A PKI approach targeting the provision of a minimum security level within Internet

Maryline Laurent-Maknavicius
CNRS Samovar UMR 5157, GET/INT/LOR
Maryline.Maknavicius@int-evry.fr

Abstract

After decades of expansion, Internet became an essential tool useful for professionals and private individuals providing a large range of services like emailing, management of bank accounts, reservation of hotels, train time schedules, real time traffic information, Internet search… If not targeted at the beginning, Information System Security became rapidly a key challenge for professionals and strong security solutions emerged on the market mainly for professionals. Internet security is thus today two-speed: pretty strong security for professionals or private individuals anxious to protect their computer equipments and no security for professionals or private individuals who can not afford security products and do no have sufficient technical expertise to set up cheap solutions by themselves.

In this context, this paper targets the provision of a minimum security level within Internet by defining a PKI solution based on LDAP and DNS (extended with DNSSEC). The originality of the paper is related to the design of the chain of trust that is built over both LDAP and DNSSEC PKIs, the certificate verification method, and indications to extend those concepts to the secure emailing application.

1. PKI technical challenges

A PKI (Public Key Infrastructure) [1] is responsible of all organizational and technical aspects to support public key management. Its duties cover the public/private keys generation and delivery to owners, as well as publication, revocation and validation of public keys. All these functions are processed by a Trusted Third Party (TTP) which is usually structured into a hierarchy of Certification Authorities (CA), each CA being legally authorized to manage digital certificates [1].

Today PKI is widely adopted within Internet and serves as a basis to strong security solutions targeting (https) electronic transactions, (SSH) remote connections, code signature, emailing…

After years of research, development and deployment, PKI is still facing strong technical and organizational challenges, as follows:

- Trust into CA

Validity of electronic certificates is partly guaranteed by the signature appended by a CA. For a system to approve a certificate as valid, trust into the issuer CA is necessary. Configuring a system with a trust level for each CA is a critical task.

The paradox is that today trust level associated to CA is usually fixed by the users themselves (more often with no security knowledge). Moreover, users may freely import new CAs in their systems at their suitability. So the risk is high that users configure fake CAs as trusted CAs, thus accept certificates from a fake CA, and next be abused by fake internet servers.

Trust into CA is today a subjective but critical parameter that serves to build secure relationships between Internet entities.

- Certificate revocation

The challenge in managing revocation is providing internet entities with information as fresh as possible. The objective is to publish the certificate “revoked” status as soon as revocation is done, to avoid entities establishing relationship with fake entities. For instance, in case of private key being compromised, the risk is high that the private key stealer usurps the identity of the private key owner.

Many revocation mechanisms were defined, but none of them are satisfying today. CRL (for Certificate Revocation List) [1] serves to periodically publish list of revoked certificates (only their serial numbers are published). However, all the certificates being revoked during one interval of time are published at the interval after. So there is at maximum a one interval delay for the revocation information to be published.

Improving freshness leads to the OCSP OCSP (Online Certificate Status Protocol) [2] and SCVP (Simple Certificate Validation Protocol) [3] servers. The OCSP server is attached to one CA and replies to simple certificate status requests relative to that issuer CA only. The SCVP server operates full verification of certificates on behalf of local clients delegating verification to that server.

These remaining key challenges make use of PKI sometimes uncomfortable from an operational point of view.

2. Provision of a minimum security level within Internet

This minimum security level is built on the idea of interconnecting two PKI, a DNSSEC PKI and an LDAP PKI. Both DNS and LDAP [4] are today standardized by the IETF and support public key publication. DNSSEC extension [5, 6] defines new registration records - like Delegation Signer (DS RR), DNSKEY record, digital signatures (RRSIG RR), and certificates (Cert RR) – and enables mapping a PKI onto the DNS hierarchy. LDAP was also enriched with new attributes to publish user certificates (UserCertificate), CA certificates (cACertificate), and CRLs (certificateRevocationList) [7].

One original idea of the proposed PKI is to interconnect very simply these two PKI, but one may wonder the interest of interconnecting these two PKIs.

LDAP is well introduced into organizations for centralizing and publishing employees' features (e.g. phone number, office number, position…); as such LDAP is the solution of choice to publish employees' certificates. However as raised in section 1, "trust into CA" is one of the most critical problems of managing PKI, and defining as many CAs as organizations to register employees' certificates into their LDAP server does not help solving this trust problem.

