HARDWARE SOLUTIONS FOR INFORMATION SECURITY IN INTERNET

Galia I. Marinova[1]

Abstract **- The paper represents an overview of the hardware solutions for information security in Internet. The solutions considered are cryptoprocessors, smart cards, tokens, I-heys and new architecture for e-business PCs. Authentication tools implementing PIN (Personal identification number) codes and biometric technologies are characterized and classified. Some conclusions for the future PC in e-business and the possibilities of integration of these topics in education are dressed.**

Keywords **- Information security, Smart cards, Cryptoprocessors, Biometric technologies, Internet and e-business**

I. INTRODUCTION

The expansion of Internet services and the e-business perspectives put a stress on information security. Software tools [1, 6, 10, 11] for firewall, antivirus and encryption were developed to ensure security in open network. Standards were defined as DES (Data encryption Standard), implementing symmetric keys, IPSec (IP Security protocol for security exchanges on TCP/IP networks) and the new AES (Advanced encryption standard) expected to replace DES. Alliances between companies for PC, PC-components and software were organized in order to specify characteristics which should make the Internet environment secure for e-business. As noted in [14], software alone is not able to guarantee the security, so efforts were made to find an optimal solution combining software and hardware.

The paper makes an overview of the hardware solutions available today. Cryptoprocessors, Smart cards, biometric technologies and the new architecture foreseen for global security in PCs are considered and estimated.

II. CRYPTOPROCESSORS

The main advantage of cryproprocessors forward software solutions is the speed of data encryption (achieving 310Mbits/s) which doesn't affect the speed of data transfer. The increasing length of keys made prohibitive the software encryption processing in terms of speed. Cryptoprocessors implement the IPSec protocol. They don't replace software [17], but act together with it. Cryptoprocessors are mainly used in routers and remote access servers, but also in smart cards and keyboards.

The architecture of a cryptoprocessor is presented on Fig.1.

Table I presents existing cryptoprocessors [12,17] and their characteristics.

Xilinx proposes in [15,16] an IP (intellectual property) of a cryptoprocessor, called Xilinx Alliance Core X_Des Cryptoprocessor. It integrates a 64-bits DES standard and performs encryption and decryption in 16 bits clock cycle.

The algorithm implemented in that IP is presented on Fig. 2. This IP is suitable for the Virtex family circuits.

Another example is Wave Systems described in [2]. It is a programmable circuit implementing ARM core and integrating security functions, counter and identification. It is embedded on the PC main board or on TV decoders.

III. SMART CARDS AND DERIVATED DEVICES

The smart card is the most popular tool for strong authentication. Its principle is to combine something that the user has with something that he knows.

A. Structure of the Smart card

B.

The basic structure of the Smart card [7,19] is presented on Fig. 3. The Smart card contains a zone protected from writing by a fusible and a zone protected from reading and writing for the PIN code. After a predefined number of false inputs for the PIN code, the Smart card is blocked. The card operating system is called COS. As shown on the figure, the Smart card demands a Smart card reader to be activated.

B. Modifications of Smart card

Some modifications of the Smart cards are:

- Simcard which is used in the GSM systems and it has the size of a postmark;
- Smart card which power supply is provided through tele-induction;
- Smart card USB, which is conceived to be connected directly to the USB port of the PC, by the use of microcontroller that integrates a USB controller and a controller 7816. The reader is then a simple connector;

[1]Galia I. Marinova is with the Faculty of Communications and Communications Technologies in Technical University of Sofia, 8, Kliment Ohridski street, Sofia - 1000, Bulgaria
e-mail: gim@vmei.acad.bg

