Main Program
To authors: A regular paper presentation would be 25 mins in total (20 min presentation and 5 min Q&A)

March 25 - March 26 - March 27

March 25 (Room: Salon D)

Registration: 07:45 am -09:00 am

Keynote I: Using AI to Detect Advanced Threats – Done Right
09:00AM - 10:00AM

Engin Kirda
Northeastern University

Session Chair: Murat Kantarcioglu, University of Texas at Dallas

Break (30 Minutes):
10:00AM - 10:30AM

Session 1: Mobile Security
10:30AM - 12:10PM

- Kailiang Ying (Syracuse University), Priyank Thavai (Syracuse University) and Wenliang Du (Syracuse University).
  Developing TrustZone User Interface for Mobile OS using Delegation Integration Model
- Tatsuhiko Yasumatsu (Waseda University), Takuya Watanabe (NTT Secure Platform Laboratories / Waseda University), Fumihiro Kanei (NTT), Eitaro Shioji (NTT), Mitsuaki Akiyama (NTT), and Tatsuya Mori (Waseda University / RIKEN AIP).
  Understanding the Responsiveness of Mobile App Developers to Software Library Updates
- Sigmund Albert Gorski Iii (North Carolina State University), Benjamin Andow (North Carolina State University), Adwait Nadkarni (William and Mary Univ.), Sunil Manandhar (William and Mary Univ.), William Enck (North Carolina State University), Eric Bodden (Paderborn University) and Alexandre Bartel (University of Luxembourg).

ACMiner: Extraction and Analysis of Authorization Checks in Android's Middleware

- Michalis Diamantaris (FORTH), Elias P. Papadopoulos (FORTH), Evangelos P. Markatos (FORTH), Sotiris Ioannidis (FORTH) and Jason Polakis (University of Illinois at Chicago).
  REAPER: Real-time App Analysis for Augmenting the Android Permission System

Session Chair: Kevin Butler University of Florida

Lunch (Salon EFG - 60 Minutes)
12:10PM - 1:10PM

Session 2: IOT/Smart Device Security

1:10PM - 2:50PM

- Nisha Panwar (University of California, Irvine), Shantanu Sharma (University of California, Irvine), Guoxi Wang (University of California, Irvine), Sharad Mehrotra (University of California, Irvine) and Nalini Venkatasubramanian (University of California, Irvine).
  Verifiable Round-Robin Scheme for Smart Homes
- Maanak Gupta (University of Texas at San Antonio), James Benson (University of Texas at San Antonio), Farhan Patwa (University of Texas at San Antonio) and Ravi Sandhu (University of Texas at San Antonio)**.**
  Dynamic Groups and Attribute-Based Access Control for Next-Generation Smart Car
- Kaushal Kafle (William & Mary University), Kevin Moran (William & Mary University), Sunil Manandhar (William & Mary University), Adwait Nadkarni (William & Mary University)and Denys Poshyvanyk (William & Mary University).
  A Study of Data Store-based Home Automation
- Amit Tambe (Singapore University of Technology and Design), Yan Lin Aung (Singapore University of Technology and Design), Ragav Sridharan (Singapore University of Technology and Design), Martin Ochoa (Universidad del Rosario), Nils Ole Tippenhauer (Center for It-Security, Privacy & Accountability (CISPA)), Asaf Shabtai (Ben Gurion University of the Negev), and Yuval Elovici (Singapore University of Technology and Design).

Detection of Threats to IoT Devices Using Scalable VPN-forwarded Honeypots

Session Chair: Maria Isabel Fernandez, Kings College London

Break (30 Minutes)
2:50PM - 3:20PM

Session 3: Data Security and Privacy
3:20PM - 5:00PM

- Ehsan Hesamifard (University of North Texas), Hassan Takabi (University of North Texas) and Mehdi Ghasemi (University of Saskatchewan).
  Deep Neural Networks Classification over Encrypted Data
- Nikolai Jannik Podlesny (Hasso-Plattner-Institute), Anne V.D.M. Kayem (Hasso-Plattner-Institute), and Christoph Meinel (Hasso-Plattner-Institute).
  Attribute Compartmentation and Greedy UCC Discovery for High-Dimensional Data Anonymization
- Z. Berkay Celik (The Pennsylvania State University), Abbas Acar (Florida International University), Hidayet Aksu (Florida International University), Ryan Sheatsley (The Pennsylvania State University), A. Selcuk Uluagac (Florida International University), and Patrick McDaniel (The Pennsylvania State University).
  Curie: Policy-based Secure Data Exchange
- Asmaa Sallam (Purdue University), and Elisa Bertino (Purdue University).
  Result-Based Detection of Insider Threats to Relational Databases

Session Chair: Vassil Roussev, University of New Orleans

Session 4: Reception and Posters (Salon EFG)
6:00PM
Session Chair: Hongxin Hu, Clemson University

March 26 (Salon D)

Keynote II: Using AI to Detect Attacks and Manage Access Control
09:00AM - 10:00AM

