SCHEDULE

of

The 11th International Conference on Security for Information Technology and Communications SECITC 2018: www.secitc.eu

Powered by

Informatics Security | CyberSecurity Master

Bucharest University of Economic Studies

Information Technology Security Master

Military Technical Academy

Advanced Technologies Institute

Conference Partners

SECITC 2018 SCHEDULE
www.secitc.eu

08 November 2018 – ON THURSDAY

On Site Registration Date:
08 November 2018, 08.30 – 09:00 AM, room “*Aula Magna*”, Bucharest University of Economic Studies

Opening Meeting Date:
08 November 2018, 09.00 AM, room “*Aula Magna*”, Bucharest University of Economic Studies

Hour	Presenter	Presentation Title	Affiliation
08:30 AM	**Conference welcome coffee and registration**		
09.00 AM	**Welcome Speeches** Jean-Louis LANET & Cristian Valeriu TOMA, Conference Chairs		
09.15 AM	**Foreword** Representatives from:		
	Military Technical Academy	Bucharest University of Economic Studies	
	Department of Computer Science and Military Information Systems	Department of Economic Informatics and Cybernetics	
	Advanced Technologies Institute (ITA)	Romanian National Computer Security Incident Response Team (CERT-RO)	
	Invited Keynote Speakers		
09.30 AM	**Paolo D'Arco**	***Ultra-lightweight authentication protocols***	Italy
10.15 AM	**Jean-François LALANDE**	***Android Malware Analysis: from technical difficulties to scientific challenges***	France
11.00 AM	Octavian SZOLGA, “***Network security and visibility analytics***”, **Datanet Systems**		
11.45 AM	Cosmin CIOBANU**, “*Economics of vulnerability disclosure*”, ENISA** – European Network and Information Security Agency		
12.10 PM	Andrei Tronaru**, “Securing Cloud Infrastructure”, ORACLE**		
	Lunch 12.40 – 13.30		

***PAPER SECTIONS* – Room 2013**

Chair(s): Jean Francois Lalande | Section: Cloud Security – Room 2013

Hour	Authors	Paper Title
13.30	Tomas Kulik, Peter W. V. Tran–Jørgensen and Jalil Boudjadar	"Formal Security Analysis of Cloud-connected Industrial Control Systems"
13.50	Stefania Loredana Nita and Marius Iulian Mihailescu	"A Hybrid Searchable Encryption Scheme for Cloud Computing"
14.10	Leith Abed, Nathan Clarke, Bogdan Ghita and Abdulrahman Alruban	"Securing Cloud Storage by Transparent Biometric Cryptography"

Chair(s): Jean-Louis LANET | Section: Software Security – Room 2013

Hour	Authors	Paper Title
14.30	Léopold Ouairy, Hélène Le Bouder and Jean-Louis Lanet	"Normalization of Java Card applets"
14.50	Veronica-Mihaela Velciu, Florin-Alexandru Stancu, Mihai Chiroiu and Răzvan Rughiniș	"HiddenApp - Securing Linux applications using ARM TrustZone"
15.10	Shao-Fang Wen, Mazaher Kianpour and Basel Katt	"Security Knowledge Management in Open Source Software Communities"

15.30-15.45: COFFEE BREAK

Chair(s): Catalin BOJA & Mihai DOINEA | Section: Machine Learning in Cyber-Security – Room 2013

Hour	Authors	Paper Title
15.45	Camil Jichici, Bogdan Groza and Pal-Stefan Murvay	"Examining the Use of Neural Networks for Intrusion Detection in Controller Area Networks"
16.05	Dan Sporici, Mihai Chiroiu and Dan Ciocîrlan	"An Evaluation of OCR Systems against Adversarial Machine Learning"
16.25	Shahadate Rezvy and Tahmina Zebin	"Intrusion detection and classification with autoencoded deep neural network"
16.45	Muhammad Mudassar Yamin and Basel Katt	"Detecting Malicious Windows Commands Using Natural Language Processing Techniques"
17.05	Hasanen Alyasiri, John Clark and Daniel Kudenko	"Evolutionary Computation Algorithms for Detecting Known and Unknown Attacks"

