The 4th IEEE International Conference on Data Science and Systems
(DSS-2018)
28-30 June 2018, Exeter, UK

Call for papers

Cyber Security Workshop (CYBERSEC 2018)

at the 4th IEEE International Conference on Data Science and Systems (DSS-2018)
Exeter, UK, June 28-30 2018
Conference website: http://cse.stfx.ca/~dss2018/
Workshop website:
https://www.wil.waw.pl/konferencje/CFP_CyberSec2018_v.1.0.pdf

(1) Workshop Organizers:

Joanna Śliwa, Ph.D., Head of Department
C4I Systems' Department
Military Communication Institute, Poland
Tel: +48-26-188-55-11
Email: j.sliwa@wil.waw.pl

Bartosz Jasiul, Ph.D., Head of Laboratory
Cyber Security Laboratory
Military Communication Institute, Poland
Tel: +48-26-188-55-92
Email: b.jasiul@wil.waw.pl

(2) General description

Although awareness about necessary security appliances seems to be common and the tools used for that purpose are getting more and more advanced, the number of successful attacks targeted on computer systems is growing. The evolution towards cloud computing, increasing use of social networks, Internet of Things, mobile and peer-to-peer networking technologies that are intrinsic part of our life today, carrying many conveniences within our personal life, business and government, create many challenges and potential path of malware propagation. The optimal balance between usability and security of the infrastructure is difficult to be defined. Computer systems are usually prone to cyber attacks even though a number of security controls are already deployed. It is getting increasingly difficult to protect the infrastructure and assess its security on the basis of e.g. security audit. Risks derive not only from the technical domain, but very often human factor plays a critical role. The attacker can act from the perimeter of the network but very often finds the weakest element in the infrastructure and uses it to get access to the network. The Advanced Persistent Threats (APTs) and targeted attacks make every infrastructure potentially vulnerable. What is more the metadata related to the data exchange itself and the behaviour of the users registered by the sensors usually becomes big in terms of volume, velocity and variety. To analyse big data researchers use machine learning algorithms, however it is envisioned that the attackers will also use these mechanisms to overcome security controls and more successfully hide in the user traffic. It is therefore important to verify the efficiency of the security controls during cyber exercises that address both technical and human factor in the face of controlled, but real, targeted attack campaign towards a model infrastructure.

The CyberSec Workshop focuses on the diversity of the systems security developments and deployments in order to highlight the most recent challenges and report the latest research results. It is intended to attract researchers and practitioners from academia and industry, and provides an international discussion forum for sharing experiences and new ideas concerning emerging aspects of the systems security in different application domains.

Conference as well as the Workshop are sponsored by IEEE, IEEE Computer Society, and IEEE Technical Committee of Scalable Computing (TCSC).

(3) Topics of Interests

This Workshop calls for original papers describing the latest developments, trends, and solutions related to the issues of cyber security. Topics of interests include, but are not limited to:

- **Decision support systems for information security**
- **Risk assessment and risk management in different application domains**
- **Tools supporting security management and development**
- **Computer network security**
- **Cyber-attack detection**
- **Attack mitigation**
- **Cyber breaches scientific reports**
- **Cryptographic solutions**
- **Network security**
- **Anomaly detection**
- **Threat analysis**
- **IT security monitoring**
- **Web/mobile application security**
- **Computer forensics**
- **Cyber Exercises' organisation and execution - experiences and best practices**

(4) Important Dates

- **Paper Submission: ~~19 March 2018~~ 3 April 2018**
- **Authors Notification: 23 April 2018**
- **Camera-Ready Paper: 15 May 2018**
- **Early Registration: 15 May 2018**
- **Conference Date: 28-30 June 2018**

(5) Program Committee

- Roberto Di Pietro, HBKU-CSE, Qatar,
- Gerard Frankowski, Poznan Supercomputing and Networking Center, Poland
- Sebastian Garcia, Czech Technical University in Prague, Czech Republic
- Hector Marco Gisbert, University of the West of Scotland, United Kingdom
- Vasileios Gkioulos, Norwegian University of Science and Technology, Norway
- Damas P. Gruska, Comenius University in Bratislava, Slovakia
- Bartosz Jasiul, Military Communication Institute, Poland
- Wojciech Mazurczyk, Warsaw University of Technology, Poland
- Ana Serrano Mamolar, University of the West of Scotland, United Kingdom
- Joanna Sliwa, Military Communication Institute, Poland
- Jerzy Surma, SGH Warsaw School of Economics, Poland
- Marcin Szpyrka, AGH University of Science and Technology, Poland
- Konrad Wrona, NATO Communication and Information Agency, Netherlands

(6) Submission and Publication

Authors are invited to submit original previously unpublished research papers written in English, of up to 8 pages (or 10 pages with over length charge) including figures and references using IEEE Computer Society Proceedings Manuscripts style (two columns, single-spaced, 10 fonts). Please find the manuscript templates and submission related information at the DSS-2018 conference webpage. All accepted papers must be presented by one of the authors who must register for the conference and pay the fee.

The papers should be submitted using the EasyChair conference tool: https://easychair.org/conferences/?conf=cybersec2018.

Presented papers will appear in the conference proceedings, available on IEEE Xplore and submitted to be indexed in CPCi (ISI conferences and part of Web of Science) and Engineering Index (EI).