Integrating security services with the automatic processing of e-mail content

Francesco Gennai, Marina Buzzi
Istituto per le Applicazioni Telematiche, CNR - Pisa, Italy
Francesco.Gennai@iat.cnr.it , Marina.Buzzi@iat.cnr.it

ABSTRACT

Digital signature can be associated with Internet messages in order to guarantee authentication, message integrity and non-repudiation of origin. Verification of incoming digitally signed messages is a critical operation requiring careful attention. Usually e-mail clients (receiving agents) implement this function on behalf of the end-user. If the verification process is not successful, the client alerts the user.

When e-mail messages (i.e. electronic forms) are used to request services of a provider, the automatic processing of message content speeds up data processing, reducing human error as well. In this context, signature verification by e-mail client could become a system bottleneck, thus justifying an automatic verification system.

In this work we briefly describe our experience in designing and implementing software in order to automate the verification process of signed e-mail. The system has been designed to simplify the registration of Internet domains under the .IT Top Level Domain [1].

In order to design the automatic "Message Verify" system we studied the way in which Public Key cryptography technology can be integrated with the electronic mail system. We were especially interested in interpretation of cryptographic security services (specifically digital signature) in received messages. In particular, we needed to solve two main problems:

- Correct recognition of MIME parts containing protected data. The RFC 1847 (S-MIME) [2] specifies how to apply security service to MIME body parts. S-MIME adds two new content types: Multipart/Signed and Multipart/Encrypted, both containing two body parts: one for the protected data and the other one for the control information necessary for removal of the protection. The RFC 2630 describes the Cryptographic Message Syntax used to digitally sign, digest, authenticate, or encrypt messages [3]. Finally, the RFC 2633 [4] defines the application/pkcs7-signature MIME type used to transport S/MIME signed messages and extensively outlines requirements and recommendations for handling of incoming messages by receiving agents.
- Correct application of the verification process to the extracted MIME parts. We needed mechanisms for retrieval and validation of the certificate. The RFC 2632 [5] specify basic rules to be applied by receiving agents in order to correctly verify a signed message. In addition the Internet draft (I-D) "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" (that is part of a family of standards for the X.509 Public Key Infrastructure (PKI) for the Internet) [6], outlines the format and semantics of certificates and certificate revocation lists for the Internet PKI. Procedures are described for processing of certification paths in the Internet environment. This I-D gave us a framework within which to manage certificates and CRLs.

Finally the OpenSSL toolkit (libraries and application samples) [7] was fundamental for implementation of the system. Thus, using a MIME-compliant mail server we were able to implement the automatic "message verify" system.

The system

In system design, it is very important to evaluate the purpose as well as the context in which the digital signature is applied. In our context, the message verification is used as a key to access one service: the registration of *domain names*. Each message contains one *domain name* registration form (other contents are refused). If the verification is successful, the request is accepted and elaborated; otherwise it is rejected and a notification is automatically sent to the sender. That means we use Public Key technology as the access key to one service (instead of a password-based mechanism).

The system is fully configurable and monitored via web interface. The Figure 1 shows the logical scheme of the Message Verify (MV) system.

Certificate of trust CAs are added to (or removed from) the *CA Database* by a system administrator. CRLs are automatically downloaded (using the Certificate's *CRL Distribution Point* field) by the *CRL Manager Process* (which uploads the local *CRL Database*). LDAP query is possible but not yet implemented.

