European Intelligence & Security Informatics Conference

The Premier European Conference on Counterterrorism and Criminology

EISIC 2018

Karlskrona, Sweden, October 24-25, 2018 http://www.eisic.org

Conference Program

EISIC 2018

Conference Organizer and Sponsor

Academic Sponsors

Technical co-sponsorship

Conference Secretariat

Conference registration takes place at the Conference Secretariat located at the lobby of the Conference Center of Blekinge Institute of Technology, during the following days and hours:

Wednesday	9:00 – 16:π0
Thursday	8:30 – 16:30

The registration fee includes:

- One lunch and two coffee breaks per conference day
- One ticket for the Conference Dinner held on Wednesday 24th of October, 2018 at the Naval Museum.
- Conference bag with the conference program, proceedings, conference gifts, etc.

Table of Contents

Honorary General Chair

Panagiotis Karampelas,
Hellenic Air Force Academy, Greece

General Chairs

Martin Boldt,
Blekinge Institute of Technology, Sweden

Anton Borg,
Blekinge Institute of Technology, Sweden

Program Chair

Joel Brynielsson,
KTH Royal Institute of Technology, Sweden

Advisory Board

Lisa Kaati,
FOI Swedish Defence Research Agency, Sweden

Margit Pohl,
TU Wien, Austria

Emelie Nilsson,
Danish National Police, Denmark

Yanfang (Fanny) Ye,
West Virginia University, USA

Thirimachos Bourlai,
West Virginia University, USA

Ioanna Lekea,
Hellenic Air Force Academy, Greece

Local Arrangement Chair

Fredrik Erlandsson,
Blekinge Institute of Technology, Sweden

EISIC 2018 – Program Committee

Mohd Helmy Abd Wahab
Universiti Tun Hussein Onn Malaysia, Malaysia

Mohamed Faouzi Atig
Uppsala University, Sweden

Igor Bernik
University of Maribor, Slovenia

Hervé Borrion
University College London, United Kingdom

Thirimachos Bourlai
West Virginia University, USA

Egon L. van den Broek
Utrecht University, Netherlands

Antwan D. Clark
Johns Hopkins University, USA

Shamal Faily
Bournemouth University, United Kingdom

Ulrik Franke
RISE SICS Swedish Institute of Computer Science, Sweden

Marianela García Lozano
FOI Swedish Defence Research Agency, Sweden

Shravan Garlapati
Virginia Tech, USA

Bénédicte Goujon
Thales Research & Technology, France

Gunther P. Grasemann
Fraunhofer IOSB, Germany

Richard Göbel
Hof University, Germany

Mohammad Hammoudeh
Manchester Metropolitan University, United Kingdom

Liangxiu Han
Manchester Metropolitan University, United Kingdom

Chris Hankin
Imperial College London, United Kingdom

Johan de Heer
Thales Research & Technology, Netherlands

Thomas J. Holt
Michigan State University, USA

Nils Jensen
Ostfalia University of Applied Sciences, Germany

Borka Jerman Blažič
Jožef Stefan Institute, Slovenia

Fredrik Johansson
FOI Swedish Defence Research Agency, Sweden

Panagiotis Karampelas
Hellenic Air Force Academy, Greece

Sergii Kavun
Kharkiv University of Technology, Ukraine

Jeroen Keppens
King's College London, United Kingdom

Latifur Khan
University of Texas at Dallas, USA

Stewart James Kowalski
Norwegian University of Science and Technology, Norway

Ioanna Lekea
Hellenic Air Force Academy, Greece

Richard May
Pacific Northwest National Laboratory, USA

Luca Mazzola
Lucerne University of Applied Sciences and Arts, Switzerland

Antonis Mouhtaropoulos
University of Warwick, United Kingdom

Rasmus Petersen
Software Improvement Group, Denmark

Jakub Piskorski
European Commission Joint Research Centre, Italy

Margit Pohl
TU Wien, Austria

Galina Rogova
State University of New York at Buffalo, USA

Virgilijus Sakalauskas
Vilnius University, Lithuania

Günter Schumacher
European Commission Joint Research Centre, Italy

Johan Sigholm
Harvard University, USA

Gerardo I. Simari
Universidad Nacional del Sur, Argentina

Yannis Stamatiou
University of Patras, Greece

Jerzy Surma
Warsaw School of Economics, Poland

Muhammad Adnan Tariq
KTH Royal Institute of Technology, Sweden

Theodora Tsikrika
Information Technologies Institute, CERTH, Greece

Stefan Varga
KTH Royal Institute of Technology, Sweden

Leon Wang
National University of Kaohsiung, Taiwan

Uffe Kock Wiil
University of Southern Denmark, Denmark

Yanfang Ye
West Virginia University, USA

Daniel Zeng
University of Arizona, USA

Yuchen Zhou
Palo Alto Networks, USA

EISIC 2018 – Message from the General Chairs

We are happy to welcome you and the European Intelligence and Security Informatics Conference (EISIC) to Karlskrona, Sweden. 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 2018 we aim to maintain the high standard, and we hope that you will enjoy the conference.