In our PKI, the trust relationship is established through DNSSEC that needs to publish the certificate of the organization's CA bound to the domain name of the organization. Details on the resulted chain of trust are given in section 2.2.

To summarize, the designed PKI relies on DNSSEC for internet entities to securely get and trust the organizations' CA public keys, and LDAP to make users' certificates publicly available.

The strength of this PKI proposal is to request no modifications to software tools already in place: LDAP serves as a common directory for managing employees within companies, and DNS is commonly employed to do the mapping between companies' domain names and IP addresses of public servers.

Actually the security level offered by this PKI depends on the security level of the DNSSEC directory managing certificates, and specifically on the more or less strong procedures defined around certificate management.

Next for illustration, we assume that company1 is provided with one official domain name (company1.fr) secured by DNSSEC. Company1 defines its own CA next referred to as Company1 root CA, and owns its own LDAP server named ldapServer where users and servers' certificates are stored and made publicly available.

2.1. Chain of trust

The certificate chain of trust that enables to securely interconnect LDAP and DNSSEC PKIs is obtained by applying the three following rules:

- DNSSEC serves to securely publish the self-signed certificate of the company1's root CA named Company1 root CA, so the root CA is known as trusted by internet entities with the same security level than assigned to DNSSEC PKI.
- This root CA certificate is also stored in the LDAP basis in an LDAP entry corresponding to Company1 root CA. That is, the Distinguished Name (DN) identifying the LDAP entry contains: "CN=Company1 root CA,ou=PKICA,o=Company1,c=FR".
- The self-signed root certificate contains both DNS and LDAP references in the fields: subjectAltName and issuerAltName fields (cf. figure 1). As such, entities getting this certificate are able to double check the certificate asking the DNSSEC and LDAP directories.

As illustrated in figure 1, the certificate of the employee Bob is signed by the Company1 root CA itself, so the root CA's DN and LDAP reference are supplied in the issuer and issuerAltName attributes. The issuerAltName field enables any entity to locate the LDAP server in charge of publishing certificate of Bob, and the issuer's certificate. Note that Bob may be also known under his email address, so the attribute subjectAltName might contain an email address. The same applies to servers being registered with their certificates into LDAP, but they are also known under their names (specified into the subjectAltName attribute).

Root CA's certificate:

issuer: C=FR, O=Company1, OU=PKICA, CN=Company1 root CA
issuerAltName: DNS:company1. fr, URI:ldap://ldapServer.company1.fr/CN=Company1 root CA;ou=PKICA;o=Company1;c=FR?cACertificate
subject: C=FR, O=Company1, OU=PKICA, CN=Company1 root CA
subjectAltName: DNS: company1.fr, URI:ldap://ldapServer.company1.fr/CN=Company1 root CA;ou=PKICA;o=Company1;c=FR?cACertificate

Certificate of employee Bob

issuer: C=FR, O=Company1, OU=PKICA, CN=Company1 root CA
issuerAltName: URI:ldap://ldapServer.company1.fr/CN=Company1 root CA;ou=PKICA;o=Company1;c=FR?cACertificate
subject: C=FR, O=Company1, OU=User, CN=Bob
subjectAltName: email:Bob@company1.fr
cRLDistributionPoint: URI:ldap://ldapServer.company1.fr/CN=Company1 root CA;ou=PKICA;o=Company1;c=FR?certificateRevocation List

Certificate of ldapServer

issuer: C=FR, O=INT, OU=PKICA, CN=CADDISC INT root CA
issuerAltName: URI:ldap://ldapServer.company1.fr/CN=CADDISC INT root CA;ou=PKICA;o=INT;c=FR?cACertificate
subject: C=FR, O=INT, OU=Server, CN=ldapServer
subjectAltName: ldapServer. company1.fr
cRLDistributionPoint: URI:ldap://ldapServer. company1.fr/CN=CADDISC INT root CA;ou=PKICA;o=INT;c=FR?certificateRevocationList

Figure 1. Certificates signed by company1 root CA, and registered into company1's LDAP directory

2.2. Revocation

As already defined within LDAP standards, a revoked certificate must be added into the CRL and published into the LDAP server. For instance, revocation of Bob's certificate results in company1's root CA generating a CRL and publishing this CRL in the LDAP server. The location of the CRL is specified into the certificate (cRLDistributionPoints field) under a URI (Uniform Resource Identifier) reference (cf. figure 1) and serves for any entities wiling to check the certificate validity against the CRL.

