Program of the third International scientific school
"Incident management and countering targeted cyber-physical attacks in distributed large-scale critical systems" (IM&CTCPA 2017)"

St. Petersburg, December, 18 - 21, 2017

SPIIRAS, St. Petersburg, 14-th Liniya V.O. 39, room 401 (December, 18)
ITMO University, St. Petersburg, Lomonosova str. 9, assembly hall (December, 19 - 21)

http://www.comsec.spb.ru/imctcpa17

December 18

Workshops of the International Laboratory "Information security of cyber-physical systems" of ITMO University

Co-chairs:

Igor V. Kotenko, Doctor of Technical Sciences, Professor, Head of Laboratory of Computer Security Problems, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, SPIIRAS, Co-Head of the International Laboratory "Information security of cyber-physical systems", ITMO University, St. Petersburg, Russia

Didier El Baz, PhD, Head of the Distributed Computing and Asynchronism team, The National Center for Scientific Research (CNRS), Toulouse, France, Co-Head of the International Laboratory "Information security of cyber-physical systems", ITMO University, St. Petersburg, Russia

1. Workshop **"Problems in development of intelligent secure distributed autonomous robot based systems"**

Moderator:

Didier El Baz, PhD, Head of the Distributed Computing and Asynchronism team, The National Center for Scientific Research (CNRS), Toulouse, France, Co-Head of the International Laboratory "Information security of cyber-physical systems", ITMO University, St. Petersburg, Russia

2. Workshop **"Security and safety problems of modern cyber-physical systems"**

Moderator:

Hakima Chaouchi, PhD, Full Professor, Telecom Sud Paris, Institut Mines Telecom, Paris, France

3. Workshop **"Development trends of secure cyber-physical car systems"**

Moderator:

Roland Rieke, PhD, Deputy Head of Secure Engineering /Trust and Compliance Department, Fraunhofer-Institute for Secure Information Technology SIT, Darmstadt, Germany

4. Workshop **"Formal approaches to security analysis of cyber-physical systems"**

Moderator:

Yannick Chevalier, PhD, Assistant Professor, Paul Sabatier University (Paul Sabatier University, Toulouse III), Toulouse, France

5. Workshop **"Formal methods for cyber-physical systems"**
Moderator:
Martin Strecker, PhD, Assistant Professor, Paul Sabatier University (Paul Sabatier University, Toulouse III), Toulouse, France

6. Workshop **"Approaches, methods and algorithms for access control in cyber-physical systems"**
Moderator:
Vladimir Oleshchuk, PhD, Professor, Head of Communication and System Security group, Department of Information and Communication Technology, Faculty of Engineering & Science, University of Agder, Agder, Norway

7. Workshop **"Methods for risk analysis in cyber-physical systems"**
Moderator:
Fabrizio Baiardi, PhD, Professor, University of Pisa, Pisa, Italy

8. Workshop **"Information security of cyber-physical systems"**
Moderators:
Igor V. Kotenko, Doctor of Technical Sciences, Professor, Head of Laboratory of Computer Security Problems, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, SPIIRAS, Co-Head of the International Laboratory "Information security of cyber-physical systems" of ITMO University, St. Petersburg, Russia
Sergey V. Bezzateev, Doctor of Technical Sciences, Professor, Head of the Department "Security of cyber-physical systems", ITMO University, St. Petersburg, Russia

