CSCT Research and CSRU

Presentation by

Dr. Phil Legg

Senior Lecturer in Computer Science

September 2017

UWE Bristol | University of the West of England

CYBER SECURITY RESEARCH UNIT

Computer Science and Creative Technologies

CSCT consists of 4 main research groups:

- Centre for Complex Cooperative Systems
- Artificial Intelligence Group
- Software Engineering Research Group
- Unconventional Computing Group

Centres are designed to facilitate smaller research Units:

- Cyber Security Research Unit

UWE Bristol University of the West of England

CYBER SECURITY RESEARCH UNIT

CSRU Staff

Dr. Abdullahi Arabo
CSRU Leader

Dr. Essam Ghaldafi

Dr. Elias Pimenidis

Dr. Theo Spyridopoulos

Dr. Shancang Li

Ian Johnson
Forensic Computing and
Security Programme Leader

Dr. Panagiotis
Andriotis

Dr. Phil Legg

Dr. Emmanuel
Ogunshile

UWE Bristol | University of the West of England

CSRU Research Interests

- Complex Systems of Systems
- AI / ML for Cyber Security
- Visual Analytics for Cyber Security
- Human-Machine Decision Support
- Application Security
- Context-Aware Systems
- Industrial Control Systems
- "Internet of Things"
- Cryptography
- Malware Analysis
- Human Factors of Security

… and probably more!

UWE Bristol University of the West of England

CYBER SECURITY RESEARCH UNIT

CSRU Recent Projects

- "Spam Detection in Social Media using Message Propagation Dynamics" Dr Andriotis (Japan Society for the Promotion of Science).
- "The Provision of a Work Package for the Digital Crime Scene Forensics Review" Dr Li (Centre for Applied Science and Technologies, Home Office).
- "An Industrial Control System testbed for Cyber-security and Digital Forensics" Dr Spyridopoulos (VC Early Career Award).
- "App Collision and its Cybersecurity Implications" Dr Arabo (VC Early Career Award).
- "Brightpearl - Cloud Security Framework" Dr Arabo (Innovation4Growth).
- "*RicherPicture:* Automated network defence through business and threat-led machine learning" Dr Legg (DSTL).
- "Enhanced Personal Situational Awareness through Network and Systems Visualization" Dr Legg (VC Early Career Award).

UWE Bristol University of the West of England

CYBER SECURITY RESEARCH UNIT

CSRU In the News

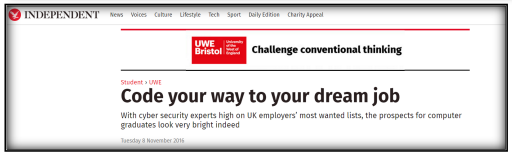
National Conference for Learning and Teaching in Cyber Security

Isaac Lau final year (2017) BSc (Hon) Forensic and Security got the prize for the best student presentation for his final year project title: "Android lock screen application to improve pattern based security" at the National Conference for Learning and Teaching in Cyber Security in hosted by Liverpool John Moores University.

Image: Dr Arabo collecting the prize on behalf of Isaac Lau.

UWE Bristol students win the Capture the Flag competition

CSRU team of students (Alan Mills - year 1, Alex Donose - year 2, Barry Gallivan - year 2, Curtis Adams - year 2 and Patrick McGrath - year 2) got the fourth place (among 16 teams) at the Capture the Flag competition which was organised by Cyber Security Challenge UK, doing better then some Russell group universities like Oxford.



