UWE Bristol | University of the West of England

Cyber Security

Computer Science Research Centre

UWEcyber

UWEcyber

Gold Award

in association with National Cyber Security Centre

Department for Science, Innovation & Technology

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

31st October 2023

UWEcyber

UWEcyber was recognised by National Cyber Security Centre (NCSC) as one of the first Academic Centres of Excellence in Cyber Security Education (ACE-CSE) in December 2020, for our commitment to teaching and learning, outreach and external industry engagement.

Our MSc Cyber Security has been NCSC-certified since it started in 2018.

Our Degree Apprenticeship with Gloucestershire College is the only NCSC-certified programme in England and Wales.

Our undergraduate programme is to be submitted for certification in 2024 following module redesign.

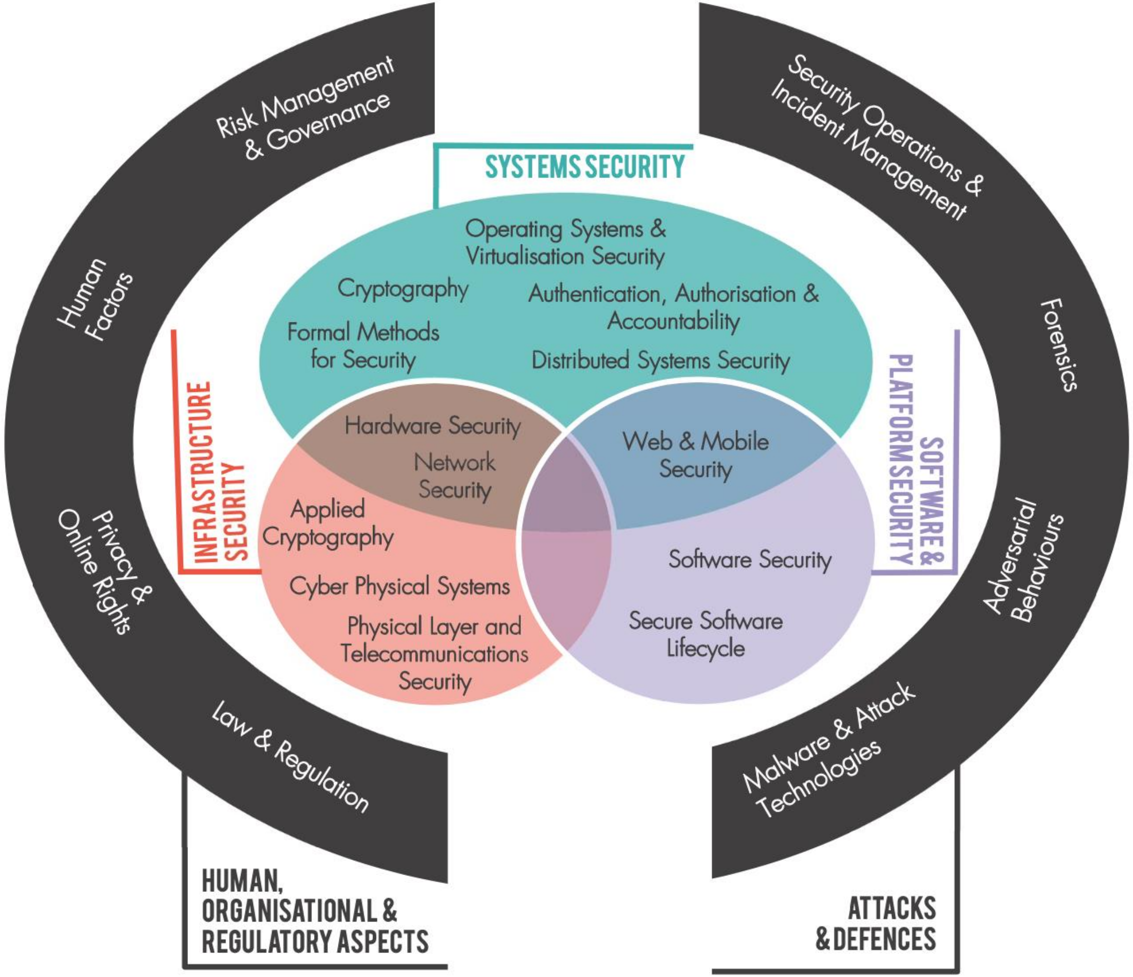
Gold Award

in association with National Cyber Security Centre

Department for Science, Innovation & Technology

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

UWE cyber UWE Bristol University of the West of England


Risk Management & Governance
Human Factors
Privacy & Online Rights
Law & Regulation
HUMAN, ORGANISATIONAL & REGULATORY ASPECTS
SYSTEMS SECURITY
Operating Systems & Virtualisation Security
Cryptography
Authentication, Authorisation & Accountability
Formal Methods for Security
Distributed Systems Security
INFRASTRUCTURE SECURITY
Hardware Security
Network Security
Applied Cryptography
Cyber Physical Systems
Physical Layer and Telecommunications Security
Web & Mobile Security
Software Security
Secure Software Lifecycle
SOFTWARE & PLATFORM SECURITY
Security Operations & Incident Management
Forensics
Adversarial Behaviours
Malware & Attack Technologies
ATTACKS & DEFENCES

CyBOK

NCSC Framework for what constitutes a Cyber Security Body of Knowledge.

Recent recognition of two new supplementary guides:

- Security and Privacy of AI
- AI for Security

All activity within our theme sits within one or more CyBOK Knowledge Areas.

