European Intelligence & Security Informatics Conference

The Premier European Conference on Counterterrorism and Criminology

Oulu, Finland, November 26-27, 2019 http://www.eisic.org

EISIC 2019

Conference Program

EISIC 2019

Conference Organizer and Sponsor

UNIVERSITY OF OULU

UBICOMP UNIVERSITY OF OULU

Center for Machine Vision and Signal Analysis

FAB LAB OULU

6G FLAGSHIP UNIVERSITY OF OULU

Academic Sponsors

FOI

KTH VETENSKAP OCH KONST

Technical co-sponsorship

IEEE

IEEE computer society

Conference Secretariat

Conference registration takes place at the Conference registration desk located at Tellus Stage Linnanmaa Campus, University of Oulu during the following days and hours:

Tuesday	8-15– 16:30
Wednesday	8:15– 16:30

The registration fee includes:

- One lunch and two coffee breaks per conference day
- One ticket for the Conference Dinner held on Tuesday 26th of November, 2019 at the Nallikari Restaurant.
- Conference bag with the conference program, proceedings, conference gifts, etc.

Table of Contents

General Chairs

Mourad Oussalah,
University of Oulu, Finland

Panos Kostakos,
University of Oulu, Finland

Program Chair

Joel Brynielsson,
KTH Royal Institute of Technology, Sweden

Publication Chair

Panagiotis Karampelas,
Hellenic Air Force Academy, Greece

Local Arrangement Chair

Anabela Berenguer,
University of Oulu, Finland

Web Chair

Panagiotis Karampelas,
Hellenic Air Force Academy, Greece

Gerhard Backfried
SAIL LABS Technology GmbH, Austria
Gabriela Bodea
TNO, Netherlands
Martin Boldt
Blekinge Institute of Technology, Sweden
Anton Borg
Blekinge Institute of Technology, Sweden
Hervé Borrion
University College London, United Kingdom
Guy De Tré
Ghent University, Belgium
Christophe Fagot
Intactile Design, France
Ulrik Franke
RISE SICS Swedish Institute of Computer Science, Sweden
Gunther P. Grasemann
Fraunhofer IOSB, Germany
Mohammad Hammoudeh
Manchester Metropolitan University, United Kingdom
Johan de Heer
Thales Research & Technology, Netherlands
Anders Holst
RISE SICS Swedish Institute of Computer Science, Sweden
Philip Inglesant
University of Oxford, United Kingdom

Fredrik Johansson
FOI Swedish Defence Research Agency, Sweden
Panagiotis Karampelas
Hellenic Air Force Academy, Greece
Jeroen Keppens
King's College London, United Kingdom
Panagiotis Kostakos
University of Oulu, Finland
Ana Kovačević
University of Belgrade, Serbia
Ioanna Lekea
Hellenic Air Force Academy, Greece
Luca Mazzola
Lucerne University of Applied Sciences and Arts, Switzerland
Mourad Oussalah
University of Oulu, Finland
Rasmus Petersen
Software Improvement Group, Denmark
Galina Rogova
State University of New York at Buffalo, USA
Günter Schumacher
European Commission Joint Research Centre, Italy
Virgilijus Sakalauskas
Vilnius University, Lithuania
Yannis Stamatiou
University of Patras, Greece
Jerzy Surma
Warsaw School of Economics, Poland

Muhammad Adnan Tariq
KTH Royal Institute of Technology, Sweden
Edward Tjörnhammar
KTH Royal Institute of Technology, Sweden
Theodora Tsikrika
Information Technologies Institute, CERTH, Greece
Erik Valldor
FOI Swedish Defence Research Agency, Sweden
Stefan Varga
KTH Royal Institute of Technology, Sweden
Cor Veenman
Netherlands Forensic Institute, Netherlands
Jozef Vyskoč
VaF s.r.o., Slovak Republic
Uffe Kock Wiil
University of Southern Denmark, Denmark
Yuchen Zhou
Palo Alto Networks, USA

We are happy to welcome you and the European Intelligence and Security Informatics Conference (EISIC) to Oulu, Finland. In the last decade, EISIC has grown to be the premier European conference on counterterrorism and criminology. The conference series has combined intriguing technical programs with good organization. For EISIC 2019 we aim to maintain the high standard, and we hope that you will enjoy the conference.

Oulu is Finland's most populous city in northern Finland, founded by King Charles IX of Sweden in 1605. The city was initially known for wood tar and then became one of the Europe's "living labs," where residents constantly experiment with new technology on a community-wide scale. We hope you will enjoy the special winter conditions in Oulu. We are also proud to present our distinguished keynote speakers Dr. Marios Thoma from European Security and Defence College in Belgium, Dr. Ian Oliver from Nokia-Bell, Finland, Professor Juha Röning from University of Oulu, Finland, and Dr. Dr. Madhusanka Liyanage Centre for Wireless Communications, University of Oulu, Finland. In addition to these four distinguished speakers, we also hope you will enjoy the presentation by the invited speaker Thi Hoang from Global Initiative Against Transnational Organized Crimes in Austria. The expectation is to provide a good mixture between academia, IT professionals and frontline practitioners alike.

The conference dinner will take place in Nallikari, at beach side of Oulu. For those of you who have the time to discover Oulu on your own, there are many possibilities. In particular, we recommend paying visits to the Science Museum in Tietomaa Science Centre, Oulu Cathedral, and and the emblematic Toripolliisi Statue in the Oulu Market square, in the very heart of City Centre.

Organizing a conference requires much work and support from many people and organizations. We would like to thank all those who have been involved in the organization of EISIC 2019. In particular, we are grateful for the hard work done by the program chair Joel Brynielsson. We are also grateful to Panagiotis Karampelas for his continuous support to keep the website updated, and to the local finance officers and technical support team at the University of Oulu for their help with the conference budget and other support related tasks. We are also thankful to the Centre for Ubiquitous Computing -UBICOMP, and the Centre for Machine Vision and Signal Processing-CMVS at University of Oulu for their sponsorship and support for this conference. A special thank you to Marta Cortés and Iván Sánchez Milara, research scientists at the UBICOMP unit for their contribution in the design and production of EISIC 2019 branded items in the Oulu's Fab Lab. Finally, we would like to send a special thanks to Anabela Berenguer, the local arrangements chair, for her tremendous effort in taking care of every organizational-related task of this conference.
As we now inaugurate the ninth EISIC meeting, we wish to welcome you to Oulu and we hope that you will enjoy EISIC 2019 and your stay in Finland.

Mourad Oussalah, CMVS, Faculty of Information Technology, University of Oulu, Finland
Panos Kostakos, UBICOMP, Faculty of Information Technology, University of Oulu, Finland

EISIC 2019 – Message from the Program Chair

Intelligence and Security Informatics (ISI) is an interdisciplinary field of research that focuses on the development, use, and evaluation of advanced information technologies, including methodologies, models and algorithms, systems, and tools, for local, national, and international security related applications. Over the past decade, the European ISI research community has matured and delivered an impressive array of research results that are both technically innovative and practically relevant.

Academic conferences have been an important mechanism for building and strengthening the ISI community. These conferences have provided stimulating forums for gathering people from previously disparate communities including those from academia, government, and industry. Participants have included academic researchers (especially in the fields of information technologies, computer science, public policy, and social and behavioral studies), law enforcement and intelligence experts, as well as information technology company representatives, industry consultants, and practitioners within the relevant fields.

The 2019 European Intelligence and Security Informatics Conference (EISIC 2019) is the ninth EISIC meeting to be organized by the European ISI community. During 2011–2018 the EISIC meetings have been held annually in Athens, Greece; Odense, Denmark; Uppsala, Sweden; The Hague, the Netherlands; Manchester, United Kingdom; Uppsala, Sweden; Athens, Greece; and Karlskrona, Sweden. EISIC 2019 is organized by the University of Oulu, and is scientifically sponsored by the Hellenic Air Force Academy, the Swedish Defence Research Agency, and the Royal Institute of Technology, Sweden, and has received technical co-sponsorship from the IEEE Computer Society and its Technical Committee on Intelligent Informatics (IEEE CS TCII). We would like to express our gratitude to these sponsors.