UWE Bristol University of the West of England

CYBER SECURITY RESEARCH UNIT

CSRU Recent Publications

- Arabo, A. "CyberMix: A roadmap of SDN-based intelligent cybersecurity immune system". *International Conference on Cyber Warfare and Security, 2017*
- Arabo, A. "Mobile app collusions and its cyber security implications". *IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud)*, 2017
- Spyridopoulos, T., Maraslis, K., Tryfonas, T. and Oikonomou, G. "Critical Infrastructure Cyber-Security Risk Management" *NATO Science for Peace and Security Series - E: Human and Societal Dynamics. Volume 136: Terrorists' Use of the Internet, IOS Press, 2017.*
- Fagade, T., Spyridopoulos, T., Albishry, N. and Tryfonas, T. "System dynamics approach to malicious insider cyber-threat analysis and modelling". *Human Aspects of Information Security, Privacy and Trust: Proceedings of 5th International Conference, 2017*
- Spyridopoulos, T., Maraslis, K., Mylonas, A., Tryfonas, T. and Oikonomou, G. "A game theoretical method for cost-benefit analysis of malware dissemination prevention" *Information Security Journal: A Global Perspective, 2015*
- Legg, P. "Human-machine decision support systems for insider threat detection". *Data Analytics and Decision Support for Cybersecurity: Trends, Methodologies and Applications. Springer, 2017*
- Erola, A., Agrafiotis, I., Happa, J., Goldsmith, M., Creese, S. and Legg, P. "RicherPicture: Semi-automated cyber defence using context-aware data analytics". *International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2017*

UWE Bristol University of the West of England

CYBER SECURITY RESEARCH UNIT

CSRU Recent Publications

- Legg, P. "Visual analytics for non-expert users in cyber situation awareness" *International Journal on Cyber Situational Awareness, 2016*
- Legg, P. "Visualizing the insider threat: Challenges and tools for identifying malicious user activity" *IEEE Visualization for Cyber Security (VizSec), 2015*
- Ghadafi, E. "Efficient round-optimal blind signatures in the standard model". *Financial Cryptography and Data Security, 2017*
- Ghadafi, E. "More Efficient Structure-Preserving Signatures - Or: Bypassing the Type-III Lower Bounds". *European Symposium on Research in Computer Security (ESORICS), 2017*
- Ghadafi, E. and Groth, J. "Towards a Classification of Non-interactive Computational Assumptions in Cyclic Groups". *International Conference on the Theory and Applications of Cryptology and Information Security (ASIACRYPT), 2017*
- Li, S. and Xu, L. "*Securing the Internet of Things*" Elsevier. ISBN 9780128044582, 2017
- Andriotis, P., Li, S., Spyridopoulos, T. and Stringhini, G. "A comparative study of Android users' privacy preferences under the runtime permission model" *Human Aspects of Information Security, Privacy and Trust: Proceedings of 5th International Conference, 2017*
- Buchanan, W., Li, S. and Asif, R. "Lightweight cryptography methods"*Journal of Cyber Security Technology, 2017*
- Andriotis, P., Oikonomou, G., Tryfonas, T. and Li, S. "Highlighting relationships of a smartphone's social ecosystem in potentially large investigations" *IEEE Transactions on Cybernetics, 2016*

UWE Bristol University of the West of England

CYBER SECURITY RESEARCH UNIT

CSRU Research Interests

- CSRU has developed from a number of new academics joining UWE within the last 3-4 years, all with common research interests.
- We are a team of experienced researchers, with strong track records of publication and obtaining funding.
  - Many held post-doctoral posts in ”research intensive” institutions prior to joining UWE.

- ***Our aim is to continue doing excellent research, collaborating with excellent teams, and having real-world impact!***

UWE Bristol University of the West of England

CYBER SECURITY RESEARCH UNIT

Thank you

UWE Bristol | University of the West of England

CYBER SECURITY RESEARCH UNIT

Dr. Abdullahi Arabo
CSRU Leader

Dr. Essam Ghaldafi

Dr. Elias Pimenidis

Dr. Theo Spyridopoulos

Dr. Shancang Li

Ian Johnson
FC&S Programme Leader

Dr. Panagiotis Andriotis

Dr. Phil Legg

Dr. Emmanuel Ogunshile

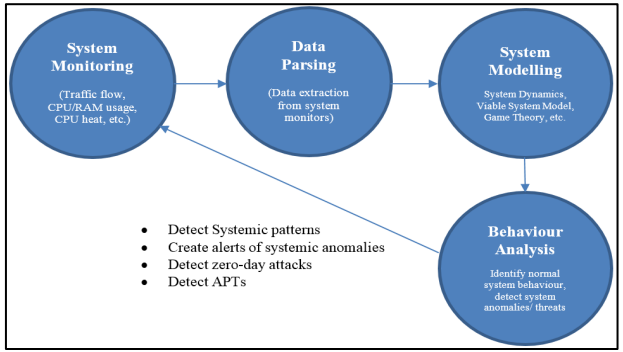
http://go.uwe.ac.uk/csru
@UWE_CSRU
@UWE_CSCT

