The security aspects of the research activities in IICT-BAS

Acad. Kiril Boyanov
Institute of Information and Communication Technologies
Bulgarian Academy of Sciences
Acad. G. Bonchev St., Block 25A, 1113 - Sofia, BULGARIA
E-mail: boyanov@acad.bg

***Abstract* - The paper presents information on past, present and future research activities in IICT-BAS in the field of ICT security. The main directions of these activities are: critical infrastructure cyberattacks protection, security of distributed systems, security of social networks and dependability of distributed systems.**

Keywords:ICT security, critical infrastructure security, distributed systems security, dependability, social networks security.

I. INTRODUCTION

The Institute of Information and Communication Technologies (IICT) at the Bulgarian Academy of Sciences (BAS) was created in 2010 as a successor of the Institute for Parallel Processing (IPP), the Institute of Information Technologies and the Institute of Computer and Communication Systems. The strategic objective for this act was to consolidate the research fragmentariness in the field of ICT in the academy that has more than half of a century history. This objective was also supported by the fact that IPP has been promoted twice for a "Center of Excellence" (2001-2004 and 2005-2007) by the European Commission and during the last ten years was a major national and significant regional player in the field of computer science.

In the rest of this paper a short description of some of the research activities in IICT-BAS will be outlined.

II. IICT-BAS RESEARCH ACTIVITIES

Generally, the mission of IICT-BAS is to carry out a fundamental and applied research in the field of computer science and ICT as well as to develop innovative interdisciplinary applications that are directly related to the main national and international priorities.

Some of the guiding lines in IICT-BAS research activities facing different security aspects are:

A. Computer networks and architectures

This activity is mainly referring to development and application of modern network technologies, distributed systems and facilities for network security, monitoring and control.

B. IT developments for emerging new security challenges

An interdisciplinary research team explores advances and applies methodologies and tools for IT governance and change management, design and analysis of architectures and capabilities, modeling and simulation for the security sector, including information security management. The activities are strongly supported and accepted both within NATO & EU integrated security sector governing level.

C. Development and maintenance of scientific infrastructure

The activity includes the development, monitoring and maintenance of Bulgarian Research and Education Network (BREN) and Grid clusters that are the biggest part of the National Grid infrastructure of the country. It is also connected with the scientific infrastructure of national significance and refers to research and support of important national infrastructure with key meaning for scientific and education institutes in the country.

D. Super computer applications

This activity is aimed at ICT driven contributions to science, technology, health, environmental protection, etc. It includes large scale computer simulation, high performance computer architectures and algorithms, computational linear algebra. The only one super computer in Bulgaria (BlueGene/P) is under the scientific maintenance of IICT-BAS.

Evidently, these research guiding lines demonstrate an environment with solid background and modern facilities for successful multi-aspect research in the field of ICT security problems.

III. PAST ACTIVITIES IN ICT SECURITY AREA

The working experience of IICT-BAS researchers on security problems of computer networks and distributed computer system is related to a solid background. General security problems in computer systems are considered in [1], [2] and [3]. The problems related to the information encoding and ciphers are object of publications [4], [5] and [6].

General network security problems are treated in [7], [8] and [9]. Network management and monitoring policy and related tools with relevance to the monitoring of the security issues are considered in [10], [11] and [12]. In these publications are described details of systems for monitoring the state of the services from the network infrastructure perfSONAR Multi-Domain Monitoring (MDM) which are used in GEANT network.

The publication [13] treats the realization of the Certification Authority (CA) for user authorization and identification in Bulgarian network and in GRID infrastructure.

The problems of user identification in distributed systems like GRIDs are discussed in [14] and [15].

A substantial work was done in the area of Information Technologies application for the Security Sector which includes:

- Methodologies and Tools for IT Governance and Change Management.
- Design and analysis of system architectures.
- Modeling and simulation for the security sector.
- Support to capabilities planning and security sector transformation.

These results [20] were supported by a number of national and international projects. A worth noting fact are the efforts for building a national Basic low-cost Environment for Simulation and Training (BEST) that will become a part of NATO Exercise Toolbox. This environment includes CIMIC communication aspects related to EDXL standard and a unique biological cryptographic solution [21].

