Deployment Issues for an Academic IT Security Infrastructure

Marius Marian*

** Department of Computers and Information Technology, University of Craiova, RO-200440,
România (e-mail: marius.marian@cs.ucv.ro).*

Abstract: This paper analyzes the issues faced during the deployment of an academic IT security infrastructure. The challenges during the planning and building of the public-key infrastructure of the Faculty of Automation, Computing and Electronics are detailed along with some of the practical solutions identified.

Keywords: public-key infrastructure, digital certificates.

1. INTRODUCTION

Today, the potential of public-key infrastructures for access control, authentication and authorization is well recognized. Digital certificates enable electronic signature operations and also privacy of communication.

Our paper presents the implementation of the first public-key infrastructure (PKI) within the University of Craiova, and also the issues and challenges faced during the deployment.

2. MOTIVATION

The issues of secure communication and management of information and peoples' identity are critical to the today's integrated networked environment of any academic institution. There are several reasons for which any university may be interested in implementing a PKI.

First of all, academia is a reputation-based environment therefore fighting identity fraud comes naturally. An identity fraud implies that an attacker steals the identity of a real person and tries to access the resources or gain some other benefits entitled only to the real person. A victim of an impersonation attack can suffer unpleasant consequences if she is held accountable for the actions of a malevolent aggressor. Moreover, in the educational environment also the entire organization may become victim of this kind of frauds (typical examples include injecting false announces on the institution website or even worse, vandalizing it).

Privacy and confidentiality of information represent the second most important aspect. Privacy belongs to an individual, and holds between her and the rest of the community. On the other hand, confidentiality involves a relationship between two or more entities that agree to have authority to the information exchanged, stored or processed in some explicit manner. In confidential arrangements, there is an implicit agreement between these entities that information will not be disclosed, and this is an implicit promise. The consent to retain secret the information is also a measure of trust between these authorized entities. In the research area, researchers promise to hold secret the results and information concerning their work in progress. In some cases, the breaking of the promise may be held not only against the individual who breaks the promise, but against the institution for which the individual works. The wide-scale availability of electronic means for communication, storing and processing of information within academia leads well too often to information leaks. What we have found so far was that at our University, there is no enforced security policy governing the privacy and confidentiality of electronic data. Fortunately, there are some ad-hoc security services implemented but obviously this is not enough and do not represent a holistic and centralized approach towards these two security objectives.

Third, digital signature is currently a common presence within the Internet. In theory everyone agrees on the importance of it, in practice so little is done about it. As is the case with most security issues, people find out the importance of having some means of protection only after an incident occurs. It's worth mentioning here that recently, an impersonation attack was carried out against the dean of our faculty. An e-mail message containing allegations about the average monthly incomes of the faculty management was sent by a perpetrator using a fake e-mail address in the name of the dean. Such an attack would have been easily avoided if digital signature were adopted and enforced on a large scale for what concerns the institutional e-mail service.

3. CURRENT STATUS

During an internal survey, we have discovered that most of our IT services (ranging from personal e-mail accounts and file-/web-servers up to more sensitive administrative services) provided by and within the university are authenticated by means of usernames and passwords.

Concerning confidentiality and privacy, we have discovered that only few of the administrative services and none of the e-mail infrastructure are taking care of this aspect.

Integrity-checking or time-stamping services are also not available on a large scale within our IT environment. Furthermore, no enforced automatic traceability exists for individual user responsibility in relation with events taking place from and within our IT environment. Although inside our networking infrastructure we have moderate up to highly protected areas, we still lack security at individual level.

A large part of this delicate and sometimes embarrassing situation derives from the fact that the security issue was not tackled in a holistic manner right from the start (i.e. when the on-line services were introduced). It is probable that this slow, prudent adjustment to the new security reality is the case with most of our large institutions in the public sector.

An essential element to any information infrastructure is a security policy, but this is still lacking due to the diversity and also due to the geographical distribution of the participants (20 faculties, 7 educational departments, 9 administrative departments, and 9 supporting or special-operational departments, distributed in two cities and having distinct locations within each city). All these participants are subordinated to the University, but they enjoy a significant level of administrative autonomy that has made difficult so far enforcing such a centralized security policy.

Even so, the security issues remain and have to be solved even without a centralized security policy.

