UWE Bristol | University of the West of England

Cyber Security

Computer Science Research Centre

UWEcyber PhD Showcase

31st October 2023

UWEcyber Gold Award

in association with National Cyber Security Centre

Department for Digital, Culture, Media & Sport

Academic Centre of Excellence in **Cyber Security Education**

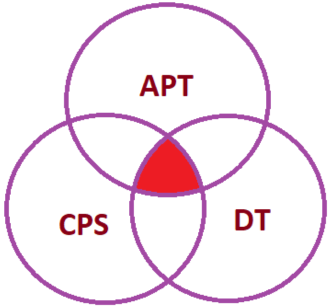
Carol Lo

PhD: Design of a secure digital twin to detect and mitigate advanced persistent threats on cyber-physical systems in Smart Manufacturing

Background

- Academic journey
  - MSc Cyber Security, graduated in March 2022
  - PhD research degree, since April 2023
    - Advanced Persistent Threats (APT), Cyber Physical Systems (CPS) and Digital Twins (DT)
- Enjoyable moments
  - Poster paper presented in IEEE Smart World in August
  - Collaborating with an undergraduate on a research project on lightweight testbed for attack simulation
  - Learning how Cyber Physical Systems are constructed and how they could be manipulated by attackers

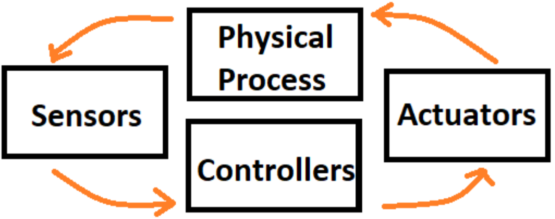
Smart Manufacturing



Siemens Festo CP Lab at 1Z005

Implications of APT Attacks on CPS

- Characteristics of Advanced Persistent Threats (APT)
  - Objectives: cyber espionage, disrupt operations
  - Strategies: stealthy, prolonged, multi-steps attack, customised tools
  - Targets: specific, high-profile organisations, critical infrastructure systems
- Cyber Physical Systems (CPS)
  - Embedded systems directly interact with the physical world through sensors, controllers and actuators
  - Examples of APT attacks on Cyber-Physical Systems (CPS)
    - 2015 – Ukraine power grid – power outages affecting >230,000 people
    - 2021 – Colonial Pipeline – shut down fuel supply for 6 days



Use of Digital Twins to Address Research Limitations

- Research aim
  - Design secure digital twins of cyber-physical systems to mitigate and detect stealthy and multi-stage APT attacks
- Research limitations
  - Attack detection often focus on specific system vulnerabilities or attack techniques
  - Limited understanding of attack stages
  - A notable shortage of APT-specific datasets for Machine Learning (ML) tools
- Potential use of digital twins
  - Replicate real-time data to DT from its physical twin for intrusion detection
  - Correlate signs of intrusion to understand the attack stage for better response
  - Simulate attack on digital twins and collect synthetic data for improving ML tools

James Barrett

PhD: Interactive machine learning for identifying threats to security and service in large-scale mobile networks

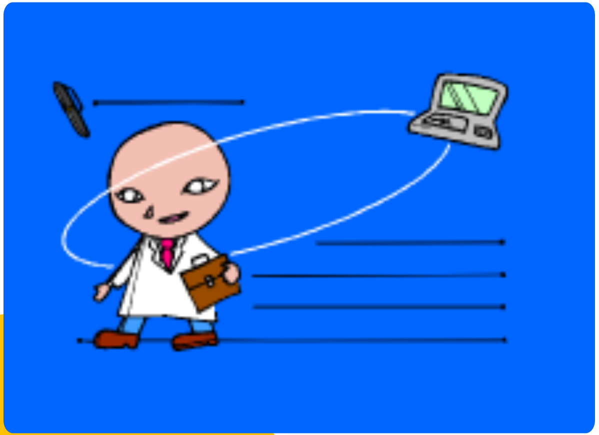
Who am I? What do I do?