Karlskrona is Sweden's only baroque city, founded in 1680 when the Royal Swedish Navy was relocated from the Stockholm area. We hope that you will enjoy this beautiful city. We are also proud to present our distinguished keynote speakers: Professor Dieter Gollmann (Hamburg University of Technology and Nanyang Technological University) and Dr. Vidya Narayanan (Oxford Internet Institute at Oxford University). In addition to these two distinguished speakers, we will also enjoy presentations by two invited speakers: Mr. Mikael Lagström (TrueSec) and Sergeant Major Freddy Widecrantz (Naval Warfare Centre, Swedish Armed Forces).

The conference dinner will take place at the Naval Museum in Karlskrona, which is also the location of the social event. For those of you who have the time to discover Karlskrona on your own, there are many possibilities. In particular, we recommend paying a visit to the central square which is the largest square in Scandinavia. Further, central Karlskrona still contains many of the baroque buildings from its founding, as well as a beautiful archipelago.

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 2018. 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, Fredrik Erlandsson for helping us with the local arrangements, as well as Lena Marminge, Camilla Johansson and Eva-Lotta Runesson for their help with the conference budget and other economy-related tasks. We would also like to thank Blekinge Institute of Technology and the IT department for hosting us.

As we now inaugurate the eighth EISIC meeting, we wish to welcome you to Karlskrona and we hope that you will enjoy EISIC 2018 and your stay in Sweden.

Martin Boldt, Blekinge Institute of Technology, Sweden
Anton Borg, Blekinge Institute of Technology, Sweden

EISIC 2018 – 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 2018 European Intelligence and Security Informatics Conference (EISIC 2018) is the eighth EISIC meeting to be organized by the European ISI community. During 2011–2017 the EISIC meetings have been held annually in Athens, Greece; Odense, Denmark; Uppsala, Sweden; The Hague, the Netherlands; Manchester, United Kingdom; Uppsala, Sweden; and Athens, Greece. EISIC 2018 is organized by Blekinge Institute of Technology, and is scientifically sponsored by the Royal Institute of Technology, Sweden and the Swedish Defence Research Agency, and has also 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 sincere gratitude to these sponsors.

EISIC 2018 received 31 submissions in total, and accepted 36% 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, and EISIC 2017 received 51 submissions and accepted 31% 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 sincere gratitude to all authors for contributing their work.

To distinguish between the submitted papers and guide the acceptance decisions, all papers have been carefully read and analyzed by at least three independent experts. Representing all the different flavors of the broad ISI field and coming from 19 different countries, the 49 program committee members generously provided 96 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

EISIC 2018 – Program at a Glance

Wednesday, October 24, 2018		
09:00-10:00	Registration/Coffee	
10:00-10:30	**Welcome Session** General Chairs / Vice Chancellor / Program Chair	
10:30-11:30	**Keynote: IoT Security – Viewed from the Application Layer** Speaker: Prof. Dieter Gollmann	Room: **J1620**
11:30-12:30	Lunch	Restaurant in J building
12:30-14:00	**Session I**	Room: **J1620**
14:00-14:30	Coffee break	Outside room J1610
14:30-16:00	**Session II**	Room: **J1620**
16:00-16:10	Short break	
16:10-16:n0	**Invited Speech: The Naval Base, a world heritage of information collection threats** Speaker: SgtMaj Freddy Widecrantz	Room: **J1620**
18:00-21:30	**Social Event & Conference Dinner**: Naval Museum	

Thursday, October 25, 2018		
08:30-09:00	Registration	
09:00-10:00	**Keynote: Computational Propaganda and Misinformation Campaigns during Important Events in Public Life** Speaker: Dr. Vidya Narayanan	Room: **J1620**
10:00-10:15	Short Break	
10:15-12:00	**Session III**	Room: **J1620**
12:00-13:00	Lunch Break	Restaurant in J building
13:00-13:45	**Invited Speech: Hands-on insights from the "Cloud hopper" incident that hit companies worldwide in 2017** Speaker: Mikael Lagström	Room: **J1620**
13:45-14:00	Short break	
14:00-15:40	**Session IV**	Room: **J1620**
15:40-15:50	**Closing Session**	Room: **J1620**
15:50-16:30	Coffee	Outside room J1610

Prof. Dieter Gollmann
Hamburg University of Technology, Germany
Nanyang Technological University, Singapore

10:30-11:30 Wednesday, 24 October 2018 Room: J1620 Chair: Martin Boldt

"IoT Security – Viewed from the Application Layer"

Abstract

If one does not get beyond the "I" in "IoT", IoT security might appear just a specific internetworking security challenge. Network and communication security are well established areas. IoT can then serve the purpose of re-selling old ideas in a new disguise, be it as products, research proposals, or research papers. This talk will take a closer look at the "T" and discuss some of the security challenges that arise when things are influenced by and influence the physical environment around them.

Bio

Professor Dieter Gollmann received his Dipl.-Ing. in Engineering Mathematics (1979) and Dr.tech. (1984) from the University of Linz, Austria in the Department for System Science. He earned the Dr. habil. at the University of Karlsruhe, Germany, where he was awarded the 'venia legendi' for Computer Science in 1991. He was a Lecturer in Computer Science at Royal Holloway, University of London, and rejoined Royal Holloway later in 1990, where he was the first Course Director of the MSc in Information Security. He's still giving guest lectures in Royal Holloway. He joined Microsoft Research in Cambridge in 1998. Then in 2003, he took the chair for Security in Distributed Applications at Hamburg University of Technology, Germany. He has contributed to national and European projects in the areas of dependable communications and computing.