EISIC 2019 received 31 submissions in total, and accepted 50% of the submitted regular papers. For comparison, EISIC 2011 received 111 submissions and accepted 27% of the papers, EISIC 2012 received 70 submissions and accepted 40% of the papers, EISIC 2013 received 87 submissions and accepted 31% of the papers, IEEE JISIC 2014 received 98 submissions and accepted 28% of the papers, EISIC 2015 received 78 submissions and accepted 35% of the papers, EISIC 2016 received 64 submissions and accepted 24% of the papers, EISIC 2017 received 51 submissions and accepted 31% of the papers, and EISIC 2018 received 31 submissions and accepted 36% of the papers.

The two-day conference program includes presentations by prominent keynote speakers, paper presentation sessions, and a poster session. We are very pleased with the technical quality of the accepted submissions, and would like to express our gratitude to all authors for contributing.

To distinguish between the submitted papers and guide the acceptance decisions, all papers have been carefully read and analyzed by independent experts. Representing all the different flavors of the broad ISI field and coming from 16 different countries, the 36 program committee members generously provided high-quality review reports. We are most grateful to the program committee members for their time spent sharing their valuable expertise with the paper authors.

Joel Brynielsson, KTH Royal Institute of Technology, Sweden

Tuesday, November 26, 2019		
08:15-9:15	Registration/Coffee	Venue: Tellus Stage
09:15-9:45	**Welcome Session** General Chairs / Dean / Program Chair	Venue: Tellus Stage
09:45-10:45	**Keynote I: A Glimpse of 5G Security: Challenges and Opportunities** Speaker: Dr. Madhusanka Liyanage	Venue: Tellus Stage
10:45-11:10	Coffee break	Venue: Tellus Stage
11:10-12:30	**Session I**	Venue: Tellus Stage
12:30-13:30	Lunch	Venue: FooBar Restaurant
13:30-14:00	Guided visit to Oulu Fab Lab	Venue: Fab Lab facilities
14:00-15:15	**Session II**	Venue: Tellus Stage
15:15-15:30	Coffee break	Venue: Tellus Stage
15:30-16:30	**Keynote II: Cyber training activities of the European Security and Defence College** Speaker: Dr. Marios Thoma	Venue: Tellus Stage
16:30-17:30	**Session III**	Venue: Tellus Stage
19:05-23:30	**Dinner and Sauna: Restaurant Nallikari**	

Wednesday, November 27, 2019		
08:30-10:00	**Session IV**	
10:00-10:15	Coffee break	
10:15-11:00	**Session V – Poster presentation**	Venue: Tellus Stage
11:00-12:00	**Keynote III: Understanding Firmware Forensics using the Trusted Platform Module** Speaker: Dr. Ian Oliver	Venue: Tellus Stage
12:00-13:00	**Keynote IV: AI: Trustworthy or Not on Software Security** Speaker: Prof. Juha Röning	Venue: Tellus Stage
13:00-14:00	Lunch & Poster session	Venue: Tellus Stage/Frost Club
14:00-14:30	Visit to the Virtual Reality Laboratory & 3D Scanning	Venue: TS 365
14:30-15:00	**Invited Speech: Upcoming Global Initiative Report** Speaker: Thi Hoang	Venue: Tellus Stage
15:00-16:30	**Session VI**	
16:30-17:00	**Announcements & Closing Session**	Venue: Tellus Stage

Dr. Marios Thoma
Training Manager (Cyber), European Security and Defence College, Belgium

15:30-16:30 Tuesday, 26 November 2019 Venue: Tellus Stage Chair: Joel Brynielsson

"Cyber training activities of the European Security and Defence College"

Abstract

During this presentation, we will introduce the European Security Defence College (ESDC) and its role in the EU Cyber Ecosystem. The ESDC is established as a network college, bringing together the existing national and international training institutes dealing with security and defence policy issues within the Union. In 2018, the existing mandate of the ESDC was broadened, and the Cyber Education Training Exercise and Evaluation (ETEE) Platform was created. Having analysed the EU cyber ecosystem and the training requirements on cyber of the Member States, a new model was identified regarding the training on cyber in ESDC. The model foresees that the Cyber ETEE Platform will deal with all cybersecurity domains, such as Cyber Crime, Network Information Security, Cyber Defence and External Relations.

Bio

Dr. Marios Thoma has graduated from the Hellenic Military Academy and joined the National Guard of Cyprus in 1997. He holds a Master of Science degree in communications and computer science from the University of Athens, Greece. He also graduated from the Hellenic Military School of Officers in Telecommunications and Electronics. In 2018 he received a PhD degree from the Department of Electrical and Computer Engineering at the University of Cyprus. His research focuses in the study of cyberspace defense and specifically in the modelling and early detection of cyber attacks. During his service in the military, he has served at various posts in the domain of communications, security and cyber, and from 11 September 2011 to 16 November 2016 he served in the Cyprus Ministry of Defence in related posts.He has been the Training Manager (Cyber) of the ESDC since the 1st of July 2018 and in this capacity he is a member of the cyber security team of the ESDC, task with the creation of the CSDP Cyber Education, Training, Exercise and Evaluation (ETEE) Platform.

Dr. Ian Oliver
Nokia Bell Labs, Finland

11:00-12:00	Thursday, 27 November 2019	Venue: Tellus Stage	Chair: Mourad Oussalah

"Understanding Firmware Forensics using the Trusted Platform Module"

Abstract

In this talk we present the Trusted Platform Module - TPM - and its role in the integrity of the boot sequence of devices, typically servers, laptops etc, but also extend this to IoT devices. By understanding what is being measured and how measurements can be trusted and utilised we can build an understanding of how firmware behaves, how changes to the firmware can be detected and how this can be used to protect the hardware and software running on those devices. We then explore notions and reasons of 'trust failure', how this is detected, techniques such as root cause analysis, failure model and effects analysis in this context and how mitigations can be constructed against firmware attacks. Finally we extend these concepts to supply-chain integrity and trust and show how integrity and trust could be utilised.

Bio

Dr Ian Oliver is a Distinguished Member of Technical Staff at Bell Labs working on Supply Chain Security, Trusted and High-integrity Network Function Virtualisation for 5G Networking and Trusted Edge/IoT, Notarisation and Blockchain for Trusted Supply Chain and Applications. Other areas of active research include Privacy Engineering and various topics related to information theory, measurement of privacy, semantics and machine learning.

He holds a Research Fellow position at the University of Brighton working with the Visual Modelling Group on diagrammatic forms of reasoning, description logics with the occasional foray into category theory.

Prior to these he has worked as the privacy architect and officer for Here and Nokia Services; and for eleven years at Nokia Research Centre working with Semantic Web, UML, formal methods and hardware-software co-design. He has also worked at Helsinki University of Technology and Aalto University teaching formal methods and modelling with UML.

He is the author of the book "Privacy Engineering: A data flow and ontological approach" and hold over 200 patents and academics papers.

Prof. Juha Röning
University of Oulu, Finland

12:00-13:00	Wednesday, 27 November 2019	Venue: Tellus Stage	Chair: Mourad Oussalah

"AI: Trustworthy or Not on Software Security"

Abstract

The National Institute of Standards and Technology plans to move to a vulnerability scoring method that uses IBM's Watson artificial intelligence system by October 2019. So far, Watson stumbled when evaluating new and complex vulnerabilities. So AI is sneaking in to cyber security business, but does it make us stronger or more vulnerable. AI in its recent form and development is a powerful tool but contains some risks and ethical questions we should be aware and consider. We should not just trust learning AI methods like a magic black box. The decision-making should be "transparent". We need to understand how it works and have command over it. At the same time, our officials' main concern is not anymore that hackers will steal data, but that they will change data. This follows that users will unwittingly rely on false information. Recent terroristic attacks with common tools or equipment have resulted to demands to test products for abusability. Tech firms should foresee the unintended consequence of technology. What about the malicious use of AI. With this talk, I would like to raise the issues, how much one can trust AI-based decisions. What risks of autonomous response actions might have? Double blade of AI i.e. AI arms race between defenders and attackers.

Bio

Prof. Juha Röning Juha Röning is a Professor of Embedded System at the University of Oulu. He serves also as Visiting Professor of Tianjin University of Technology, P. R. China. He is principal investigator of the Biomimetics and Intelligent Systems Group (BISG). In 1985 he received Asla/Fullbright scholarship. From 1985 to 1986 he was a visiting research scientist in the Center for Robotic Research at the University of Cincinnati. From1986 to1989 he held a Young Researcher Position in the Finnish Academy. In 2000 he was nominated as Fellow of SPIE. He has two patents and has published more than 300 papers in the areas of computer vision, robotics, intelligent signal analysis, and software security. He is currently serving as a Board of Director for euRobotics aisbl. He is also a steering board member of ARTMIS-IA.

