MOBILE SECURITY ASSURANCE METHOD

Marian Cristescu

FSE – ULB Sibiu

- this paper presents a method of designing and developing mobile applications that aims to limit or eliminate their security issues;

- the paper deals with the mobile application security issue, and a secure general architecture of mobile applications is proposed;

- the specific objectives of the paper are:

- identify ways to optimize application security;
- establishing new secure application architectures.

ARCHITECTURAL OPTION TO ENSURE MOBILE SECURITY

Security features are highlighted in the following by analyzing a BI application (Business Intelligence). The application was designed and developed using the Windows Phone 7 platform facilities, and the following hypotheses were made for implementation:

- access to the app is only allowed to users passing through the authentication stage.

- external data can be downloaded through the application, which is stored on a server placed inside the organization and downloaded via a web service;
- another feature of the application is that it offers the possibility of saving the intermediate and final results of the reports, the results being placed on a server outside the organization;
- as functionality, it should be considered and the possibility of carrying out some processing on the initial data.

The main features of the new architecture are as follows:

- a new architecture is based on implementing a solution that requires a symmetric key;

- the security assurance process within the new architecture implies the availability of a functional component of the organization to generate a password p_u (PasswordUser) that is unique to each user;

- encrypting and decrypting data on the Isolated Storage media requires multiple versions of the k_u (KeyUser) user key operation that takes place inside the application;

- the user authentication action in the web service involves the use of the Ku key in the web services dialogue, after which the authentication process has been completed, a mutually exchanged, encrypted, share of the web service will start.

The authentication process requires a dialogue that involves following the steps outlined below :

- the user name is required to be able to connect to the web service;
- upon login, the web service will generate, as a response, a random string encrypted using the key obtained from the user name that was provided to it in the connection process;

- the random string decryption assumes that the application must use the received key at authentication, and the string will be retransmitted to the web service;

- in the next step, the web service compares the string received with the random generated one, and user authentication takes place only when the two rows are equal;

- as a result of authentication, the application will have access to the web service interface.

OBTAINED RESULTS

In order to obtain optimal secure architecture, four scenarios were considered at which application-level attacks were considered, as follows:

- **at the platform level** - where security was provided by encrypting files with a password derived from the user's password that is never saved, the name of the non-malicious files;
- **at the level of the communication channel** between the mobile application and the web service - a third entity can intercept the interchanged message but can not understand it without decrypting it;

- **at the network level** - a third person can not access data or send information within the network because they can not use them without decrypting them;

- **at the application server and database level** associated with password storage, they can not be accessed because they are saved at the level of the authority that issued the certificate and the keys, not at the level of the application or the web service.

CONCLUSIONS

Based on the mobile-specific features and features identified, a number of secure architectures have been proposed for implementing Business Intelligence mobile applications.

Architectures consider a standalone mobile application that communicates with a web service. The application also stores information locally in the allocated Isolated Storage module.

The solution takes into account the use of a symmetric key and the existence of a central authority that allocates passwords. The dialogue between entities initially carries out the authentication of the parties.

Data streams for application usage scenarios are identified and presented, practical aspects related to implementation in several variants, depending on the life cycle of the web service.

This proposed architecture is easy to deploy and at the same time provides robust protection for the traffic data.

By identifying common elements with other types of applications, this architecture could also be adapted for mobile m-learning applications.