Dr. Vidya Narayanan
Oxford Internet Institute at Oxford University

09:00-10:00 Thursday, 25 October 2018 Room: J1620 Chair: Lisa Kaati

"Computational Propaganda and Misinformation Campaigns during Important Events in Public Life"

Abstract

Social media provides a platform for active public participation in political discourse. However, recently we have witnessed attempts to influence voter preferences using misinformation campaigns using social media platforms both by domestic and foreign actors. We have also seen coordinated efforts to seed division and polarization in societies by amplifying specific issues on social media platforms through the use of automation. Further, some of these techniques are used by authoritarian regimes to intimidate activist groups and suppress dissent. It is in this context, that the Computational Propaganda project analyses data collected from these platforms and maps the amount of polarizing and junk news content that audience groups have been exposed to. This talk will describe in detail, some of our research efforts and findings related to recent elections in Sweden and Latin American countries.

Bio

Vidya works as a researcher in the Oxford Internet Institute at Oxford University, where she mainly works in the Computational Propaganda Project. She has several years of experience working as a researcher in Artificial Intelligence, with groups at both universities and in commercial environments. Her research interests, lie in the interface between technology, ethics and policy, and she is primarily engaged in developing systems that use technology for the greater good of society. She completed her PhD in Computer Science from the University of Southampton, building adaptive techniques for automated negotiations. Prior to this, she completed her M.S., in Industrial Engineering from Pennsylvania State University, working on problems in decentralized decision making, specifically in the defense logistics domain. Her basic background is in Mathematics, which she studied at the Masters level at the Indian Institute of Technology, Madras, and as an undergraduate at the University of Madras. She has also worked as a scientific coordinator at BAE Systems and as a software engineer at Tech Mahindra.

Sergeant Major Freddy Widecrantz
Naval Warfare Centre, Sweden

16:00-16:30 Wednesday, 24 October 2018 Room: J1620 Chair: Anton Borg

"The Naval Base, a world heritage of information collection threats"

Abstract

A short brief about the challenges with having a naval base, a warfare center and a shipyard in the same geographical area in a high-tech weapon industry developing country.

Bio

Sergeant Major Widecrantz has been working within the intelligence branch for some ten years. He has also been working with security service in support of the Swedish submarine systems. Today he is developing the method of intelligence support for Swedish maritime commanders at the level from task unit and higher. The development includes aspects regarding information flows, training of personnel to computer systems that serves the purpose.

Mikael Lagström
TrueSec, Stockholm, Sweden

13:00-13:45 Thursday, 25 October 2018 Room: J1620 Chair: Anton Borg

"Hands-on insights from the "Cloud hopper" incident that hit companies worldwide in 2017"

Abstract

The Cloudhopper operation were exposed in 2017, being a systematic hacking operation with an extensive web of global victims over many years. Listen to the insights from one of the many forensic investigations, and learn once again that no-one can be truly trusted, not even the large international well-known vendors – when it comes to being in the spotlight of an attack – and potential cover-up operation.

Bio

Mikael Lagström has several years of experience from IT, Telecom and Cybersecurity on management level, successfully building up global security services organizations. Mikael works at TrueSec, which is a highly regarded company that focuses on cyber-security, IT infrastructure, and secure development. TrueSec holds a key position in the Swedish market and have a strong reputation internationally due to worldwide security-related assignments.

Wednesday, October 24, 2018	
09:00-10:00	Registration/Coffee
10:00-10:30	**Opening: Welcome Session** General Chairs / Vice chancellor / Program Chair
10:30-11:30	**Keynote: IoT Security – Viewed from the Application Layer** Speaker: Prof. Dieter Gollmann, J1620, Chair: Martin Boldt
11:30-12:30	Lunch
12:30-14:00	**Session I**
Room J1620	Chair: Gunther Grasemann
	On Wash Trade Detection in Energy Markets Umid Akhmedov
	Digital Transformation in Border Checks: Mapping Border Guard Training in Automated Processes Laura Salmela, Sirra Toivonen, Minna Kulju, Mari Ylikauppila
	Towards Mobile Contactless 4-Fingerprint Authentication for Border Control Axel Weissenfeld, Andreas Zoufal, Christoph Weiss, Bernhard Strobl, Gustavo Fernández Domínguez
	A Heuristic Method for Identifying Scam Ads on Craigslist Hamad Alsaleh, Lina Zhou
14:00-14:30	Coffee Break
14:30-16:00	**Session II**
Room J1620	Chair: Joel Brynielsson
	Time of Day Anomaly Detection Matthew Price-Williams, Melissa Turcotte, Nick Heard
	Optical Covert Channel from Air-Gapped Networks via Remote Orchestration of Router/Switch LEDs Mordechai Guri
	Analysis and Evaluation of Antivirus Engines in Detecting Android Malware: A Data Analytics Approach Ignacio Martín, José Alberto Hernández, Sergio de los Santos, Antonio Guzmán
16:00-16:10	Short Break
16:10-16:40	**Invited Speech: The Naval Base, a world heritage of information collection threats** Speaker: Freddy Widecrantz , J1620, Chair: Anton Borg
18:00-21:30	**Social Event & Conference Dinner:** Naval Museum