Chair(s): Ion BICA & Mihai TOGAN | Section: Network Security – Room 2013

Hour	Authors	Paper Title
17.25	Stefan Bodoarca and Mihai Lica Pura	"Assuring Privacy in Surfing the Internet"
17.45	Isha Singh, Silke Holtmanns and Raimo Kantola	"Roaming Interface Signaling Security for LTE Networks"
18.05	Islam Faisal and Sherif El-Kassas	"Limited Proxying for Content Filtering Based on X.509 Proxy Certificate Profile"
18.25	Samir Puuska, Tero Kokkonen, Janne Alatalo and Eppu Heilimo	"Anomaly-based Network Intrusion Detection using Wavelets and Adversarial Autoencoders"

09 November 2018 – ON FRIDAY

Hour	Presenter	Presentation Title	Affiliation
08:30 AM	**Conference welcome coffee and registration**		
09.00 AM	**Denis Jean-Michel BAHEUX**	***Implications of applied cryptography for digital forensics investigations***	France
09.45 AM	**Emil Simion and Diana Maimut**	***Post-Quantum Cryptography and a (Qu)Bit More***	Romania

Chair(s): Marius POPA | Section – Viruses and Malware – Room 2013

Hour	Authors	Paper Title
10.15	Mert Nar, Arzu Kakisim, Necmettin Carkaci and Ibrahim Sogukpinar	"Analysis and Evaluation of Dynamic Feature-based Malware Detection Methods"
10.25	Andrei-Catalin Mogage, Emil Simion and Vlad Craciun	"Trends in design of ransomware viruses"

10.45-11.00: COFFEE BREAK

Chair(s): Cristian TOMA | Section – IoT, M2M and Blockchain Security – Room 2013

Hour	Authors	Paper Title
11.00	Hao Cheng, Daniel Dinu and Johann Großschädl	"Efficient Implementation of the SHA-512 Hash Function for 8-bit AVR Microcontrollers"
11.20	Cristian Toma, Bogdan Talpiga, Catalin Boja, Marius Popa, Bogdan Iancu and Madalina Zurini	"Secure IoT Supply Chain Management Solution using Blockchain and Smart Contracts Technology"
11.40	Konstantinos Rantos, George Drosatos, Konstantinos Demertzis, Christos Ilioudis, Alexandros Papanikolaou and Antonios Kritsas	"ADvoCATE: A Consent Management Platform for Personal Data Processing in the IoT using Blockchain Technology"
12.00	Nicolas Bruneau, Jean-Luc Danger, Adrien Facon, Sylvain Guilley, Soshi Hamaguchi, Yohei Hori, You Sung Kang and Alexander Schaub	"Development of the unified security requirements of PUFs during the standardization process"
12.20	Cristian Hristea and Ferucio Laurentiu Tiplea	"A PUF-based Destructive-private Mutual Authentication RFID Protocol"

LUNCH BREAK: 12.40-13.30

Chair(s): Emil Simion and Diana Maimut | Section – Security Models, Cryptanalysis and Side-Channel Attacks – Room 2013

Hour	Authors	Paper Title
13.30	Masayuki Tezuka, Yusuke Yoshida and Keisuke Tanaka	"Weakened Random Oracle Models with Target Prefix"
13.50	Ceyda Mangır, Murat Cenk and Murat Manguoglu	"An Improved Algorithm for Iterative Matrix-Vector Multiplications over Finite Fields"
14.10	Adrian Schipor	"On the security of Jhanwar-Barua Identity-Based Encryption Scheme"
14.30	Dragoi Vlad, Beiu Valeriu and Bucerzan Dominic	"Vulnerabilities of the McEliece variants based on Polar codes"
14.50	Damien Marion, Adrien Facon, Sylvain Guilley, Thomas Perianin and Matthieu Lechvien	"Binary Data Analysis for Source Code Leakage Assessment"
15.10	Zihao Wang, ShuangHe Peng, Wenbin Jiang and Xinyue Guo	"Zero in and TimeFuzz: Detection and Mitigation of Cache Side-Channel Attacks"

