure for Personal Services. Proceedings of TOOLS Europe 2000, 5-8 June 2000, Le Mont-St-Michel, France.