Another interesting example for our proposal concerns the Students' Evidence service which basically provides to students their academic status (number and types of exams passed, scheduled exams, grades obtained for each exam, etc.). Such a service requires a consistent level of privacy and confidentiality. Currently, the students accessing this service are identified by means of their *personal numeric identifier* (PNI). This solution was chosen because of the ease in management. The problem with the PNI is that it is a governmentally-assigned number and according to the latest Romanian laws concerning citizens' privacy rights, it should remain private and be allowed for processing only when two conditions are met: first, it exists an explicit written agreement from the owner and second, when a law has already described and allowed that type of processing of the PNI. None of these conditions are met and therefore the Students' Evidence service must change as soon as possible the approach for identifying its users. An immediate solution would be at central level to start assigning new electronic identifiers for all students by using the students' registration numbers (matriculations).

Last but not least important is the issue of institutional e-mail. Here too, after conducting an internal verification we have discovered that on one side, user authentication is based on username and password, and on the other side, the issues of confidentiality and privacy are in most cases neglected. The e-mail servers used do support these security features, but they are neither used nor enforced. In an open educational IT environment in which most of the employees and students are using wireless connectivity, leaving the traffic unprotected may become dangerous. E-mail messages can be intercepted and faked by third parties causing thus moral, economic and professional prejudices to the entitled/authorized peoples. One immediate solution for the administrators was to tunnel – via the SSL protocol – the communication between the client mail user agent and the server. Nevertheless, another sensitive problem may appear. Most e-mail servers today are handling and storing personal accounts by leaving the message data in clear. This is an issue if an attacker captures the root credentials of that server. In such a case, e-mail accounts of employees of a public institution can be vandalized, or only data mined (moreover, malevolent service administrators may abusively use their privileges to read the messages of higher-positioned colleagues in order to gain unauthorized information or even sell certain sensitive information).

It becomes evident that a security infrastructure is necessary.

4. IMPLEMENTATION

3.1 Critical requirements

A public-key cryptosystem implies that each participant holds a pair of cryptographic keys: a public one (made available to all other parties), and the private one; the keys being mathematically linked with each other such that if a crypto-operation (encryption or decryption) is performed with one of the keys then the reverse operation can only be performed by means of the second key.

This particular feature contributed to the wide acceptance within the user community of this technique. The presence of a pair of keys is the reason why authentication and digital signature can be easily achieved by the participating entities. Other security properties such as confidentiality, integrity, and non-repudiation are also derived. Moreover, the fundamental issue of symmetric cryptography (i.e. secret key distribution) is easily handled with public-key cryptography.

Up to a certain point, the distribution of public keys to the participants seemed to give space to masquerade attacks against asymmetric cryptography. Digital certificates containing the value of the public key and the identity of its owner, signed by a trusted third party (TTP) were proposed to mitigate this problem. There are several standards that specify the format of public-key certificates. Among them, ITU-T Recommendation X.509 (2005) is the most popular and is frequently employed in a multitude of other protocols and applications. This standard specifies a model of certification authorities (CA) that issue certificates for subordinated CAs and end entities (individual users, servers, network devices, etc.). Usually, a digital certificate issued by a CA will contain the public key, the identity of the entity owning the corresponding private key, the validity period and the serial number of the certificate, the name and the digital signature of the issuing CA, and a specific set of certificate extensions.

A definition formalized in Myers et al. (1999) follows: the set of people, procedures, software, and hardware used to create, manage, store, distribute, revoke and use digital certificates is called a public-key infrastructure.

3.2 Types of Certificates

The implemented CA will only issue a small subset of all possible digital certificates. First of all, the format of these certificates is conform with the standard X.509 version 3, and similarly, the format for the certificate revocation lists is X.509 version 2. There will be issued: client certificates, VPN certificates, SSL certificates, and less frequently, code signing certificates.

Client certificates are used by individuals affiliated with the university. They will always contain the category of the subscriber (didactics, administration and support, students), and also her e-mail address. The VPN certificates are useful in establishing secure virtual networks using IPsec and they will mainly contain the IP address of the participating device/system and also the e-mail address of its human administrator. The SSL certificates will be used by the university's web-servers (also for the web-mail servers) for their own authentication and they will facilitate the enforcement of SSL tunnels between the client browsers and the server. Just as the previous category, these certificates will contain the DNS name of the server and also the e-mail address of the administrator. The code-signing certificates will be issued for certain development projects within the university perimeter.

3.3 Critical Requirements for Selecting the Solution

The attributes required for the solution are described in what follows. First of all, it is the ease of management. In a distributed IT environment, administering multiple entities and corresponding certificate-related operations must be done via delegation and subordination of multiple levels of certification authorities. Creating this hierarchy of CAs should not require a high degree of complexity since that may decrease the success of adopting the solution at university level.

Second, it is the fast integration of the solution with the existing systems. We have already mentioned that currently, most user authentications are made via username and password. Good news is most applications (ranging from web servers to file servers and e-mail servers, and also virtual private networks) do support or can be adapted to support user authentication by means of digital certificates.

