KHARKOV NATIONAL UNIVERSITY OF RADIOELECTRONICS

Proceedings of IEEE East-West Design & Test Symposium (EWDTS'2011)

Technically Co-Sponsored by

Sevastopol, Ukraine, September 9 – 12, 2011

IEEE EAST-WEST DESIGN AND TEST SYMPOSIUM 2011
ORGANISING COMMITTEE

General Chairs
V. Hahanov – Ukraine
Y. Zorian – USA

General Vice-Chairs
R. Ubar – Estonia
E. Pashkov – Ukraine
P. Prinetto – Italy

Program Chairs
S. Shoukourian – Armenia
D. Speranskiy – Russia

Program Vice-Chairs
M. Renovell – France
Z. Navabi – Iran

Steering Committee
M. Bondarenko – Ukraine
V. Hahanov – Ukraine
R. Ubar – Estonia
Y. Zorian – USA

Publicity Chairs
G. Markosyan – Armenia
S. Mosin – Russia

Public Relation Chair
V. Djigan – Russia

Program Committee
E. J. Aas – Norway
J. Abraham – USA
M. Adamski – Poland
A . Barkalov – Poland
R. Bazylevych – Ukraine
A. Chaterjee – USA
V. Djigan – Russia
A. Drozd – Ukraine
E. Evdokimov – Ukraine
E. Gramatova – Slovakia
A. Ivanov – Canada
M. Karavay – Russia
V. Kharchenko – Ukraine
K. Kuchukjan – Armenia
W. Kuzmicz – Poland
A. Matrosova – Russia
V. Melikyan – Armenia
L. Miklea – Romania
O. Novak – Czech Republic
Z. Peng – Sweden
A. Petrenko – Ukraine
D. Puzankov – Russia
J. Raik – Estonia
A. Romankevich – Ukraine
A. Ryjov – Russia
R. Seinauskas – Lithuania
S. Sharshunov – Russia
A. Singh – USA
J. Skobtsov – Ukraine
V. Tverdokhlebov –- Russia
V. Vardanian – Armenia
V. Yarmolik – Byelorussia

Organizing Committee
Yu. Gimpilevich – Ukraine
S. Chumachenko – Ukraine
E. Litvinova – Ukraine

EWDTS 2011 CONTACT INFORMATION

Prof. Vladimir Hahanov
Design Automation Department
Kharkov National University of Radio Electronics,
14 Lenin ave,
Kharkov, 61166, Ukraine.

Tel.: +380 (57)-702-13-26
E-mail: hahanov@kture.kharkov.ua
Web: www.ewdtest.com/conf/

9th IEEE EAST-WEST DESIGN & TEST SYMPOSIUM (EWDTS 2011)

Sevastopol, Ukraine, September 9-12, 2011

The main target of the IEEE East-West Design & Test Symposium (EWDTS) is to exchange experiences in the field of design, design automation and test of electronic circuits and systems, between the technologists and scientists from Eastern and Western Europe, as well as North America and other parts of the world. The symposium aims at attracting attendees especially from the Newly Independent States (NIS) and countries around the Black Sea and Central Asia.

We cordially invite you to participate and submit your contribution(s) to EWDTS'11 which covers (but is not limited to) the following topics:

- Analog, Mixed-Signal and RF Test
- Analysis and Optimization
- ATPG and High-Level TPG
- Built-In Self Test
- Debug and Diagnosis
- Defect/Fault Tolerance and Reliability
- Design for Testability
- Design Verification and Validation
- EDA Tools for Design and Test
- Embedded Software Performance
- Failure Analysis, Defect and Fault
- FPGA Test
- HDL in test and test languages
- High-level Synthesis
- High-Performance Networks and Systems on a Chip
- Low-power Design
- Memory and Processor Test
- Modeling & Fault Simulation
- Network-on-Chip Design & Test
- Modeling and Synthesis of Embedded Systems
- Object-Oriented System Specification and Design
- On-Line Test
- Power Issues in Testing
- Real Time Embedded Systems
- Reliability of Digital Systems
- Scan-Based Techniques
- Self-Repair and Reconfigurable Architectures
- Signal and Information Processing in Radio and Communication Engineering
- System Level Modeling, Simulation & Test Generation
- Using UML for Embedded System Specification