Gold Award

in association with National Cyber Security Centre

Department for Science, Innovation & Technology

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

UWEcyber Research Strategy

Software, Cloud and Infrastructure Security

Container-based, Software Security, IoT, CAV, Hardware

Cyber Security Data Analytics

ML for Security, Security of ML, Explainable AI, Privacy, Transparency and Trust

Cyber Crime and Domestic Cyber Security

Online Harms, Forensic Analysis, Dark Web, Financial Crime

Pedagogical Research for Cyber Security

Effective interactive methods for teaching and learning

NCA
National Crime Agency

SOUTH WEST POLICE
ROCU
Regional Organised Crime Unit

Cyber First

Ministry of Defence

amazon web services

CyBOK

AVON & SOMERSET CONSTABULARY

SYNALOGiK

ribbon communications

LEONARDO

TECHMODAL

PA

VQ COMMUNICATIONS

Fusion Processing

MONTVIEUX

[dstl]

BAE SYSTEMS

CYNAM

TRIMETIS

UK CYBER SECURITY COUNCIL

splunk>

THE CYBER RESILIENCE CENTRE FOR THE SOUTH WEST

paloalto NETWORKS

Configured THINGS

UWE Bristol University of the West of England

UWE cyber

Gold Award

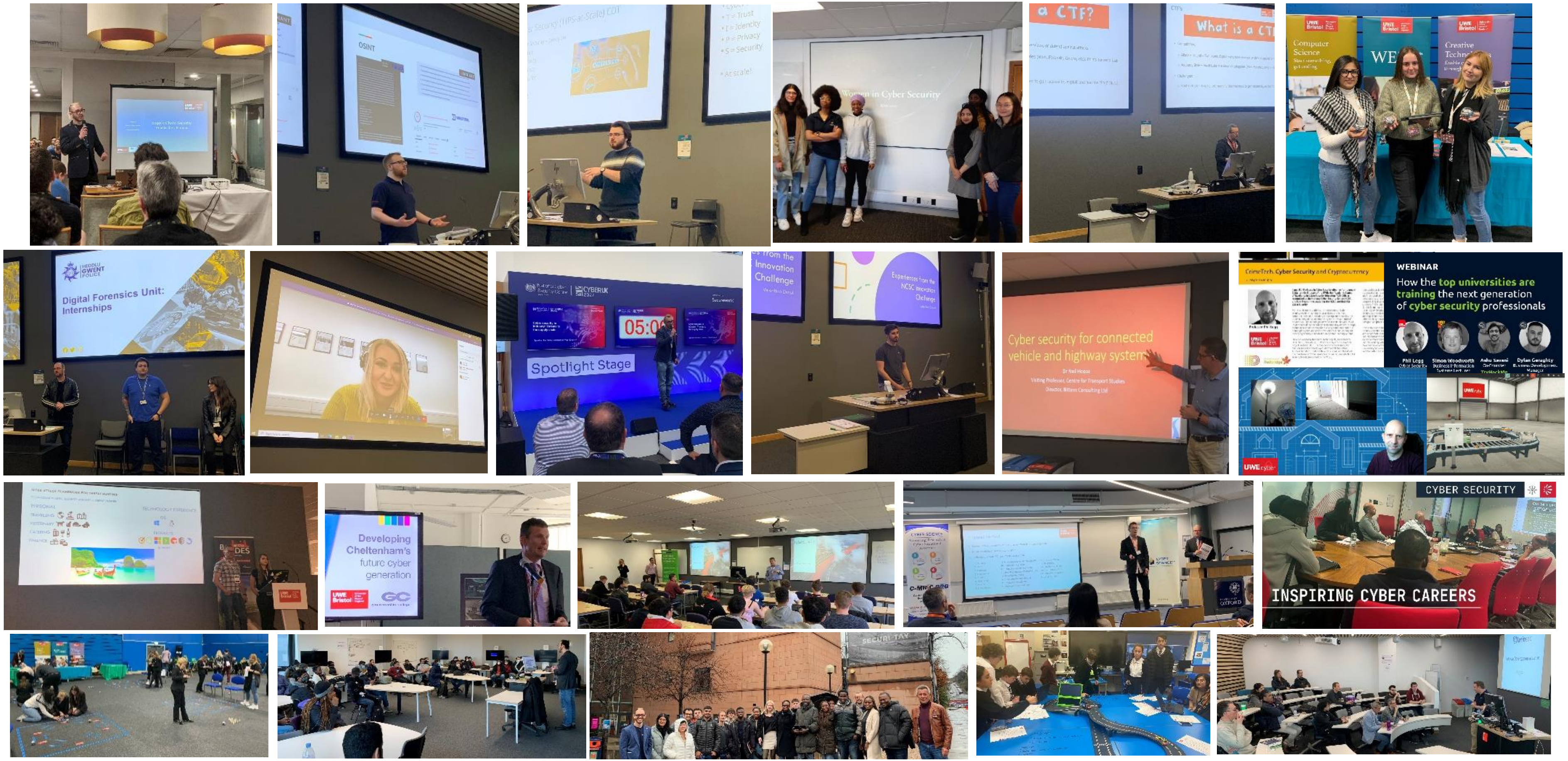
in association with National Cyber Security Centre