December 19

Timing	Title of presentation	Presenter
9.00-9.30	Registration of the participants	
9.30-9.50	Opening the **3rd International scientific school IM&CTCPA 2017** Introduction	**Igor V. Kotenko**, Doctor of Technical Sciences, Professor, Head of Laboratory of Computer Security Problems, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, SPIIRAS, Co-Head of the International Laboratory "Information security of cyber-physical systems", ITMO University, St. Petersburg, Russia
Session 1.1. Chair - Prof. Dr. Igor V. Kotenko		
10.00-10.50	Cyber physical systems and various computer science issues in smart distributed autonomous robots	**Didier El Baz**, PhD, Head of the Distributed Computing and Asynchronism team, The National Center for Scientific Research (CNRS), Toulouse, France, Co-Head of the International Laboratory "Information security of cyber-physical systems", ITMO University, St. Petersburg, Russia
11.00-11.50	Security and Safety in Cyber Physical Systems era	**Hakima Chaouchi**, PhD, Full Professor, Telecom Sud Paris, Institut Mines Telecom, Paris, France
12.00-13.00	Lunch	
Session 1.2. Chair – Dr. Andrey A. Chechulin		
13.00-13.50	Cybersecurity in the Internet of Vehicles	**Roland Rieke**, PhD, Deputy Head of Secure Engineering /Trust and Compliance Department, Fraunhofer-Institute for Secure Information Technology SIT, Darmstadt, Germany
14.00-14.50	Finitary deduction systems for formal analysis of security applications	**Yannick Chevalier**, PhD, Assistant Professor, Paul Sabatier University (Paul Sabatier University, Toulouse III), Toulouse, France
14.50-15.10	Coffee-break	
Session 1.3. Chair – Dr. Vasily A. Desnitsky		
15.10-16.00	Modeling programming languages with proof assistants	**Martin Strecker**, PhD, Assistant Professor, Paul Sabatier University (Paul Sabatier University, Toulouse III), Toulouse, France
16.10-17.00	Using distributed ledgers to assess and manage ICT risk	**Fabrizio Baiardi**, PhD, Professor, University of Pisa, Pisa, Italy
Session 1.4. Chair – Dr. Sergey V. Bezzateev		
17.10-17.25	Next-generation applications of moving mission-critical systems	**Sergey Andreev**, PhD, Senior Research Scientist, Tampere University of Technology, Tampere, Finland
17.25-17.40	Applied Cryptography on Programmable Smart Cards	**Lukas Malina**, PhD, Senior Researcher at Brno University of Technology (BUT), Brno, Czech Republic
17.40-17.55	Security Issues in the LPWAN Technologies	**Radek Fujdiak**, PhD, Researcher at the Brno University of Technology, Brno, Czech Republic
17.55-18.10	High-Speed Encryption with Strong Authentication on the FPGA Platform	**David Smekal**, Researcher of Technical University of Brno, Brno, Czech Republic

December 20

Timing	Title of Presentation	Presenter
Session 2.1. Chair – Prof. Dr. Igor V. Kotenko		
10.00-10.50	Access Control for Cyber-Physical Systems	**Vladimir Oleshchuk**, PhD, Professor, Head of Communication and System Security group, Department of Information and Communication Technology, Faculty of Engineering & Science, University of Agder, Agder, Norway
11.00-11.50	Big Data Technologies for Cyber Security Monitoring and Incident Management in SIEM Systems	**Igor V. Kotenko**, Doctor of Technical Sciences, Professor, Head of Laboratory of Computer Security Problems, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), Co-Head of the International Laboratory "Information security of cyber-physical systems" of ITMO University, St. Petersburg, Russia
12.00-13.00	Lunch	
Session 2.2. Chair – Prof. Dr. Igor B. Saenko		
13.00-13.50	Application of a system of parallel stream computing for processing big data for solving problems of security event correlation	**Igor B. Saenko**, Doctor of Technical Sciences, Professor, leading researcher of SPIIRAS, St. Petersburg, Russia
14.00-14.50	Control of industrial and mobile cyber-physical systems: actual problems in the context of security	**Sergey A. Kolyubin**, PhD, Associate Professor, Acting Head of Mechatronics Dept., Vice Director for Science & Technology Foresight, School of Computer Technologies & Control, ITMO University, St. Petersburg, Russia
14.50-15.10	Coffee-break	
Session 2.3. Chair – Dr. Andrey A. Chechulin		
15.10-16.00	An example of data mining application in the provision of information security: metadata-based management of network connections	**Aleksandr A. Grusho**, Doctor of Physical and Mathematical Sciences, Professor, Head of Laboratory of Information Security of IPI RAS, Moscow, Russia
16.10-17.00	Contemporary conceptions of information security risk management	**Anatoliy A. Minzov**, Doctor of Technical Sciences, Professor of the Department of Information and Economic Security of MPEI, Moscow, Russia
17.10-18.00	The Promising Areas of Cyberattack Research	**Alexander Adamov**, CEO of NioGuard Security Lab, teaches the Advanced Malware Analysis course at Blekinge Institute of Technology and NURE, Kharkov, Ukraine

