Proceedings of the 8th International Conference on Applied Informatics
Eger, Hungary, January 27–30, 2010. Vol. 1. pp. 265–272.

Secure Utilization of Local and Regional Data Assets Through Mobile Environments*

László Aszalós, Norbert Bátfai, László Csirmaz, János Folláth, Enikő Hajdúné Pocsai, Tamás Herendi, Tünde Kovács, Zoltán Matolcsy, Attila Pethő, Péter Varga

University of Debrecen

Abstract

Our aim is the development of local and regional content industry, establishment of the framework of innovative value added service for the utilization of data assets. In this paper we describe the advances we made in this direction.

Keywords: Cryptography, Data, Autonomy, Implementation

MSC: 94A60, 94A62

1. Introduction

In 2008 we started the National Technology Program TARIPAR3 together within a consortium under the leadership Geoview Systems Ltd. The aim of the project is the development of local and regional content industry, establishment of the framework of innovative value added service for the utilization of data assets.

This requires the secure utilization of data through mobile environments. Our task is to develop a package, which enables secure authorization, authentication and data exchange. Moreover, it is possible to perform digital signature to ensure data integrity. The speciality of the problem is that the data providers and clients have different computational powers and are running on different platforms. Typically the providers are computers, which are accessible through TCP/IP, while the clients are programmable mobile phones. Mobile phones usually utilize the WAP protocol suite for communication. The security provided by the WTLS protocol is insufficent, and the TLS protocol can only be established between the server and

*Research supported by TARIPAR3 project (grant Nr. TECH_08-A2/2-2008-0086).

the gateway. A further difficulty is, that the gateway translating between the protocols is in the possession of telephone providers: altering their implementation is not an option. Taken all round: a new high level protocol is required, that provides the desirable security.

2. Project management tool

Although the members of the Faculty of Informatics at University of Debrecen participated in many projects, for example introducing new programs, modules and subjects, take part in accreditations and researches; we did not use any software tool to organize these projects. These tools make easy the administration of the project, the members of the project can get the latest versions of the relevant documents.

Of course there are methods to replace these kind of tools. For example the email became a de facto standard to distribute and organize documents. The mail clients (even the browser based) allow us to search messages by tags, date and persons. This method is more convenient than to use a common directory on an ftp-site restricted to the group.

The project-management software has many advantages to the mail based management.

- It stores the documents in one place, and only one version of them. It is less probable, that the members work on different versions in parallel, which generates extra work.
- It is easier the archive and backup the collection of the documents then separate emails. An average user usually does not archive his/her files, but it is the duty of the administrator of the management software.
- The users cannot be sure that his/her emails are arrived because we do not like the acknowledgement in email clients. If we upload a document into the collection, everybody (with sufficient authorities) can reach it.
- The perfect management tool can warn its users about deadlines and different kind of its duties.

After the decision of introducing management software, we needed to choose suitable software. Our requirements were the followings:

- store the documents of the project
- store the forum-like conversations
- all member could add new material
- ability of searching, tagging
- privacy

We made a survey, and tried several software including groupware products and wiki systems. Finally we chose the TeamRoom of the Lotus Notes. The Lotus Notes is the default email client at our faculty. Most of our colleagues use only the mailer part; and almost nobody use the calendar and the to-do section, although these could be a killer application. The Lotus server called Domino can store many databases and applications can be develop based on these databases. The TeamRoom is such application including the standard distribution. Albeit this application is widespread, its documentation is poor. We made many efforts to come to know it, and produced teaching materials even for our colleagues, because we employed this tool in the management of corresponding studies and accreditations, too.

At first, we wrote a series a fictive letters, to show the base concepts in an enjoyable style. Next, we asked the members of the project to solve simple problems. Although the colleagues are experts in computer usage, at first only just few of them could complete them. Hopefully, after one year everybody could use it. To help the first steps we made several screen-casts to make unnecessary the reading of the manual, and made available .for everybody. These little movies show the steps of the simple tasks, demonstrate all the clicks.

Of course, there are inadequacies in the TeamRoom. The version control did not solve, hence we rewrite the document and we lost the original version; or we edit the copy of it. However this tools have advantages. The most important, that the Notes allow the replicas, so we can manage the database offline, too.

The members of the project are not fan of this tool, but they use it regularly, and it helps a lot to produce the reports.

3. Communication model

In this section we describe the model of data transmission and cryptographic tools we apply.

The communication between the data source and client device is done on a basically unsecure channel. To fulfill the expected security requirements we split this unsecure channel into logical subchannels having higher security level.