- My name is James Barrett, I am a 2nd year PhD student and postgraduate researcher here at UWE.
- I study Artificial Intelligence for Cybersecurity; this involves studying the methods and research behind machine learning.
- Phil Legg & Jim Smith are my PhD supervisors. I spend most of my time reading, writing, and developing experimentations to test new ideas I have discovered from my research.
- It is very rewarding! Although challenging the PhD process is one I would recommend to any dedicated student.

How did I get here?

- I have always liked computers from a young age, I had dial up growing up!
- I began with taking GCSE ICT in secondary school and studying a BTEC in IT at college.
- I studied for a FdSc in computer technology, before taking my BSc in applied computing technologies (I started a GitHub when I started uni, I would suggest you all do too!)
- I then studied for my MSc in cybersecurity, leading to a position as a lecturer at Plymouth University.
- I was accepted onto this PhD programme on the 1st Jan 2022! This has led my start into research and continuation of my teaching career.

Why Research is Great, and important



- Building and discovering unexplored areas of computer science is seriously rewarding.
- You can contribute a paper, an idea to science and see that work being used to influence new research too!
- Without researchers, innovation fails to exist, we need academics! For industry and society.
- Constantly learning: One of the key reasons I enjoy what I do is that I am always growing, learning to achieve new goals everyday!

UWE cyber UWE Bristol University of the West of England

Sadegh Bamohabbat Chafjiri

PhD: Fuzzing by adapting cryptanalytic techniques and game theory

Background

- A postgraduate researcher at the University of the West of England, specializing in vulnerability assessment and software testing. His Ph.D. focuses on an AI-enabled software security framework, with an emphasis on fuzz testing.
- With a background in entrepreneurship and IT management, Sadegh holds a bachelor’s degree in electrical engineering and two master’s degrees in telecommunication engineering, specializing in cryptography and IT management with a data analytics focus.
- He has extensive experience in security engineering, data analytics, AI-enabled solutions, and the Internet of Things. Leveraging his expertise, Sadegh has consistently delivered innovative solutions in software security and sustainable infrastructures.