Department for Science, Innovation & Technology

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

gloucestershire college

GCHQ


OSINT
Trust
Identity
Privacy
Security
At scale!
Women in Cyber Security
a CTF?
What is a CTF
Computer Science
Creative Technologies
Digital Forensics Unit: Internships
CYBERUK
Spotlight Stage
05:0
Innovation Challenge
Experiences from the NCSC Innovation Challenge
Cyber security for connected vehicle and highway systems
CrimeTech, Cyber Security and Cryptocurrency
WEBINAR
How the top universities are training the next generation of cyber security professionals
Phil Legg
Simon Woodworth
Ashu Savani
Dylan Geraghty
Developing Cheltenham's future cyber generation
CYBER SECURITY
INSPIRING CYBER CAREERS
OXFORD
SECURI-TAY

UWE Bristol | University of the West of England

UWEcyber

Gold Award

in association with National Cyber Security Centre

Department for Science, Innovation & Technology

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

Staff Profiles and Research

UWE cyber

UWE Bristol University of the West of England

Research Staff Members

Cyber Threat Intelligence in Industry 4.0

- Current research: Cyber Threat Intelligence in Distributed Environments
- PhD supervision: Digital Twins-based Advanced Persistent Threats in Smart Manufacturing Environments
  - PhD candidate: Ms. Carol Lok Yi Lo

- Publications
  - C.Lo, TY.Win, Z.Rezaeifar, Z.Khan, P.Legg, 2023, "Digital Twins in Industry 4.0 Cyber Security". Submitted to the IEEE Smart World Congress 2023, Portsmouth, United Kingdom.

Dr Thomas Win
Thomas.Win@uwe.ac.uk

Low Resource Virtualisation Security

- What does that mean?
  - Containerisation and similar virtualisation tech
- Why is it important?
  - Because of their real world usage ->
- What am I doing?
  - Focus on real world security
  - Vulnerability analysis in Computers and Security
  - Visualisation software in IEEE CSR

Lockheed Martin in November conducted a flight test mission featuring distributed processing onboard a U-2 via the Kubernetes software containerisation technology. Kubernetes, for military applications, will enable weapon systems to pool onboard computing power to meet advanced system and software needs on demand. (Lockheed Martin)

https://www.janes.com/defence-news/news-detail/lockheed-martin-conducts-u-2-flight-with-kubernetes-software-containerisation-technology

Alan Mills
Alan.Mills@uwe.ac.uk

CySec and DFIR Research

Gareth Davies

Senior Academic & Researcher

Forensics Consultant

First Forensic Forum (F3) Chairman

UK Digital Forensics Specialist Group

Criminal Justice Board (Digital Evidence)

Interpol DF & Car Cyber Threat Expert Group

Interests include:

❑ HDD Physical and Logical Restoration
❑ Embedded Device Data Recovery
❑ NAND Flash Technology
❑ Cars (JDM mostly)
❑ Vehicle Systems Analysis
❑ Fundraising for Charity (Mountains / Hiking)

Recent Research Output:

Digital Investigator Journal:

‘**Defining User Requirements and Technical Specifications to Assist with Effective Validation of Digital Forensics methods.**’

in conjunction with UK Government (FCN) and Kings College London.

19th International Conference on Cyber Warfare and Security (ICCWS 2024):**‘A.I. Lifecycle Forensics’, ‘Who Controls The Future of A.I.?’**(CySec perspective)

& **‘Resilience, Dependability and Security’** (CySec skills shortage)

Gareth Davies
Gareth13.Davies@uwe.ac.uk

Protection in Armed conflicts: Security for vulnerable data

- **Area of research**: protection of personal data in a digital form during armed conflicts – case study Ukraine.
- **Main aim**: to investigate public attitudes towards cyberattacks in relation to privacy and data security through engaging with those Ukrainians who: who: 1) live in Ukraine, 2) are temporarily living in the UK, and 3) are permanently settled in the UK but have family connections in Ukraine.
- **Impact**: To develop and disseminate an evidence-based human-centric framework on cybersecurity and data protection during armed conflict.

Dr Aida Abzhaparova
Aida2.Abzhaparova@uwe.ac.uk

Research Topics

- Internet of Things (IoT) and Cyber Security
- Advanced Machine Learning and IoT/Smart City applications
- Mobile and Wireless Networks
- Distributed Systems and Network Security
- Smart builds and smart transportation

Publications:

https://scholar.google.com/citations?user=B0rtByAAAAAJ&hl=en

Dr Djamel Djenouri
Djamel.Djenouri@uwe.ac.uk

UWE cyber

UWE Bristol University of the West of England

Cyber Attacks Detection and Mitigation Approaches in Smart City Technologies (Cloud and IoT)

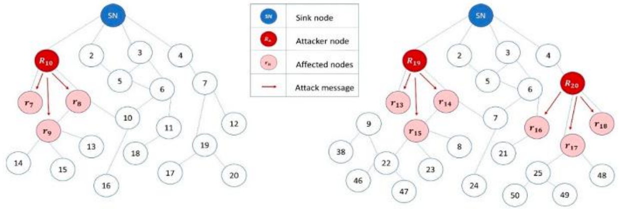
- My research focuses on cloud and IoT security in smart cities and recently I have been working on Routing Protocol for Low-power and Lossy Networks (RPL).

