SPIIRAS

ITMO UNIVERSITY

ORGANIZED BY ST.PETERSBURG INSTITUTE FOR INFORMATICS AND AUTOMATION OF THE RUSSIAN ACADEMY OF SCIENCES (SPIIRAS) AND ITMO UNIVERSITY.

INTERNATIONAL SCIENTIFIC SCHOOL «INCIDENT MANAGEMENT AND COUNTERING TARGETED CYBER-PHYSICAL ATTACKS IN DISTRIBUTED LARGE-SCALE CRITICAL SYSTEMS» (IM&CTCPA 2019)

ITMO UNIVERSITY, ST. PETERSBURG

Lomonosova str. 9, assembly hall (October, 9-10)

Register

October 9

Timing	Title of presentation	Presenter	Annotation
14:00-15.00	Registration of the school participants		
15:00-15:10	**Welcoming speech**	**Igor Kotenko,** Chief Scientist and 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	
15:10-16:10	**Societies, networks, big data, graphs and algorithms**	**Didier El Baz**, 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	The importance of networks and graphs in human societies is highlighted. Some primitive graphs like family trees, genealogical trees, which have conditioned the history of humanity, are firstly presented. Then their influences on the arts are considered. The modern societies and social networks generating huge data are studied. The talk focuses on parallel graph algorithms that can quickly analyze the graphical structures of social networks.
16:10-17:10	**IT-Security for E-mobility**	**Christoph Krauss,** Head of the Cyber-Physical	Electric vehicles can make a significant contribution for protecting the environment and reducing emissions. To successfully integrate electric vehicles into the power grid, smart charging is required. This includes

		Security Department, Fraunhofer-Institute for Secure Information Technology SIT, Darmstadt, Germany	demand response for adjusting the demand for power (e.g., based on variable price tariffs), load management for efficiently charging multiple vehicles within a given connected load, or Vehicle-to-Grid (V2G) enabling vehicles to store and return electricity to the grid. However, this requires the use of information and communication technology (ICT) which also introduces new security and privacy threats. In this talk, an overview of typical threats and challenges in the context of electric mobility as well as possible solutions to address these threats are given. Threats are for example privacy-related, e.g., the generation of movement profiles of a vehicle user by analyzing the used charge points, monetary threats, e.g., charging for free or on the account of someone else, or safety-threats, e.g., influencing the power grid. The possible solutions, e.g., for securing charge points or protecting contract credentials, are presented.
17:10-18:10	**Industrial Internet of Things (IIoT) Security**	**Diethelm Bienhaus,** Professor, the University of Applied Sciences, Mittelhessen, Germany	Industrial production systems and manufacturing information infrastructure is changing towards IP based communication. Connectivity of shop floor devices like sensors with server or cloud based applications is intended. The Internet of Things (IoT) approach aims on connecting physical objects (sensors, machines, cars, buildings, and other items) to enable interaction and cooperation of such objects. While IoT in general covers domains like healthcare, or smart homes, the Industrial Internet of Things (IIoT) refers in particular to industrial environments with goals like more process transparency or improvements in product quality and system maintenance. In this context, terms like Cyber Manufacturing Systems (CMS) or Cyber Physical Production Systems (CPPS) are significant. Ethernet-based protocols are getting more and more important for CPPS. In this talk, a survey of important protocols is presented. First, a general feature comparison of OPC UA, ROS, DDS, and MQTT, is given followed by an overview of important information interchange formats and a discussion of security aspects.