Supplementary Materials: CSRU Research Activities

UWE Bristol | University of the West of England

CYBER SECURITY RESEARCH UNIT

Improving **Anomaly Detection** through the use of Systems Theory



- DSTL application for funding
- 1st year student already working on some areas of this idea

- Detect cyber threats in **Industrial Control Systems**, but can be used in many areas.
- Improve the way machine learning is used by adding the element of correlation between the datasets.
- Detect malicious activities that come from benign actions.
- Detect Advanced Persistent Threats (APTs).
- Can be used in multiple disciplines to detect anomalies that are not easily detected.

Dr. Theo Spyidopoulos
Theo.Spyridopoulos@uwe.ac.uk

UWE Bristol University of the West of England

CYBER SECURITY RESEARCH UNIT

An Industrial Control System testbed for Cyber-security and Digital Forensics

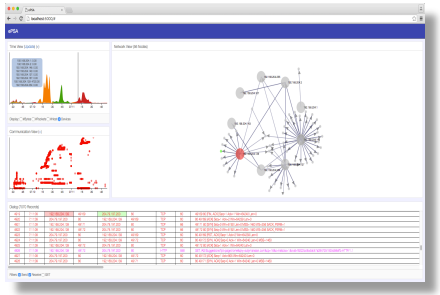
- **VC ECR Award** - Objectives of the project:
- Build an ICS testbed (a small industrial application controlled by commercial hardware and software) for cyber-security and digital forensics.
- Identify and collect digital evidence from the ICS testbed.
- Propose ways to improve forensic readiness in ICS.
- Further uses of the testbed:
- Testing cyber-security ideas (e.g. anomaly detection methods) on real case scenarios.
- Teaching platform in the Forensic Computing and Security programme.

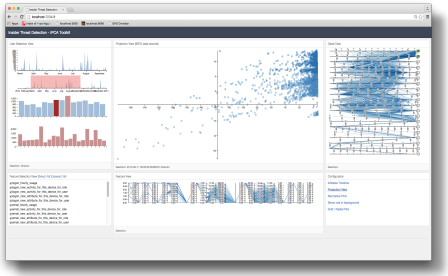
Dr. Theo Spyidopoulos
Theo.Spyridopoulos@uwe.ac.uk

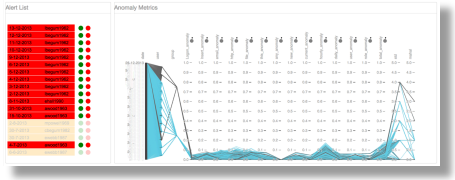
UWE Bristol University of the West of England

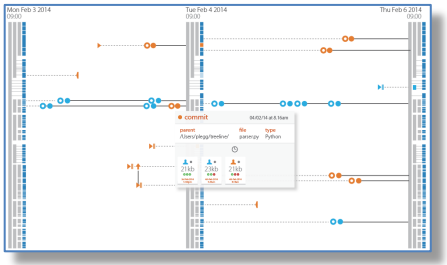
CYBER SECURITY RESEARCH UNIT

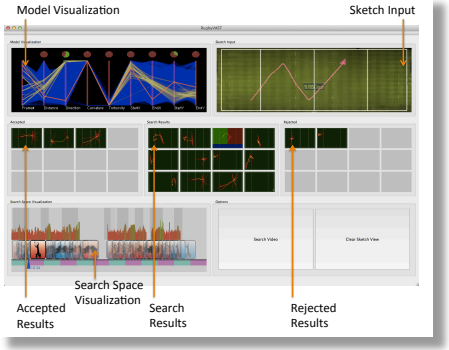
Visual Analytics and **Machine Learning** for Understanding Cyber-Security.