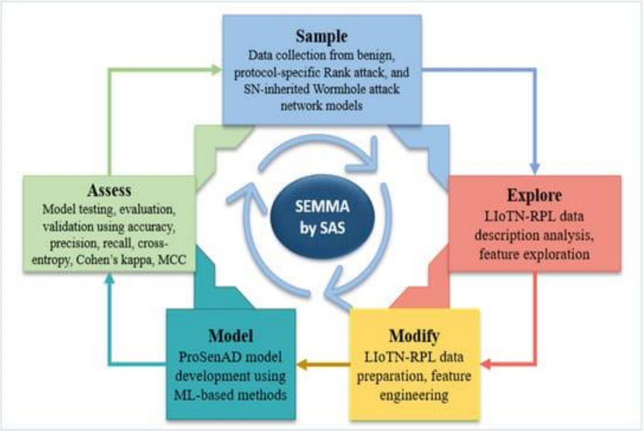
- For networks with limited resources, such as IoT-enabled smart homes, smart industrial equipment, and urban infrastructures, the Routing Protocol for Low-power and Lossy Networks (RPL) was developed.

- The lack of active security features in RPL makes them vulnerable to attacks. The types of attacks include protocol-specific ones and those inherited by wireless sensor networks.

- In our latest research we developed a security approach to improve the security against PS-R attacks as well as SN-W attacks. Our model is developed based on multiclass classification approaches and it effectively detects attacks sensor inherited RPL attacks in comparison to the related research contributions.

- My upcoming research focuses more on developing cloud security approaches for smart cities to protect data-in-motion.





Sample
Data collection from benign, protocol-specific Rank attack, and SN-inherited Wormhole attack network models

Explore
LIoTN-RPL data description analysis, feature exploration

Modify
LIoTN-RPL data preparation, feature engineering

Model
ProSenAD model development using ML-based methods

Assess
Model testing, evaluation, validation using accuracy, precision, recall, cross-entropy, Cohen's kappa, MCC

SEMMA by SAS

Dr Sarfraz Brohi
Sarfraz.Brohi@uwe.ac.uk

Recent publication: Zahra, F.; Jhanjhi, N.Z.; Khan, N.A.; Brohi, S.N.; Masud, M.; Aljahdali, S. Protocol-Specific and Sensor Network-Inherited Attack Detection in IoT Using Machine Learning. Appl. Sci. 2022, 12, 11598. https://doi.org/10.3390/app122211598

Cyber Security Research

- **PhD students' projects**
  - **Graph-based group anomaly detection in IoT with deep learning :** in this project, we look at graph-based method that leverage deep learning approaches to detect group anomaly (*PhD student: Dalila Khettaf Supervisors: Djamel Djenouri and Zeinab Rezaeifar*)
  - **Design a Secure Digital Twin to Detect and Mitigate Advanced Persistent Threats on Cyber-Physical Systems in Smart Manufacturing**: in this project, we are exploring a secure method based on Digital Twin to detect and mitigate Advanced Persistent Threats (APTs). (*PhD student: Lok Yi Lo (Carol) Supervisors: Thomas Win, Phil Legg, Zaheer Khan, and Zeinab Rezaeifar*)

- **BTIIC-Situation Awareness**
  - It is a part of BT Ireland Innovation Centre (BTIIC) project which is funded by Invest Northern Ireland and representing major partnership between BT and Ulster University. The aim of the Situation Awareness project is to reconstruct and detect multi-step attack scenarios (APT attacks) through automated correlation of alert data. (April 2020-Present)(*RA: Zeinab Rezaeifar* (BT Ireland Innovation Centre (ulster.ac.uk)))

Dr Zeinab Rezaeifar
Zeinab.Rezaeifar@uwe.ac.uk

Research Interests

UWE cyber UWE Bristol University of the West of England

Federated Learning

Collaborative machine learning, training a shared model without exchanging private data

- **Application of FL to cyber security domain**
- **Security of FL mechanisms**

Container Security

Tools & techniques to secure infrastructure, images, & runtime environment of Docker

- **Visualisation of threats**
- **Analysis of threats over time**

Network-based Anomaly Detection

Identifying abnormal network traffic indicating malware or unauthorised access

- **Detection and remediation of Home IoT threats**

White, J. and Legg, P. (2023a). Federated Learning: Data Privacy and Cyber Security in Edge-Based Machine Learning. In *Data Protection in a Post-Pandemic Society: Laws, Regulations, Best Practices and Recent Solutions* (pp. 169-193). Cham: Springer International Publishing.

White, J. and Legg, P. (2023b) Evaluating Data Distribution Strategies in Federated Learning: A Trade-off Analysis between Privacy and Performance for IoT Security. *9th International Conference on Cyber Security, Privacy in Communication Networks (ICCS) 2023* (*Under Review*)

White, J., & Legg, P. (2021). Unsupervised one-class learning for anomaly detection on home IoT network devices. In 2021 International Conference on Cyber Situational Awareness (CyberSA).

Jonathan White
Jonathan6.White@uwe.ac.uk

Cyber Research

Dr. Andrew McCarthy – Senior Lecturer

Research Interests

Methods for improving Robustness against adversarial Machine learning Attacks.

Evasion attacks on Intrusion Detection Systems

Secure and Safer Machine Learning Models

Supported Decision Making

Research outputs

Functionality-Preserving Adversarial Machine Learning for Robust Classification in Cybersecurity and Intrusion Detection Domains: A Survey
A McCarthy, E Ghadafi, P Andriotis, P Legg
Journal of Cybersecurity and Privacy 2 (1), 154-190

Feature Vulnerability and Robustness Assessment against Adversarial Machine Learning Attacks
A McCarthy, P Andriotis, E Ghadafi, P Legg
2021 International Conference on Cyber Situational Awareness, Data Analytics …

GRAIMATTER Green Paper: Recommendations for disclosure control of trained Machine Learning (ML) models from Trusted Research Environments (TREs)
E Jefferson, J Liley, M Malone, S Reel, A Crespi-Boixader, X Kerasidou, ...