October 10

Timing	Title of presentation	Presenter	Annotation
10.00-10.50	**Cybersecurity Research: Challenges and Course of Action**	**Roland Rieke,** PhD, Senior researcher of Cyber-Physical Systems Security Department, Fraunhofer-Institute for Secure Information Technology SIT, Darmstadt, Germany	This talk will present key challenges in IT security research that have been identified by about 30 European researchers from academia and industry coordinated by the project secUnity. The classical and new research fields examined include quantifiable security, security despite untrustworthy components, big data privacy, IT security and data protection for machine learning as well as trustworthy platforms. Moreover, in the roadmap selected applications and technologies are studied from the IT security perspective. For example, blockchain technology, autonomous driving, the phenomenon of fake news and possible privacy tools will be discussed in more detail. The economic and legal aspects of IT security and human-centered Security are addressed separately.
11.00-11.50	**Log Analysis based on Data Exchange**	**Yannick Chevalier,** Assistant Professor, Paul Sabatier University (Paul Sabatier University, Toulouse III), Toulouse, France	Data Exchange was defined to model migrations in a database. New tables are created from existing ones by tuples generating constraints. We build on this model a log analysis framework. We assume that there exists a database with such constraints that correctly classify the events in a log, and will present heuristics that can be employed to learn these constraints.
12.00-12.50	**Social Network Analysis:**	**Andrey Chechulin,** Leading researcher of the laboratory of computer security	The development of information technologies and the emergence of a global Internet, social networks, mass media requires the scientific community to review existing ideas about wars. In the strategies of the

	Challenges and Trends	problems of SPIIRAS, senior researcher of ITMO University, St. Petersburg, Russia	leading countries of the world, the information space is included among the areas of warfare. The challenge here is how to recognize targeted information impacts (attacks) on subjects (individual or collective, for example, aimed to a person, family, group or organization) and to counteract such attacks. The talk will be devoted to the new approach which combines various methods, namely the graph analysis, text and images mining, visualization, distributed data processing and other technologies for providing security in information space of social networks.
13.00-14.00	Lunch		
14.00-14.50	**Artificial intelligence in cybersecurity**	**Olga Tushkanova,** Senior researcher of the laboratory of computer security problems of SPIIRAS; Assistant professor of SPbPU, St. Petersburg, Russia	In the talk the speaker will try to cover some of the most common use-cases, trends and key challenges of artificial intelligence in cybersecurity.
15.00-15.50	**Battery depletion attacks on cyber-physical devices**	**Vasiliy Desnitsky,** Senior researcher of the laboratory of computer security problems of SPIIRAS; senior researcher of ITMO University, St. Petersburg, Russia	Currently, energy depletion attacks aimed at contemporary autonomously working cyber-physical devices are becoming increasingly important. Such attacks aimed at nodes of wireless sensor networks, mobile devices, quadrocopters and other types of devices can lead to serious malfunctions and damage associated with their improper execution or crash. This lecture reveals the problems of such attacks, as well as some approaches to their modeling, evaluation and detection.
16.00-16.20	Coffee-break		
16.30-17.20	**Security assessment of information systems based**	**Elena Doynikova,** Senior researcher of the laboratory of computer security problems of SPIIRAS, senior researcher of	The talk covers main open security data sources and their application for security assessment using attack graphs and service dependencies, and the system of security metrics. The limitations of the approach are analyzed, including the main challenges, related to the incompleteness and inconsistency of the input data. The prospects of extension and

	on the open data sources: approach, challenges and prospects	ITMO University, St. Petersburg, Russia	enhancement of the existing approach using ontology of security metrics are considered, as well as possibility of consideration of zero-days while security assessment on the basis of analysis of exploits source code is proposed.
17.25-18.15	**Information Security Trends in Computer Networks: Review of the Cisco Security Solutions**	**Igor Ushakov,** Senior Lecturer, Department of Secure Communication Systems, Bonch-Bruevich St. Petersburg State University of Telecommications, St. Petersburg, Russia	Cisco is one of the lead companies that develop solutions in security area, including solutions to protect networks against inside, outside and man-in-the-middle attacks. The most relevant products to protect your network include: Identity Services Engine, Cisco Stealthwatch, Next-Generation Firewalls, Cisco Umbrella and Advanced Malware Protection. During the lecture you will know the general principles of work, best design practices, configurations examples, including real network scenarios.
18.20-18.30	**Concluding remarks**	**Igor Kotenko**, Chief Scientist and 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	