December 21

Timing	Presentation	Presenter
Session 3.1. Chair – Prof. Dr. Igor B. Saenko		
10.00-10.50	Multifactor Authentication protocols for cyber-physical systems	**Sergey V. Bezzateev**, Doctor of Technical Sciences, Professor, Head of the Department "Security of cyber-physical systems", ITMO University, St. Petersburg, Russia
11.00-11.50	Providing security in a telecommunication IT infrastructure of Russian Railways: problems and trends	**Andrey V. Chernov**, Doctor of Technical Sciences, Professor, Head of the Department "Computer science and computer-aided management" of RSTU, Rostov-na-Donu, Russia
12.00-13.00	Lunch	
Session 3.2. Chair – Dr. Vasily A. Desnitsky		
13.00-13.50	Visualization driven security	**Maxim V. Kolomeec**, Researcher of the laboratory of computer security problems of SPIIRAS, postgraduate student of ITMO University, St. Petersburg, Russia
14.00-14.50	A technique for complex design of secure systems based on embedded devices	**Dmitry S. Levshun**, Researcher of the laboratory of computer security problems of SPIIRAS, postgraduate student of ITMO University, St. Petersburg, Russia
14.50-15.10	Coffee-break	
15.10-16.00	A method of data quality verification in cyber-physical systems on the base of social mechanisms	**Ilya I. Viksnin**, assistant of the Department of Design and Security of Computer Systems, ITMO University, St. Petersburg, Russia
16.10-16.20	Concluding remarks	

Lecture annotations:

1. **Didier El Baz**, PhD, Head of the Distributed Computing and Asynchronism team, The National Center for Scientific Research (CNRS), Toulouse, France, Co-Head of the International Laboratory "Information security of cyber-physical systems", ITMO University, St. Petersburg, Russia. Lecture **"Cyber physical systems and various computer science issues in smart distributed autonomous robots"**.

In this Lecture, we consider cyber physical systems and more particularly, smart distributed autonomous robots like smart reconfigurable conveyors for factory of the future. We present the goal, the design of these modular robot systems and several issues related to distributed algorithms for controlling the modules and reconfigure them in order to adapt to new goals as well as faults in the system. We emphasize on several computer science issues like designing efficient distributed algorithms, fault tolerance, statistics and security.

2. **Hakima Chaouchi**, PhD, Full Professor, Telecom Sud Paris, Institut Mines Telecom, Paris, France. Lecture **"Security and Safety in Cyber Physical Systems era"**.

Cyber Physical System relates to the set of digital processes that can monitor, control and acts on a physical system that can be a robot, a car, a drone or any system with critical communication, critical time response and processing. In this Lecture we will bring the main pillars related to security of Cyber physical systems and the safety requirement in different domains as in Industry 4.0, citizen safety and also health and well being.

3. **Roland Rieke**, PhD, Deputy Head of Secure Engineering /Trust and Compliance Department, Fraunhofer-Institute for Secure Information Technology SIT, Darmstadt, Germany. Lecture **"Cybersecurity in the Internet of Vehicles"**.

The Internet of Vehicles (IoV) is an emerging ecosystem that is composed of vehicles, road-side units, and various other elements in the Internet of services and things. However, the connectivity of vehicles via various interfaces opens up new ways for attackers to remotely access safety relevant subsystems within connected cars. This lecture will address security requirements elicitation in this complex context. This important step in the security engineering process for automotive systems and ecosystems not only provides input to the secure on-board architecture design but also contributes to security compliance verification for testing and runtime monitoring.