Anupam Joshi, University of Maryland Baltimore County

Session Chair: Bhavani Thuraisingham, University of Texas at Dallas

Break (30 Minutes)
10:00AM - 10:30AM

Session 5: Access Control and Information Flow
10:30AM - 12:10PM

- Maribel Fernandez (Kings College London), Ian Mackie (LIX) and Bhavani Thuraisingham (The University of Texas at Dallas).
  Specification and analysis of ABAC policies via the category-based metamodel
- Philip W. L. Fong (University of Calgary).
  Results in Workflow Resiliency: Complexity, New Formulation, and ASP Encoding
- Tobias Pfeffer (TU Berlin), Thomas Göthel (TU Berlin), and Sabine Glesner (TU Berlin).
  Efficient and Precise Information Flow Control for Machine Code through Demand-Driven Secure Multi-Execution
- Yuseok Jeon (Purdue University), Junghwan Rhee (NEC Laboratories America), Chung Hwan Kim (NEC Laboratories America), Zhichun Li (NEC Laboratories America), Mathias Payer (Purdue University), Byoungyoung Lee (Seoul National University) and Zhenyu Wu (NEC Laboratories America)**.**
  PoLPer: Process-Aware Restriction of Over-Privileged Setuid Calls in Legacy Applications

Session Chair: Martin Ochoa, Cyxtera Technologies

Lunch (Salon EFG - 60 Minutes)
12:10AM - 1:10PM

Panel:
1:10PM - 2:50PM

Title: AI + Cyber Security + Big Data
Panelists:

Latifur Khan, UT Dallas (Moderator)
Rakesh Verma, UH
Anoop Singhal, NIST (tentative)

Cuneyt Akcora, UT Dallas

Break (30 Minutes)
2:50PM - 3:20PM

Session 6: Hardware Assisted Data Security
3:20PM - 5:00PM

- Mathias Morbitzer (Fraunhofer), Manuel Huber (Fraunhofer), and Julian Horsch (Fraunhofer).
  Extracting Secrets from Encrypted Virtual Machines
- Flavio Toffalini (Singapore University of Technology and Design), Martín Ochoa (Universidad del Rosario), Jun Sun (Singapore University of Technology and Design), and Jianying Zhou (Singapore University of Technology and Design)**.**
  Careful-Packing: A Practical and Scalable Anti-Tampering Software Protection enforced by Trusted Computing
- Cory Thoma (University of Pittsburgh), Adam J. Lee (University of Pittsburgh), and Alexandros Labrinidis (University of Pittsburgh).
  Behind Enemy Lines: Exploring Trusted Data Stream Processing on Untrusted Systems
- Dave Tian (University of Florida), Joseph Choi (University of Florida), Grant Hernandez (University of Florida), Patrick Traynor (University of Florida), and Kevin Butler (University of Florida)**.**
  A Practical Intel SGX Setting for Linux Containers in the Cloud

Session Chair: Rakesh Verma, University of Houston

Banquet (Room: Salon EFG)
6:00PM

March 27 (Room: Salon D)

Session 7: Web Security and Privacy
8:30AM - 10:10AM

- Blake Anderson (Cisco), Andrew Chi (The University of North Carolina at Chapel Hill), Scott Dunlop (Cisco) and David McGrew (Cisco).
  Limitless HTTP in an HTTPS World: Inferring the Semantics of the HTTPS Protocol without Decryption
- Hasan Alan (The University of North Carolina at Chapel Hill) and Jasleen Kaur (The University of North Carolina at Chapel Hill).
  Client Diversity Factor in HTTPS Webpage Fingerprinting
- Alina Matyukhina (University of New Brunswick), Natalia Stakhanova (University of New Brunswick), Mila Dalla Preda (University of Verona), and Celine Perley (University of New Brunswick).
  Adversarial Author Attribution in Open-source Projects
- Zhibo Sun (Arizona State University), Carlos E. Rubio-Medrano (Arizona State University), Ziming Zhao (Arizona State University), Tiffany Bao (Arizona State University), Adam Doupé (Arizona State University), and Gail-Joon Ahn (Arizona State University).
  Understanding and Predicting Private Interactions in Underground Forums

Session Chair: Ram Krishnan, University of Texas at San Antonio

Break (20 Minutes)
10:10AM – 10:30AM

Session 8: System Security and Authentication

10:30AM - 12:10PM

- Ronny Chevalier (CentraleSupélec), Stefano Cristalli (University of Milan), Christophe Hauser (University of Southern California), Yan Shoshitaishvili (Arizona State University), Ruoyu Wang (University of California, Santa Barbara), Christopher Kruegel (University of California, Santa Barbara), Giovanni Vigna (University of California, Santa Barbara), Danilo Bruschi (University of Milan) and Andrea Lanzi (University of Milan).
  BootKeeper: Validating Software Integrity Properties on Boot Firmware Images
- Peiying Wang (Institute of Information Engineering,Chinese Academy of Sciences), Shijie Jia (Institute of Information Engineering,Chinese Academy of Sciences), Bo Chen (Michigan Technological University), Luning Xia

(Institute of Information Engineering,Chinese Academy of Sciences) and Peng Liu (The Pennsylvania State University).
MimosaFTL: Adding Secure and Practical Ransomware Defense Strategy to Flash Translation Layer

- Gaurav Panwar (New Mexico State University), Satyajayant Misra (New Mexico State University), and Roopa Vishwanathan (New Mexico State University)**.**
  BlAnC: Blockchain-based Anonymous and Decentralized Credit Networks
- Laleh Eskandarian (Sabancı University), Dilara Akdoğan (Sabancı University), Duygu Karaoğlan Altop (Sabancı University), and Albert Levi (Sabancı University).
  SKA-CaNPT: Secure Key Agreement using Cancelable and Noninvertible Biometrics based on Periodic Transformation

Session Chair: Hassan Takabi, University of North Texas

Take-out Lunch
12:10PM