Software Testing

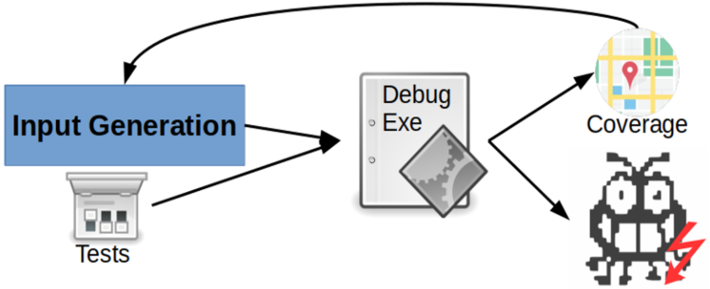
Cybersecurity Analytics

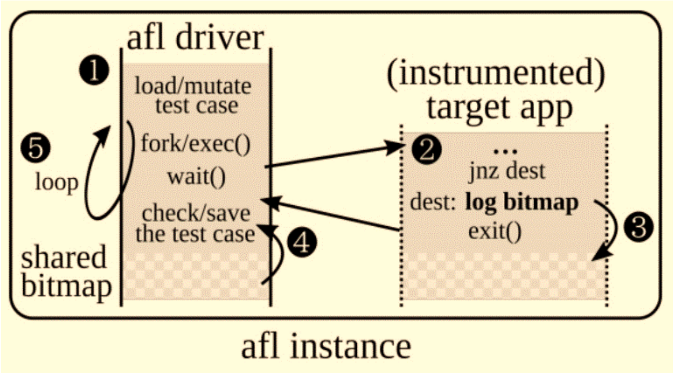
Security Engineering and Cryptography

Game Theory and Optimisation Techniques

Transferable and AI-enabled software security framework

Recent cyber security incidents like "Wannacry" underscore the importance of proactive program analysis to detect software vulnerabilities. Vulnerability discovery methodologies involve analysing software either statically or dynamically to identify weaknesses. These weaknesses can be exploited by attackers to unauthorisedly access or compromise systems. In the 90s, "fuzzing," a novel vulnerability detection method for UNIX systems, was introduced. Fuzzers use random input (invalid data) to discover vulnerabilities. Fuzz testing is a critical technique for finding zero-day vulnerabilities and is gaining popularity in the cybersecurity community. My research project explores a transferable Machine Learning-based framework's feasibility and effectiveness for efficient fuzz testing in diverse systems





UWE cyber

UWE Bristol University of the West of England

Dalila Khettaf

PhD: Graph-based group anomaly detection in IoT with Deep Learning

Anomalies!

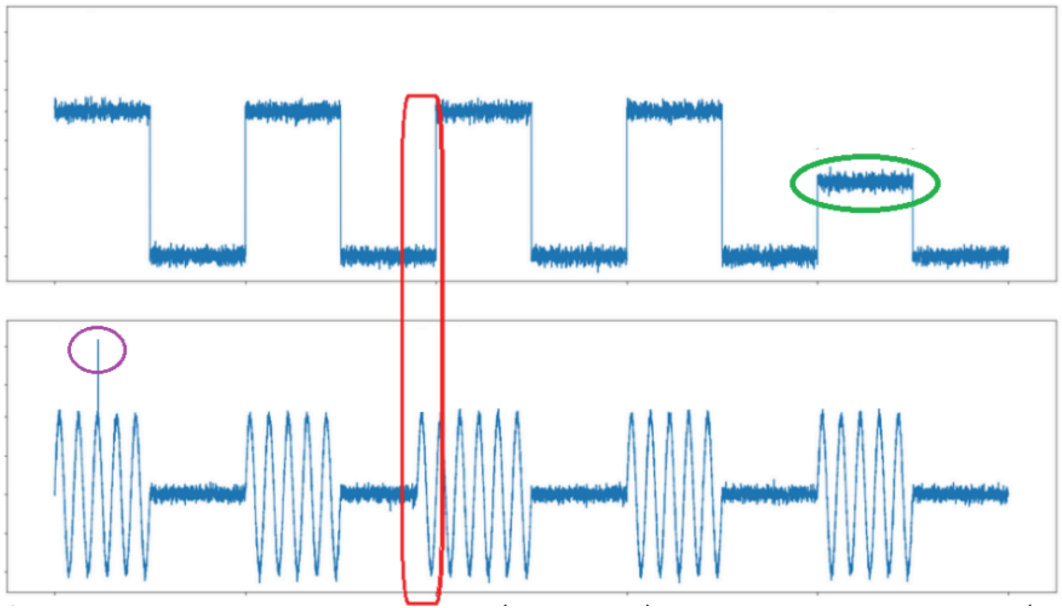


Figure 1: The three anomaly types (Audibert et al, 2022)

Audibert, J., Michiardi, P., Guyard, F., Marti, S., & Zuluaga, M. A. (2022). Do deep neural networks contribute to multivariate time series anomaly detection?. *Pattern Recognition*, *132*, 108945.