Shouting Through Letterboxes: A study on attack susceptibility of voice assistants
A Mccarthy, BR Gaster, P Legg
2020 International Conference on Cyber Security and Protection of Digital …

Defending against adversarial machine learning attacks using hierarchical learning: A case study on network traffic attack classification
A McCarthy, E Ghadafi, P Andriotis, P Legg
Journal of Information Security and Applications 72, 103398

Safe machine learning model release from Trusted Research Environments: The AI-SDC package
J Smith, R Preen, A McCarthy, AC Boixander, J Liley, S Rogers

Dr Andrew McCarthy
Andrew6.McCarthy@uwe.ac.uk

Cyber Forensic Research

Jay Murphy – Programme leader and Senior Lecturer BSc – Cyber Security and Digital Forensics.

Developing research interests

Dynamic crime scene triage, Dark web(DW) Investigations and mobile device forensics.

Research output

Social Media and Dark Web analysis for Digital Investigations: Contextualising Dark Web Investigations (House, Murphy, Legg – In progress/2023)

DPhil - 2024

Lifting the Fog of War: Preserving Digital Fingerprints on the modern battlefield

This project aims to confront the challenges and add to the body of knowledge of digital forensic practices conducted on the modern battlefield, specifically to identify, preserve, maintain and leverage evidence that will be used in the prosecution of war crimes committed during armed conflicts.

(Bellingcat, 2022)

Team, B.I. (2022) *Tracking the Faceless Killers who Mutilated and Executed a Ukrainian POW bellingcat*. 5 August 2022 [online]. Available from: https://www.bellingcat.com/news/2022/08/05/tracking-the-faceless-killers-who-mutilated-and-executed-a-ukrainian-pow/ [Accessed 29 October 2023].

Jay Murphy
Jay.Murphy@uwe.ac.uk

A secure routing approach based on league championship algorithm for wireless body sensor networks in healthcare.

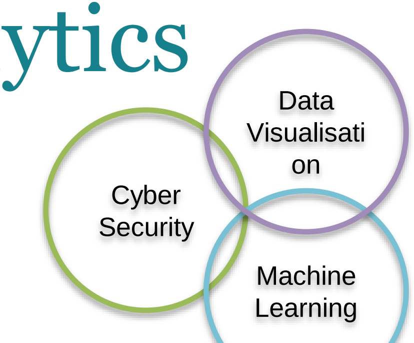
This research work introduced a secure routing approach for wireless body sensor networks in healthcare, aiming to balance energy efficiency and security. The approach employs the league championship algorithm for cluster head selection and utilizes both symmetric and asymmetric encryption for intra-cluster and inter-cluster secure connections. Simulation results demonstrate its efficiency in terms of energy consumption, delay, throughput, packet delivery rate, and packet loss rate.

Hosseinzadeh, M., Mohammed, A. H., Rahmani, A. M., A Alenizi, F., Zandavi, S. M., Yousefpoor, E., …Tightiz, L. (2023). A secure routing approach based on league championship algorithm for wireless body sensor networks in healthcare. *PLoS ONE*, *18(10)*, Article e0290119. https://doi.org/10.1371/journal.pone.0290119. Available from https://uwe-repository.worktribe.com/output/11149364

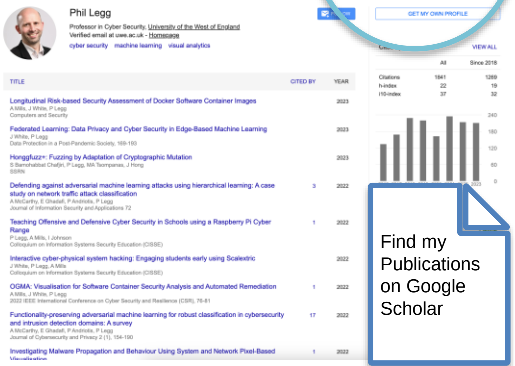
Dr Mazhar Malik
Mazhar.Malik@uwe.ac.uk

Cyber Security Data Analytics

How to make effective real-time decisions to manage Cyber Security challenges and threats, informed by both human and machine operators?



- **Recent Funded projects:**
  - InnovateUK - Transforming Suspicious Activity Reports
  - DSTL - Decision Support in Military Cyber Operations
  - DSTL - Human-as-a-Sensor for Mitigating Cyber Threats
  - DSTL - Autonomous Resilience for Cyber Defence



Phil Legg

Professor in Cyber Security, University of the West of England
Verified email at uwe.ac.uk - Homepage
cyber security machine learning visual analytics

GET MY OWN PROFILE

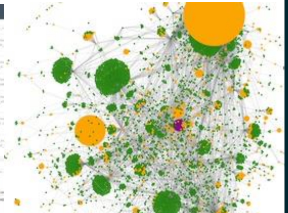
VIEW ALL

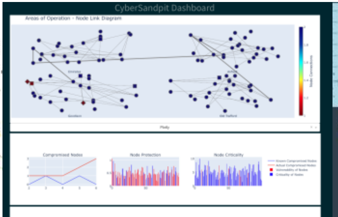
	All	Since 2018
Citations	1841	1269
h-index	22	19
i10-index	37	32