Thursday, October 25, 2018	
08:30-09:00	Registration
09:00-10:00	**Keynote: Computational Propaganda and Misinformation Campaigns during Important Events in Public Life** Speaker: Dr. Vidya Narayanan, J1620, Chair: Lisa Kaati
10:00-10:15	Short Break
10:15-12:00	**Session III**
Room J1620	Chair: Mordechai Guri
	Policing the Cyber Threat: Exploring the Threat from Cyber Crime and the Ability of Local Law Enforcement to Respond Matthew Hull, Thaddeus Eze, Lee Speakman
	Harmonizing Criminal Law Provisions on Money Laundering – A Litmus Test of European Integration Tatu Hyttinen, Saila Heinikoski
	Conceptualising Cyber Security Information Sharing: A Stakeholder Survey Adam Zibak, Andrew Simpson
	Generic Object and Motion Analytics for Accelerating Video Analysis within VICTORIA David Schreiber, Martin Boyer, Elisabeth Broneder, Andreas Opitz and Stephan Veigl
12:00-13:00	Lunch
13:00-13:45	**Invited Speech: Hands-on insights from the "Cloud hopper" incident that hit companies worldwide in 2017** Speaker: Mikael Lagström, J1620, Chair: Anton Borg
13:45-14:00	Short Break
14:00-15:40	**Session IV**
Room J1620	Chair: Gerhard Backfried
	Online Monitoring of Large Events Johan Fernquist and Lisa Kaati
	Now You See Me: Identifying Duplicate Network Personas Sean Suehr, Chrysafis Vogiatzis
	Multi-expert Estimations of Burglars' Risk Exposure and Level of Pre-crime Preparation Using Coded Crime Scene Data: Work in Progress Martin Boldt, Veselka Boeva, Anton Borg
	Inferring Demographic data of Marginalized Users in Twitter with Computer Vision APIs Panos Kostakos , Abhinay Pandya, Olga Kyriakouli, Mourad Oussalah
15:40-15:50	**Closing Session**
15:50-16:30	Coffee

Session I			
12:30-14:00	Wednesday, October 24, 2018	Room: J1620	Chair: Gunther Grasemann

Paper I Short

On Wash Trade Detection in Energy Markets

Umid Akhmedov

A wash trade in energy markets refers to entering into arrangements for the sale or purchase of a financial or physical instrument, a related spot commodity contract, or an auctioned product based on emission allowances, where there is no change in beneficial interests or market risk or where beneficial interest or market risk is transferred between parties who are acting in concert or collusion. Market abuse scenarios such as wash trade compromise the efficiency and integrity of energy markets. The research of abusive trading behavior in financial markets is well ahead of peers in energy markets. Effective solutions for monitoring abusive scenarios such as wash trade in energy markets are yet to be developed. This paper describes a practical implementation example of detecting wash trade behavior in energy markets using simple techniques. An easily reusable method is then proposed to detect the potential wash trade activities involved in an instrument by first detecting trades resulting in no overall change in market risk and then further identifying the collusive behavior between the counterparties. The proposed method is tested and evaluated on energy instruments order data sets from the Trayport trading platform. We find that the proposed approach can effectively detect all primary wash trade indicators across energy instruments.

Paper II Short

Digital Transformation in Border Checks: Mapping Border Guard Training in Automated Processes

Laura Salmela, Sirra Toivonen, Minna Kulju, Mari Ylikauppila

Automated border control represents one area in the digital transformation of border control. It is gradually becoming a commonplace particularly at air borders, where the concept of self-service has had the strongest business case also in other steps of the passenger's journey, such as check-in or baggage drop. Besides providing a means to enhance efficiency and security in passenger clearing processes, the new technology significantly reshapes current ways of conducting border checks from employee perspective. Successful implementation of automated border check technologies thus demands border organizations to equip their workforce with new skills and remodel existing ones. This paper presents a preliminary analysis on current technology training of border guards and assesses its effects on how the new technology is received among employees at the frontline. The results are based on field studies conducted in five EU member states. The study loosely applies a Technology Training Model that extends traditional Technology Acceptance Model by incorporating training as an additional variable to explain employee intention to use new technology.

Paper III Short

Towards Mobile Contactless 4-Fingerprint Authentication for Border Control

Axel Weissenfeld, Andreas Zoufal, Christoph Weiss, Bernhard Strobl, Gustavo Fernández Domínguez

In the last years the importance of biometric authentication in border control procedures increased in a way that biometrics have become the core of most border management systems. Current commercial products for mobile border control have not satisfactorily solved both the demand for increasing security checks and the user requirements driven by security personnel such as border guards yet. Due to their flexibility, portable devices are commonly desired during the control process. This paper presents on-going work of an advanced mobile device for border control focusing on usability and integrating new technologies to envision next-generation of mobile devices. The device is based on the MobilePass device [13] but significantly improved. A key technology of the new device is a contactless 4-fingerprint authentication instead of only one in existing solutions. Results based on real data shows the advantages of 4-fingerprint versus 1-fingerprint authentication.