Collective anomalies

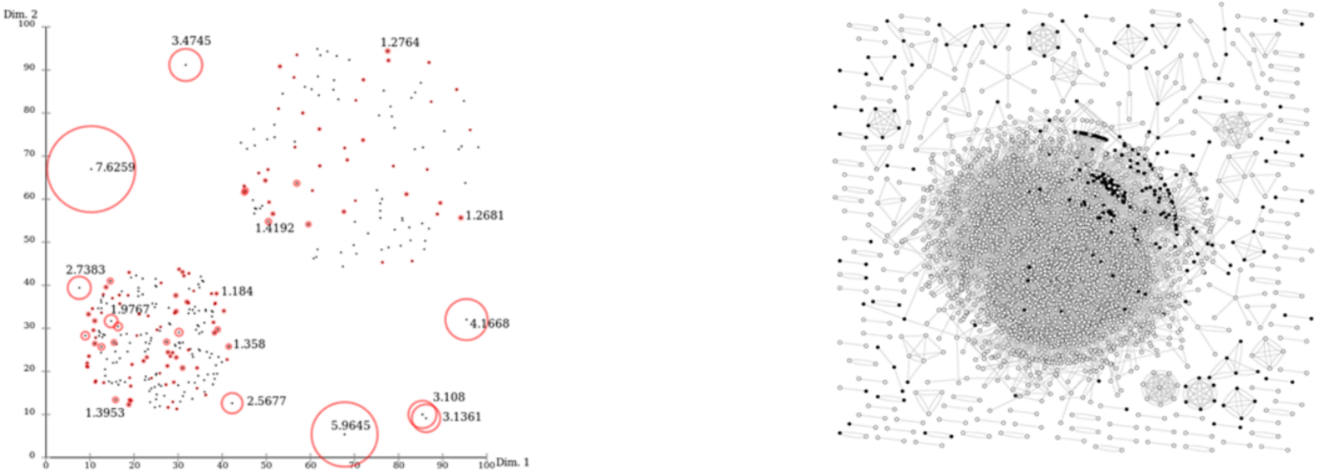


Figure 2: Point Vs group anomalies

Akoglu, L., Tong, H., & Koutra, D. (2015). Graph based anomaly detection and description: a survey. *Data mining and knowledge discovery*, *29*, 626-688

Great potential

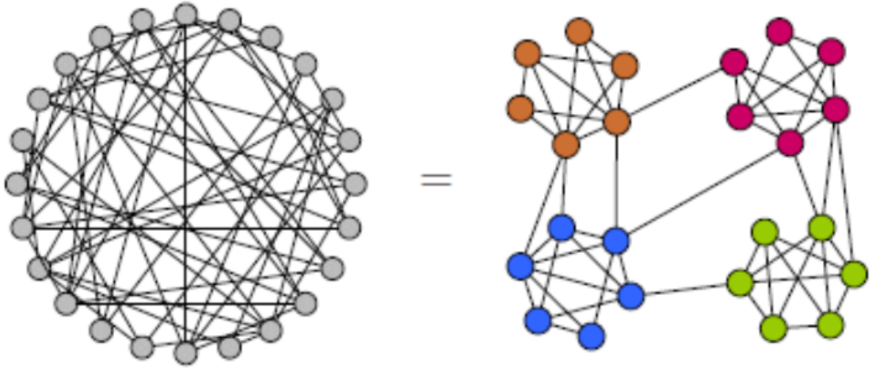


Figure 4: Graphs for group anomaly detection

Tahmassebi, A., Pinker-Domenig, K., Wengert, G., Lobbes, M., Stadlbauer, A., Wildburger, N. C., ... & Meyer-Bäse, A. (2017, May). The driving regulators of the connectivity protein network of brain malignancies. In *Smart Biomedical and Physiological Sensor Technology XIV* (Vol. 10216, pp. 8-15). SPIE.

UWE cyber UWE Bristol University of the West of England

Aimen Djemaa

PhD: Adversarial Machine Learning Attacks on Federated Learning Models

Background

- Academic:
  - BSc Information System and Software Engineer, Graduated November 2020.
  - PM Science, Graduated 2021.
  - MSc Cyber Security, Graduated in June 2023.
  - PhD Computer Science, since October 2023.