Another sensitive attribute is the end-users ease of adoption of this new solution. Through training and workshops, the solution can be demonstrated to be at least as intuitive as that based on username and password. Furthermore, the fact that in an mail user agent (such as Microsoft Outlook or Mozilla Thunderbird) a user will have installed a pair of private key and digital certificate will make people even more interested in facilities such as message signing and confidentiality. Additionally, for those that use frequently webmail systems it would be most interesting to see that when the browser has a digital certificate installed the authentication becomes transparent (the browser and the webmail system validate the users' identity using that certificate, no longer requiring filling-in username/password form – however, the browser may require the pass-phrase that unlocks the private key of the user).

Scalability is always a challenge when deploying PKI within any collaborative, open environment. Our university has a student population of 28.000, circa 950 didactic staff and also as many people in administration and other support services. That counts for approximately 30.000 people each year. In addition to these client certificates, our PKI will have to be able to handle certificates for the network devices, systems and various types of servers (file, web, e-mail, etc.) that are available in such environment. The chosen PKI solution is made not only of software and hardware, but also of a bunch of people that will actually handle this targeted volume of certificates. In the first phase of our project, we intend to issue and handle certificates only for the entities and the community of users of the Faculty of Automation, Computing and Electronics (A.C.E.). The actual figures for this faculty list circa 1400 students, 60 didactic personnel, and 20 administrative and support employees. Aside from these client certificates, the local CA will issue certificates for the servers and various applications pertaining to the A.C.E. community.

Flexibility is a key factor. The PKI solution must be tailored in a timely manner to fit various environments and purposes. Of course, it is primarily the task of the PKI personnel to do that but the software applications composing the PKI must also be designed to allow flexibility of configuration and deployment.

Cost of ownership is always a problem with both commercial and open-source solutions. However in case of open-source solutions, if the mother project stops, or fails to continue delivering support (in form of updates, patches/fixes or new versions) then the costs supported by the owners that operate it tend to increase abruptly. A perfect and most convenient solution does not exist to this problem. It is worth taking a serious risk analysis before deploying any PKI solution, and also having a recovery plan.

Accreditations are a plus to any PKI solutions. It is a good attribute if the solution is conformant to standards and offering interoperability. As long as the standards are open, the PKI solution will avoid being locked-in specific vendor's standards and formats. In addition, it is a great plus if the PKI solution has been audited and accredited by recognized organizations (e.g. ETSI – European Telecommunication Standards Institute, Web Trust, etc.), and/or certified with respect to international standards, such as Common Criteria (1999).

Support from the vendor or developer is always important. Having a support group available facilitates solving the problems that may appear in front of the PKI administration team during setup, operation and maintenance.

Relating to the latter attribute it is important to choose whether the deployment will be in-house or out-sourced. An in-house PKI means that the organisation remains in control of the CA core functions. An out-sourced PKI means that the core CA functions are managed by a third party. There are advantages for each alternative. It is evident that the choice depends directly on the size of budget available to the project, or in other words the choice is between convenience and cost savings. For our implementation, we have opted for the in-house model in which the root CA, the subordinated CAs, and the certificates are created and managed within the domain of the university. This adds up to the flexibility of the PKI and also requires more care (i.e. security mechanisms) about the protection of the root CA private key.

Having said all these, we have opted for an in-house open-source PKI solution – OpenCA, and that mainly because of the budget limitation. There are several other distributions available: DogTag, EJBCA, NewPKI, OpenCA and OpenXPKI. Of these five, the three most popular implementations are: EJBCA, DogTag, and OpenCA – in this order. OpenCA is minimal and offers support for all the essential standards necessary for PKI operations. It fits well for a small to medium PKI community of subscribers as is the case with our first implementation. Furthermore, starting with a simpler implementation allows building up the knowledge and experience in operating a PKI for the team in charge.

3.4 Structure of OpenCA

The OpenCA solution fits well any hierarchical organization. A real-case customization for our academic environment is given in Fig. 1.