15.30-15.45 : COFFEE BREAK

Chair(s): Cezar PLESCA | Section – Cryptographic Algorithms – Room 2013

Hour	Authors	Paper Title
15:45	Aguilar Melchor Carlos, Killijian Marc-Olivier, Lefebvre Cédric and Ricosset Thomas	A Comparison of the Homomorphic Encryption Libraries HElib, SEAL and FV-NFLlib
16.05	Augustin Ousmanou Ahgue, Jean De Dieu Nkapkop, Joseph Yves Effa, Samuel Franz, Raul Malutan and Monica Borda	"A new DNA-Combining Chaos Scheme for Fas and Secure Image Encryption"
16.25	Victor Talif	"Implementing Searchable Encryption schemes over Multilinear Maps (secret shared scheme encryption)"
16.45	Diana Maimut and George Teseleanu	"A Unified Security Perspective on Legally Fair Contract Signing Protocols"
17.05	Madalina Bolboceanu	"Relating different Polynomial-LWE problems"
17.25	Mugurel Barcau, Vicentiu Pasol and Cezar Plesca	"Monoidal encryption over (F2, .)"
17.45	Koki Nishigami and Keiichi Iwamura	"Geometric pairwise key-sharing scheme"

CLOSING THE SCIENTIFIC CONFERENCE – www.secitc.eu: 18:05 - 18:15

www.secitc.eu

These activities are not connected with the Springer LNCS.

ATLAS Project Workshop - On Friday, 09 November 2018, Room 2416, 10:30-12:30

Hour	Partners	Project
10.30	Military Technical Academy (www.mta.ro), Bucharest University of Economic Studies (www.ase.ro), University "Politehnica" of Bucharest (www.upb.ro), Bucharest University (www.unibuc.ro)	Contract 17PCCDI / 2018

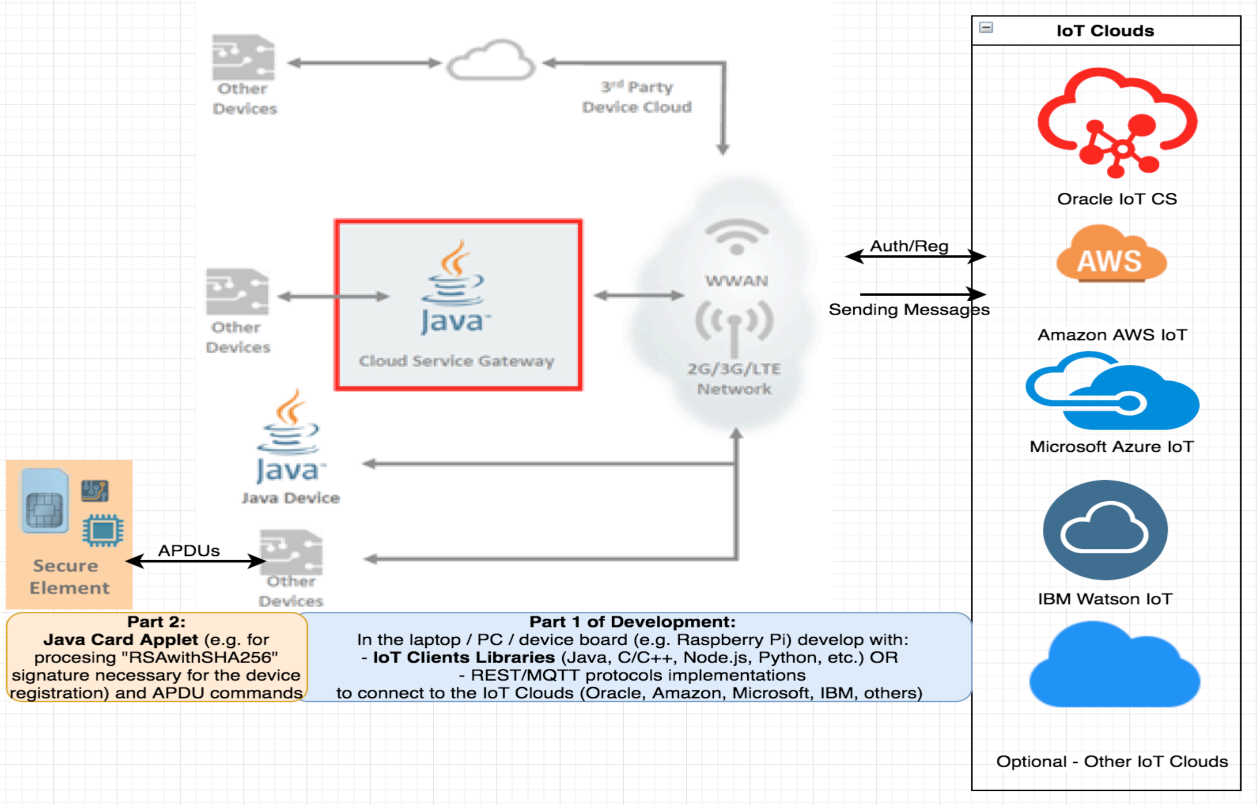
Hackathon - On Friday, 09 November 2018, Room 2001D, 18:00-19:30 / Zoom.us