Dr. Madhusanka Liyanage
Adjunct Professor – Docent, University of Oulu, Finland

09:45-10:45 Tuesday, 26 November 2019 Venue: Tellus Stage Chair: Mourad Oussalah

The evolution of mobile telecommunication networks is accompanied by new demands for the performance, portability, elasticity and energy efficiency of network functions. As a result, 5G mobile networks will adopt new networking concepts to improve the performance. The telecommunication standardization bodies are working on integrating novel networking concepts such as Software Defined Networking (SDN), Network Function Virtualization (NFV), Cloud Computing, Multi-access Edge Computing (MEC) and Network Slicing principles to telecommunication networks. The target of such efforts is to innovate and develop new network concepts for meeting the future requirements of the evolving mobile networks. Present-day, mobile networks are suffering from many security limitations such as Securing only the perimeter, Distributed and uncoordinated security mechanisms, tightly coupled to physical resources, lack of adaptation and interoperability, over-provisioned security mechanisms, vulnerability to various IP based attacks, lack of visibility and high network monitoring overhead. The introduction of network softwarization, programmability, NFV, the separation of the control and data planes, the introduction of new network functions and even the introduction of new stakeholders such as Mobile Virtual network Operators (MVNO) are expected to solve the security limitation of current telecommunication networks. Despite the expected advantages, the adaptation of SDN, NFV, MEC and slicing concepts also brings many security disadvantages as well. For instance, adaptation of these technologies will minimize the technological gap between the common IP networks and 5G telecommunication networks. As a result, 5G mobile networks will be vulnerable to most the attacks which are available in general SDN and IP networks. Therefore, the introduction of all these new features have impact on how security needs to be assured and managed in 5G networks. This talk is not only focused on new opportunities but also new challenges and vulnerabilities related to 5G security.

Bio

Dr. Madhusanka Liyanage is an Adjunct Professor - Docent at the Centre for Wireless Communications, ITEE Faculty, University of Oulu, Finland. With 58 peer reviewed publications in international journals, Dr. Liyanage's publications have been cited 820 times. Researcher with eight years of experience in various domains including Network Security, 5G, SDN, NFV, Mobile networks, IoT, Blockchain, MEC and Virtual Private Network (VPN) domains. Three years of experience in research project management, research group leadership, project proposal preparation, project progress documentation and graduate student supervision. Responsible roles in international, EU and national research projects. Experience in teaching and conducting lab work for both postgraduate and undergraduate students. He is also recipient of Marie Skłodowska-Curie Actions (MSCA) - Individual Fellowship (IF).

Invited NGO Speaker

Thi Hoang
Global Initiative Against Transnational Organised Crime, Vienna, Austria

14:30-15:00	Wednesday, 27 November 2019	Venue: Tellus Stage	Chair: Panos Kostakos

" Upcoming Global Initiative Report "

Abstract

Digital technologies have changed the 'traditional' organized crime landscape in various ways, specifically with regard to the criminal groups' operating structure, modus operandi and their member profiles. In a recent survey conducted with more than 400 experts of the Global Initiative's Network of experts, cybercrime has been cited as the biggest global trend in organized crime (OC) over the next decade, followed by drug trafficking and human trafficking. Concerning the cross-cutting issues having the most impact on the European illicit markets, technology has been ranked in the top three, alongside geopolitics and demographics shifts / migration. In our upcoming 'cyber primer', we have therefore explored how technologies and their growth have affected the five major illicit markets and their dynamics, as well as the resulting law enforcement challenges. Finally, to illustrate how technologies can also be used as a counter-strategy to transnational organized crime, examples of tech tools developed to fight human trafficking will be discussed.

Bio

Thi is an Analyst at the Global Initiative Against Transnational Organized Crime. She is coordinating and managing projects under the Responsible and Ethical Private Sector Coalition against Trafficking (RESPECT) Initiative (http://www.respect.international/), which serves as a platform to mobilise the business community as a strategic partner to tackle human trafficking. She is also the Research Lead of the Tech Against Trafficking initiative, a coalition of technology companies (Amazon, AT&T, BT, Microsoft, Nokia, Salesforce.org, and Vodafone) and stakeholders aiming to help eradicate human trafficking using technology. Thi is also managing and overseeing the updates and expansion of the Modern Slavery Map (http://www.modernslaverymap.org/), an interactive map for business of anti-human trafficking organisations, with partner organisations including the ILO Child Labour Platform, United Nations Global Compact and Global Business Coalition Against Trafficking.

Tuesday, November 26, 2019	
09:00-10:00	Registration/Coffee
09:15-09:45	**Opening: Welcome Session** General Chairs / Dean / Program Chair Mourad Oussalah and Panos Kostakos/ Jukka Riekki – Professor & Dean at the UBICOMP-ITEE Faculty/ Joel Brynielsson
09:45-10:45	**Keynote I:** A Glimpse of 5G Security: Challenges and Opportunities Speaker: Dr. Madhusanka Liyanage, *University of Oulu, Finland*; Chair: Mourad Oussalah
10:45-11:10	Coffee break
11:10-12:30	**Session I**
Tellus Stage	Chair: Panos Kostakos
	Identification and Detection of Human Trafficking Using Language Models Jessica Zhu, Lin Li and Cara Jones
	Mining Security discussions in Suomi24 Eetu Haapamaki and Juho Mikkola, Mourad Oussalah
	Identifying deceptive reviews: feature exploration, model transferability and classification attack Marianela Garcia Lozano and Johan Fernquist
12:30-13:30	Lunch
13:30-14:00	Guided visit to Oulu Fab Lab
14:00-15:15	**Session II**
Tellus Stage	Chair: Mourad Oussalah
	Predicting the Offender: Frequency Beats Bayes August Daniel Sutmuller, Mariëlle den Hengst, Ana Isabel Barros, Bob van der Vecht, Wouter Noordkamp and Pieter van Gelder
	Firearm Detection and Segmentation using an Ensemble of Semantic Neural Networks Alexander Egiazarov, Vasileios Mavroeidis, Fabio Massimo Zennaro and Kamer Vishi
	Evaluation of Deep Learning Models for Ear Recognition Against Image Distortions Susan El-Naggar and Thirimachos Bourlai (Skype call)
	Prototype and Analytics for Discovery and Exploitation of Threat Networks on Social Media Olga Simek, Danelle Shah and Andrew Heier
15:15-15:30	Coffee break
15:30-16:30	**Keynote II: Cyber training activities of the European Security and Defence College** Speaker: Dr. Marios Thoma -*European Security and Defence College, Belgium*; Chair: Joel Brynielsson
16:300-17:30	Session III- Short papers;
	Chair: Johan Fernquist
	Characterization of Disinformation Networks Using Graph Embeddings and Opinion Mining Olga Simek, Alyssa Mensch, Lin Li and Charlie Dagli
	Semi-Automatic Geometric Normalization of Profile Faces using Random Sample Consensus Feature Matching Justin Romeo and Thirimachos Bourlai
	Remote KYC: Attacks and Counter-measures Marc Pic, Gaël Mahfoudi and Anis Trabelsi
	Privacy preserving sentiment analysis on multiple edge data streams with Apache NiFi Abhinay Pandya, Panos Kostakos, Hassan Mahmood, Marta Cortes, Ekaterina Gilman, Mourad Oussalah and Susanna Pirttikangas
	Crime Prediction Using Hotel Reviews? Panos Kostakos, Somkiadcharoen Robroo, Bofan Lin and Mourad Oussalah
19:05-23:30	**Dinner and Sauna: Restaurant Nallikari**

