ISPEC Keynote

Wenjing Lou

Virginia Tech, US

Strengthening Machine Learning-based Intrusion Detection Systems in Adversarial Environments

Machine learning has seen significant advancements in recent years and has proven to be highly effective in a wide array of applications, including intrusion detection systems (IDS). However, while working in adversarial environments, machine learning-based systems are known to be vulnerable to a range of attacks. In this talk, we will discuss techniques aimed at strengthening machine learning-based IDS.

On the one hand, we explore techniques for enhancing the performance and robustness of IDS in adversarial environments, where we propose a contrastive learning-based approach that builds highly differentiating IDS. On the other hand, we develop efficient security mechanisms to thwart common attacks, including an adversarial example (AE) detector that filters out suspicious inputs at the model testing time, and a robust model evaluation method that leverages latent space representations to build resiliency in model aggregation against model poisoning attacks in federated learning. This talk will report our research results along this line of research.

Yang Xiang

Swinburne
Univ. of Tech, AU

Enhancing Security in Software and AI

Cybersecurity has emerged as one of the foremost priorities on the global research and development agenda today. The urgent need for new and innovative cybersecurity technologies capable of effectively addressing this pressing danger cannot be overstated. Software security is paramount to maintaining the integrity of modern software applications.

Given the broad spectrum of real-world applications, different security challenges are evaluated based on the specific use case. In this presentation, we will dissect a variety of security issues that have arisen in diverse applications, examining both the associated challenges and effective strategies in software security.

We will delve into the technique of fuzzing, an efficient and effective automated process vital for software testing. Additionally, we will explore strategies for detecting security vulnerabilities in software. We will also scrutinize security considerations in binary code applications, including those in IoT devices and Windows low-level components. By viewing AI models as software, we will further address the significant security problems present within deep learning models.

ISPEC Program

August 24

09:15 Welcome Ceremony

09:30 Keynote: Yang Xiang

10:30 Morning Tea Break

11:00
A.I. Security - M1 (Room M1)
- Secure and Efficient Federated Learning By Combining Homomorphic Encryption and Gradient Pruning in Speech Emotion Recognition
- FedLS: An Anti-poisoning Attack Mechanism for Federated Network Intrusion Detection Systems using Autoencoder-based Latent Space Representations.
- Mitigating Sybil Attacks in Federated Learning.

Privacy and Data Security - S1 (Room S9)
- Privacy-Preserving Authentication Scheme for 5G Cloud-Fog Hybrid with Soft Biometrics.
- Obfuscation padding schemes that minimize Renyi min-entropy for Privacy
- Cross-Border Data Security from the Perspective of Risk Assessment.

12:00 Luncheon

14:00 Keynote: Wenjing Lou

15:00 Afternoon Coffee Break

15:30
Smart City Security - M1 (Room M1)
- IoT-REX: A Secure Remote-Control System for IoT Devices from Centralized Multi-Designated Verifier Signatures.
- CVAR-FL IoV Intrusion Detection Framework
- Transparent Security Method for Automating IoT Security Assessments.

Web and Network Security - S1 (Room S9)
- DIDO: Data Provenance from Restricted TLS 1.3 Websites.
- QR-SACP: Quantitative Risk-based Situational Awareness Calculation and Projection through Threat Information Sharing
- Dynamic Trust Boundary Identification for the Secure Communications of the Entities via 6G.

18:00 Le Dîner de Gala (Brede Høker)

ISPEC Program

August 25

09:30
Malware & Software Security - M1 (Room M1)
- RTR-Shield: Early Detection of Ransomware using Registry and Trap Files.
- MalXCap: A Method for Malware Capability Extraction
- Multimodal Software Defect Severity Prediction Based on Sentiment Probability.

Applied Cryptography - S1 (Room S9)
- Recovering Multi-Prime RSA Keys with Erasures and Errors
- Performance Impact Analysis of Homomorphic Encryption: A Case Study Using Linear Regression as an Example.
- Chosen Ciphertext Security for Blind Identify-Based Encryption with Certified Identities.

10:30 Morning Tea Break

11:00
Applied Cryptography - M1 (Room M1)
- A New Gadget Decomposition Algorithm with Less Noise Growth in HE schemes.
- Malicious Player Card-based Cryptographic Protocols with a Standard Deck of Cards Using Private Operations.
- Cryptanalysis of Human Identification Protocol with Human-Computable Passwords.

Smart City Security - S1 (Room S9)
- A Source Hiding Protocol for Cooperative Intelligent Transportation Systems (C-ITS)

- A Revocable Outsourced Data Accessing Control Scheme with Black-Box Traceability.
- LocKey: Location-based Key Extraction from the WiFi Environment in the User's Vicinity.

12:00 Luncheon

Blockchain - M1 (Room M1)
- BAHS: Blockchain-Aided Hash-Based Signature Scheme
14:00 - Lever: Making Intensive Validation Practical on Blockchain
- Tikuna: An Ethereum Blockchain Network Security Monitor System.

Applied Cryptography - S2 (Room S9)
- Isogeny-based Multi-Signature Scheme.
- Security Analysis of WAGE against Division Property based Cube Attack
- When MPC in the Head meets VC.

15:00 Afternoon Coffee Break

Web and Network Security - M1
- Quantum Key Distribution as a Service and Its Injection into TLS
15:30 - XFedGraph-Hunter: An Interpretable Federated Learning Framework for Hunting Advanced Persistent Threat in Provenance Graph
- XSS attack detection by attention mechanism based on script tags in URLs.

Blockchain - S1
- Mining for Better: An Energy-Recycling Consensus Algorithm to Enhance Stability with Deep Learning.
- SIOCEN: Secure Integrity Verification of Outsourced Data in Cloud Storage using Blockahin.

16:30 Closing Ceremony.

ISPEC Social

Brede Værk Garden

Get up close to 250 years of industrial architecture with factory buildings, workers' homes and master's homes, and get an impression of the small community. The river Mølleåen is dammed and the course of the water can be flowed beneath the buildings.

ISPEC Gala

Brede Høker

The charming restaurant itself is located in Brede Værk's old building, dating back to 1893. A historic location for Danish industry, over the centuries the buildings have produced grain, gunpowder, copper and textiles. And now, exquisite cuisine.

The Høker (Høkeren) is a combined grocery store, cafe and community center. Throughout the year, Brede Høker organizes lots of events such as flea markets, concerts in Slusegården, Mardi Gras, Halloween, Christmas parties and much more.

ISPEC More Websites

ISPEC 2023 Website

ISPEC

Thank you for choosing ISPEC