Paper IV Short

A Heuristic Method for Identifying Scam Ads on Craigslist

Hamad Alsaleh, Lina Zhou

Craigslist is a popular online customer-to-customer marketplace, which has attracted millions of consumers for trading and purchasing secondhand items. Because of the high financial return that sellers could gain from using this site and the anonymity option that the website provides to its users, Craigslist is highly subject to fraudulent activities. The primary objective of this study is to detect scam ads on Craigslist. Based on the related literature and our observations of ads collected from the platform, we develop a heuristic method for identifying scam ads. We evaluate the proposed heuristics by conducting an experiment and performing additional data analyses using real data. The results provide preliminary evidence for efficacy of the heuristics developed in this study.

Session II

14:30-16:00 Wednesday, October 24, 2018 Room: J1620 Chair: Joel Brynielsson

Paper I Full

Time of Day Anomaly Detection

Matthew Price-Williams, Melissa Turcotte, Nick Heard

Anomaly detection systems have been shown to perfor m well in detecting compromised user credentials within an enterprise computer network. Most existing appr oaches have focused on modelling activities that users perform within the network but not the time at whic h users are active. This article presents an approach for identifying compromised user credentials based on m odelling their time of day or diurnal patterns. Anomalous behaviour in this respect would correspond to a use r working during hours that deviate from their normal historical behaviour. The methodology is demonstrated using authentication data from Los Alamos National Laboratory's enterprise computer network.

Paper II Full

Optical Covert Channel from Air-Gapped Networks via Remote Orchestration of Router/Switch LEDs

Mordechai Guri

Air-gapped networks are separated from the Internet due to the sensitive information they store. It is shown that attackers can use the status LEDs of routers and switches to exfiltrate data optically. However, the current methods require the compromise of the network device (e.g., router) by infecting its firmware.
In this paper we show how attackers can covertly leak sensitive data from air-gapped networks via the row of status LEDs on non-compromised networking equipment such as LAN switches and routers. We introduce new types of attack called host-level attack, in which a malicious code run in a host connected to the network can indirectly control the LEDs, without requiring a code execution within the LAN switch or router. We present a version of the host- level attack that doesn't require special privileges (e.g., root or admin) and is also effective when running from within a Virtual Machine (VM), despite the network isolation. We provide the technical background and implementation details and discuss set of preventive countermeasures.

Paper III Full

Analysis and Evaluation of Antivirus Engines in Detecting Android Malware: A Data Analytics Approach

Ignacio Martín, José Alberto Hernández, Sergio de los Santos, Antonio Guzmán

Given the high popularity of Android devices, the amount of malware applications in Android markets has been growing at a fast pace in the past few years. However, the concept of malware is something vague since it often occurs that AntiVirus engines flag an application as malware while others do not, having no real consensus between different engines. With the help of data analytics applied to more than 80 thousand malware applications, this work further investigates on the relationships between different AntiVirus engines, showing that some of them are highly correlated while others behave totally uncorrelated from others. Finally, we propose a new metric based on Latent Variable Models to identify which engines are more powerful in identifying true malware applications

Session III

10:15-12:00 Thursday, October 25, 2018 Room: J1620 Chair: Mordechai Guri

Paper I Full

Policing the Cyber Threat: Exploring the Threat from Cyber Crime and the Ability of Local Law Enforcement to Respond

Matthew Hull, Thaddeus Eze, Lee Speakman

The landscape in which UK policing operates today is a dynamic one, and growing threats such as the proliferation of cyber crime are increasing the demand on police resources. The response to cyber crime by national and regional law enforcement agencies has been robust, with significant investment in mitigating against, and tackling cyber threats. However, at a local level, police forces have to deal with an unknown demand, whilst trying to come to terms with new crime types, terminology and criminal techniques which are far from traditional. This paper looks to identify the demand from cyber crime in one police force in the United Kingdom, and whether there is consistency in the recording of crime. As well as this, it looks to understand whether the force can deal with cyber crime from the point of view of the Police Officers and Police Staff in the organisation.

Paper II Full

Harmonizing Criminal Law Provisions on Money Laundering – A Litmus Test of European Integration

Tatu Hyttinen, Saila Heinikoski

This article discusses the harmonization of penal provisions concerning money laundering in the European Union (EU), in particular, the recent Commission proposal for a Directive on tackling money laundering by criminal law (COM(2016) 826 final). The perspective is both legal and political, pointing out to the different legal solutions in the European Union and analyzing the development from a European integration perspective, particularly in terms of a so- called spill-over process, whereby integration in one field leads to integration in adjacent fields. We put forward two main arguments in this article: (1) We argue that in order for the spill-over to succeed in a field crucial for national sovereignty such as criminal law, spill-over needs to be complemented with securitization and policy laundering, the latter referring to the phenomenon whereby issues are agreed at an international non- binding arena in order to later introduce these "international standards" into binding legislation. (2) We argue that harmonization in the money laundering context provides an example of a successful spill-over enhanced by policy laundering and securitization; tackling money laundering ostensibly requires spilling over European integration also in the field of criminal law, a core issue of national sovereignty. A testament to this is the fact that European countries have even harmonized their criminalization of self-laundering, although punishable self- laundering has been previously considered contrary to the general doctrines and principles of criminal law in many countries. A case in point is Finland, the only country bound by the proposed directive where parties to the crime are not punished for money laundering, except in rare cases and there is no case law for self-laundering (Section 11 Chapter 32 of the Criminal Code of Finland).