Whereas revocation of employees' certificates and servers' certificates are managed by LDAP PKI, revocation of root CA is managed by DNSSEC PKI.

2.3. Certificate verification

An internet entity needing to verify the validity of an employee's certificate asks its local SCVP server. The verification processing is decomposed into three steps, the first one to download the certificates belonging to the chain of trust, the second one to trust the root CA certificate (of Company1), and the third one to check the validity of each certificate of the chain, as follows:

1. All the certificates belonging to the certificate chain are downloaded from the bottom-level certificate (issuer) up to the high-level certificate based on the issuerAltName information within the certificates. For Bob's certificate, the LDAP server will be solicited only once to get the root CA's certificate, because the LDAP PKI is a one-level CA hierarchy.
2. As soon as the root certificate is found in the chain, the DNS hierarchy is solicited to provide the CERT RR containing the root CA's certificates. This CERT RR is get from the DNS reference given either in the issuerAltName or subjectAltName field of the root CA's certificate. The validity of the returned CERT RR is ensured by the DNSSEC PKI, but it will be definitely considered as valid if the root certificates registered in DNSSEC and LDAP PKIs are exactly the same.
3. All the downloaded certificates are then verified checking their validity period (validity), the signature (signatureValue) and, if possible, the CRL [1]. The verification is done from the high-level certificate down to the bottom-level certificate. For revocation verification, it is required to download the CRL corresponding to the CrlDistributionPoints URI of the certificate under test, and to check its own validity period, and signature.

2.4. Defining a minimum security level within Internet

With the designed PKI, any internet entities are provided with mechanisms to get certificates and to verify their authenticity and validity. This helps introducing a homogeneous security level within Internet and lets private individuals benefiting from that more secure Internet.

The overall security level depends on how LDAP and DNSSEC PKI are managed. If strict procedures for managing public and private keys are imposed by regulating or standardized bodies, the resulted security level will be significant. Otherwise, it will serve as a basic security level. Anyway, the security level get from that solution will never be as high as with CSP (Certificate Service Provider), and so its application will concern scenarios which are not too much security demanding.

2.5. Limitations

The efficiency of the proposed PKI is closely related to the deployment of DNSSEC. Today, DNSSEC is still experimental and for management and organization difficulties, administrators of zones are reluctant to deploy DNSSEC. As a consequence, there is not only one DNSSEC PKI mapped on to the DNS hierarchy, but a number of small DNSSEC islands being independent from each other. It means that today the system must trust each root CA independently, and the DNSSEC PKI as required in this paper does not meet its original objectives of simplicity. However, international collaborative efforts must be underlined towards a secure DNS like the international DNSSEC experiment being realized within the rs.net testbed (http://www.**rs.net**/). Also some DNSSEC shadow zones are already operational, and applied at a pretty large scale as they are synchronized with real non-DNSSEC zones like ".fr", ".nl"… All these experiments contribute to the progressive installation of DNSSEC.

LDAP server must be accessible by any internet entities. To avoid the risk that a private LDAP information is divulged to unauthorized users intruding the LDAP server system, an LDAP proxy may be installed as a front end. For instance, this LDAP proxy might be initialized with public information only.

3. Testing platform

A platform was developed as a proof of concept during CADDISC and VERICERT projects [8, 9]. Resulted software modules are depicted in figure 2. We selected OpenLDAP to implement the LDAP server, BIND (Berkeley Internet Name Domain) [10] for the DNS server, and OpenCA for certificate/CRL generation and automatic publication into OpenLDAP. SCVP opensource softwares (responder and client) were developed for the client and server and encompass LDAP and DNSSEC clients.

The certificate verification module extends the OpenSSL verify function and required the development of a new trust method and a new lookup method for OpenSSL. More precisely, the trust method was extracted from the DNSSEC validator of the French IDsA project (DNSToolKit library) so that certificates verified by a DNS client are considered as trusted by OpenSSL. The LDAP lookup method was defined to get certificates from LDAP servers.