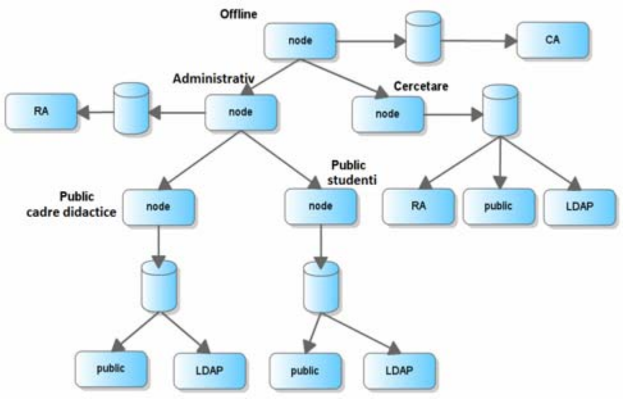

Fig. 1. OpenCA components

The certification authority is in charge with creation and revocation of certificates, and also for issuing CRLs. The RA can handle a variety of certificate signing requests (CSR). These CSR can be edited, approved, and deleted. The RA can also generate the pair of cryptographic keys for smart-cards, on behalf of the subscriber. The LDAP interface is implemented to separate the management of the LDAP component from all other software components since not all LDAP functionalities are necessary all the time to PKI administrators. The Public interface in Fig. 1 represents the only interface available to PKI users. Some of the functionalities of this interface include: generation of the cryptographic pair and of the corresponding CSR (by means of various web browsers), handling of CSRs for servers in PKCS#10 format – Nystrom et al. (2000), certificate installation, CRL installation, certificate search, and certificate revocation. The Node interface is used for the database management and also for the data exchange between the different levels of the PKI hierarchy. Typical operations performed with this interface include database initialization, information back-up and recovery, and also synchronizing the data between different levels of the hierarchy, Marian et al. (2011).

3.5 Setup and Administration

For the implementation, we have chosen a hierarchical organization, using a root CA that will issue certificates only for the subordinated top-level CAs. The main reason for this is to allow for extension of the PKI (to other faculties of our university and even to other universities within the national education network), and also for a certain flexibility in the management of the PKI achieved via delegation of responsibility.

The root CA is installed on an off-line workstation. On this same workstation is also installed the first subordinated CA (dedicated to the community of the Faculty of Automation, Computers and Electronics of the University of Craiova). This subordinated CA will handle certificates for the local community of subscribers (students and professors) and also for other entities (e.g. network devices, servers, etc.).

On a second, on-line workstation, we have installed the public interface of the subordinated CA that will take care of all certificate signing requests (CSR) and all certificate revocation requests (CRR), plus the CRLs of the CAs. A scheme of the two installed PKI components is presented in Marian et al. (2011).

3.6 Time to Implement and Associated Costs

The time for planning, acquiring the hardware, training the personnel, installing and configuring the PKI solution is of approximately 6 months. Developing additional applications in Perl programming languages requires every now and then at least one part-time programmer for medium-length periods of time. Prior to installation of the production environment, a testing environment and also a sandbox for development must be at hand.

Hardware acquisition (the secured rack hosting the servers running the certification authority front and back ends, the related hardware and networking equipment) is a substantial financial effort that appeared at the beginning of the work.

Approximately one month was dedicated to the writing and reviewing of the certificate policy (CP) and certification practice statements (CPS) – the documents governing the PKI.

We have known from the planning phase that the budget for an academic PKI deployment will be minimal and that is why we opted for an open source solution in order to avoid the costs of the software. However, there is no such thing as a free meal therefore it makes sense to estimate the costs associated to an operational solution if the solution is run for several years. A certificate is a certificate but there are some hidden costs associated with each subscriber (starting from the moment when she applies for a certificate up to the moment when the certificate is issued, published and subsequently installed into the subscriber's applications). Suppose only the community of our faculty of Automation, Computing and Electronics and take a life time of one year per client certificate; it means that annually, the subscribers' certificates will at least once be renewed or issued, some of them will get revoked, CRLs will be signed and published. With an optimistic estimation, the cost associated with processing one subscriber certificate is 1 RON leading to circa 1,500 RON per year costs for handling client certificates within our community. The initial hardware acquisition is approximated to 33,000 RON. The team operating the PKI is at minimum formed by one person. The certificate issuance can be distributed along categories of subscribers (didactic and administrative personnel on one side, students on the other) and also along the calendar of the academic year. This is necessary to avoid large volumes of CSRs appearing at the same moment (typically, at the beginning of the academic year). If the solution is not to be operated by enthusiastic volunteers, then the average monthly costs for the technical personnel are 1,500 RON/month/person. Taking into account only these three categories of costs the estimated annual cost for the first year of operation amounts to a staggering 52,500 RON. Over a period of 5 years the solution's estimated costs add up to 130,500 RON. If the solution were to be extended to the entire university population, then the estimated costs will reach even higher figures (and the operating personnel needs to be at least doubled). These costs might seem exaggerated considering the national educational budget but the obvious truth is security costs; and people find it out how much it does only after an incident occurs.