Wednesday, November 27, 2019	
08:30-10:00	**Session IV**
Tellus Stage	Chair: Mordechai Guri
	A model of quantifying social relationships Disa Sariola
	Extracting Account Attributes for Analyzing Influence on Twitter Lisa Kaati, Johan Fernquist, Fredrik Johansson and Ola Svenonius
	Statistical Analysis of Identity Risk of Exposure and Cost Using the Ecosystem of Identity Attributes Chia-Ju Chen, Razieh Nokhbeh Zaeem and Suzanne Barber
	Attack Hypothesis Generation Aviad Elitzur, Rami Puzis and Polina Zilberman
10:00-10:15	Coffee break
10:15-11:00	**Session V – Poster presentation**
Tellus Stage	Chair: Panos Kostakos
	A comparative study of clustering methods using word embeddings Nikolaos Bastas, George Kalpakis, Theodora Tsikrika, Stefanos Vrochidis and Ioannis Kompatsiaris
	Secure exchange of Information for all actors involved in MLAs (EIOs for Europe) and police cooperation Fabrizia Bemer
	Timing Covert Channels Detection Cases via Machine Learning Anna Epishkina, Mikhail Finoshin, Konstantin Kogos and Aleksandra Yazykova
	Moving Target Defense (MTD) as a Cyber Security Measure Mordechai Guri, Yuval Elovici and Dov Shirtz
	Mobile user authentication using keystroke dynamics Anna Epishkina, Konstantin Kogos and Daria Frolova
	Analysis of Vancouver Crime and Census Data Using Various Machine Learning Algorithms Kyle Behiels, Andrew Park, Justin Song, Valerie Spicer and Herbert H. T sang
	The Development of Lone Wolf Terrorism in Southeast Asia Pujo Widodo, Tri Legionosuko and David Yacobus
11:00-12:00	**Keynote II: Understanding Firmware Forensics using the Trusted Platform Module** Speaker: Dr. Ian Oliver; Nokia Bell Labs, Finland; Chair: Mourad Oussalah
12:00-13:00	**Keynote III: AI: Trustworthy or Not on Software Security** Speaker: Prof. Juha Röning, University of Oulu, Finland: Chair: Mourad Oussalah
13:00-14:00	Lunch & Poster session
14:00-14:30	Visit to the Virtual Reality Laboratory & 3D Scanning
14:30-15:00	**Invited Speech: Upcoming Global Initiative Report**
	Speaker: Thi Hoang , Chair: Panos Kostakos
15:00-16:30	**Session VI**
Tellus Stage	Chair: Gerhard Backfried
	Continuous Authentication of Smartphone Users via Swipes and Taps Analysis Anna Epishkina, Alina Garbuz and Konstantin Kogos
	Devising and Optimizing Crowd Control Strategies Using Agent- Based Modeling and Simulation Andrew Park, Ryan Ficocelli, Lee Patterson, Valerie Spicer, Herbert H. Tsang and Justin Song
	HOTSPOT: Crossing the Air-Gap Between Isolated PCs and Nearby Smartphones using Temperature Mordechai Guri
16:30-17:00	**Announcements & Closing Session**

Session I			
11:10-12:30	Tuesday, November 26, 2019	Venue: Tellus Stage	Chair: Panos Kostakos

Paper I Full

Identification and Detection of Human Trafficking Using Language Models

Zhu Jessica, Lin Li and Cara Jones

In this paper, we present a novel language model-based method for detecting both human trafficking ads and trafficking indicators. The proposed system leverages language models to learn language structures in adult service ads, automatically select a list of keyword features, and train a machine learning model to detect human trafficking ads. The method is interpretable and adaptable to changing keywords used by traffickers. We apply this method to the Trafficking-10k dataset and show that it achieves better results than the previous models that leverage both ad text and images for detection. Furthermore, we demonstrate that our system can be successfully applied to detect suspected human trafficking organizations and rank these organizations based on their risk scores. This method provides a powerful new capability for law enforcement to rapidly identify ads and organizations that are suspected of human trafficking and allow more proactive policing using data.

Paper II Full **moved to Wednesday session V*

A comparative study of clustering methods using word embeddings

Nikolaos Bastas, George Kalpakis, Theodora Tsikrika, Stefanos Vrochidisand Ioannis Kompatsiaris

Grouping large amounts of data is critical for various tasks, including the identification of content on a specific topic of interest (such as terrorism-related content) within a collection of material gathered from online sources. Various existing approaches typically extract relevant features using topic distributions and/or embedding methods, and subsequently apply clustering techniques in the derived representation space. In this work, we present a comparative study using Latent Dirichlet Allocation (LDA), Paragraph-Vector Distributed Bag-of-Words (PV-DBOW), and Paragraph-Vector Distributed Memory (PV-DM) models as representation methods, in conjunction with five traditional clustering algorithms, namely k-means, spherical kmeans, possibilistic fuzzy c-means, agglomerative clustering and NMF, on two publicly available and one proprietary datasets. Fifteen combinations are formed which are assessed using external clustering validity measures, such as Adjusted Mutual Information (AMI) and Adjusted Rand Index (ARI) against available ground-truth. Our results indicate that using PV-DBOW leads in general to better clustering performance in all datasets.

Paper III Full

Mining Security discussions in Suomi24

Eetu Haapamaki and Juho Mikkola, Mourad Oussalah

This study examines how social network-based approach can be applied in order to mine the security-oriented discussions in Suomi24 online forum. The approach employs a student survey questionnaire to collect a dictionary related to Finland national security. In subsequent analysis, the vocabulary terms are mapped to Suomi24 corpus in order to construct the associated social network analysis that quantifies the dependency among the various vocabulary terms. Especially, the analysis of the dynamic variation of the network topology would enable the decision-maker to devise appropriate communication scheme to maximize intervention in the public sphere and reach a wider audience. Besides, a parser that finds the keywords from VeRticalzed text data format is developed to aid the construction of the underlined social network.

Paper IV Full

Identifying deceptive reviews: feature exploration, model transferability and classification attack

Marianela Garcia Lozano and Johan Fernquist

The temptation to influence and sway public opinion most certainly increases with the growth of open online forums where anyone anonymously can express their views and opinions. Since online review sites are a popular venue for opinion influencing attacks, there is a need to automatically identify deceptive posts. The main focus of this work is on automatic identification of deceptive reviews, both positive and negative biased. With this objective, we build a deceptive review SVM based classification model and explore the performance impact of using different feature types (TF-IDF, word2vec, PCFG). Moreover, we study the transferability of trained classification models applied to review data sets of other types of products, and, the classifier robustness, i.e., the

accuracy impact, against attacks by stylometry obfuscation trough machine translation. Our findings show that i) we achieve an accuracy of over 90% using different feature types, ii) the trained classification models do not perform well when applied on other data sets containing reviews of different products, and iii) machine translation only slightly impacts the results and can not be used as a viable attack method.

Session II			
14:00-15:15	Tuesday, November 26, 2019	Venue: Tellus Stage	Chair: Mourad Oussalah

Paper I Full

Predicting the Offender: Frequency Beats Bayes

August Daniel Sutmuller, Mariëlle den Hengst, Ana Isabel Barros, Bob van der Vecht, Wouter Noordkamp and Pieter van Gelder

In this paper two Bayesian approaches and a frequency approach are compared on predicting offender output variables based on the input of crime scene and victim variables. The K2 algorithm, Naïve Bayes and frequency approach were trained to make the correct prediction using a database of 233 solved Dutch single offender/single victim homicide cases. The comparison between the approaches was made using the measures of overall prediction accuracy and confidence level analysis on 35 solved Dutch single offender/single victim homicide cases. Besides the comparison of the three approaches, the correct predicted nodes per output variable and the correct predicted nodes per validation case were analyzed to investigate whether the approaches could be used as a decision tool in practice to limit the incorporation of persons of interest into homicide investigations. The results of this study can be summarized as: the non-intelligent frequency approach shows similar or better results than the intelligent Bayesian approaches and the usability of the approaches as a decision tool to limit the number of persons of interest in homicide investigations should be questioned.

Paper II Full

Firearm Detection and Segmentation using an Ensemble of Semantic Neural Networks

Alexander Egiazarov, Vasileios Mavroeidis, Fabio Massimo Zennaro and Kamer Vishi

In recent years we have seen an upsurge in terror attacks around the world. Such attacks usually happen in public places with large crowds to cause the most damage possible and get the most attention. Even though surveillance cameras are assumed to be a powerful tool, their effect in preventing crime is far from clear due to either limitation in the ability of humans to vigilantly monitor video surveillance or for the simple reason that they are operating passively. In this paper, we present a weapon detection system based on an ensemble of semantic Convolutional Neural Networks that decomposes the problem of detecting and locating a weapon into a set of smaller problems concerned with the individual component parts of a weapon. This approach has computational and practical advantages: a set of simpler neural networks dedicated to specific tasks requires less computational resources and can be trained in parallel; the overall output of the system given by the aggregation of the outputs of individual networks can be tuned by a user to trade-off false positives and false negatives; finally, according to ensemble theory, the output of the overall system will be robust and reliable even in the presence of weak individual models. We evaluated our system running simulations aimed at assessing the accuracy of individual networks and the whole system. The results on synthetic data and real-world data are promising, and they suggest that our approach may have advantages compared to the monolithic approach based on a single deep convolutional neural network.