4. **Yannick Chevalier**, PhD, Assistant Professor, Paul Sabatier University (Paul Sabatier University, Toulouse III), Toulouse, France. Lecture **"Finitary deduction systems for formal analysis of security applications"**.

When analyzing formally the security of an application or a system, one has to account for the possible actions of a misbehaving individual, or group of individual, hereafter called intruder. In particular, when analyzing the security provided by a cryptographic protocol beyond the security provided by the cryptographic primitives it employs, one models the intruder by a set of axioms in first-order logic, and uses specific proof procedures to compute whether the analyzed system is correct or flawed. In most cases, the specific proof procedure consists in computing a finite number of possible solved form [ChevalierVigneron01,MillenShmatikov01] lazily satisfying constraints. Some examples and properties of such systems, called finitary given that property, will be presented.

5. **Martin Strecker**, PhD, Assistant Professor, Paul Sabatier University (Paul Sabatier University, Toulouse III), Toulouse, France. Lecture **"Modeling programming languages with proof assistants"**.
For establishing the safety and security of software systems, a precise semantics of the programming languages involved, and of the correctness of transformations of the languages is becoming increasingly important. We will show how programming language semantics can be formally defined in proof assistants (illustrated by the Isabelle prover), how semantics preservation during compilation can be ensured, and how it is possibly to map programs to more abstract models (such as automata) in order to carry out fully automated, but semantically well-founded analyses.

6. **Fabrizio Baiardi**, PhD, Professor, University of Pisa, Pisa, Italy. Lecture **"Using distributed ledgers to assess and manage ICT risk"**.
In the lecture the main notion of distributed ledger, its alternative version and the various conditions, that can be adopted to preserve consistency and integrity of this distributed data structure, are introduced. Then, it is discussed how this data structure can support the evaluation and the management of the risk posed by an Information & Communication Technology (ICT) infrastructure. It is also considered how these activities can be implemented in real time.

7. **Sergey Andreev**, PhD, Senior Research Scientist, Tampere University of Technology, Tampere, Finland. Lecture **"Next-generation applications of moving mission-critical systems"**.
As fifth-generation (5G) communication technology is taking shape, a crucial question arises on the types of applications to be enabled by the rapidly maturing 5G ecosystem and beyond. Along these lines, formidable challenges are imposed by advanced use cases that involve moving vehicles, drones, and industrial robots. Complex mobility of these emerging mission-critical systems requires dedicated communication enables that confront the existing security and privacy solutions. This talk is a brief summary on recent advancements in research results and methods to support such next-generation applications of moving mission-critical systems.

8. **Lukas Malina**, PhD, Senior Researcher at Brno University of Technology (BUT), Brno, Czech Republic. Lecture **"Applied Cryptography on Programmable Smart Cards"**.
The presentation starts with a short introduction of the Cryptology Research Group at Brno University of Technology. The main topic of the presentation is which cryptographic primitives can be computed by current smart cards. After a short introduction of most spread platforms such as JAVA Cards, MultOS Cards, Basic Cards and .NET Cards, the presentation introduces the assessment of ECC primitives and cryptographic operations on the cards.

9. **Radek Fujdiak**, PhD, Researcher at the Brno University of Technology, Brno, Czech Republic. **Lecture "Security Issues in the LPWAN Technologies".**
We are living in the digital age, where the types of communication develop every day. Nowadays, we are witnessing the rise of activators for the internet of things. New communication technologies are coming with a very long range of more than 10 kilometers with keeping the power consumption low enough to serve without batteries more than 10 years. However, these technologies activate the idea of the internet of things, but also bring us many challenges on different levels of development and research. This presentation will speak about these new activators and its security issues in the real application.

10. **David Smekal**, Researcher of Technical University of Brno, Brno, Czech Republic. Lecture **"High-Speed Encryption with Strong Authentication on the FPGA Platform"**.
The topic describes the design of an encryption system with algorithm AES (Advanced Encryption Standard) using mode GCM (Galois Counter Mode) and its implementation on the FPGA (Field Programmable Gate Array) platform. The main goal is a description of the implementation of the VHDL encryption subsystem for programmable cards using the Xilinx Virtex-7 chip.