During the EU/FP7 project ICT-FORWARD (http://www.ict-forward.eu/) IICT-BAS, as a partner in the project, was involved in the efforts to identify the emerging and future cyber threats [16]. The ultimate goal of the work was to identify the areas in which cyber threats could occur and cause serious and undesirable consequences. The research group from IICT-BAS was focused particularly on the threats to critical systems. Based on the specifics of these systems several areas were identified where security threats might grow in the future and where new solutions should be sought for [17]. The identified threats to critical systems (CSs) summarize the views of many experts both from information security, industrial automation and critical infrastructures. They reflect the general vision that critical systems can become an attractive target to cyber attacks and the cross-area of ICT and CS is an open field for security research.

IV. Future directions in ICT Security

The main future directions of the research plans in IICT-BAS are related to several aspects:

A). To summarize and analyze possible cyberattack scenarios against Critical infrastructures (CI). The research of cyberattacks on CI will be based on modeling with different concepts, software environments and scenarios that allow both static/dynamic behavior and nature exploration. In these areas IICT-BAS researchers have significant experience. The recent Stuxnet attacks on SCADA show an evident necessity for effective and specific countermeasures in this domain. The role of the human factor and its analysis (HFA) is extremely important in these environments where the human-system interaction affects safety and could have serious consequences for the society.

Within HFA, IICT-BAS is already working in cooperation with subject matter experts and modern lab facilities in the framework of a research project funded by the National Science Fund (http://cleverstance.com).

B). We plan to work for further extension of the set of emerging cyber threats using as an initial base the White book classification resulting from the FORWARD project [16]. Additionally, we plan to implement a detailed questionnaires based survey and sensitivity analysis, which will result in an improved classification and scenarios that should allow to better foreseen the different emerging cyber threats following the methodology presented in [20].

C). In the field of distributed systems security we plan to summarize and analyze some of the security issues with possible cyber attacks on parallel systems like Grid environments. We have experience with the exploitation of Grid clusters located in the IICT-BAS. The core of the CSIRT (Computer Security Incident Response Team) for Bulgarian Grid infrastructure is located in the institute. This group of security officers also actively gathers and analyzes detailed information related to security incidents, potential threats and precautions from a huge archive of logs collected from many Grid nodes in the last few years. Our future plans and interests in this area are to do research on:

- Security issues specific to parallel processing applications which are typically executed on a distributed environments like Grid.
- Analyzing and developing additional software tools for automating and monitoring the security activities and administration.

The highly possible and desired evolution of this IICT-BAS activity is towards security problems in Cloud Computing environments.

IICT-BAS was a participant in one of the research projects related to developing future Internet technologies – PSIRP (Publish-Subscribe Internet Routing Paradigm) which is funded by the European Commission 7th Framework Program (http://www.psirp.org/). The main goal of this project was the research and development of a brand new future Internet architecture based on publish/subscribe paradigm. In this model, security instruments and mobile devices support are integrated in the model in principle [18]. Our plans are to analyze some of the possible security issues of PSIRP.

D). In the Social networks security area the plans are to implement a survey [19], case study of Facebook and Twitter and also some analysis about psycho-social and ICT aspects of the intrusions' motivation.

E). Our recent research interests are also related to cybersecurity in heterogeneous networks and application of

dependability mechanisms in network security. Based on our experience in dependability of distributed systems and networks there are plans for work on approaches to apply fault-tolerance mechanisms and techniques for improving IT security. We have developed algorithms for fault-tolerant clock synchronization in distributed real-time process control systems that, with the necessary modifications, could be implemented in sensor networks where the efficient use of system resources is a critical task.

V. CONCLUSIONS

The presented research activities of IICT-BAS will be realized from an international and interdisciplinary team within the next 3 years since 2011. The work will be performed in collaboration with the integrated security sector and in the framework of EU FP7 projects like SysSec "Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet: Europe for the World" (www.syssec-project.eu/).

REFERENCES

[1] Ville E., N. Sinyagina, P. Borovska. Deploying Trusted Computing. Information technologies and Controls, 2009, pp 28-32, ISSN 1312-2622-1.

[2] Dobrinkova N., N. Sinyagina. Information security – bell la Padula model. Problems of Engineering Cybernetics and Robotics, 2009 62, pp. 15-20, ISSN 0204-98.

[3] Kolev A., N. Sinyagina. Discover of the Critical Directories in the Computer System. Collection of scientific works "Military-scientific forum", National military university Vasil Levski, pp. 76-82, 2006 (in Bulgarian).

[4] Sinyagina, N., B. Aleksandrov. 3-D Structure of Block Cryptografic Ciphers. Proceedings of the Fourth Bulgarian-Greek Scientific Conference "COMPUTER SCIENCE 2008", Kavala, Greece, pp. 791-797, 2008.