Paper III Full

Evaluation of Deep Learning Models for Ear Recognition Against Image Distortions

Susan El-Naggar and Thirimachos Bourlai ; [*proxy: Abhinay Pandya]*

Automated human authentication is becoming increasingly popular on a variety of daily activities, ranging from surveillance to commercial related applications. While there are many biometric modalities that can be used, ear recognition has earned its value if and when available to be captured. Ears demonstrate specific advantages over other competitors in an effort to identify cooperative and non-cooperative individuals in either controlled or challenging environments. The performance of ear recognition systems can be impacted by several factors, including standoff distance, ear pose angle, and ear image quality. While all three factors can degrade ear recognition performance, here we focus on the latter two using real data, and assess the standoff distance factor by synthetically generating blurry and noisy images to simulate longer distance ear images. Thus, in this work we are inspired by various studies in the literature that discuss the how and why challenging biometric images of different modalities impact the associated biometric system recognition. Specifically, we focus on how different ear image distortions and yaw pose angles affect the performance of various deep learning based ear recognition models. Our contributions are threefold. Firstly, we are using challenging ear dataset, with a wide range of yaw pose angles, to evaluate the ear recognition performance of various original ear matching approaches. Secondly, by examining multiple convolutional neural network (CNN) architectures and employing multiple techniques for the learning process, we determine the most efficient CNN-based ear recognition approach. Thirdly, we investigated the impact on

performance of a set of ear recognition CNN models in the presence of multiple image degradation factors, including variations of blurriness, additive noise, brightness and contrast.

Paper IV Full

Prototype and Analytics for Discovery and Exploitation of Threat Networks on Social Media

Olga Simek, Danelle Shah and Andrew Heier

Identifying and profiling threat actors are high priority tasks for a number of governmental organizations. These threat actors may operate actively, using the Internet to promote propaganda, recruit new members, or exert command and control over their networks. Alternatively, threat actors may operate passively, demonstrating operational security awareness online while using their Internet presence to gather information they need to pose an offline physical threat. This paper presents a flexible new prototype system that allows analysts to automatically detect, monitor and characterize threat actors and their networks using publicly available information. The proposed prototype system fills a need in the intelligence community for a capability to automate manual construction and analysis of online threat networks. Leveraging graph sampling approaches, we perform targeted data collection of extremist social media accounts and their networks. We design and incorporate new algorithms for role classification and radicalization detection using insights from social science literature of extremism. Additionally, we develop and implement analytics to facilitate monitoring the dynamic social networks over time. The prototype also incorporates several novel machine learning algorithms for threat actor discovery and characterization, such as classification of user posts into discourse categories, user post summaries and gender prediction.

Session III			
16:30-17:30	Tuesday, November 26, 2019	Venue: Tellus Stage	Chair: Johan Fernquist

Paper I Short

Characterization of Disinformation Networks Using Graph Embeddings and Opinion Mining

Olga Simek, Alyssa Mensch, Lin Li and Charlie Dagli

The large-scale growth of worldwide social media networks is built upon their essential features of universal access, immediacy, and power to communicate with and influence others. These key design features have also created a potent new medium and an enabling technology for disinformation and propaganda. We present a novel approach for characterizing disinformation networks on social media and distinguishing between different network roles using graph embeddings and hierarchical clustering. In addition, using topic filtering, we correlate the node characterization results with proxy opinion estimates. We plan to study opinion dynamics using signal processing on graphs approaches using longer-timescale social media datasets with the goal to model and infer influence among users in social media networks.

Paper II Short

Semi-Automatic Geometric Normalization of Profile Faces using Random Sample Consensus Feature Matching

Justin Romeo and Thirimachos Bourlai

This paper proposes a correlation point matching approach, i.e. an efficient methodology for applying geometric normalization for profile face images. This method is used to increase accuracy without imposing a significant increase in face matching computational time when using different feature descriptors. In our work, several such descriptors are tested to compare the accuracy with which low level facial features (edges), useful for profile face image geometric normalization, are extracted. Hence, we determined the most efficient normalization approach that does not substantially increase computational time. Experimental results show that the use of eigenvalues produces a higher than average edge point count, while having a lower increase in computational complexity compared to other similar algorithms. Then, the extracted features are matched using the random sample consensus algorithm (RANSAC). Next, the rotational angles between the pairs of features are calculated and averaged to yield the angle of rotation necessary to achieve a proper profile face image normalization representation. After applying our proposed approach to a deep learning-based profile face recognition algorithm, an increase of 7.2% accuracy is achieved when compared to the baseline (non-normalized profile faces). To the best of our knowledge, this is the first time in the open literature that the impact of automated profile face normalization is being investigated to improve deep learning-based profile face matching performance.

Paper III Short

Remote KYC: Attacks and Counter-measures

Marc Pic, Gaël Mahfoudi and Anis Trabelsi

Onboarding of new customers is a sensitive task for various services, like Banks who have to follow the Know Your Customer (KYC) rules. Mobile Onboarding Applications or KYC by Streaming are expanding rapidly to provide this capacity at home. Unfortunately, this leaves the authentication tools in the hand of end-users, allowing the attacker to directly tamper the video stream. With the rise of new digital face manipulation technologies, traditional face spoofing attacks such as presentation attacks or replay attacks should not be the only one to be considered. A new kind of face spoofing attacks (i.e. digital face spoofing) needs to be studied carefully. In this paper, we analyze those new kinds of attacks and propose a method to secure identity documents against both the traditional attacks and the new ones.

Paper IV Short

Privacy preserving sentiment analysis on multiple edge data streams with Apache NiFi

Abhinay Pandya, Panos Kostakos, Hassan Mahmood, Marta Cortes, Ekaterina Gilman, Mourad Oussalah and Susanna Pirttikangas

Sentiment analysis, also known as opinion mining, plays a big role in both private and public sector Business Intelligence (BI); it attempts to improve public and customer experience. Nevertheless, de-identified sentiment scores from public social media posts can compromise individual privacy due to their vulnerability to record linkage attacks. Established privacy-preserving methods like k-anonymity, l-diversity and t-closeness are offline models exclusively designed for data at rest. Recently, a number of online anonymization algorithms (CASTLE, SKY, SWAF) have been proposed to complement the functional requirements of streaming applications, but without open-source implementation. In this paper, we present a reusable Apache NiFi dataflow that buffers tweets from multiple edge devices and performs anonymized sentiment analysis in real-time, using randomization. The solution can be easily adapted to suit different scenarios, enabling researchers to deploy custom anonymization algorithms.

Paper V Short

Crime Prediction Using Hotel Reviews?

Panos Kostakos, Somkiadcharoen Robroo, Bofan Lin and Mourad Oussalah

Can hotel reviews be used as a proxy for predicting crime hotspots? Domain knowledge indicates that hotels are crime attractors, and therefore, hotel guests might be reliable “human crime sensors”. In order to assess this heuristic, we propose a novel method by mapping actual crime events into hotel reviews from London, using spatial clustering and sentiment feedback. Preliminary findings indicate that sentiment scores from hotel reviews are inversely correlated with crime intensity. Hotels with positive reviews are more likely to be adjacent to crime hotspots, and vice versa. One possible explanation for this counterintuitive finding that the review data are not mapped against specific crime types, and thus the crime data capture mostly police visibility on the site. More research and domain knowledge are needed to establish the strength of hotel reviews as a proxy for crime prediction.

Session IV			
08:30-10:00	Wednesday, November 27, 2019	Venue: Tellus Stage	Chair: Mordechair Guri

Paper I Full

A model of quantifying social relationships

Disa Sariola

This article proposes a mathematical model for quantifying relationships between agents within a network based on their similarity, dissimilarity, level of friendship, group and activity status of the agent. We propose a set of functions to facilitate quantifying social dynamics. Our functions cover the comparison of an agent with group and comparing a group with groups based on their set of attributes. We also propose a model of comparison for agent vs. agent based on their attributes, features and the likelihood of attribute similarity between agents. The model employs a method of determining connection probabilities between nodes in order to find hidden connections between agents. We build on existing work in the study of social networks.