Paper III Full

Conceptualising Cyber Security Information Sharing: A Stakeholder Survey

Adam Zibak, Andrew Simpson

Despite the growing calls for cyber security information sharing and the increasing use of the term, consensus with regards to the term's definition is lacking. Further, there is a degree of inconsistency between different stakeholders when it comes to distinguishing between the various forms of information sharing. In this paper we review the different definitions of cyber security information sharing with a view to untangling the different forms of sharing. In addition, we review which types of sharing stakeholders perceive as more useful and are more willing to engage in. A review of both the academic and grey literature and a stakeholder online survey are used to compile data. We then analyse the data to develop a more nuanced understanding of cyber security information sharing, outlining key categories of sharing, before setting the scene for future research.

Paper IV Poster

Generic Object and Motion Analytics for Accelerating Video Analysis within VICTORIA

David Schreiber, Martin Boyer, Elisabeth Broneder, Andreas Opitz, Stephan Veigl

Video recordings have become a major resource for legal investigations after crimes and terrorist acts. However, currently no mature video investigation tools are available and trusted by LEAs. The project VICTORIA (Video analysis for Investigation of Criminal and TerrORist Activities) [1] addresses this need and aims to deliver a Video Analysis Platform (VAP) that will accelerate video analysis tasks by a factor of 15 to 100. We describe concept and work in progress done by AIT GmbH within the project, focusing on the development of a state-of-the-art tool for generic object detection and tracking in videos. We develop a detection, classification and tracking tool, based on Deep Neural Networks (DNNs), trained on a large number of object classes, and optimized for the project context. Tracking is extended to the multi-class multi-target case. The generic object and motion analytics is integrated in a novel framework developed by AIT, denoted as Connected Vision.

Session IV

14:00-15:40 Thursday, October 25, 2018 Room: J1620 Chair: Gerhard Backfried

Paper I Full

Online Monitoring of Large Events

Johan Fernquist and Lisa Kaati

In this paper, we describe an approach that can be used to monitor activity online that concerns large events. We propose six different tasks that can be used separately or in combination. The different tasks include analyzing messages from various actors, understanding the impact of messages to receivers, studying online discussions, analyzing hate and threats directed towards people and threats towards the execution of the large event and finally if there are any ongoing influential operations directed towards the general public.

To illustrate how the approach can be used, we provide some examples of the different steps when monitoring online environments a few months before the Swedish general election in 2018.

Paper II Full

Now You See Me: Identifying Duplicate Network Personas

Sean Suehr, Chrysafis Vogiatzis

This work provides a decision-making framework at the intersection of social network analysis and law enforcement intelligence with the goal of identifying persons of interest in a social network. Criminal social networks are complex due to the limited and imperfect information available. Moreover, the participating entities tend to misrepresent themselves in order to stay hidden and covert. In this work, we propose a new integer programming formulation to assist in the identification of entities who are prone to misrepresent themselves in a social network. Our insight is that such personas will form large subgraphs of restricted diameter that are connected to other entities who do not communicate directly or within a short number of intermediates. We formally define the problem and derive its computational complexity. Additionally, we provide an integer programming formulation to solve it exactly with the use of a commercial solver. We then show how our framework behaves on the Krebs 9/11 network. Our approach is able to identify what are believed to be two distinct clusters of criminals participating in two separate subplots: the multiple flight hijacking on September 11; as well as a plot against the U.S. embassy in Paris in the year 2001.

Paper III Short

Multi-expert Estimations of Burglars' Risk Exposure and Level of Pre-crime Preparation Using Coded Crime Scene Data: Work in Progress

Martin Boldt, Veselka Boeva, Anton Borg

Law enforcement agencies strive to link crimes perpetrated by the same offenders into crime series in order to improve investigation efficiency. Such crime linkage can be done using both physical traces (e.g., DNA or fingerprints) or "soft evidence" in the form of offenders' modus operandi (MO), i.e. their behaviors during crimes. However, physical traces are only present for a fraction of crimes, unlike behavioral evidence. This work-in-progress paper presents a method for aggregating multiple criminal profilers' ratings of offenders' behavioral characteristics based on feature-rich crime scene descriptions. The method calculates consensus ratings from individual experts' ratings, which then are used as a basis for classification algorithms. The classification algorithms can automatically generalize offenders' behavioral characteristics from cues in the crime scene data. Models trained on the consensus rating are evaluated against models trained on individual profiler's ratings. Thus, whether the consensus model shows improved performance over individual models.