3.7 Problems Encountered

One of the first problems identified at the beginning of our analysis was the lack of a unitary naming scheme for the employees and the students of the university. On a normal basis each employee of the university should own an e-mail address of the form *firstname.lastname@ucv.ro*. This would be important for the identity that will be enclosed in the digital certificate. Additionally, students of the university should also own an e-mail address of the form *student_registration_number@ucv.ro*. Instead, there is a multitude of e-mail naming schemes within the university and what is even more curious, some of the didactic personnel are using commercial webmail instead of their institutional addresses. On the other hand, for the length of their studies, students do not receive on regular basis an institutional e-mail account. The problem with e-mail addresses and certificates reside in the proper identification of the person owning it and her affiliation to the institution. If one employee or student wants to use her webmail address in her certificate, then she will provide proof that the webmail address is indeed under her control.

A second problem is concerning the concept of Trusted Root. Commercial PKIs have agreements with software vendors so that their root certificates are pre-installed in all their applications (operating systems, browsers, mail user/transfer agents, etc.). That is why a commercial digital certificate is recognized by these applications. In case of our in-house PKI solution, we have developed procedures and scripts so that at installation time, our subscribers will be able to insert our root certificate within their local Trusted Root repositories.

A third major problem concerns dissemination of information and the transfer of know-how. One key to success in such a heterogeneous and distributed environment is to motivate the subscribers to adopt the solution, not to obligate them. This means instructing people the benefits of using public-key technologies, how to subscribe, to generate a pair of keys, to download and install a certificate, to back-up and to handle within other applications the pair of private key and digital certificate.

4. FUTURE ACTIVITIES

One of the features that will be approached next is the LDAP support for our PKI implementation. LDAP directories are meant to disseminate the public information of the PKI. Relying parties will be able via LDAP to search and download subscribers' certificates before sending encrypted messages or verifying digital signatures. Additionally, certificate revocation lists can be also published here.

Another activity will be to rectify the problem of using Romanian diacritics within digital certificates (mainly for the Distinguished Name field of a public-key certificate).

A third activity will be the extension of the public-key infrastructure first to all didactic personnel of the faculty and then to the personnel of other faculties within our university. Once the mass of subscribers will grow, we will be able to better approximate the success of the solution.

5. CONCLUSION

The PKI based on OpenCA was implemented as part of the security infrastructure of the University of Craiova. A certification authority for the community of the Faculty of Automation, Computing and Electronics was set up (subordinated to the already operating root CA). This CA is available on-line for the subscribers at http://ca.ucv.ro.

What matters most is what your organization does with the certificate once it is issued. Our experience so far proved that subscribers appreciate automated certificate delivery and installation (via web interfaces). We expect end entities to use certificates mainly for digital signing of e-mail messages, rarely for code or document signing. Also, encryption of e-mail messages and digital signing of mass e-mail to the community will be of high interest.

ACKNOWLEDGMENT

This work was supported by the strategic grant POSDRU/89/1.5/S/61968, Project ID61968 (2009), co-financed by the European Social Fund within the Sectorial Operational Program Human Resources Development 2007 – 2013.

REFERENCES

Common Criteria for Information Technology Security Evaluation (1999), Part 1: Introduction and general model, version 2.1

Common Criteria for Information Technology Security Evaluation (1999), Part 2: Security functional requirements, version 2.1

Common Criteria for Information Technology Security Evaluation (1999), Part 3: Security assurance requirements, version 2.1

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

ITU-T Recommendation X.509, Information Technology (2005), Open Systems Interconnection - The Directory: Public-key and attribute certificates frameworks

M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams (1999), X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP), IETF RFC 2560

M. Marian, A. Pîrvan, Implementing a Public-Key Infrastructure for the Academic Environment, Automatic Control and Computer Science section, Buletinul Institutului Politehnic din Ia i, fascicle no. 3/2011, ISSN 1220 – 2169

NewPKI project, available on-line at http://www.newpki.org

OpenCA project, available on-line at http://www.openca.org

OpenXPKI project, available on-line at http://www.openxpki.org

OpenCA guide (2010), available on-line at http://www.openca.org/projects/ openca/docs/openca-guide.pdf

OpenSSL cryptographic library, available on-line at http://www.openssl.org

PrimeKey open-source PKI – EJBCA, available on-line at http://www.primekey.se

Redhat Fedora Project, Dogtag certification system, available on-line at http://pki.fedoraproject.org/wiki/ PKI_Main_Page

ROCA (2010), Romanian Certification Authority available on-line at http://ca.ucv.ro

J. Semersheim (2006), Lightweight Directory Access Protocol (LDAP): The Protocol, IETF RFC4511

R. Shirey (2000), Internet Security Glossary, Internet Engineering Task Force Request for Comments (RFC) 2828