CAD Session:

- CAD and EDA Tools, Methods and Algorithms
- Design and Process Engineering
- Logic, Schematic and System Synthesis
- Place and Route
- Thermal, Timing and Electrostatic Analysis of SoCs and Systems on Board
- Wireless Systems Synthesis
- Digital Satellite Television

The EWDTS'2011 will take place in Sevastopol, Ukraine. Sevastopol is a port city, located on the Black Sea coast of the Crimea peninsula. The city, formerly the home of the Soviet Black Sea Fleet, is now home to a Ukrainian naval base and facilities leased by the Russian Navy and used as the headquarters of both the Ukrainian Naval Forces and Russia's Black Sea Fleet.

The symposium is organized by Kharkov National University of Radio Electronics in cooperation with Sevastopol National Technical University and Tallinn University of Technology. It is technically co-sponsored by the IEEE Computer Society Test Technology Technical Council (TTTC) and financially supported by Virage Logic, Synopsys, Aldec, Kaspersky Lab, DataArt Lab, Tallinn Technical University, Cadence.

CONTENTS

A Security Model of Individual Cyberspace

Alexander Adamov, Vladimir Hahanov
Kharkov National University of Radio Electronics,
Lenin ave, 14, Kharkov, 61166 Ukraine,
E-mail: Alexander.Adamov@dnt-lab.com

Abstract

This paper describes a security model for protection of individual cyberspace (ICS) as a way of ensuring a secured user's virtual environment. A concept of cyberspace and its main definitions is determined, as well as a formal model that describes mapping of prototypes in cyberspace into real-world objects. Based on analysis of contemporary security threats and methods of protection against them basic requirements for a security model were declared to ensure availability, integrity and confidentiality of user data within cyberspace. Information on cyber threats, as well as a review of existing security solutions in cloud computing was taken as a basis for the proposed ICS security model.

The goal of the paper is to represent an analysis of security issues related to ICS and propose the conceptual model of a modern security environment.

1. Introduction

Previous studies in the field of cyberspace security were mostly based on an analysis of a computer network state and identifying vulnerabilities in it [1], or using as security criterion multi-perspective parameters to assess and predict a security state of a network system [2]. In later studies, this approach has been recognized as untenable because it ignores the behaviour of a user when a system anomaly occurs. According to [3] cyberspace is defined as "a massive socio technical system of systems, with a significant component being the humans involved". Thus, the authors attribute the cyber attacks with social, political, economic and cultural phenomena.

Today an individual virtual space expanded by the widespread expansion of social networking and Internet services that allow process and store data in the cloud. Thus, users are becoming less tied to their personal digital device, which is only used for access to online services to obtain the necessary data and perform operations.

This approach allows us to abstract from hardware characteristics accessing the Internet and use any mobile hardware and software platform for a wide range of tasks in the "cloud" [4]. The examples of such services are cloud office (Google Documents, Microsoft Office Live), sharing of files and images, map services, interpreters, calendars, and, finally, social networks, where each member of a network can store personal information and gain access to multimedia content of other users. All these are evidence of humanity's transition to cloud technology everywhere.

The protection of cloud services is hot topic today because these technologies are widely used by organizations to create a business service infrastructure. Accordingly, it is necessary to guarantee the security of corporate data in the cloud, which is an elusive task. Solving this task a company may sign Service Level Agreement (SLA) with a service provider, where all security issues are determined at different levels of representation [5]. For instance, Intel has developed a suite of solutions for secure access and data storage in the cloud. Intel's technologies are supported by leading antivirus companies Symantec and McAfee [6].

Taking in consideration the existing technologies in this area a new model of ICS protection is suggested, which implies the creation of a secure environment for data storage and processing with the help of a cloud computing technology.

2. General Definitions of Individual Cyberspace

Based on these facts, we can speak about the concept of ICS, in which a person is represented as a set of virtual avatars. This concept is described in [7], where the term of cyberspace is defined as "a metaphoric abstraction used in philosophy and computers, which is a virtual reality, Noosphere or the Second World inside computer networks".