Paper IV Short

Inferring Demographic data of Marginalized Users in Twitter with Computer Vision APIs

Panos Kostakos , Abhinay Pandya, Olga Kyriakouli, Mourad Oussalah

Inferring demographic intelligence from unlabeled social media data is an actively growing area of research, challenged by low availability of ground truth annotated training corpora. High-accuracy approaches for labeling demographic traits of social media users employ various heuristics that do not scale up and often discount non-English texts and marginalized users. First, we present a framework for inferring the demographic attributes of Twitter users from their profile pictures (avatars) using the Microsoft Azure Face API. Second, we measure the inter-rater agreement between annotations made using our framework against two pre-labeled samples of Twitter users (N1=1163; N2=659) whose age labels were manually annotated. Our results indicate that the strength of the inter-rater agreement (Gwet's AC1=0.89; 0.90) between the gold standard and our approach is 'very good' for labelling the age group of users. The paper provides a use case of Computer Vision for enabling the development of large cross-sectional labeled datasets, and further advances novel solutions in the field of demographic inference from short social media texts.

Blekinge Institute of Technology (BTH), Karlskrona, Sweden

Conference venue address: Campus Gräsvik, 371 79 Karlskrona

EISIC 2018 is hosted by Blekinge Institute of Technology (BTH) in Karlskrona, Sweden. BTH is a small institute of technology with a clear focus on applied ICT, strategic sustainability, and innovation. It has a strong research and education environment in software engineering and emerging environments in innovative product development and data science.

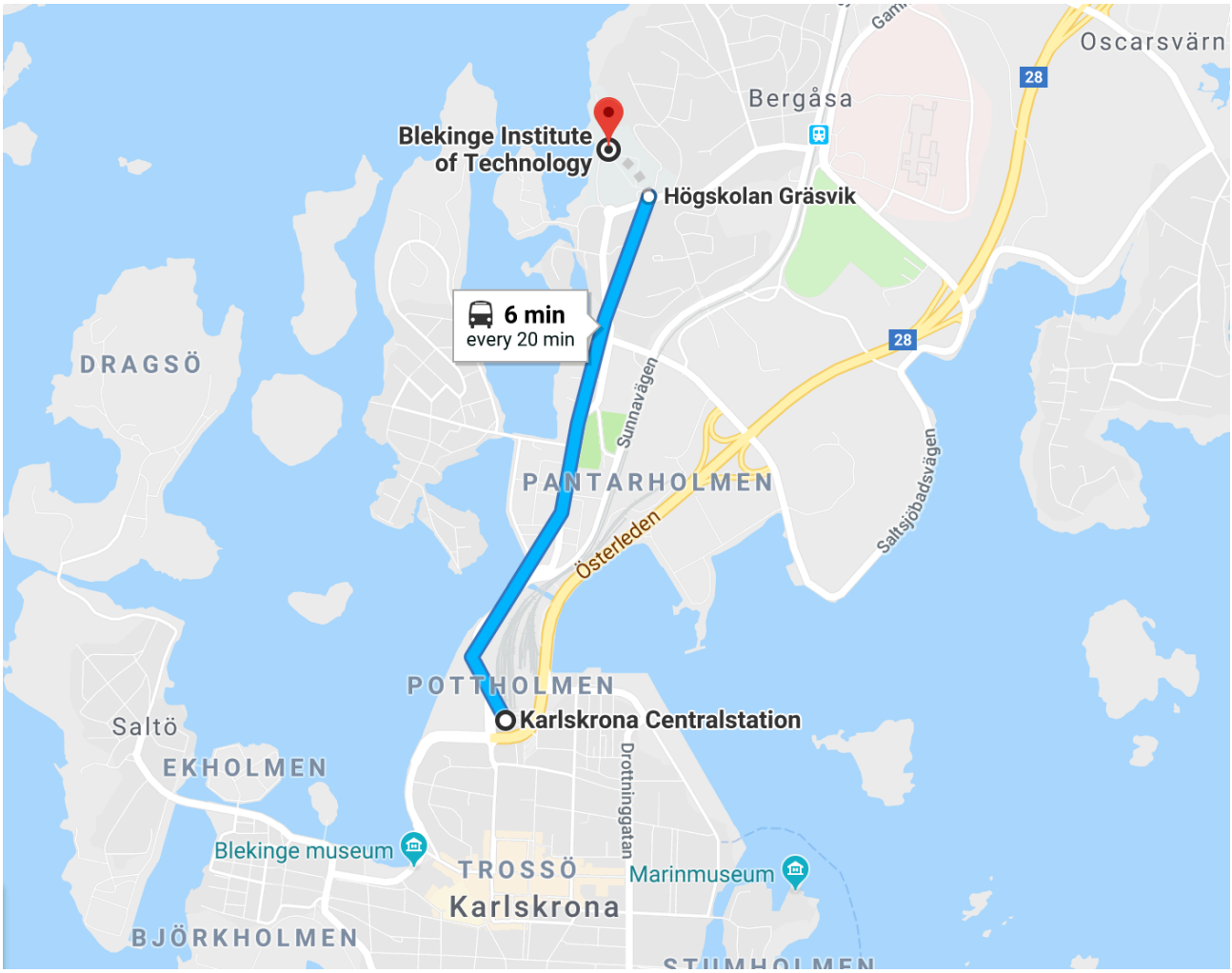
Karlskrona, founded 1680 during the reign of Charles XI, hosts Sweden's only remaining naval base and the headquarters of the Swedish Coast Guard. It is the capital of Blekinge county. The city is positioned at the south east corner of Sweden with excellent connections across the Baltic Sea.

The main reception is in house A on the map, and the conference will be held in house J.