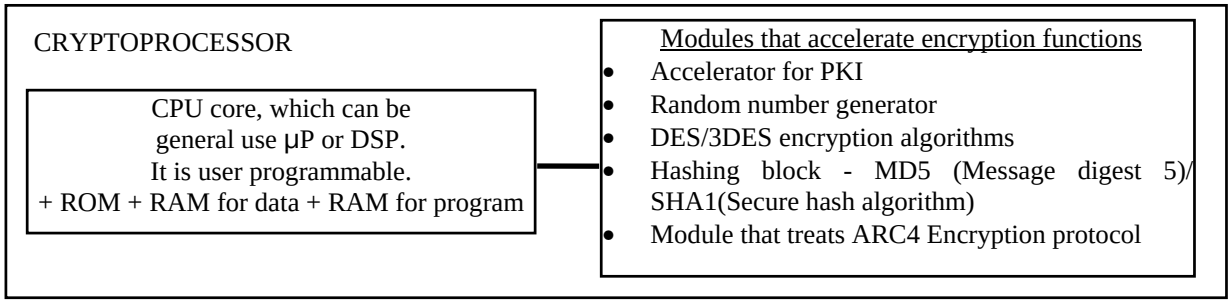


Fig. 1. Architecture of a cryptoprocessor

TABLE I
CARACHTERISTICS OF CRYPTOPROCESSORS

Cryptoprocessor (Company)	**Characteristics**
SafeNet (Analog Device)	DSP-16bits;155Mbits/s for data transfer; PCI interface or Card bus;
CryptoNet (BroadCom)	310Mbits/s for data transfer; PCI interface;
Netware security Processor (Hi/fn)	310 MBits/s for data transfer; 500Mbits/s for IPSec protocol (DES and SHA-1are included, AES is foreseen); 700Mbits/s for LZS (Lempel-Ziv-Ztac) compression and MPPC (Microsoft -point-to-point compression); PCI interface;
VMxxx(Philips)	205-393Mbits/s for different encryption algorithms; It integrates exponent and multiplier for keys of 1024 bits in RSA (Rivest, Shamir, Adleman) algorithm; It is based on Philips cryptographic coprocessor for Smart cards;
MC180 (Motorolla) MC180e	310 Mbits/s for data transfer; without PCI Interface; It is economic; MPC180e integrates a module accelerating the algorithm for elliptic curves for wireless communications as WAP.
Bluming2, Bluming-1k(ANKAD, Russia)	0,32Mbytes/s for data transfer;
Itinium (project of Intel)	The processor integrates a set of instructions adapted for encryption calculations.

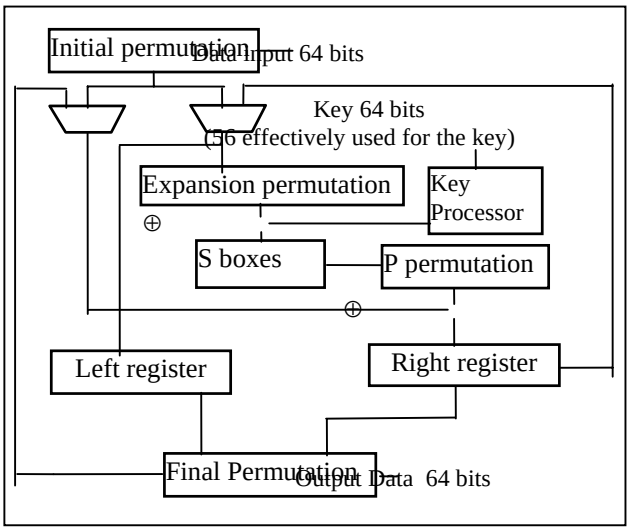


Figure 2. Algorithm implemented in Xilinx X-Des Cryptoprocessor IP

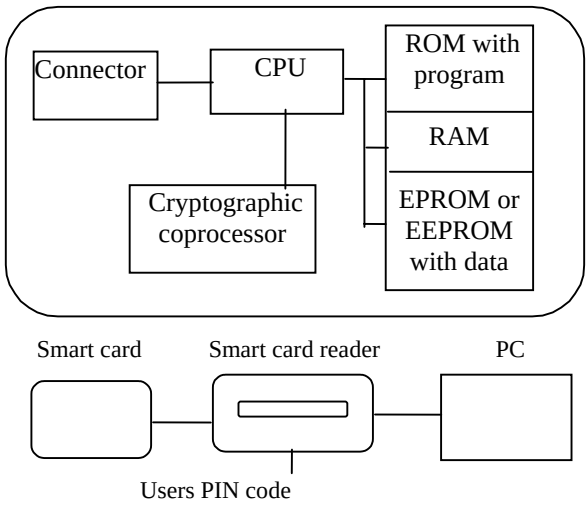


Figure 3. General structure of a Smart card. Activation with Smart card reader

• LPKI, described in [5] is an economic Smart card for PKI; It generates a couple of private and public keys following the RSA algorithm and delivers a certificate. The LPKI smart card doesn't integrate a cryptoprocessor;
• Active Card, Active Reader and Token presented in [18] are devices that use one-time valid password elaborated with a random number generator. Token generates a one-time-use dynamic password with a standard based - 3 variable algorithm, as shown on Fig. 4.