When we want to use an unsecure channel as a secure one, we have to insert an extra interface in the chain of data transmission. This interface will serve as a transmission management device and as a cipher.

The data provided by the source contains an assignment to a proper security level. The interface device recognizes the side information attached to the main data and tries to establish a proper security level logical subchannel with the mobile client device. If a suitable active subchannel is opened yet, then the interface applies the necessary encryption methods to reach the security level described by the side information. If there are no such an active channel opened, then the interface initiates a handshake like process with the client's corresponding interface device and agree the parameters of a secure communication channel. The communication between the two interface during this process is made on a dedicated secure

subchannel, powered by an asymmetric cryptographic protocol, such as RSA. The result of the discussion is a pair of keys for a symmetric encryption protocol, which has much higher data transmission rate than the asymmetric one. Establishing this secure channel finish with the activation of the new communication line and setting the expiration time. After the expiration time has spent, the channel become inactive. To make it active again a new handshake process should be executed.

If the data does not contain any side information or the side information permits the use of an unsecure channel, then the interface module uses a permanently opened unsecure subchannel, which obviously does not contains any kind of cryptographic encoding method.

4. Fast exponentiation

In this section we describe a new method for fast exponentiation. The problem we want to solve is the following:

Let $< A\ ,\ \cdot >$ be a group, $a \in A$ and $n \in \mathbb{N}$. Compute a^n.

Although the problem is defined precisely, there are several algorithmic solution, depending on the particular circumstances.

4.1. Binary exponentiation

The well known binary exponentiation is based on the binary digit expansion of the exponent n. Let

$$n = 2^k + \sum_{i=0}^{k-1} n_i 2^i \quad n_i \in \{0,1\} \text{ for all } 0 \leq i < k\ ,$$

and the sequence x_i is defined as follows:

$$\begin{aligned} x_0 &= a \\ x_i &= x_{i-1}^2 \cdot a^{n_{k-i}} \text{ for } i = 1, \ldots, k\ . \end{aligned}$$

Then $x_k = a^n$.

Clearly the number of necessary operations are at most $2k \approx 2 \log n$. More precisely, the exact number of operations is $k + W(n) - 1$, where $W(.)$ is the Hamming-weight of the vector $[n_0, \ldots, n_k]$ i.e. the amount of nonzero elements.

One can fine tune the above algorithm decreasing the number of nonzero elements of the digit expansion of n.

4.2. Modified binary exponentiation

Let $n \in \mathbb{N}$. Then n can be represented in the form:

$$n = \sum_{i=0}^{k} n_i 2^i \quad n_i \in \{-1,0,1\} \text{ for all } 0 \leq i < k\ .$$

The representation is not unique.

Since $0 \leq k + W([n_0, \ldots, n_k])$, there is always a not necessarily unique minimal representation of n.

Similarly as before, one can define the following sequence:

$$\begin{aligned} x_{-1} &= e \\ x_i &= x_{i-1}^2 \cdot a^{n_{k-i}} \text{ for } i = 0, \ldots, k \ , \end{aligned}$$

where again $x_k = a^n$.

4.3. Synchronous powering

Let $a, b \in A$ and $n, m \in \mathbb{N}$. We want to compute $a^n \cdot b^m$ (assume n and m are of the same magnitude).

The trivial solution computes a^n and b^n separately and then multiplies them together.

There is however a less trivial solution. Let

$$n = \sum_{i=0}^{k} n_i 2^i \quad n_i \in \{0, 1\} \text{ for all } 0 \leq i < k$$

and

$$m = \sum_{i=0}^{k} m_i 2^i \quad m_i \in \{0, 1\} \text{ for all } 0 \leq i < k \ .$$

Define the sequence x_i by the following:

$$\begin{aligned} x_{-1} &= e \\ x_i &= \begin{cases} x_{i-1}^2 \cdot a & if \ n_{k-i} = 1 \ \& \ m_{k-i} = 0 \\ x_{i-1}^2 \cdot b & if \ n_{k-i} = 0 \ \& \ m_{k-i} = 1 \\ x_{i-1}^2 \cdot ab & if \ n_{k-i} = 1 \ \& \ m_{k-i} = 1 \end{cases} \quad \text{for } i = 0, \ldots, k \ . \end{aligned}$$

One can easily proove that $x_k = a^n \cdot b^m$.

It is also clear that the time complexity of the computation is not greater than $2k$, which is approximately the half of the time complexity of the trivial solution.

4.4. Modular split exponentiation

Let m_1 and m_2 be different, coprime integers of the same magnitude, s.t. $n \leq m_1 \cdot m_2$ but the same magnitude and let $n_i \equiv n \mod m_i$ for all i.