TITLE	CITED BY	YEAR
Longitudinal Risk-based Security Assessment of Docker Software Container Images A Mills, J White, P Legg Computers and Security		2023
Federated Learning: Data Privacy and Cyber Security in Edge-Based Machine Learning J White, P Legg Data Protection in a Post-Pandemic Society, 169-193		2023
Honggfuzz+: Fuzzing by Adaptation of Cryptographic Mutation S Bamohabbat Chafjiri, P Legg, MA Tsompanas, J Hong SSRN		2023
Defending against adversarial machine learning attacks using hierarchical learning: A case study on network traffic attack classification A McCarthy, E Ghadafi, P Andriotis, P Legg Journal of Information Security and Applications 72	3	2022
Teaching Offensive and Defensive Cyber Security in Schools using a Raspberry Pi Cyber Range P Legg, A Mills, I Johnson Colloquium on Information Systems Security Education (CISSE)	1	2022
Interactive cyber-physical system hacking: Engaging students early using Scalextric J White, P Legg, A Mills Colloquium on Information Systems Security Education (CISSE)		2022
OGMA: Visualisation for Software Container Security Analysis and Automated Remediation A Mills, J White, P Legg 2022 IEEE International Conference on Cyber Security and Resilience (CSR), 76-81	1	2022
Functionality-preserving adversarial machine learning for robust classification in cybersecurity and intrusion detection domains: A survey A McCarthy, E Ghadafi, P Andriotis, P Legg Journal of Cybersecurity and Privacy 2 (1), 154-190	17	2022
Investigating Malware Propagation and Behaviour Using System and Network Pixel-Based Visualisation	1	2022

Find my Publications on Google Scholar

Professor Phil Legg
Phil.Legg@uwe.ac.uk





PhD Students

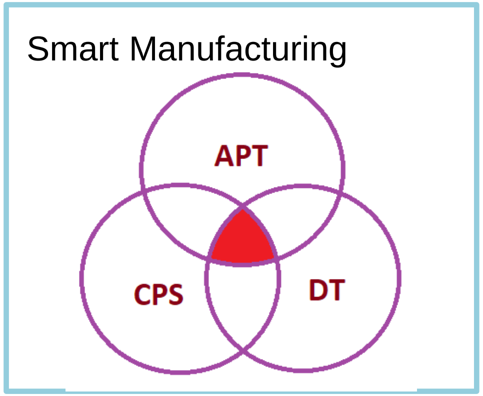
PhD Students

Carol Lo

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

Background

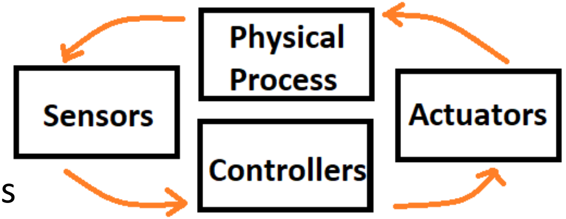
- Academic journey
  - MSc Cyber Security, graduated in March 2022
  - PhD research degree, since April 2023
    - Advanced Persistent Threats (APT), Cyber Physical Systems (CPS) and Digital Twins (DT)
- Enjoyable moments
  - Poster paper presented in IEEE Smart World in August
  - Collaborating with 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



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

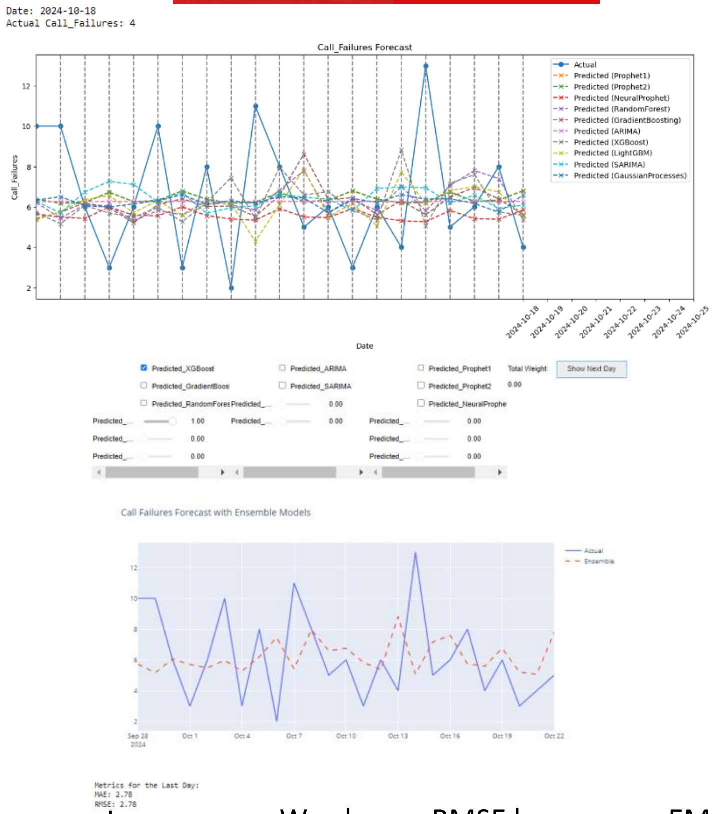
PhD: Interactive machine learning for identifying threats to security and service in large-scale mobile networks

Background Profile

- My PhD is in **interactive machine learning for identifying threats to security and service in large scale mobile networks.**
- I am a 2nd year postgraduate researcher and PhD student here at UWE.
- We are working in partnership with Ribbon Communications to align with the telecommunications industry in research outcomes.
- I studied a BSc in Applied Computing Technologies and an MSc in Cybersecurity.
- I was a lecturer at Plymouth university teaching years 1-3 of the cybersecurity and applied computing programmes.
- I have around 6 years of experience in open-source development both as a professional and hobbyist.