11. **Vladimir Oleshchuk**, PhD, Professor, Head of Communication and System Security group, Department of Information and Communication Technology, Faculty of Engineering & Science, University of Agder, Agder, Norway. Lecture **"Access Control for Cyber-Physical Systems"**.
Cyber-physical systems (CPSs) involve interactions between a large number of entities (both from the cyber world and the physical world), that can span different domains and jurisdictions. They provide services and functionalities that can require to use the knowledge of surrounding physical spaces. Uncontrolled disclosure of such knowledge or unconstrained interactions among entities can be exploited and cause serious security and privacy issues. Most of traditional approaches are rarely address these issues. The new models and access control mechanisms more adequate to protect sensitive resources from unauthorized access are needed. In this presentation, we consider challenges of access control for CPSs and examples of solutions that demonstrate how to address some of these challenges.

12. **Sergey A. Kolyubin**, PhD, Associate Professor, Acting Head of Mechatronics Dept., Vice Director for Science & Technology Foresight, School of Computer Technologies & Control, ITMO University, St. Petersburg, Russia. Lecture **"Control of industrial and mobile cyber-physical systems: actual problems in the context of security"**.
The lecture will examine key technologies, trends and prospects for the development of cyber-physical systems. Key requirements are formulated for their development. Important applications will be considered, including in the context of security. Special attention will be paid to research in a field of industrial and mobile cyber-physical systems at the ITMO University.

13. **Igor V. Kotenko**, Doctor of Technical Sciences, Professor, Head of Laboratory of Computer Security Problems, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, SPIIRAS, Co-Head of the International Laboratory "Information security of cyber-physical systems", ITMO University, St. Petersburg, Russia. Lecture **"Big Data Technologies for Cyber Security Monitoring and Incident Management in SIEM Systems"**.
The current state of research and development in the field of big data is considered; the models, methods, methods and tools for using big data technologies in perspective SIEM systems are presented. The peculiarity of the considered solutions is an emphasis on the integration of big data technologies and technologies of information management and security events. Aspects of providing security for big data technology are presented. Examples of developed systems for monitoring security and incident management based on big data technologies, including commercial, open source, research and own developments are given. The various implementations of security monitoring and incident management systems are compared. Perspective research directions and development of SIEM systems based on big data technologies, including those aimed at monitoring and managing incidents in cyber-physical systems are outlined.

14. **Aleksandr A. Grusho**, Doctor of Physical and Mathematical Sciences, Professor, Head of Laboratory of Information Security of IPI RAS, Moscow, Russia. Lecture **"An example of data mining application in the provision of information security: metadata-based management of network connections"**.
The task of information security in management of network connections is considered. The emphasis is on using metadata to manage connections. Formation of metadata is represented as a task of data mining.

15. **Anatoliy S. Minzov**, Doctor of Technical Sciences, Professor of the Department of Information and Economic Security of MPEI, Moscow, Russia. Lecture **"Contemporary conceptions of information security risk management"**.
Today there are several concepts for creation of information security management systems, but the most interesting and spread ones for business are risk management based conceptions. The existing standard GOST R ISO/IEC 27005 harmonized with the International Standard ISO/MEC 27005 gives only a general idea of risk management in a form of recommendations. At the same time links between individual risk indicators, methods for calculating risk metrics, mechanisms for determining approaches for their processing are not taken into account. In the Lecture we will examine modern risk management algorithms based on generalized multifactor risk models, including economic estimates of process costs on risks, mechanisms for identifying risk aggregates and their analysis and applying fuzzy sets to calculate risk metrics. The results of applying new approaches to risk management will be demonstrated on the simulation model of risk management.

16. **Igor B. Saenko**, Doctor of Technical Sciences, Professor, leading researcher of SPIIRAS, St. Petersburg, Russia. Lecture **"Application of a system of parallel stream computing for processing big data for solving problems of security event correlation"**.
The essence of parallel stream computing technology is considered using the example of Complex Event Processing technology, which underlies the functioning of the Spark software system. The mathematical foundations of individual problems of correlation of security events and algorithms for implementing their solutions in the Spark system are discussed. Results of the experimental evaluation of the developed method, algorithms and software prototype are demonstrated.