Speaking about the model of cyberspace each user should consider the use of various cloud services, such as: 1) office tools (Microsoft Office Live, Google Docs); 2) social networks (Facebook, Wikipedia, Youtube, OpenID), 3) online banking (also PayPal); 4)

online games; 5) file-sharing networks, 6) IP communication services (Skype), corporate services (WebEx), etc.

This raises the question of safe access to a service, storing multiple passwords for each service and confidentiality of stored data in the cloud. Unfortunately, at present time there is no uniform standard of protection of ICS, which would guarantee security of data in the cloud, and provide secure access to the cloud from a user.

3. A FORMAL MODEL FOR ICS ANALYSIS

Let us consider a formal model of real objects mapping into a cyberspace and determine properties which are peculiar to such mapping.

Definition 3.1. Let R denote the set of the real world objects, and C – the set of objects in a cyberspace. The objects of the set C are mapping of R, i.e. each object of $r \in R$ corresponds to an object or subset of objects $c \in C$. If an object r corresponds to c, then c is called an **image** of an object r in a cyberspace, and r – is the **original** of the object c:

$$R \to C. \quad (1)$$

The main goal of ICS protection is guaranteeing the following correspondence between objects in the real world R and objects in a cyberspace C:

$$r_1 \to \{c_1^1, c_1^2, \ldots, c_1^n\}. \quad (2)$$

The expression (2) shows mapping, in which one object in the real world corresponds to several images in a cyberspace. At the same time every object in a cyberspace has only one original. Otherwise, if a cyberspace image has two or more originals, it says about unauthorized access and data integrity violation from the side of one of the real world objects (e.g., copyright violation or stealing a user's account).

Let us denote the term of compositions of binary relations [8].

Definition 3.2. Let $R \subseteq X \times Y$ and $S \subseteq Y \times Z$. The *composition* of R and S is the binary relation between X and Z, which is denoted by $S \circ R$ given by:

$$S \circ R = \{(x, z) \mid \text{exists } y \in Y \text{ such that } x \to y, y \to z\}. \quad (3)$$

The new relation set up the connection between X and Z using elements from Y as intermediary.

Let us consider the example and find the composition of objects in a cyberspace. Assume the real world object $John \in R$ has images (accounts) in such services as *Facebook*, *Google* $\in C$, and the object $Dave \in R$ – image *Twitter* $\in C$. Using such accounts objects *John* and *Dave* can get the access to *MySpace* and *LiveJournal* $\in C^*$ by means of *associated accounts*.

Let P and Q defined by the following directed graphs shown on Figure 3.1.

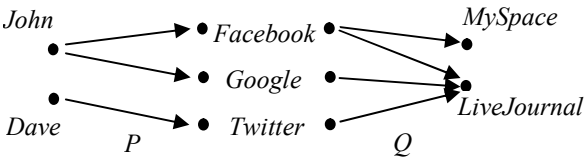

Figure 3.1 – The mapping of the users John and Dave into the cyberspace C and C*.

Let us represent the relations in matrix form M and N. Accordingly, each element of M for the relation P will be calculated according to the formula:

$$M(i, j) = 1, \text{ if } (x_i, y_i) \in P, \quad (4)$$
$$M(i, j) = 0, \text{ if } (x_i, y_i) \notin P.$$

Similarly, the matrix N for the relation Q:

$$N(i, j) = 1, \text{ if } (y_i, z_i) \in Q, \quad (5)$$
$$N(i, j) = 0, \text{ if } (y_i, z_i) \notin Q.$$

Then the matrices have the form:

$$M = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, N = \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}. \quad (6)$$

Let us calculate composition PoQ as Boolean matrix product:

$$P \circ Q = M \cdot N = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}. \quad (7)$$

Or as the binary directional graph (Figure 3.2):

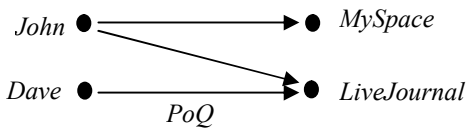

Figure 3.2 –The graph of P**o**Q composition.

Thus, through the composition of relations is possible to identify a number of additional objects in a cyberspace, which may be a part of ICS with associated accounts.