Paper II Full

Extracting Account Attributes for Analyzing Influence on Twitter

Lisa Kaati, Johan Fernquist, Fredrik Johansson and Ola Svenonius

The last years has witnessed a surge of auto-generated content on social media. While many uses are legitimate, bots have also been deployed in influence operations to manipulate election results, affect public opinion in a desired direction, or to divert attention from a specific event or phenomenon. Today, many approaches exist to automatically identify bot-like behaviour in order to curb illegitimate influence operations. While progress has been made, existing models are exceedingly complex and nontransparent, rendering validation and model testing difficult. We present a transparent and parsimonious method to study influence operations on Twitter. We define nine different attributes that can be used to describe and reason about different characteristics of a Twitter account. The attributes can be used to group accounts that have similar characteristics and the result can be used to identify accounts that are likely to be used to influence public opinion. The method has been tested on a Twitter data set consisting of 66,000 accounts. Clustering the accounts based on the proposed features show promising results for separating between different groups of reference accounts.

Paper III Full

Statistical Analysis of Identity Risk of Exposure and Cost Using the Ecosystem of Identity Attributes

Chia-Ju Chen, Razieh Nokhbeh Zaeem and Suzanne Barber

Personally Identifiable Information (PII) is often called the "currency of the Internet" as identity assets are collected, shared, sold, and used for almost every transaction on the Internet. PII is used for all types of applications from access control to credit score calculations to targeted advertising. Every market sector relies on PII to know and authenticate their customers and their employees. With so many businesses and government agencies relying on PII to make important decisions and so many people being asked to share personal data, it is critical to better understand the fundamentals of identity to protect it and responsibly use it. Previously developed comprehensive Identity Ecosystem utilizes graphs to model PII assets and their relationships and is powered by empirical data from almost 6,000 real-world identity theft and fraud news reports to populate the UT CID Identity Ecosystem. We obtained UT CID Identity Ecosystem from its authors to analyze using graph theory. We report numerous novel statistics using identity asset content, structure, value, accessibility, and impact. Our work sheds light on how identity is used and paves the way for improving identity protection.

Paper IV Full

Attack Hypothesis Generation

Aviad Elitzur, Rami Puzis and Polina Zilberman

In recent years, the perpetrators of cyber-attacks have been playing a dynamic cat and mouse game with cybersecurity analysts who try to trace the attack and reconstruct the attack steps. While analysts rely on alert correlations, machine learning, and advanced visualizations in order to come up with sound attack hypotheses, they primarily rely on their knowledge and experience. Cyber Threat Intelligence (CTI) on past similar attacks may help with attack reconstruction by providing a deeper understanding of the tools and attack patterns used by attackers. In this paper, we present the Attack Hypothesis Generator (AHG) which takes advantage of a knowledge graph derived from threat intelligence in order to generate hypotheses regarding attacks that may be present in an organizational network. Based on five recommendation algorithms we have developed and preliminary analysis provided by a security analyst, AHG provides an attack hypothesis comprised of yet unobserved attack patterns and tools presumed to have been used by the attacker. The proposed algorithms can help security analysts by improving attack reconstruction and proposing new directions for investigation. Experiments show that when implemented with the MITRE ATT&CK knowledge graph, our algorithms can significantly increase the accuracy of the analyst's preliminary analysis.

Session V			
10:15-11:00	Wednesday, November 27, 2019	Venue: Tellus Stage	Chair: Panos Kostakos

Paper I Poster

Secure exchange of Information for all actors involved in MLAs (EIOs for Europe) and police cooperation

Fabrizia Bemer

The EIO is an important contribution to the topic of the conference, because security informatics is strictly related to the EIO in the way the transmission occurs between authorities.

Paper I Poster

Timing Covert Channels Detection Cases via Machine Learning

Anna Epishkina, Mikhail Finoshin, Konstantin Kogos and Aleksandra Yazykova

Currently, packet data networks are widespread. Their architectural features allow constructing covert channels that are able to transmit covert data under the conditions of using standard protection measures. However, encryption or packets length normalization, leave the possibility for an intruder to transfer covert data via timing covert channels (TCCs). In turn, inter-packet delay (IPD) normalization leads to reducing communication channel capacity. Detection is an alternative countermeasure. At the present time, detection methods based on machine learning are widely studied. The complexity of TCCs detection based on machine learning depends on the availability of traffic samples, and on the possibility of an intruder to change covert channels parameters. In the current work, we explore the cases of TCCs detection via machine learning and study the possibility to implement learning machines algorithms for detecting TCCs under conditions of varying covert channel characteristics: flow capacity and encoding scheme.

Paper I Poster

Moving Target Defense (MTD) as a Cyber Security Measure

Mordechai Guri, Yuval Elovici and Dov Shirtz

Information Communication Technologies (ICT) environments are built as static configurations. Some of the reasons for having such configurations are complexity—in that modern information systems are considered to be complex systems—as well as the need to ease maintenance, to support rapid change implementation and change management, to support rapid failure management, and so on. Therefore, in order to reduce the organizational costs and efforts, an organization prefers static configurations or at least one with minimal changes. However, from the perspective of information security and cyber security, such a static environment eases adversarial efforts to penetrate the information systems. In this paper we overview the set of Moving Target Defense (MTD) methodologies, policies, standards, concepts and remedies that tries to eliminate or to minimize the probability that an adversarial attack over organizational information systems will occur.

Paper I Poster

Mobile user authentication using keystroke dynamics

Anna Epishkina, Konstantin Kogos and Daria Frolova

Behavioral biometrics identifies individuals according to their unique way of interacting with computer devices. Keystroke dynamics can be used to identify people, and it can replace the second factor in two-factor authentication. This paper presents a keystroke dynamics biometric system for user authentication in mobile devices. We propose to use data from sensors of motion and position as features for the biometric system to improve the quality of user recognition. The proposed novel model combines different anomaly detection methods (distance-based and density-based) in an ensemble. We achieved the average EER of 8.0%. Our model has a retraining module that updates the keystroke dynamics template of a user each time after a successful authentication in the system. All the process of training and retraining a model and making a decision is made directly on a mobile device using our mobile application, as well as keystroke data is stored on a device.

Paper II Poster

Analysis of Vancouver Crime and Census Data Using Various Machine Learning Algorithms

Kyle Behiels, Andrew Park, Justin Song, Valerie Spicer and Herbert H. Tsang

In recent years mass storage of criminal data has become a common practice for many law enforcement agencies around the world. As these data sets grow, so does the amount of potential knowledge that we can gain from analyzing these data. When combined with census data and the open crime data set of Vancouver (non-violent crimes from between 2003 and 2019), we have a unique opportunity to explore the spatio-temporal snapshot of crime rate and causation. The resulting data lends itself extremely well to the application of various machine learning algorithms. In this paper, we employs various machine learning algorithms to show the attributes correlation with most strongly with both high and low crime rates.

Paper I Poster

The Development of Lone Wolf Terrorism in Southeast Asia

Pujo Widodo, Tri Legionosuko and David Yacobus

Since the development of Islam in the 13th century in Southeast Asia, the traders who came from Arabia and Persia initially spread the religion using peaceful means rather than by violence. However, the current condition of the development of Islam in Southeast Asia are stained by acts of terrors carried out by various Lone Wolf where some of them have experienced violent jihad in other countries such as Iraq and Syria. Their losses in the battlefield forced them to return to their countries as returnees. These Lone Wolf returnees problem has quickly become a worldwide concern, especially with various evidence that they are related to recruitment and suicide bomber activities in Southeast Asia. As the results of social media propaganda on the Internet they obtain new followers such as the support of young people from Thailand, Malaysia, the Philippines and Indonesia. The purpose of this study is to analyze and uncover the development of Lone Wolf Terrorism in Southeast Asia. The results of this study include: First, identifying the forms of threats of Lone Wolf Terrorism in Southeast Asia which are divided into three types of threats, namely the first, second, and third generations of terror. Second, revealing the Lone Wolf Terrorism network on the Internet that is filled with propaganda to attract sympathy of younger generation to join the Al-Qaeda, ISIS, and Islamic State (IS) networks. Third, Analyzing the IS Terror Network in Southeast Asia by revealing the activities and organizational structure of Al-Qaeda, ISIS, and IS.