My Research; then done!

- I am currently focused on a research contribution in the field of **interactive time series forecasting**.
- My objective is to publish the results of my experimentation with **interactive dynamic model interrogation and calibration**, over traditional industry forecasting measures.
- Our hypothesis is that a **human-machine teaming** approach to IML leads to strong and more robust forecasts with better outcomes for **external unknown events** in time series.
- So far, we have built an expansive review of interactive, explainable ML literature and furthered this process by completing synthetically replicated real world data to drive new IML experimentation.



```
Date: 2024-10-18
Actual Call_Failures: 4
```

☑ Predicted_XGBoost ☐ Predicted_ARIMA ☐ Predicted_Prophet1 Total Weight: Show Next Day

☐ Predicted_GradientBoos ☐ Predicted_SARIMA ☐ Predicted_Prophet2 0.00

☐ Predicted_RandomFores Predicted_... 0.00 ☐ Predicted_NeuralProphe

Predicted_... 1.00 Predicted_... 0.00 Predicted_... 0.00

Predicted_... 0.00 Predicted_... 0.00

Predicted_... 0.00 Predicted_... 0.00

```
Metrics for the Last Day:
MAE: 2.78
RMSE: 2.78
```

$$RMSE = \sqrt{\sum_{i=1}^{n} \frac{(\hat{y}_i - y_i)^2}{n}}$$

We choose RMSE here as our EM to make active model reconfigurations upon.

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

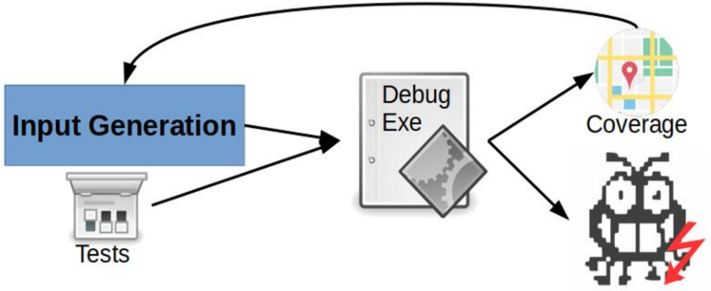
Cybersecurity Analytics

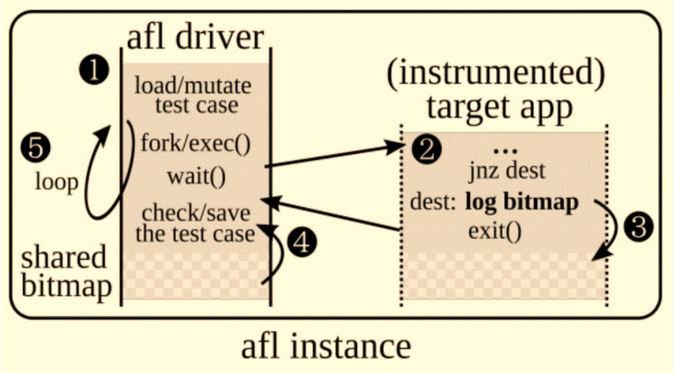
Security Engineering and Cryptography

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!

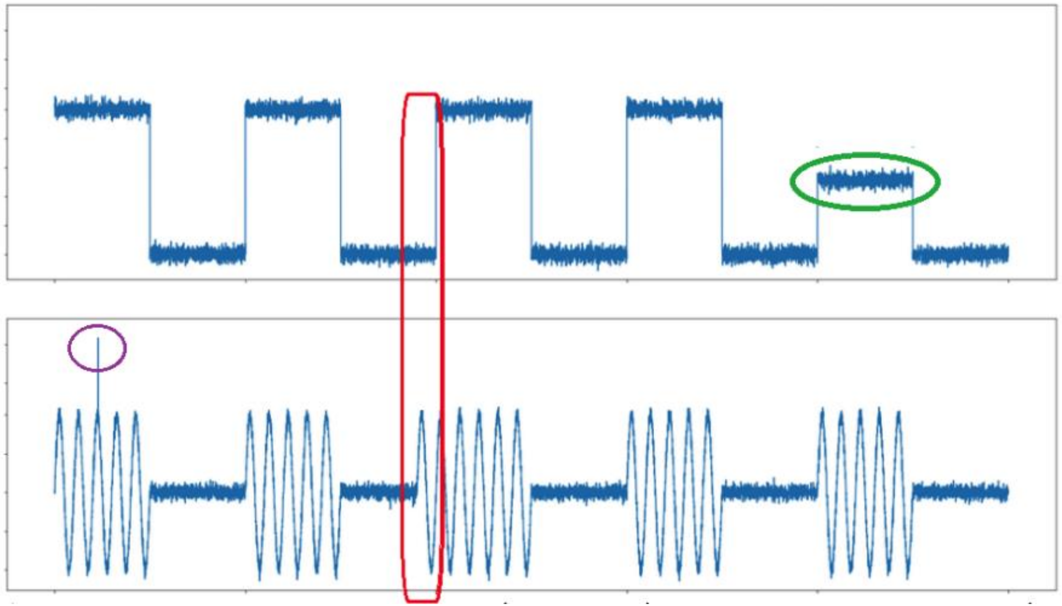


Figure 1: The three anomaly types (Audibert et al, 2022)