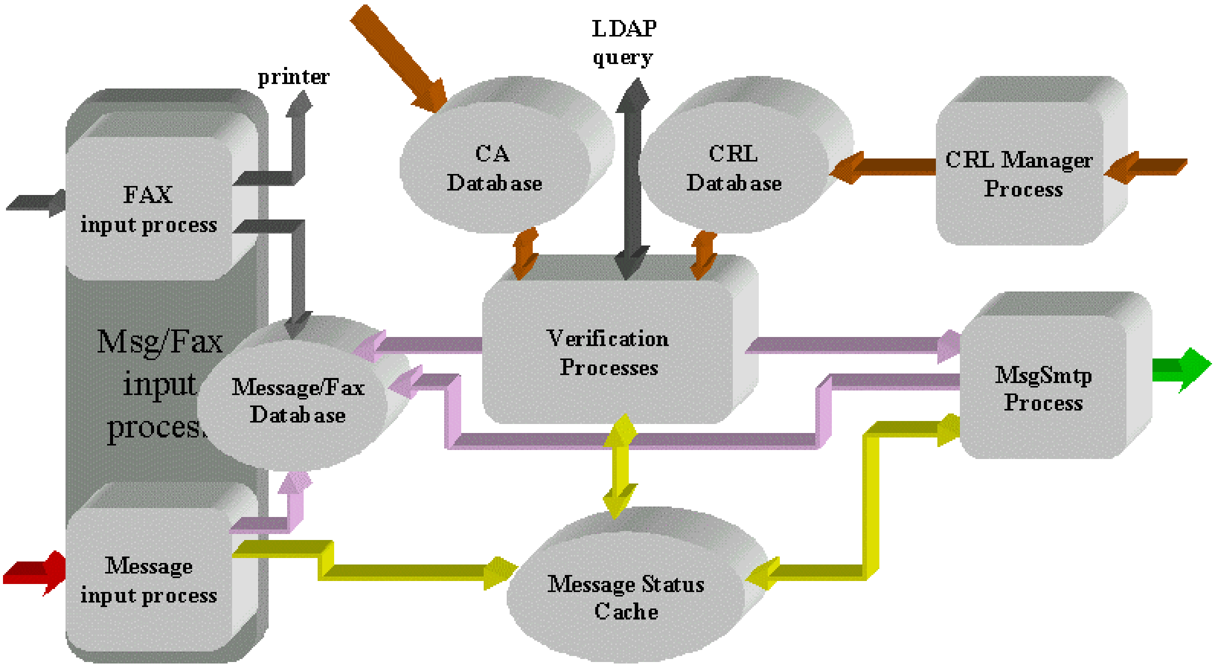

Fig.1 - Logical scheme of the MV system

The Message database also includes requests received via fax, stored as postscript files (*Message/Fax Database*). A global identifier is assigned to each message or fax entering the system, thus maintaining the temporal sequence of the requests; this is very important in order to resolve collisions on requests for the same *domain name*.

The *Message Status Cache* is used for greater efficiency: it maintains temporary information on the message status, while it undergoes elaboration.

The *Verification Process* adds three header fields to the message, specifying respectively: the *Certificate Issuer Distinguished Name*, the *Certificate Subject Distinguished Name* and the concatenation between the *Verification Process* return code and the message global identifier (X-Mvcertissuer:, X-Mvcertsubject:, X-Mvglobalid:). These values are also useful for the (help desk) operators who use web interface for accessing the Msg/Fax database.

Last, because messages are processed in parallel on a 2-node cluster, they may be out of sequence after verification. The *MsgSmtp Process* re-orders messages in the correct temporal sequence.

The system has been running smoothly since its installation. This work progresses as we continually learn of new proposals and international recommendation in order to improve the system.

REFERENCES

1. The Italian Registration Authority - http://www.nic.it/RA/en/
2. J. Galvin, S. Murphy, S. Crocker N. Freed - RFC 1847. Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted. http://www.imc.org/rfc1847, October 1995.
3. R. Housley. RFC 2630: Cryptographic Message Syntax, http://www.imc.org/rfc2630, June 1999.
4. R B. Ramsdell - RFC 2633: S/MIME Version 3 Message Specification. http://www.imc.org/rfc2633, June 1999.
5. B. Ramsdell. RFC 2632: S/MIME Version 3 Certificate Handling. http://www.imc.org/rfc2632, June1999.
6. Housley,W. Ford, W. Polk, D. Solo - I-D: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, http://www.imc.org/draft-ietf-pkix-new-part1 July 14, 2000
7. The OpenSSL Project - http://www.openssl.org/