JOURNAL OF TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY

# Preface

Trusted and secure computing properties of computer system are usually believed to behave in a well-defined way and enable the processed information to be properly protected. Nowadays, the need to protect information is increasing, particularly on the type of computers that we use directly for processing data with different levels of sensitivity. A computing system that supports multiple levels of security (MLS) provides the protections to guarantee that information which is assigned to different security levels is handled appropriately. The problem of processing information with different levels of sensitivity has been extensively studied since the early 70s of the twentieth century. To ensure the confidentiality and integrity of information, there are often used several models (B-LP, Biba, Clark-Wilson), which provide mandatory access control (MAC) entity (called subject) to the resource (called object).

The design of MLS systems guaranteed the correct performance with respect to security considerations, which is a daunting challenge. There are two main approaches to the construction of MLS systems: centralized and distributed one. Nowadays, the centralized (i.e., no distributed) approach to build computer system with multi-level security is mainly based on the virtualization technology for the separation of independent security domains as different virtual machines. The implementation of this type of MLS system design requires the integration of available virtualization technology (software and hardware), application of cryptographic protection and formal methods for both ensuring and control of the confidentiality and integrity of data, and advanced techniques for user authentication. Virtualization is now becoming more broadly available and is supported in off-the-shelf systems based on Intel and AMD architecture hardware. Virtualization can improve overall system security and reliability by isolating multiple software stacks in their own VMs. The application of some selected security concerned solutions for building a secure and trust environment called Secure Workstation for Special Applications (SWSA) is a key topic of the current issue. So, we have a developed method of secure MLS type system constructing an application of a RT-family trust management language for an access control model, a method of cryptographic protection of removable storage devices with USB interface, a design of hybrid cluster system for encryption and decryption of large amounts of data, an application of the Zak-Gabor-based iris coding to build a secure biometric verification station, designed a simple verification protocol for autonomous verification modules, and a solution that allows to combine hard drive encryption with a trustful boot process. Additional three papers present some results, applications and developments concerning the reduction of the traffic volume of user location data updating in a cellular network, an experimental evaluation of YouTube video transmission examining the quality of experience of end user applications, and the method of optimal pump scheduling for large scale water transmission system by linear programming.

The problem of building a secure and trust specialized computer systems (SCS), which are processing data with different levels of sensitivity becomes particularly topical, especially in regard to the SCS applications in government institutions, military or financial. One of the essential questions concerning development of SCS involves a method of secure software designing. Z. Zieliński *et al.* present a component based approach to development secure SCS (SWSA) by means of integration of available software and hardware virtualization technology, application of formal methods, cryptographic protection of data stored on hard and removable disks and using biometrics techniques for user authentication. Also, an interesting approach to integration of security models with models of architecture of the system described in UML, which allows models simulation, has been proposed.

In the SWSA, multiple virtual machines simultaneously running (VMs) are used to process sensitive information from multiple security domains, providing strict separation of the domains. The users of SWSA may act in several different roles, with different access rights. The problem is how to control the access of SWSA users to particular VMs in the situation when users may have different periods of validity of different credentials. K. Lasota and A. Kozakiewicz have proposed an interesting solution of this problem which is based on an application of an RT-family trust management language, as a basis for an access control model to VMs. In prototype implementation of SWSA this model is mapped into a set of SELinux policy rules.

One of the necessary capabilities of Secure Workstation for Special Applications is cryptographic protection of hard and removable storage devices with USB interface. The use of solutions from ordinary systems with multilevel security (MLS), which include the SWSA, is insufficient. J. Chudzikiewicz and J. Furtak present a mechanisms to ensure an adequate level of protection of data stored on removable storage in MLS type workstation which is enabling to such a preparation of data stored in Flash RAM, so that the sender of data is assured that data will be available only for designated recipient, and the recipient is assured that the received data comes from the expected sender. In addition, the selected elements of these mechanisms implementation used in Windows operating system have been described.

Data encryption and decryption involve cumbersome calculations, especially when considering the processing of large amount of data. On the other hand, cryptography algorithms are natural candidates for massively parallel computations. E. Niewiadomska-Szynkiewicz *et al.* present a hybrid cluster system – a novel computing architecture with multi-core CPUs working together with many-core GPUs for encryption and decryption of large amounts of data. The experimental results presented in the paper demonstrate the effectiveness and scalability of such a cluster system.

In the next two papers the authors present the solutions for building a secure verification station acting as a server of biometric-based verification within secure workstation (SWSA) and consisting of a professional iris capture camera, a processing unit with specially designed iris recognition and a communication software. The iris recognition used in this work is based on the original methodology employing Zak-Gabor transformation. A. Czajka and K. Piech propose an automatic iris feature selection mechanism employing, among others, the minimum redundancy, maximum relevance (mRMR) methodology as one, yet more importantly, a step to assess the optimal set of wavelets used in this iris recognition application. The electronic communication between SWSA and the station is secured by a protocol that is specially designed to the purpose of such an application. A. Kozakiewicz and T. Pałka present the design and the rationale behind a simple verification protocol for autonomous verification modules.

A workstation may be regarded as secure only if it runs an original, unmodified software. The question is how we could assure that the workstation has not been modified in any way? M. Małowidzki *et al.* propose a solution that allows to combine hard drive encryption with a trustful boot process, preventing risk of software tampering. The logon process, which have been proposed, offers a reasonable level of security and could be increased by some additional mechanisms.

The key aspects in design of modern ‘ad hoc’ sensor networks are data security and energy aware communication. K. Daniluk and E. Niewiadomska-Szynkiewicz give in their paper an excellent survey of energy efficient security architectures and protocols for wireless sensor networks. Also, the security requirements for wireless sensor networks are presented and the relationships between network security and network lifetime limited by often insufficient resources of network nodes are explained.

In mobile communications (e.g., GSM, UMTS, 3G, ...), the location of users may change in time. To make a communication between two users, the system must first find the location of destination user which must be extracted from databases. Thus, the most important criterion of a location tracking algorithm is to provide a small database access time. M. V. Dolama and A. G. Rahbar propose a new location tracking scheme, called Virtual Overlap Region with Forwarding Pointer, for cellular networks which reduces the updating information when a user frequently moves within the boundaries of several cells grouped into a Location Area.

Video sharing services like YouTube have become very popular recently. This situation results in a drastic growth of the Internet traffic statistic. On the other hand, when transmitting video content over packet based networks, stringent quality of service (QoS) constraints must be met in order to provide the comparable level of quality to a traditional broadcast television. A. Biernacki *et al.* conducted an experimental evaluation of YouTube video transmission (HTTP based) examining the quality of experience of end user applications expressed as a function of playback buffer occupancy.

The last paper of the issue is focused on the model for large scale potable water transmission system. J. Błaszczyk *et al.* describe in this paper a linear, the so-called Simplified Model (SM), based on mass-balance equations, which is solved on a week horizon and delivers boundary conditions for the so-called Full Model (FM) that is nonlinear and takes into account hydraulic phenomena and water quality.

Zbigniew Zieliński
Guest Editor