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

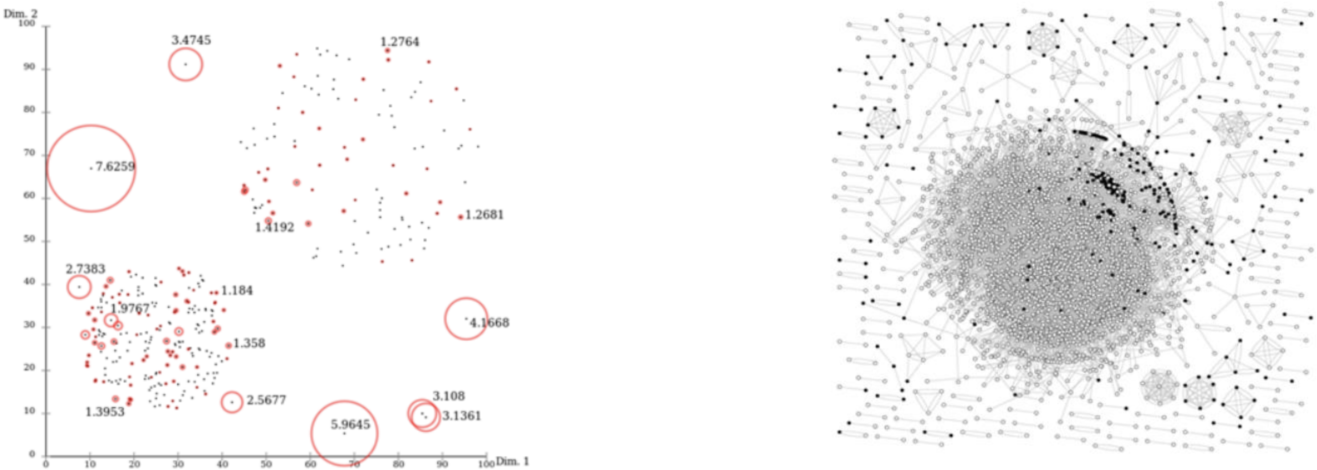


Figure 2: Point Vs group anomalies

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

Great potential

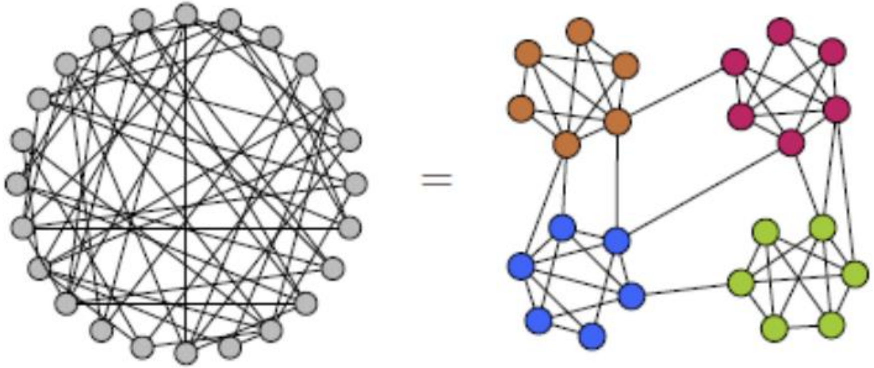


Figure 4: Graphs for group anomaly detection

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.

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.

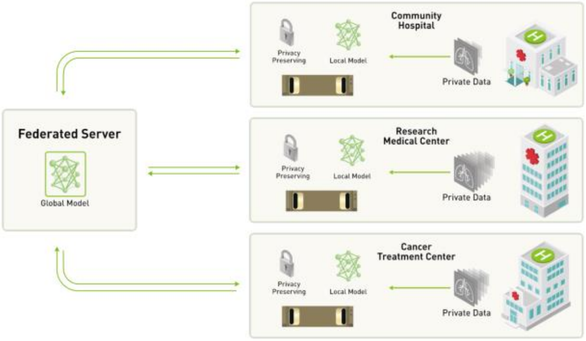
- Professional:
  - Summer Research Internship at UWE 2022: "Redactable Blockchain".
  - In process of submitting a paper: "Hybrid Outlier Clustering Method for IDS".

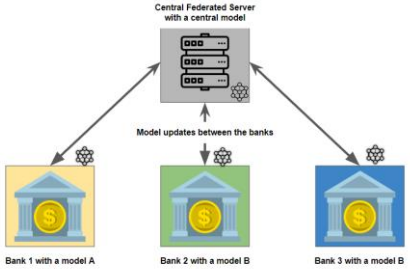
Federated Learning

- 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

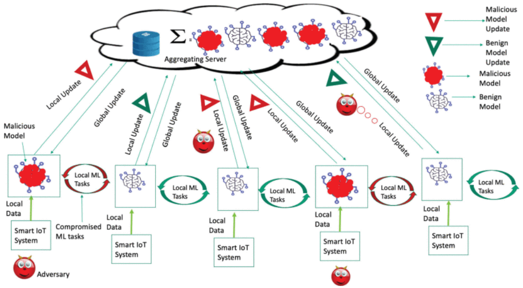
Federated Learning and Cyber Security.

- Cyber Security for Federated Learning:

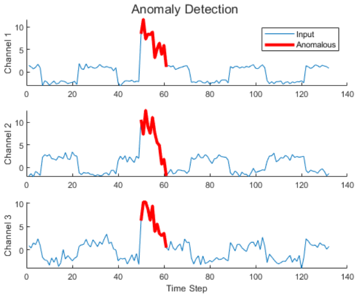
It involves implementing security measures and protocols to protect the privacy, integrity and confidentiality of data and models before, during and after the learning process.

- 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

Discussion

Collaborative opportunities?