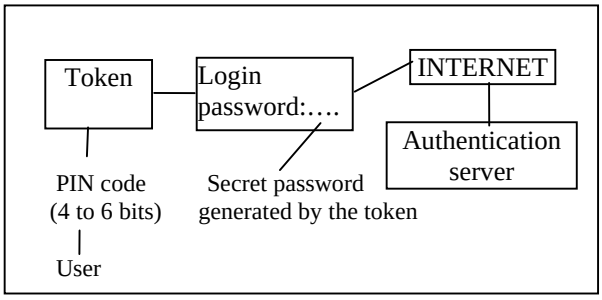


Figure 4. Token based authentication

TABLE II.
MAIN COMPONENTS IN BIOMETRIC DEVICES

Source of biometric data	Sensors
Fingerprints	• Optical sensor • Capacitive sensor ; It uses CMOS active sensing technology. • Heat sensor ; The difference between the thermal conductivity of skin and air is used for recognition of ridges and valleys on the finger.
Iris or retina profile	• CCD monochrome sensor and laser diode for iris lightening • Camera
Facial characteristics	• Camera
Vein pattern on the back of the hand	• Camera, creating infrared image through infrared LED array
Voice	• Microphone
Signature	• 3D pressure sensor • Time and speed meter • Line shape recognition • Angles in various directions • 2 dimensional tilt and acceleration sensor.

C. Device ikey

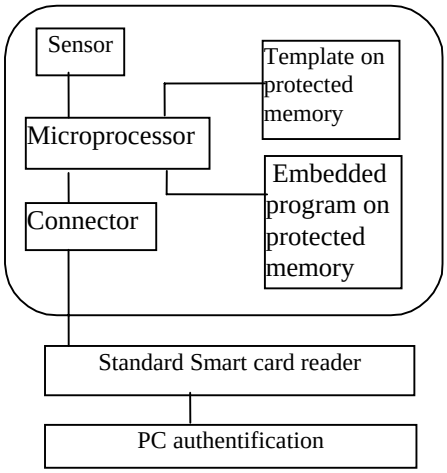
The ikey (Rainbow) presented in [8] has a microelectronic structure similar to the one of the Smart card. It implements a hashing block MD5, a random number generator and 8-64kb personalized EEPROM and it contains an unique serial 64 bits number. The form of the ikey is different and more robust than the Smart card. The ikey is connected to the USB port of the PC and it doesn't need a special reader. It makes the technology more economic. The user inserts the ikey in the USB port and types the PIN code on the PC.

The applications of the ikey are:
•Access control for system and framework;
• Internet access and Web pages access;
• Storage of digital certificates;
• Electronic wallet;
• Profiling;
• Protection of sensible information;
• VPN development.

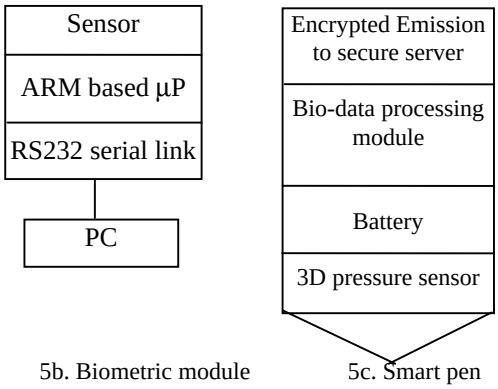
IV. BIOMETRIC TECHNOLOGIES

Biometric technologies are more secure than PIN code or passwords. Table II presents the main components [3,4,9] in different BiAS (Biometric Authentication System) in terms of source for biologic data and sensors applied. A template of the authentication unit is stored on a protected memory. The processing is realized on collected biometric date, by the microprocessor following the program embedded on a secure memory. It consists in image processing, compression, encryption and template matching.

Three applications of biometric technologies for strong authentication are presented on Fig.5. The full BiAS (Biometric Authentication System) on a card from Fig.5a can be read by any standard Smart card reader.



5a. Full BiAS on a smart card



5b. Biometric module 5c. Smart pen

Figure 5. Applications of biometric technologies

This technology is compatible to any existing equipment. The biometric personal data are not transmitted to the PC and don't need to be stored in a secure data-base. When the biometric data collected from the user are matched, the card is activated and establishes a communication with the host system The module from Fig. 5b can be connected to the serial port of the PC. The Smart pen from Fig. 5c is applied for signature recognition. Another tool is the e-signature pad for signing Windows 2000/95/98/NT and Adobe/Acrobat documents. The verification consists on matching with a signer-signature template.

V. PC ARCHITECTURE FOR INTERNET SECURITY

Since 1999 several initiatives from software and hardware companies were lanced in order to specify global security for PCs in e-business.