Session VI			
15:00-16:30	Wednesday, November 27, 2019	Venue: Tellus Stage	Chair: Gerhard Backfried

Paper I Full

Continuous Authentication of Smartphone Users via Swipes and Taps Analysis

Anna Epishkina, Konstantin Kogos and Alina Garbuz

Nowadays, smartphones are used for getting access to sensitive and private data. As a result, we need an authentication system that will provide smartphones with additional security and at the same time will not cause annoyance to users. Existing authentication mechanisms provide just a one-time user verification and do not perform re-authentication in the process of further interaction. In this paper, we present a continuous user authentication system based on user's interaction with the touchscreen in conjunction with micromovements, performed by smartphones at the same time. We consider two of the most common types of gestures performed by users (vertical swipes up and down, and taps). The novelty of our approach is that swipes and taps are both analyzed to provide continuous authentication. Swipes are informative gestures, while taps are the most common gestures. This way, we aim to reduce the time of impostors' detection. The proposed scheme collects data from the touchscreen and multiple 3-dimensional sensors integrated in all modern smartphones. We use One-Class Support Vector Machine (OSVM) algorithm to get a model of a legitimate user. The obtained results show that the proposed scheme of continuous authentication can improve smartphone security.

Paper II Full

HOTSPOT: Crossing the Air-Gap Between Isolated PCs and Nearby Smartphones Using Temperature

Mordechai Guri

Air-gapped computers are hermetically isolated from the Internet to eliminate any means of information leakage. In this paper we present HOTSPOT - a new type of airgap crossing technique. Signals can be sent secretly from airgapped computers to nearby smartphones and then on to the Internet - in the form of thermal pings. The thermal signals are generated by the CPUs and GPUs and intercepted by a nearby smartphone. We examine this covert channel and discuss other work in the field of air-gap covert communication channels. We present technical background and describe thermal sensing in modern smartphones. We implement a transmitter on the computer side and a receiver Android App on the smartphone side, and discuss the implementation details. We evaluate the covert channel and tested it in a typical work place. Our results show that it possible to send covert signals from air-gapped PCs to the attacker on the Internet through the thermal pings. We also propose countermeasures for this type of covert channel which has thus far been overlooked.

Paper III Full

Devising and Optimizing Crowd Control Strategies Using Agent-Based Modeling and Simulation

Andrew Park, Ryan Ficocelli, Lee Patterson, Valerie Spicer, Herbert H. Tsang and Justin Song

Sporting events can attract large crowds who are capable of spurring on their teams. Emotionally charged crowds have a potential to become violent and disruptive, damaging and destroying public properties. Managing and controlling riotous crowds is an important responsibility for police officersto keep public order and safety. Devising and optimizing crowd management strategies is difficult without the knowledge of the scale and situations of the crowd in advance. This paper presents a three-dimensional (3D) simulation framework that simulates a riot and the police response to the riot. The simulation framework is based on agent-based modeling and simulation, consisting of crowd agents, police agents, and transit systems. This study focuses on a specific crowd control strategy: pushing the crowd to the public transit. The police officers in this simulation form police lines which move towards targeted positions pushing the crowd towards the position. In order to optimally disperse the crowd, the police lines move towards public access stations in the transit systems, coercing the crowd to the vicinity of the public transit and containing them there. By directing the crowd into the area where public transit picks up passengers, the crowd would dissipate as crowd occupants got on the transit to leave. The 2011 Vancouver Stanley Cup riot is used in the simulation as a case study. The result of the actual crowd control of the event and that of the crowd control simulation are compared. The framework of this study can be used for other sporting or large crowd events at various locations and for devising different crowd control planning strategies.

University of Oulu, Linnanmaa Campus, Oulu, Finland

Conference venue address: Tellus Arena, Pentti Kaiteran katu 1, 90570 Oulu

EISIC 2019 is hosted by **University of Oulu, in Oulu, Finland**. The University of Oulu (UOulu) is among the largest universities in Finland with 16 000 students and 2800 staff members working in 8 faculties. UOulu is an international research and innovation university engaged in multidisciplinary basic research and academic education. The university encompasses eight fields of study: Humanities, Education, Economics and Business, Science, Medicine, Dentistry, Health Sciences, and Technology. UOulu is an associate member of the EIT Digital, EIT Raw Materials, BBI Bio-based Industries Consortium, among others, and has been involved in the EU R&D Framework programs since FP4, having participated in more than 250 EU projects and networks.
EISIC 2019 is hosted by two Research Units at the Faculty of Information Technology and Electrical Engineering (ITEE): the Center for Ubiquitous Computing -UBICOMP (http://ubicomp.oulu.fi/), and the Center for Machine Vision and Signal Analysis (CMVS). In Academy of Finland's report "State of scientific research 2018," the ITEE is ranked in scientific impact (Top-10 index) the 1st among the Finnish universities in the field of ICT and electrical engineering, with the UBICOMP Center reporting an annual budget of €2.6 million, of which 70% is externally competed. The UBICOMP Center is involved, among others, in multiple Academy of Finland, Business Finland, FP7 and EU H2020 projects, featuring renowned national & international academic & non-academic institutions, and is involved in the cutting-edge 6Genesis Flagship Program. The Center for Machine Vision and Signal Analysis (CMVS) combines the expertise of University of Oulu computer vision and biosignal analysis scientists, with extensive international collaboration networks. CMVS has achieved ground-breaking research results in many areas of its activity, including texture analysis, facial image analysis, 3D computer vision, energy-efficient architectures for embedded systems, and biomedical engineering.

EISIC 2019 will be held at Tellus Arena (https://www.oulu.fi/tellusarena/venue), a well-equipped, professional venue for large-scale events, designed to foster collaboration and promote inspiring ideas for the tomorrow.

Aerial view of the Oulu University, Linnanmaa Campus
(Campus map: https://www.oulu.fi/sites/default/files/content/Kartta_Linnanmaa_Map_A3_14.pdf)

Getting to the Campus

Transportation:

Bus transportation to and from the University and also to/from Dinner site will be available for both days of the conference:

TRANSPORTATION DETAILS:

26th November (Tuesday)

i) first pick up point at Scandic Hotel, at Saaristonkatu 4, Oulu (in front of Finnkino Plaza, at 7:40 (bus waits there for about 9 minutes);
ii) second pickup point: Torikatu 10-time of arrival- aprox. 7:50 am (bus waits there for 10 minutes)
iii) Time of departure from City Centre to University of Oulu -entrance E- at exactly 8:00 am.
iv) **Please note**- the bus should arrive at the university at about **8:15 am**. We will then guide you to the registration desk, by the entrance of the conference venue.
v) bus picks up participants from University at 17:45 to the City Centre [drop off points, the same as the pick-up points, first Torikatu 10, and then Saaristonkatu 4).
vi) You can use this time to drop of your gear at your respective hotels and/or take a walk in the City Centre, before we head out to dinner.
vii) Bus picks up participants at 18:45 (from Saaristonkatu 4), then at 18:55 from Torikatu 10;
viii) Bus departs at 19:05 to Nallikari Restaurant (Nallikarinranta 15, FI-90510 Oulu; https://ravintolanallikari.fi/en/contact)
ix) Bus picks up participants from Nallikari Restaurant Oulu at around 23:30 to the city center - drop-off point 1: Torikatu 10; drop-off point 2: Saaristonkatu 4

27th November (Wednesday):

i) bus departs from Oulu city center at 8:00 am - to the University of Oulu (entrance E) [same schedule and pick-up points as in previous day]-
ii) at 17:15 bus picks up participants from the University to the Oulu city centre (drop off point 1: Torikatu 10), and drop-off point 2: Saaristonkatu 4, Oulu).

Please make sure that you are as punctual as possible, as to avoid any delays in the overall programme.