4. Comparison with similar PKI approach

D.A. Wheeler proposed in 2002 to use LDAP and DNS directories for public key publication, and online web documentation was updated from time to time until 2006 [11]. D.A. Wheeler also considers LDAP and DNSSEC PKIs. Despite few technical details are missing (like revocation management), as we can guess, the DNSSEC PKI only serves to publish the LDAP server's certificate, and LDAP server supports publication of users' certificates, and their CA's certificate. Any internet entities can establish a secure communication to the LDAP server, and access to certificates registered into the LDAP server.

Contrary to our approach, in [11], the chain of trust is not provided between DNSSEC and LDAP PKI. That results in severe vulnerabilities. If DNSSEC PKI makes it possible to be sure to be connected to the LDAP server, it does not prove the integrity of the LDAP content. As such in case of successful intrusions on to the LDAP server and modifications of LDAP entries, there might be no possibility to detect the problem.

5. Application to secure emailing

Emailing is the very first application that might be satisfied with the basic security level offered by our PKI approach. Private individuals might be interested in participating to emergence of such PKI. The provider could provide their subscribers with certificates, register certificates in their LDAP server, and provide certificate verification tools to their subscribers. Immediate benefit would be detection of masquerading and spamming.

However integration of the designed PKI approach requires adaptation of emailing tools. The two following functions must be provided:

- Verification of users' certificates authenticity;
- Getting a certificate associated to a user's email address.

This paper provides solution to the first problem, and the second problem might be solved using the SRV Registration Record (SRV RR) within DNSSEC server to publish the LDAP server attached to a domain name and managing certificates of users of that domain.

One possible procedure to get the certificate associated to an email address is composed of four steps. First, the domain name to which the user belongs is extracted from the email address. Second, the DNS hierarchy is requested to search for the LDAP server address corresponding to that domain name (SRV RR). Third, an LDAP request is sent to the LDAP server (for instance on the conventional port number - 389) for searching the certificate attached to the email address; actually this search consists in finding the LDAP entry corresponding to the email address, and returning the userCertificate attribute. Fourth, the certificate is validated using the defined chain of trust (cf. section 2.1).

6. Conclusions

LDAP PKI and DNSSEC PKI are not new concepts, but the combination of both of them is pretty original. Moreover the chain of trust that securely interconnects these two PKIs helps offering a homogeneous and minimum security level within Internet.

This paper presents technical details for constructing this chain of trust and explains that the resulted security level depends on how security certificates and public keys are managed within the DNSSEC PKI and LDAP PKI. At the moment, this level is expected to be pretty low as no strict procedures are defined for public key management.

With the partial deployment of DNSSEC, our PKI approach is today limited to few DNSSEC zones. As such, for this PKI approach to be operational today, few more conditions should be met: LDAP should be attached to one secure DNSSEC zone, and each DNSSEC zone should be registered into the verification tools as root CA of trust.

7. Glossary

CA	Certification Authority
CRL	Certificate Revocation List
CSP	Certificate Service Provider
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
SCVP	Simple Certificate Validation Protocol
URI	Uniform Resource Identifier

8. References

[1] R. Housley, W. Polk, W. Ford, and D. Solo, 2002, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, RFC 3280.

[2] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, 1999, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*, RFC 2560.

[3] T. Freeman, R. Housley, A. Malpani, D. Cooper, and T. Polk, "Standard Certificate Validation Protocol (SCVP)", draft-ietf-pkix-scvp-23.txt, March 2006.

[4] K. Zeilenga, *Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map*, RFC 4510.

[5] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, 2005, *DNS Security Introduction and Requirements*, RFC 4033.

[6] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, 2005, *Resource Records for the DNS Security Extensions*, RFC4034.

[7] K. Zeilenga, 2006, *Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates*, RFC 4523.

[8] CADDISC project, http://www-lor.int-evry.fr/~maknavic/CADDISC/Caddisc-eng.html.

[9] VERICERT project, http://www-lor.int-evry.fr/~maknavic/VERICERT/VeriCert-eng.html.

[10] P. Albitz, and C. Liu, 2002, *DNS et Bind*, 4th edition, O'Reilly, ISBN: 2-84177-150-4.

[11] D.A. Wheeler, 2006, *Easier Email Security is on the Way?*,http://www.dwheeler.com/essays/easy-email-sec.html.