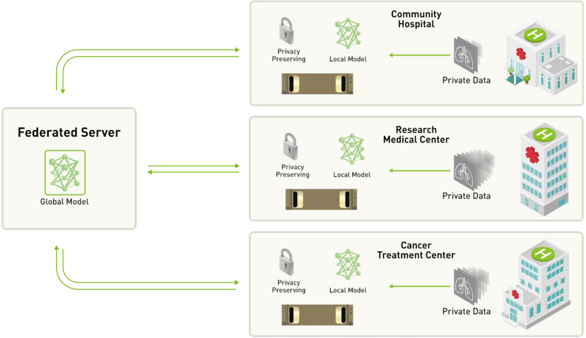
- Professional:
  - Summer Research Internship at UWE 2022: "Redactable Blockchain".
  - In process of submitting a paper: "Hybrid Outlier Clustering Method for IDS".

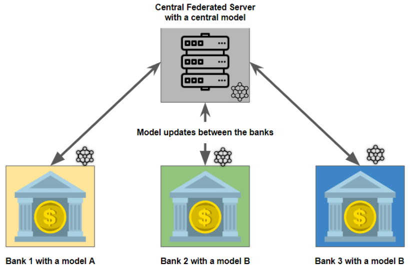
Federated Learning

- What is FL?

It is a machine learning approach allows multiple parties to collaborate in building a shared ML model while data decentralised and private.

- Applications of FL:
    - Healthcare and Medical Records.
    - Financial Services.
    - Retail and E-commerce.




Central Federated Server with a central model
Model updates between the banks
Bank 1 with a model A
Bank 2 with a model B
Bank 3 with a model B

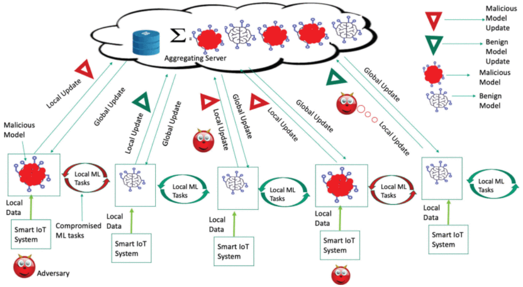
Federated Learning and Cyber Security.

- Cyber Security for Federated Learning:

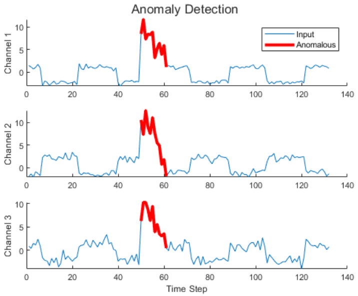
It involves implementing security measures and protocols to protect the privacy, integrity and confidentiality of data and models before, during and after the learning process.

- Federated Learning for Cyber Security:

It involves implementing federated learning techniques to improve security measures. FL can be applied to detect and respond to cyber threats.

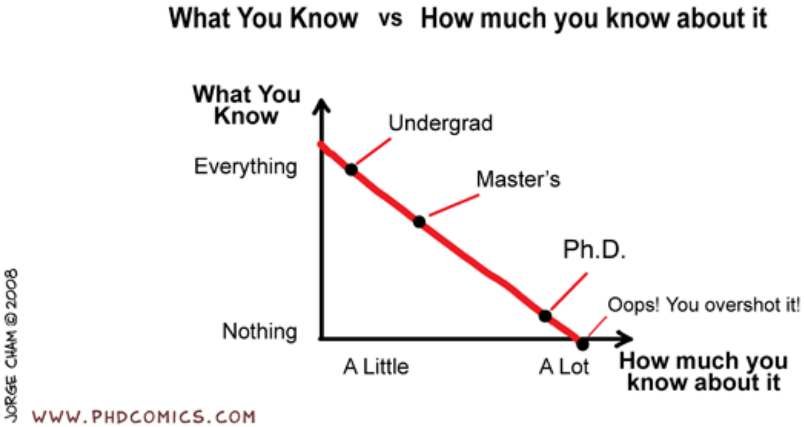


Data poisoning



Anomaly Detection

Questions



https://phdcomics.com/comics/archive.php?comicid=1056