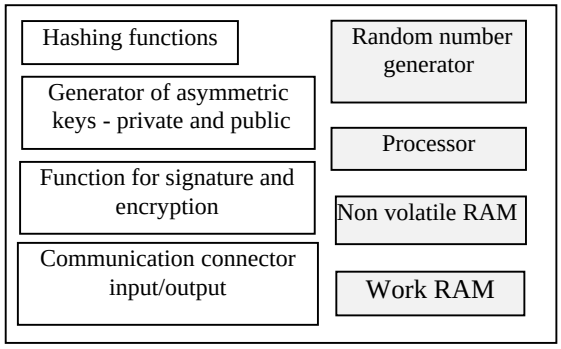


Figure 6. Architecture of a security module, defined by TCPA

Intel, Compaq and IBM have experienced more or less successful solutions, described in [2]. An industrial standard interface of Windows 2000 for Smart card use was defined and it was called PC/SC. MUSCLE was a similar solution for LINUX and OCF for Sun and Java.

In 1999, Compaq, Microsoft, HP and IBM organize TCPA - Trusted Computing Platform Alliance. TCPA defines the general specifications for the PC companies, for the PC component companies and for the programmers as a security label for the future generation PCs for e-business.

The TCPA main concept is the TPM (trusted platform module) which acts on the BIOS, on the OS on the drivers for periphery and on the software related. The security module in the PC should support human recognition services. The TPM should be inaccessible physically and it should react to any tentative for illegal access. The architecture of the security module defined by TCPA is presented on Fig. 6.

Some realizations of security modules are already on the market - Tamper Resistant (New Image, Taiwan) from [2], Sonic Wall from [4,13] and Compaq keyboard integrating security tools.

VI. CONCLUSION

In order to make e-business acceptable for large number of
users, companies try to standardize a specific architecture for PCs.

The best solutions for strong authentication seem to be Smart cards and ikey, especially when PIN code is used to produce a one-time-use password or when they integrate biometric data. Full biometric authentication system on a Smart card seems to be an acceptable solution from any point of view.

It would be interesting to integrate topics on hardware solutions for information security in education programs. An implementation in education, of a software tool for information security was presented in [6]. It is now planned to integrate theoretical and practical examples for hardware tools in different disciplines as "Computer-aided design in communications" and "Internet and JAVA" for students in Bachelor and Master degree in Communication Technologies in Technical University of Sofia.

REFERENCES

[1] Accéder à vos applications centralisées en toute sécurité, COMPAQ, CITRIX, CHECKPOINT, 4.07.2000
[2] Avenel Y., Le PC cherche ses clés, Intégration N°8, February 2001, pp.52-58
[3] Avenel Y., La reconnaissance de l'iris se marie à la visioconférence, Intégration N°7, January, 2001, pp.26
[4] Avenel Y., Sécurité Internet: les solutions "tout-en-un" arrivent, Intégration N°7, January, 2001, pp.26
[5] Avenel Y., La carte a puce LPKI allège les coûts de la sécurité forte, Intégration N°7, January, 2001, pp.27
[6] Cholakov S., G. Marinova, "Software tool for encryption - Cryptograph 1.0", Energy and information systems and technologies, Volume III, Bitolia, Macedonia, 2001, pp.790-995
[7] Guelle Pathrick, "Cartes à puce", DUNOD, Paris, 1998
[8] Ikey characteristics, Rainbow technologies, www.rainbow.fr
[9] Happish Julien, "Are you really who you claim to be", Smart card 2001, London, EPN, V. 30, N°4, April 2001, pp. 74-75
[10] La e-security, Vidati, 26.10.2001, Paris, France
[11] Les 10 défis à relever pour sécuriser votre réseau, Check point software technologies, May 2000
[12] Rakitin V.V., Romanets Y.V., "Difficult way of Russian cryptoprocessor", Chip news, No7-8(16-17), 1997
[13] Risk Technology, L'expert sécurité, PCWorld, June 1999, pp.14-15
[14] Timofeev P.A., "Principes de sécurité de l'information dans les systèmes i à nformatiques", "Zastita informatsii Konfident", N°3, 1998
[15] X_DES Cryptoprocessor, Xilinx Inc., March 14, 2000
[16] http://www.castinc.com/cores/xdes.htm
[17] Trezenguet Hélène, "Les cryptoprocesseurs conjuguent vitesse et sécurité sur l'Internet", Electronique, N°110, January 2001, pp48-50
[18] http://www.activcard.com
[19] http:/ds.dial.pipex.com/town/close/new52/glossary.htm