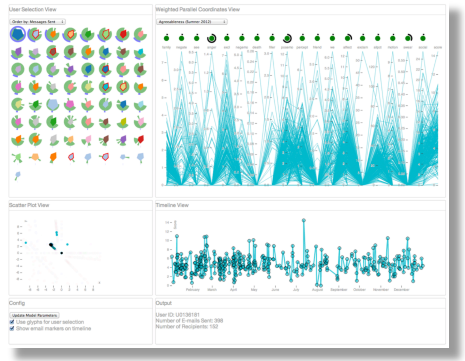












Dr. Phil Legg
Phil.Legg@uwe.ac.uk
http://plegg.me.uk
@dr_plegg

UWE Bristol University of the West of England

CYBER SECURITY RESEARCH UNIT

Visual Analytics and **Machine Learning** for Understanding Cyber-Security.

- *"Can users understand ML processes better using VA?"*
- *"Can ML be used to learn about user confidence and capability, based on their system interactions?"*
- *"Can ML learn to identify and ignore 'imperfect' and 'inconsistent' user input?"*
- *"How do we develop systems that effectively utilise both machine and user capabilities for data investigations?"*
- *"Can VA and ML support multiple user consensus in decision support, and facilitate conflict resolution?"*

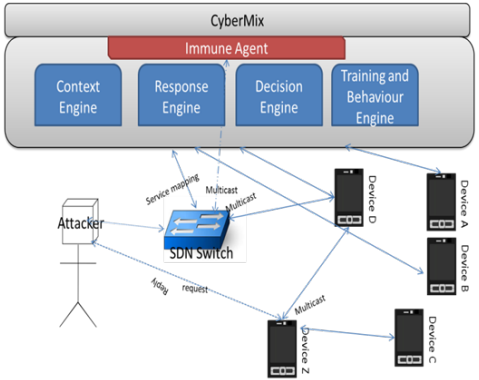
Dr. Phil Legg
Phil.Legg@uwe.ac.uk
http://plegg.me.uk
@dr_plegg

UWE Bristol | University of the West of England

CYBER SECURITY RESEARCH UNIT

CyberMix: A Roadmap of SDN-based Intelligent Cybersecurity Immune System

1. Develop a means to create dynamic, self-healing, pro-active and self-organisation protection rules
2. Use this knowledge to create dynamic CoA protection rules
3. Use the HIS algorithms scalability to protect very large infrastructures ecosystems
4. Demonstrate the protection using developed rules (in 1) on various smart device ecosystems.
5. Take a pro-active approach.



Dr. Adbullahi Arabo
Abdullahi.Arabo@uwe.ac.uk

UWE Bristol University of the West of England

CYBER SECURITY RESEARCH UNIT

Lightweight end-to-end security and privacy assurance in the IoT

- Aim: to develop end-to-end lightweight security and privacy assurance solutions for (IoT).
- Objectives:

1. Identifying security vulnerabilities of the resource-constrained smart devices in IoT and exploring the cyberthreats;
2. Developing lightweight cryptography primitives to achieve end-to-end security, supporting the implementation of energy efficient symmetric key algorithms over resource constrained smart objects within IoT, and

- Developing secure device access control framework for the interconnectivity of a large number of smart objects.

Dr. Shancang Li
Shancang.Li@uwe.ac.uk

UWE Bristol University of the West of England

CYBER SECURITY RESEARCH UNIT

Research Interests

- **Crypotography and Information Security**
- Provable Security
- Design of Practical Crypto Protocols
- Anonymous Attestation & Trusted Computing
- Attribute-Based Crypto
- Anonymous Credentials
- Digital Cash
- Post-Quantum Secure Protocols/Systems
- Digital Currencies & Blockchains
- Smart Metering
- New Applications of Crypto Techniques

UWE Bristol University of the West of England

Dr. Essam Ghaldafi
Essam.Ghadafi@uwe.ac.uk

CYBER SECURITY RESEARCH UNIT

Research Interests

- Digital Forensics (preferably on mobile devices, methods to automate DF tasks)
- Android Malware Analysis (static and behavioural analysis)
- Text mining for Security (sentiment analysis for short texts, LDA topic modelling for spam and bot detection on social media)
- Security and Privacy
- Blind Steganography detection on digital images
- Human factors of Information Security, Privacy and Trust (Android Pattern lock-screen biases, Android runtime permissions adoption, users' security profiles, implementation of security aware recommendation systems for digital markets)

Dr. Panagiotis Andriotis
Panagiotis.Andriotis@uwe.ac.uk

UWE Bristol University of the West of England

CYBER SECURITY RESEARCH UNIT