The composition of relations in the cyberspace $P \circ Q$ allows to obtain a list of trusted services within ICS. On this basis, it is possible to build a mechanism to protect against *phishing* and *pharming* attacks aimed to counterfeit an access to legal services and steal authentication data. While the problem of secure storage of passwords can be solved within the relation P.

In case when the object $Dave \in R$ through **attack on ICS** of *John* obtained the access to *Facebook* account $\in C$ of $John \in R$, then *Dave* will also have the access to *John's* accounts in *MySpace* and *LiveJournal*

through composition. The relation matrix P and the composition PoQ will be as follows:

$$M^A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}, \mathrm{P\,o\,Q}^{\mathrm{A}} = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}. \quad (8)$$

To detect access violations to objects in a cyberspace, it is necessary to **compare relation matrices before and after attack** by *xor* operation.

$$M \oplus M^A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \oplus \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix},$$
$$\mathrm{PoQ} \oplus \mathrm{PoQ}^{\mathrm{A}} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \oplus \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}. \quad (9)$$

From a comparison of the matrices M and M^A it follows the changes have taken place with the access to object *Facebook* by *John* and *Dave*. When comparing the composite matrices the changes have occurred with objects *MySpace* and *LiveJournal* by *John*, while the relation of object *Dave* to *MySpace* was also changed.

Thus, **the verification of objects' relations** within a cyberspace can be summarized as follows:

$$\mathrm{W} \oplus \mathrm{W}^{\mathrm{A}} = \mathrm{V}, \quad (10)$$
$$\mathrm{W} \oplus \mathrm{W}^{\mathrm{A}} \oplus \mathrm{V} = 0,$$

where W – an initial matrix of a binary relation; W^A – a matrix of binary relations obtained as a result an attack on ICS; V – a result of binary comparison of matrices.

4. A Model of ICS Security Environment

In order to determine the requirements for ICS security system, let us consider firstly the most topical threats [9].

1. Web-based and network-based attacks – exploits, sniffing, sidejacking.
2. Malware – viruses, worms, trojans, PUPs (potentially unwanted programs).
3. System modifications – rootkits, bootkits, jailbreaking.
4. Social engineering attacks – phishing, pharming.
5. Resource and service abuse – unauthorized dialing, spam, overcharging.
6. Malicious and unintentional data loss – unsafe storage and transmission.
7. Attacks on the integrity – malicious encryption with ransom, system locking.

The system of ICS protection should be invariant to a device through which a user gets an access to ICS. At the same time it is necessary to ensure a secure access to all resources in the cloud as a part of cyberspace. From this it follows that the security as a service may also be imposed to the cloud, giving customers a web interface to integrated security system.

Based on current research in this field, as well as topical threats let us formulate the following *requirements* to security model of ICS:

- independence from the platform and hardware resources;
- protection of data transmitted over open channels (e.g., public Wi-Fi networks) [10];
- data protection (locally and in the cloud) from unauthorized access and modification;
- protection against malware attacks and the 0-day attacks in real time [11, 12];
- management of passwords and user accounts;
- protection against passwords stealing by social engineering attacks;
- self-protection of systems and critical applications against malware injecting through vaccination and certification.

Based on the above requirements, a security model of ICS was developed shown on Figure 4.1.

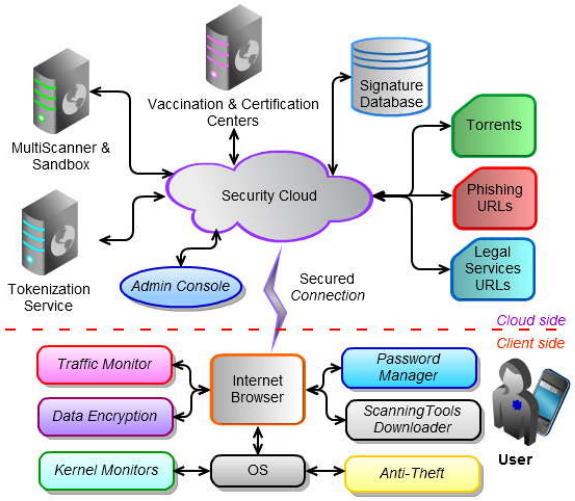

Figure 4.1 – A security model of ICS environment.