Please use google maps to accurately find the pick-up/drop-off points;

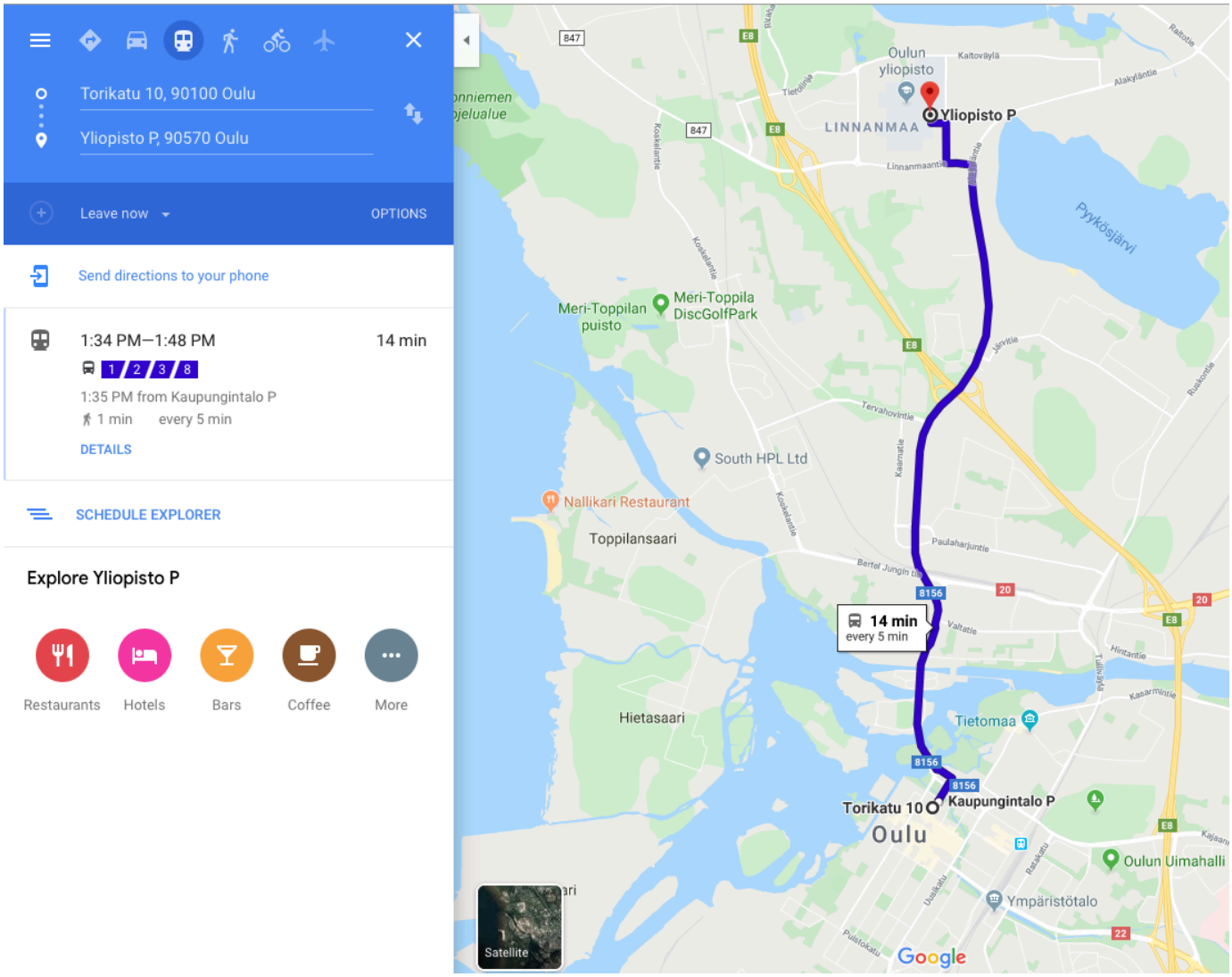
In case you miss the bus and/or choose an alternative means of transportation:

By bus: Buses coming from and to the University are numbers 1, 2, 3 and 8. You can buy a single ticket from the driver as you get on the bus. Please have small change ready as drivers only accept cash (€4 per ticket). You can check for more information about routes and timetables at https://www.oulunjoukkoliikenne.fi/routes-and-timetables

By taxi: You can get a taxi from a taxi rank or by phone. Please ask the driver to drop you off at the University of Oulu (Linnanmaa campus) near the bus stop, or nearby Entrance E (call a taxi: +358 600 30081).

Oulu University [in finnish: Oulun Yliopisto] (Linnanmaa Campus) Google maps location:

https://www.google.fi/maps/dir/65.0584879,25.4698717//@65.05923,25.465305,1182m/data=!3m1!1e3



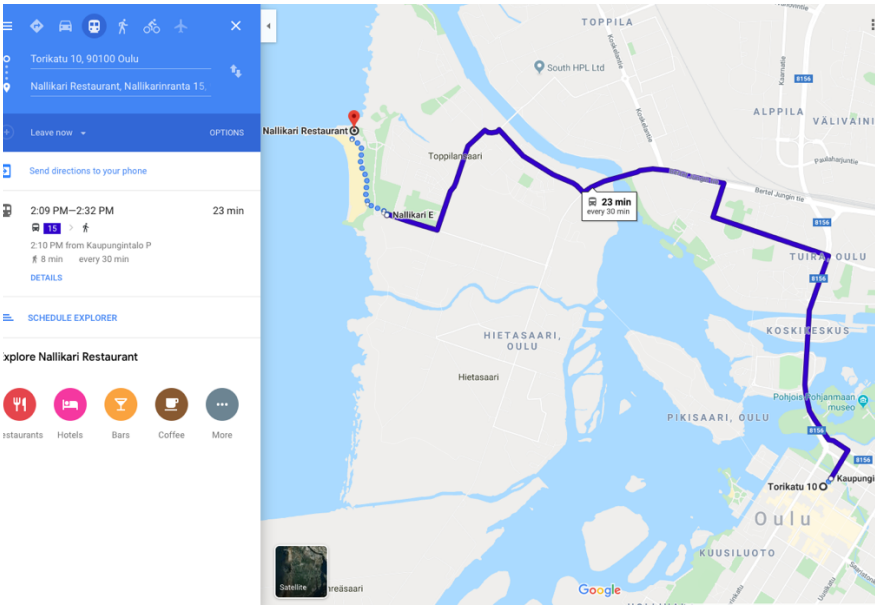
Getting to Nallikari Restaurant

As mentioned before, we will have a bus transporting all conference participants to the dinner Venue, as follows:

i) Bus picks up participants at 18:45 (from Saaristonkatu 4), then at 18:55 from Torikatu 10;
ii) Bus departs at 19:05 to Nallikari Restaurant (Nallikarinranta 15, FI-90510 Oulu; https://ravintolanallikari.fi/en/contact)
iii) Bus picks up participants from Nallikari Restaurant Oulu at around 23:30 to the city center - drop-off point 1: Torikatu 10; drop-off point 2: Saaristonkatu 4

The Nallikari Restaurant Restaurant Nallikari was originally designed by architect Risto Harju in 1975 as a venue for parties and restaurant dining. After various incarnations, it has been given a new lease of life. Restaurant Nallikari is open year-round, offering a great, relaxed place to eat and enjoy life on the beach.

Outside view of Nallikari Restaurant and its famed Jacuzzi Tower.



Information for Presenters

Full papers are allocated approximately 30 minutes while Short papers 20 minutes including a question-and-answer period after the presentation. The Session Chair introduces the speakers and moderates the question-and-answer period. A basic audio-visual installation (speakers, projection screen, data projector and computer) will be available in the room. Please inform the local area chair prior to the start of the conference if you must use your own laptop during your presentation.

Poster Session

Posters will be hosted in the Tellus Arena area during the coffee breaks. The physical dimensions of the poster are A0 portrait (84cm x119cm/ 33in x 47in). Individual poster stands (120cm x 150 cm) will be made available on site.

Photographs

Photographs are allowed inside and outside the conference complex and in the area around the University of Oulu, Linnanmaa Campus.

Smoking Policy

Smoking is not permitted inside the areas of the conference. Smokers can be accommodated outside the conference complex.

Mobile Phone Policy

As a courtesy to speakers and attendees please refrain from using mobile phones during the keynote speeches and presentations. Set your mobile phone silent mode before entering a session and leave the session if you receive a call.

WiFi

Free WiFi will be available to conference participants in the conference area and throughout all campus (panoulu wi-fi) and also at the Dinner/social gathering venue (further information available from the site). Further information can be obtained from the registration desk available in Tellus Arena area, opened for the two conference days.

European Intelligence and Security Informatics Conference (EISIC) 2019

November 26-27, 2019,

University of Oulu, Oulu, Finland http://www.eisic.org

The Premier European Conference on Counterterrorism and Criminology

Designed by Panagiotis Karampelas, EISIC 2019