17. **Alexander Adamov**, CEO of NioGuard Security Lab, teaches the Advanced Malware Analysis course at Blekinge Institute of Technology and NURE, Kharkov, Ukraine. Lecture **"The Promising Areas of Cyberattack Research"**.
The lecture will look at the promising areas of research related to the analysis of cyber attacks including critical infrastructure attacks. These areas include but not limited to automation of analysis, extraction and analysis of configurations in SaaS-based malware, detection bypass technology using polymorphic encryption and code obfuscation, as well as countering automated analysis systems, detection technologies based on cluster analysis of dumps of network traffic and processes, and modeling of cyber attacks.

18. **Sergey V. Bezzateev**, Doctor of Technical Sciences, Professor, Head of the Department "Security of cyber-physical systems", St. Petersburg, Russia. Lecture **"Multifactor Authentication protocols for cyber-physical systems"**.

Authentication protocols that use factors of different type and purpose are proposed. In particular we consider a set of factors that take into account the user's location and state as well as factors blocking the authentication process or required for it. The use of multi-factor authentication systems can significantly improve security and safety of data processing, transmitting and storage in cyber-physical systems. For multifactor authentication systems the usage of threshold schemes is discussed. Such approach will give a possibility to provide a multilevel access to information.

19. **Andrey V. Chernov**, Doctor of Technical Sciences, Professor, Head of the Department "Computer science and computer-aided management" of RSTU, Rostov-na-Donu, Russia. Lecture **"Providing security in a telecommunication IT infrastructure of Russian Railways: problems and trends"**.

In the Lecture we consider the current state of the IT infrastructure of Russian Railways. Due to a wide variety of IT technologies, namely telecommunication facilities, automated workstations, server applications and telecommunications services provided by the Main Computing Center of Russian Railways, the Lecture will address information security issues related to a corporate data network.

20. **Maxim V. Kolomeec**, Researcher of the laboratory of computer security problems of SPIIRAS, postgraduate student of ITMO, St. Petersburg, Russia. Lecture **"Visualization driven security"**.

The key principles of data visualization and their application in information security are discussed. The history of visual analytics, architecture of visualization systems, visualization models with examples of application in cyber and cyber-physical security, ready visual analytic tools as well as psychological features of visual perception are considered. The material of the lecture is aimed at formation of a comprehensive understanding of possibilities of visual analytics for the analysis of security data. It demonstrates ways to abstract physical elements of systems and can serve as a necessary foundation for the design of their own systems for visual analysis of security data.

21. **Dmitry S. Levshun**, Researcher of the laboratory of computer security problems of SPIIRAS, postgraduate student of ITMO, St. Petersburg, Russia. Lecture **"A technique for complex design of secure systems based on embedded devices"**.

The problems of designing protected systems based on embedded devices are considered. Modern approaches to a design of secure embedded devices and systems based on them as well as approaches to the development of secure software are analyzed. Limits of their applicability are defined for the construction of secure systems based on embedded devices. A technique for designing secure systems based on embedded devices is proposed. An example of its application in the development of an integrated cyber security system is presented.

22. **Ilya I. Viksnin**, assistant of the Department of Design and Security of Computer Systems, ITMO, St. Petersburg, Russia. Lecture **"A method of data quality verification in cyber-physical systems on the base of social mechanisms"**.

An approach to improve the quality of particular information security indicators in the process of information interaction of elements of the cyber-physical system is presented. The main levels and flows of information interaction of elements and specific mechanisms for ensuring secure information interaction are determined. An approach to analyze information coming from the source element on the base of subjective information about this element is proposed. A measure to quantify quality of subjective information on an element on the basis of social mechanisms based on the concepts of truth, reputation and trust is introduced. The effect of reducing a reaction time of the cyber-physical system on detection and counteraction of the hidden destructive information impact, achieved by using the proposed approach is demonstrated.