SciSec 2024 Program

The 6th International Conference on Science of Cyber Security
14-16 August 2024 | Copenhagen, Denmark

Day 1: August 14, 2024 (GMT+2, Room M1 - Meeting Center at DTU)

Zoom link: https://ntu-sg.zoom.us/j/5176983759?pwd=d05YaFBkalhHNFpxN3VLaEJhdmZ4Zz09

08:00 – 9:00 Registration

8:45 – 10:00 Welcome and Keynote I (Prof. Audun Jøsang)
(Room M1)

10:00 – 10:20 Coffee Break

10:20 – 11:40 Session 1: Cybersecurity Awareness (Session Chair: Weizhi Meng)

Smart Home Cyber Insurance Pricing
Xiaoyu Zhang, Maochao Xu and Shouhuai Xu

Exploring the Effects of Cybersecurity Awareness and Decision-Making Under Risk
Jan Hörnemann, Oskar Braun, Daniel Theis, Norbert Pohlmann, Tobias Urban and Matteo Große-Kampmann,

Characterizing the Evolution of Psychological Factors Exploited by Malicious Emails
Theodore Longtchi and Shouhuai Xu

Characterizing the Evolution of Psychological Tactics and Techniques Exploited by Malicious Emails
Theodore Longtchi and Shouhuai Xu

11:40 - 13:30 Lunch

13:40 - 14:20 Panel Discussion

14:20 – 15:20 Session 2: Cryptography and Privacy (Session Chair: Tiange Xie)

Performance Evaluation of Lightweight Cryptographic Ciphers on ARM Processor for IoT Deployments
Mohsin Khan, Dag Johansen and Håvard Dagenborg

SVSM-KMS: Safeguarding Keys for Cloud Services with Encrypted Virtualization
Benshan Mei, Wenhao Wang and Dongdai Lin

Integrating CP-ABE and Device Fingerprint into Federated Learning
Chunlu Chen, Rodrigo Roman, Kevin I-Kai Wang and Kouichi Sakurai

15:20 – 16:00 Coffee Break

16:00 – 17:40 Session 3: Intrusion Detection and Malware Analysis
(Session Chair: Krishna Roy)
GNNexPIDS: An Interpretation Method for Provenance-based Intrusion Detection Based on GNNExplainer
Ziyang Yu, Wentao Li, Xiu Ma, Xinbo Han, Baorui Zheng, Qiujian Lv, Ning Li and Weiqing Huang (https://youtu.be/2u4j8QpNTQU?si=4Z0OpqiXWZ6FxyVL)

LogSHIELD: A Graph-based Real-time Anomaly Detection Framework using Frequency Analysis
Krishna Roy and Qian Chen

FAF-BM: An Approach for False Alerts Filtering using BERT Model with Semi-supervised Active Learning (https://youtu.be/uVEZFv8aaqQ)
Dan Du, Yunpeng Li, Yiyang Cao, Yuling Liu, Guozhu Meng, Ning Li, Dongxu Han and Huamin Feng

Malware Variant Detection Based on Knowledge Transfer and Ensemble Learning
Rans Ford and Haoliang Sun

STARMAP: Multi-machine Malware Analysis System for Lateral Movement Observation
Shota Fujii, Yoichi Tsuzuki, Takanori Okamoto, Yu Tamura and Takayuki Sato

17:40 – 18:30 Business Meeting (M1)

18:30 – 20:00 Welcome Reception (outside M1)

Day 2: August 15, 2024 (GMT+2, Room M1 - Meeting Center at DTU)

Zoom link: https://ntu-sg.zoom.us/j/5176983759?pwd=d05YaFBkalhHNFpxN3VLaEJhdmZ4Zz09

9:00 – 10:00 Keynote II (Prof. Jeff Yan) (Room M1)

10:00 – 10:20 Coffee Break

10:20 - 11:40 Session 4: Malware Analysis and Threat Management
(Session Chair: Kéren A Saint-Hilaire)

Identifying Ransomware Functions through Microarchitectural Side-channel Analysis
Connor Startzel, Dane Brown, Owens Walker and Jennie Hill