Then $\log n_i \approx \frac{1}{2} \log n$ for $i = 1, 2$. By Chinese Remainder Theorem: $\exists c_1, c_2 \in \mathbb{N}$ s.t.

$$n = c_1 \cdot n_1 + c_2 \cdot n_2 \ .$$

Precomputing $a_i = a^{c_i}$, we have to compute $a^n = a_1^{n_1} \cdot a_2^{n_2}$, which problem can be solved by an algorithm of time complexity $\log n_i$ instead of $\log n$.

In the case we want to compute several powers of the same base – which can appear in cryptographic applications, e.g. in El Gamal cryptosystems – we have a real gain in speed of a factor 2, since the precomputation of a_i should be done only once.

However, one have to take it in account, that the computation of n_1 and n_2 are also requires some amount of time, but if the group operation is more expensive than computing the residues modulo m_1 and m_2, then it is worth to do the extra job.

5. Trusted computing

Trusted Computing is a technology developed and promoted by the Trusted Computing Group. This group is the successor to the Trusted Computing Platform Alliance, which is developed by AMD, Hewlett-Packard, IBM, Intel, and Microsoft in order to define and implement Trusted Computing. The technology contains a number of protocols, policies and ISO standards, which are cannot be live out of consideration during the building of a secure channel.
The definition of term of Trusted computing is the following:
"With Trusted Computing, the computer will consistently behave in expected ways, and those behaviors will be enforced by hardware and software."
There are six key concepts which are formulated by the Trusted Computing Group:

1. Endorsement key
   is a 2048-bit RSA public and private key pair, which is created randomly on the chip at manufacture time and cannot be changed.
2. Secure input and output
3. Memory curtaining / protected execution
   is a kind of memory protection techniques to provide full isolation of sensitive areas of memory.
4. Sealed storage
   protects private information by binding it to platform configuration information including the software and hardware being used.
5. Remote attestation allows changes to the user's computer/mobile to be detected by authorized parties.
6. Trusted Third Party (TTP)

6. Implementation

Bouncy Castle is an application programming interface, which contains classes and interfaces developed for implementing the basic and advanced security algorithms.

It has a version for Java and .NET technology as well. We decided to implement the secure communication channel in Java, and because of it's sdk just contains the basic secure algorithms, we had to find an affix for it. We tried to use some of the application programming interfaces which can be found, we decided to use Bouncy Castle because of the features of it.
The Bouncy Castle Crypto APIs for Java consist of the following, which can be found on the api's web site as well:

- A lightweight cryptography API for Java.
- A provider for the Java Cryptography Extension and the Java Cryptography Architecture.
- A clean room implementation of the JCE 1.2.1.
- A library for reading and writing encoded ASN.1 objects.
- A light weight client-side TLS API.
- Generators for Version 1 and Version 3 X.509 certificates, Version 2 CRLs, and PKCS12 files.
- Generators for Version 2 X.509 attribute certificates.
- Generators/Processors for S/MIME and CMS (PKCS7/RFC 3852).
- Generators/Processors for OCSP (RFC 2560).
- Generators/Processors for TSP (RFC 3161).
- Generators/Processors for OpenPGP (RFC 2440).
- A signed jar version suitable for JDK 1.4-1.6 and the Sun JCE.

In close collaboration with the Debrecen Developer Network (DDN) we have developed a hybrid cryptographic test web application based on Bouncy Castle Crypto API. On the server side, we are working in Java EE environment (with Tomcat and Glassfish) and our clients are Java ME MIDP (Mobile Information Device Profile) mobile phones. The developed test application can be used to perform cryptographic measurements on real mobile phones. The measurements are achieved by involving the students of DDN.

References

[1] A. Bérczes, J. Folláth, A. Pethő *On a Family of Preimage-Resistant Function*, accepted (Proceedings Trebic)

[2] A. F. Webster, S.E. Tavares *On the Design of S-Boxes*, Advances in Cryptology: Crypto '85 proceedings, Springer, 1986

Debreceni Egyetem - 4032 Debrecen, Egyetem tér 1.
e-mail:
aszalos@inf.unideb.hu
nbatfai@inf.unideb.hu
csirmaz@renyi.hu
follathj@inf.unideb.hu
pocsai.eniko@inf.unideb.hu
herendi@inf.unideb.hu
tkovacs@math.unideb.hu
mato@inf.unideb.hu
pethoe@inf.unideb.hu
pvarga@inf.unideb.hu