In order to meet the requirements for ICS security system the proposed model includes the set of modules on the client side and in the cloud. The process of threats analysis and detection imposed in the Security Cloud. On the user's side there are tools of interaction with the cloud, as well as to monitor and protect integrity of the user's data and operational system. Using Internet browser to run security modules this model becomes platform-independent, as well as it does not depend on a device performance, which can be a smartphone or a tablet PC.

5. Conclusion

ICS security issues were investigated with the help of formal model within the paper. As a result a model of security system was proposed based on analysis of contemporary cyber threats and cloud technologies, thereby creating a safe virtual environment for a user. This model is invariant to OS platform and device performance, because of using security services in the cloud aimed to analyze and detect a cyber threat, as well as provides a range of services such as vaccination, certification and tokenization to ensure certain level of user's security. At the same time on the client side, users will be able to easily manage their safety profile through the Internet browser.

6. References

[1] Wei Hu Jianhua, Li Jianjun Shi, "A Novel Approach to Cyberspace Security Situation Based on the Vulnerabilities Analysis", Intelligent Control and Automation, WCICA, 2006.

[2] Xiaobin, Tan Yong, Zhang Hongsheng, Xi, "Multi-Perspective Quantization Model for Cyberspace Security Situation Awareness", Computational Intelligence and Security, 2007.

[3] Gandhi, R. Sharma, A. Mahoney and others, "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political", Technology and Society Magazine, IEEE, Spring 2011.

[4] C. Hewitt, "ORGs for Scalable, Robust, Privacy-Friendly Client Cloud Computing", IEEE Internet Computing, Issue No. 5, 2008, pp. 96-99.

[5] Kandukuri B.R., Paturi V.R., Rakshit A., "Cloud Security Issues", Services Computing, SCC '09, 2009.

[6] A. Priestley, "Building Trust from Client to Cloud Webinar", Intel, June 2011, available at http://www.brighttalk.com/community/it-security/webcast/2216/30355.

[7] T. Yves, S.V. Chumachenko, V.I. Hahanov, "Actual Problems of Cyberspace Analysis", Radioelectronics and Informatics, 2011.

[8] Haggarty R., Discrete mathematics for computing, Addison Wesley, 2002, pp. 91-113.

[9] V. Jirasek, "Top 10 Mobile Risks", BrightTalk Webinar, July 2011, available at http://www.brighttalk.com/webcast/288/27855.

[10] Lai A., "Sidejacking", An Organization for Local Information Security, 2008, available at http://www.pisa.org.hk/event/live-wifi-attack-defense/WiFi-Attack-SideJacking.pdf.

[11] Gostev A., «Slammer is over?», Kaspersky Lab, 2011, available at http://www.securelist.com/ru/blog/44128/Slammer_vs yo.

[12] "The Real Face of Koobface", Trend Micro, July 2009, available at http://us.trendmicro.com/imperia/md/content/us/trend watch/researchandanalysis/the_real_face_of_koobface _jul2009.pdf.

Camera-ready was prepared in Kharkov National University of Radio Electronics
Lenin Ave, 14, KNURE, Kharkov, 61166, Ukraine

Approved for publication: 26.08.2011. Format 60×841/8.
Relative printer's sheets: 42. Circulation: 150 copies.
Published by SPD FL Stepanov V.V.
Ukraine, 61168, Kharkov, Ak. Pavlova st., 311

Матеріали симпозіуму «Схід-Захід Проектування та Діагностування – 2011»
Макет підготовлено у Харківському національному університеті радіоелектроніки
Редактори: Володимир Хаханов, Світлана Чумаченко, Євгенія Литвинова
Пр. Леніна, 14, ХНУРЕ, Харків, 61166, Україна

Підписано до публікації: 26.08.2011. Формат 60×84$^{1}/_{8}$.
Умов. друк. Арк. 42. Тираж: 150 прим.
Видано: СПД ФЛ Степанов В.В.
Вул. Ак. Павлова, 311, Харків, 61168, Україна