Automatic Alert Categories Standardization for Heterogeneous Devices with Incomplete Semantic Knowledge Based on LSTM
Haiping Wang, Jianqiang Li, Binbin Li, Tianning Zang, Yifei Yang, Siyu Jia, Zisen Qi and Yu Ding

AutoCRAT: Automatic Cumulative Reconstruction of Alert Trees
Eric Ficke, Raymond Bateman and Shouhuai Xu

An Efficient IOC-Driven BigData Tracing and Backtracking Model for Emergency Response
Haiping Wang, Jianqiang Li, Binbin Li, Tianning Zang, Zisen Qi, Siyu Jia, Yu Ding and Yifei Yang

11:40 – 13:20 Lunch

13:20 – 14:40 Session 5: Network and IoT Security (Session Chair: Owens Walker)

Matching Knowledge Graphs for Cybersecurity Countermeasures Selection
Kéren A Saint-Hilaire, Christopher Neal, Frédéric Cuppens, Nora Cuppens-Boulahia and Makhlouf Hadji

An Enhanced Firewall for IoT Security
Sai Veerya Mahadevan, Yuuki Takano and Atsuko Miyaji

A Novel Scoring Algorithm Against HID Attacks Based on Static Text Feature Matching (*https://youtu.be/pA3PsoIR-zY?si=MmBqt1J2zs54S5Aq*)
Haiyang Li, Zhiqiang Lv, Yixin Zhang and Yanan Xue

Integrating Consortium Blockchain and Attribute-Based Searchable Encryption for Automotive Threat Intelligence Sharing Model
Tiange Xie, Feng Liu, Jiechao Gao and Yinghui Wang

14:40 – 15:20 Coffee Break

15:20 - 17:00 Session 6: Vulnerability and Privacy (Session Chair: Xiaofu Chen&Yaxin Luo)

Graph-Based Profiling of Dependency Vulnerability Remediation

Fernando Vera Buschmann, Palina Pauliuchenka, Ethan Oh, Bai Chien Kao, Louis DiValentin and David A. Bader

Completeness Analysis of Mobile Apps' Privacy Policies by Using Deep Learning
Khalid Alkhattabi and Chuan Yue

Exhaustive Exploratory Analysis of Low Degree Maximum Period NLFSRs Using Graph Analysis
Eric Filiol and Pierre Filiol

Family Similarity-Enhanced Implicit Data Augmentation for Malware Classification
Zisen Qi, Yijing Wang, Binbin Li, Tianning Zang, Hao Cui, Xingbang Tan and Yu Ding

Multi-Modal Multi-Task Tiered Expert (M3TTE): An Effective Method for CDN Website Classification
Yulong Zhan, Yang Cai, Gang Xiong, Gaopeng Gou and Xiaoqian Li

18:00 Bus Departure (Pick-up point – outside 101A)

18:30 –21:00 Banquet (Venue) and Conference ending

21:00 Bus Return

Day 3 August 16, 2023 (GMT+2)

Leaving day

Keynote 1

Audun Jøsang

Title: AI and Cybersecurity

ABSTRACT:
AI will have radical consequences for cybersecurity. Threat actors will weaponize AI to launch increasingly potent and destructive attacks. AI-based tools can create advanced deceptions and deepfakes that are already being used in real attacks, and the volume will only increase. To counter the threat of offensive AI, companies and research organizations are currently investing Big in the development of AI-based cyber defence technologies. Defenders need expertise in offensive uses of AI to better understand how defensive AI should work. In addition, the AI systems themselves can be the target of attacks, and hence we need to develop techniques for the defence of AI systems. This talk covers the basic principles of AI (Artificial Intelligence) and ML (Machine Learning) . Then it focuses on how AI is being used for both offensive and defensive purposes. Finally it focuses on how AI systems themselves have vulnerabilities that can be exploited by threat actors, with possible ways to protect AI systems against such attacks.

Keynote 2

Jeff Yan

Title: Who was behind the Camera?

ABSTRACT:
How can we deduce the photographer from a single photo? This seemed like an impossible problem, and my postdocs understandably all refused to tackle it. Determined to pursue it, I teamed up with a friend at MIT, and this collaboration resulted in the invention of novel forensic techniques. In this keynote, I will discuss some of our research findings and explore future opportunities. No prerequisites are needed, just a curious mind.