Getting to the Campus

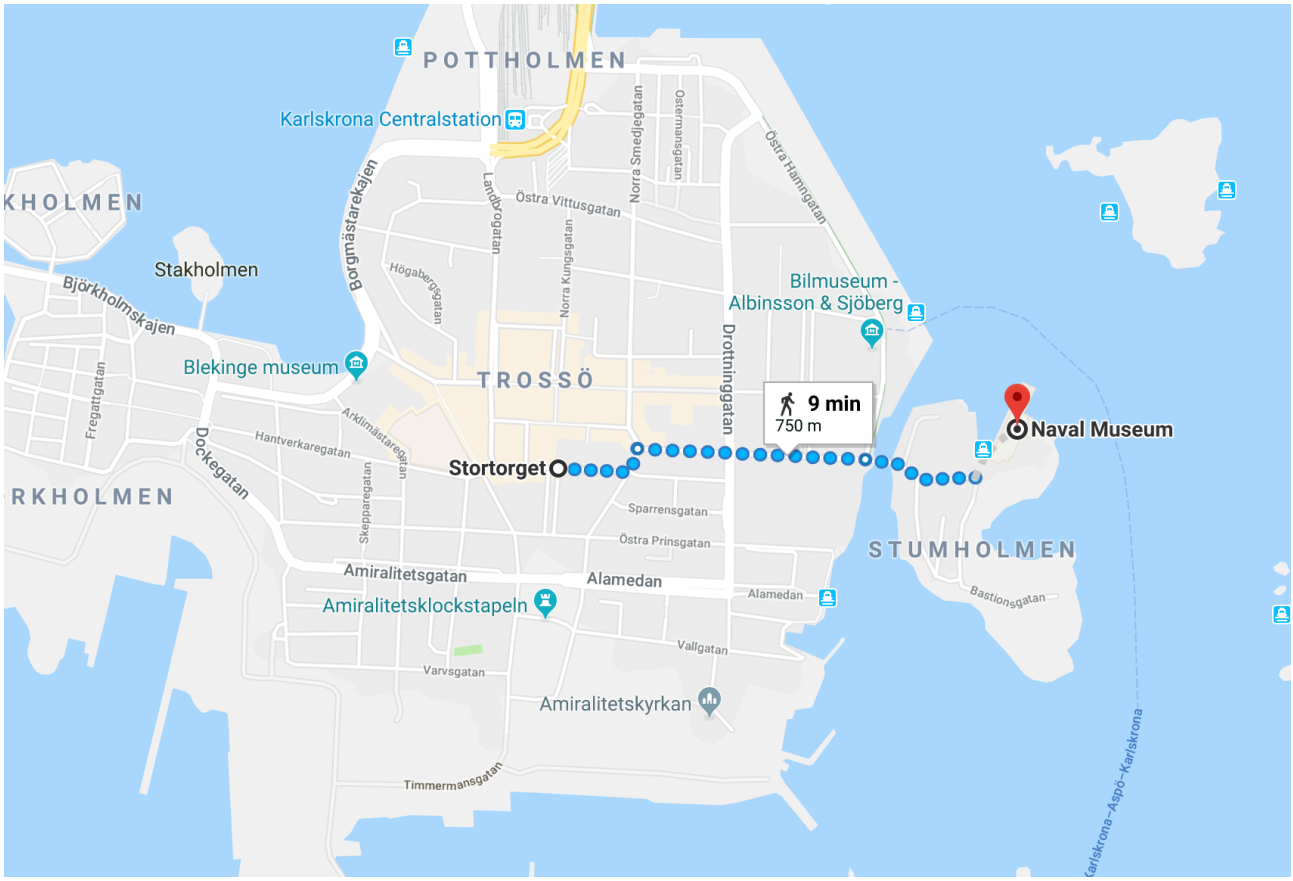
There is a regular bus that leaves from the bus station (next to the train-station). Bus no. 1 leaves towards campus from this stop (every 7 minutes). The local buses are run by Blekingetrafiken and you can get an up to date timetable on their website: www.blekingetrafiken.se

A trip from Kungsplan to campus takes 8 minutes and costs 30 SEK (no cash accepted, credit/debit card only). Driving (6 minutes) or walking (30 minutes). See the map below for detailed directions from the central station to the campus.



Getting to the Naval Museum

The Marinmuseum is within walking distance from the city center, located in the easternmost parts of the city center. Bus no. 1 from BTH has two stops along Drottninggatan which are within about 5 minutes walking distance, the stop Drottninggatan and the stop Sparre.



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) will be available in the room. Please inform the local area chair prior to the start of the conference if you don't have your own laptop during your presentation.

Poster Session

Posters will be hosted in the Foyer during the coffee breaks. Maximum height of the poster can be 140 cm and maximum width 104 cm.

Photographs

Photographs are allowed inside and outside the conference complex and in the area of Blekinge Institute of Technology.

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 complex using a code that will be provided at the time of the registration and will be available for all the days of the conference.

European Intelligence and Security Informatics Conference (EISIC) 2018

October 24-25, 2018,

Blekinge Institute of Technology, Karlskrona, Sweden

http://www.eisic.org

The Premier European Conference on Counterterrorism and Criminology

Designed by Panagiotis Karampelas, EISIC 2018