Analysis of Use Wireless Smart-cards for Authentication on Web-sites and Web-services

Roman Zharinov, Sergey Shevelev
SUAI
Saint-Petersburg, Russia
roman@fruct.org, shevelev.2s@gmail.com

***Abstract*—There are many ways to confirm transactions or person using the second communications channel. This paper describes how to use a secure contactless smart-card as a second communications channel and unified way of verifying a user's identity.**

I. Introduction

Our work is devoted to develop of software for authorization on the Web-services using the mobile wireless technology. As wireless technologies are selected Bluetooth and NFC.

With increasing of modern computer's power and widely using of weak hash methods of passwords, password cracking is not particularly complex task. Using public key cryptography with a secure private key storage on the user's device (mobile phone or smart-card), allow safely use the same key to many Web-services. Our final purpose is to develop a complex system for authorization on web-services using mobile device, digital certificates, smart-cards and wireless technologies.

The main necessary modules are listed below:

- Secure data processing on a contactless smart-card;
- Data transmission between the smart-card and the mobile device via NFC;
- Data transmission between the mobile device and PC via Bluetooth;
- Data processing on Web-services.

II. Description of the system

This project is an analogue of the two-factor authentication, such as smart cards or e-tokens. The second factor is the contactless smart-card and smartphone. This coupling is due to several reasons: first of all most of Web-services ported or used on mobile devices, and secondly nowadays there are a few notebooks with built-in NFC chip.

On initialization phase we are planned to link the contactless smart-card with a smartphone. As a unique identifier take phone IMEI. This is 15-bit number in decimal representation and it's unique for each device. IMEI is assigned to the phone during the manufacturing factory. It serves to identify the device on the network and stored in the firmware of the machine. In modern phones IMEI is stored in one-time programmable memory area, and cannot be changed by software.

III. Existing systems

Nowadays there are no analogs having full functionality of our proposed solution. But there are a several commercial and open source products that implement some of the functions.

A. Authentication by a random one-time code transmitted via SMS

This system currently has the most widespread among the services to confirm the identity. Two-factor authentication is used in such systems as: Internet banking (banking transactions confirmation), social networks, email services, etc.

Disadvantages of technology: cost, delivery confirmation.

B. USB-keys and systems of generation one-time code

Electronic USB-keys are compact devices for information security designed for corporate and private users [4]. These devices usually contain a cryptographic processor, memory module and have its own operating system. Generate one-time passwords based on cryptographic hash-chains with preliminary initialization vector. Devices used successfully only in the corporate sector, as requires an integrated infrastructure management system.

C. Google Authenticator

This is open-source system for two-factor authentication but having only software implementation [5]. Is installed on two sides: the server and the client's smartphone. To work correctly, need to generate and store the unique initialization vectors. Generate one-time codes depends on the current time and is valid for 30 seconds.

IV. Overview of other technologies

There are several ways to secure storage and processing of information on the smartphone:

ISSN 2305-7254

1) Security element (SE) is integrated in the SIM card (UICC) - the connection between the security element in the SIM card and NFC Controller is via a standard set of libraries SmartCard API or using the Single Wire Protocol SWP [3];
2) SE is built into the SD card - communication is performed similar to UICC. Not supported in Android version 4.4 and higher due to the limitations of the permission to external media;
3) SE is built into the smartphone (eSE) [1], such eSE embedded directly in the NFC chip in the card or phone - Built-in security element is connected to the NFC Controller via SignalIn / SignalOut connection.

V. Conclusion

This developed system will allow login (using the personal public key infrastructure) on a Web-service via one or two factor authentication. Also smart-cards [2] may use for pass into the room.

The system is aimed at physical persons and business. Individuals can use the system as secure access to Web-services, such as social, email, local, etc. For corporate clients are building infrastructure control access to rooms, account and user identification.

References

[1] Zhiqun Chen, Java Card Technology for Smart Cards: Architecture and Programmer's Guide., 2000.
[2] Zharinov R.,Trifonova U., Gorin A., “Using RFID Techniques for a Universal Identification Device”, *Proceedings of the 13th Conference of Open Innovations Association FRUCT and 2nd Seminar on e-Tourism for Karelia and Oulu Region*, Petrozavodsk, Russia. Publisher: SUAI, ISSN 2305-7254, pp. 244-248.
[3] "Digital signature and authentication: made in Russia", *Zhurnal setevih resheniy/LAN*, № 9 (212), september, 2014.
[4] Analytical review of the company's products "Aladdin RD"
[5] Web: https://code.google.com/p/google-authenticator/