MSc. and PhD. Students, who want to participate and start the Dev Hackthon on IoT & Security are invited. Single student or teams of two candidates are accepted. **More details on the conference website: www.secitc.eu**

Deadline for the hack-days projects by sending the source code for the solution/challenge: on Monday, 12 Nov. 2018, 23:59 GMT to secitc@gmail.com | secitc@ase.ro (the submission must contain the source code, configuration files and compile/running info; also, the submission is flexible in terms of receiving the source code via public repositories GitHub, SVN, etc., although GitHub is preferred). The challenge for this Software Development Hackathon is to provide a solution into two parts for connecting a device to various IoT Clouds:

- Part 1 – connect a laptop or PC or Dev board (e.g. Raspberry Pi) to all this Internet of Things (IoT) Clouds by using directly the communications protocols (e.g. REST API – HTTP, MQTT, etc.) or the device client libraries (e.g. Java, C/C++, node.js – ECMAScript/JavaScript, Python, etc.):
    - Oracle IoT CS: https://cloud.oracle.com/iot (Get 30 days free: https://myservices.us.oraclecloud.com/mycloud/signup?language=en&sourceType=_ref_coc-asset-opcPAASIoT)
    - Amazon AWS IoT: https://aws.amazon.com/iot/
    - Microsoft Azure IoT: https://azure.microsoft.com/en-gb/overview/iot/ (Get free account: https://azure.microsoft.com/en-gb/free/)
    - IBM Watson IoT: https://www.ibm.com/internet-of-things / https://www.ibm.com/us-en/marketplace/internet-of-things-cloud
- Part 2 – Try to separate the cryptographic security execution from the host/device client library into Java Card simulator or real Java Card – card / token / element for creating an Java Card applet and host client side (for APDUs exchange) in order to externalize parts of the cryptographic secure algorithms used for signing the registration/authentication messages to the IoT Clouds.

Architecture – partial copyright Oracle / partial www.ism.ase.ro done with draw.io tool:



Part 2:
Java Card Applet (e.g. for procesing "RSAwithSHA256" signature necessary for the device registration) and APDU commands

Part 1 of Development:
In the laptop / PC / device board (e.g. Raspberry Pi) develop with:
- **IoT Clients Libraries** (Java, C/C++, Node.js, Python, etc.) OR
- REST/MQTT protocols implementations
to connect to the IoT Clouds (Oracle, Amazon, Microsoft, IBM, others)