Chapter 20
Hardware Secure Access to Servers and Applications

J. A. Álvarez Bermejo
Universidad de Almería, Spain

J. A. López Ramos
Universidad de Almería, Spain

F. Gálvez Sánchez
Universidad de Almería, Spain

ABSTRACT

In this work, we propose a powerful yet inexpensive method for protecting and discriminating unauthorized accesses to sensible digital information (or even to the entire system) via common and conventional tools such as USB devices. The result of this work allows that the access to servers or the execution and access to specific data, take place only under a controlled and defined scenario.

INTRODUCTION

Current legislation at every country provides means to regulate the use and control of digital information (an useful standard to ensure a certain structured information security risk assessment can be found under the norm ISO/IEC 27002), specifically if its character compromises the private sphere or intimacy of persons. Operating systems provides standard protection methods, but nothing can be done to protect the data if the use of the operating system is not adequate (uncontrolled software installation may produce data stealing via Trojans, etc.). In addition, one may consider how security is at hand of everybody. Abelson, Ledeen & Lewis (2008) underlined two unexpected behaviours experienced in the new digital era we are now living in (1) people give up their privacy too easily, and in the process may give up third party’s privacy, and (2) little brother is watching, even non-experienced kids may run scripts to attack your data. Cryptography plays an important role offering privacy nowadays although few users employ it.

In this chapter we propose a system for granting secure access to stored data and even to applications that deal with them, based on a protocol of sharing secrets. The aim of this software is to avoid unauthorized uses of programs and their related data or even a whole system. Operating systems
Hardware Secure Access to Servers and Applications

are in charge of protecting us from intrusions and our software will be responsible of converting the stolen information into a useless chunk of bits.

Restricted access to information stored in a system is turned into an issue of truly vital importance in certain circumstances. When access to such information is a privilege of only one person then it is usual that this information is encrypted using a symmetric cryptosystem, where the secret key is a property of the owner of the information. PGP (http://www.pgpi.org/) is a protocol that can be used to that end. However a problem arises when protected data should be accessible for a group of people and not only for a unique user. In that case, making copies of the key used to protect the information and giving them to authorized people is something that decreases the level of security in a significant way. Secret sharing schemes come to the rescue in such scenario (Menezes, A., 1996; Schneier, B., 2003). These algorithms are protocols that allow the sharing of the key used to protect the information in such a way that the original key can be recovered from a minimum number (maybe all) of the shares and, even if a lesser number keys are present such shares does not reveal any information about the shared key. Another issue of interest regarding the security scheme is one that has to do with length of the key. Keys used for any cryptosystem and thus, also the shares, are excessively long to be memorized which makes necessary providing any storing method, making the key susceptible of being stolen.

In this chapter we present an implementation that provides a security system based in USB devices for protecting data and applications on information systems, this can be carried out in an individual, shared or hierarchical way, also preventing the key or any sharing from being stolen was a desired objective. Section 2 will introduce the foundations of the cryptography used. Section 3 will show a roadmap of the decisions taken for choosing the Operating System where the software was to be deployed in, the language to build the software, the way of using the USB device in order to use the secret sharing, etc. Section 4 will show the implementation details, how we dealt with big numbers. Section 5 will show the conclusions and issues to be improved.

2 BACKGROUND: CRYPTOGRAPHIC AND SECURITY BASIS

Secret keys used in cryptographic protocols give raise to several practical problems concerning key generation, storing and distribution. The most efficient solution to these is to keep the key in a unique and safe place, known only by its owner. However, in this way we have the risk that the information protected by the key becomes completely inaccessible if the owner loses it. Additionally, in many practical cases we need to distribute the key between the members of a group in such a way that it cannot be recovered without the cooperation of a minimal number of such persons. This scheme is especially suitable in the case that the secret is a responsibility of a group and not only a unique person due to the high level of privacy required (Lederman, 2004; Peterson, 2005; Tang, 2008).

Likewise, in some situations it could be necessary that the recovering of a determined secret key must be done in absence of its direct responsible, i.e. a key can be recovered by its owner or determined hierarchical groups chosen by him/her to this end. This can be done making that some of the shares of the key have a preferential role to others (Menezes, van Oorsch & Vanstone, 1996).

Key Generation

One of the initial problems to solve is the generation of the secret key, since it is clear, the fortress of our system lays on the security of the key. One possible solution to this is to use a hash algorithm such as MD5 (Menezes, 1996; Schneier, 2003). MD5 generates a hexadecimal 128 digits value in
Related Content

Applying Continuous Authentication to Protect Electronic Transactions
[www.igi-global.com/chapter/applying-continuous-authentication-protect-electronic/75102?camid=4v1a](www.igi-global.com/chapter/applying-continuous-authentication-protect-electronic/75102?camid=4v1a)

Cyber Security: Future IT-Security Challenges for Tomorrow's Leaders and Businesses
[www.igi-global.com/chapter/cyber-security/125355?camid=4v1a](www.igi-global.com/chapter/cyber-security/125355?camid=4v1a)

Patents and Standards in the ICT Sector: Are Submarine Patents a Substantive Problem or a Red Herring?
[www.igi-global.com/article/patents-standards-ict-sector/2583?camid=4v1a](www.igi-global.com/article/patents-standards-ict-sector/2583?camid=4v1a)

The Role of Individuals and Social Capital in POSIX Standardization
[www.igi-global.com/chapter/role-individuals-social-capital-posix/29682?camid=4v1a](www.igi-global.com/chapter/role-individuals-social-capital-posix/29682?camid=4v1a)