[5] Sinyagina, N., M. Yordanova. Distributed Secret on the Basis of the Linear Correcting Codes. Proceedings of the International Scientific Conference UNITECH-2008, Gabrovo, pp I-436-441, 2008.

[6] Aleksandrov B., N. Sinyagina. Modification of Block Cryptfgraphic Ciphers. Proceedings of the International Scientific Conference UNITECH-2008, Gabrovo, pp. I-474-480, 2008.

[7] Iliev, L., H. Turlakov. Current Problems in Network Security. Proceedings of the International Workshop on Network and GRID Infrastructure, Sofia, pp. 125-139, 2007.

[8] Boyanov K., D. Todorov, H. Turlakov. ICT, democracy, Internet treats and ethics. "Automation and Information" journal, pp. 7-12, 2008, (in Bulgarian).

[9] Sinyagina, N., S. Ruseva. Defense mechanisms against computer attacks 'Distributed denial of service' type. UNWE International conference "Management of secure related RMD research in support of defense industrial transformation", pp. 85-91, 2007.

[10] Hanemann A., V. Jeliazkov, O. Kvittem, L. Marta, J. Metzger, I. Velimirovic. Complementary Visualization of perfSONAR Network Performance Measurements. International Conference on Internet Surveillance and Protection (ICISP'06), IARIA/IEEE, Cap Esterel, France, pp. 6-6, 2006. (best paper award).

[11] Gajin, S., V. Jeliazkov, C. Kotsokalis, Y. Mitsos. Seamless Integration of Network Management Tools in a Multi-Domain Environment. 10th IFIP/IEEE International Symposium on Integrated Network Management, Munich, Germany, pp. 745-748, 2007.

[12] Jeliazkova, N., L. Iliev. Extending and Monitoring the Prefsonar Infrastructure. Proceedings of the International Workshop on Network and GRID Infrastructure, Sofia, pp. 36-41, 2007.

[13] Dimitrov, V., L. Iliev, L. Boyanov, H. Turlakov. Bulgarian Academic Certification Authority. Proceedings of the International Workshop on Network and GRID Infrastructure, Sofia, pp. 23-28, 2007.

[14] Weigold T., P. Buhler, J. Thiyagalingam, A. Basukoski, V. Getov. Advanced Grid Programming with Components: A Biometric Identification Case Study. Proc. IEEE COMPSAC, IEEE CS Press, pp. 401-408, 2008.

[15] Naydenova I., Kaloyanova K., Ivanov S. Multi-Source Customer Identification. Information Systems & GRID Technologies, 28-29 May 2009, Sofia, Bulgaria, pp.77-85.

[16] ICT FORWARD, White Book: Emerging ICT Threats, January 2010, http://www.ict-forward.eu/media/publications/forward-whitebook.pdf.

[17] E. Djambazova, M. Almgren, K. Dimitrov, E. Jonsson, "Emerging and Future Cyber Threats to Critical Systems", in J. Camenisch, V. Kisimov, and M. Dubovitskaya (Eds.): iNetSec 2010, LNCS 6555: Open Research Problems in Network Security, pp. 29 – 46, 2011.

[18] Dimitrov V., V. Koptchev. PSIRP project – Publish-Subscribe Internet Routing Paradigm. New ideas for future Internet. International conference CompSysTech'2010, Sofia, 17-18.06.2010. Published in "ACM International Conference Proceeding Series (ICPS)", ISBN:978-1-4503-0243-2, Vol. 471, pp. 167-171, 2010.

[19] Minchev Zl., M. Petkova "Information Processes and Threats in Social Networks", A Case Study. At Conjoint Scientific Seminar "Modeling and Control of Information Processes", 22 November 2010, Organized by College of Telecommunications, Institute of ICT - Bulgarian Academy of Sciences, Institute of Mathematics and Informatics - Bulgarian Academy of Sciences, Sofia, Bulgaria, 2010

[20] Bulgarian Knowledge Portal on OA & CAX, Available at: http://www.gcmarshall.bg/KP/Bulgarian_CAX_OA_Knowledge_Portal.htm

[21] Oscar, H., Z. Minchev, and D. Popivanov "Non-linear System for Digital Information Transmission", Patent 107414/20.12.02, BG 6, 2004 (published on 13.12.2006, BG 840 Y1).