Centre for Cyber Security Research

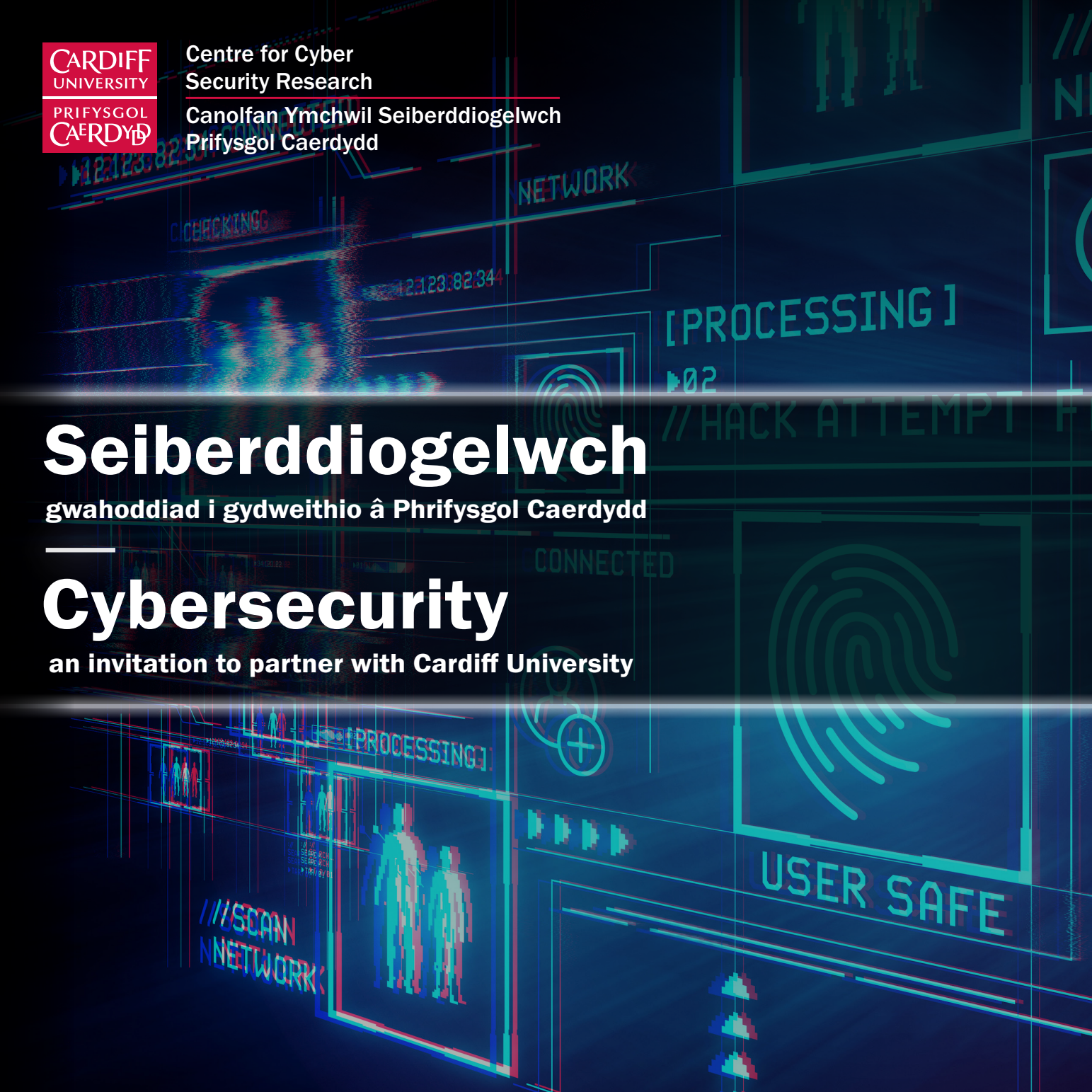
Canolfan Ymchwil Seiberddiogelwch Prifysgol Caerdydd

Seiberddiogelwch

gwahoddiad i gydweithio â Phrifysgol Caerdydd

Cybersecurity

an invitation to partner with Cardiff University



Ers dros ddegawd mae Prifysgol Caerdydd wedi bod ar flaen y gad o ran ymchwil seiberddiogelwch ac rydym wedi cael enw da am ein harbenigedd sy'n arwain y byd. Cafodd y Brifysgol ei henwi yn Ganolfan Ragoriaeth mewn Ymchwil Seiberddiogelwch gan Ganolfan Seiberddiogelwch Genedlaethol y DU (NCSC) yn 2018.

Rydym yn falch mai ni yw'r sefydliad cyntaf yng Nghymru i ennill y statws hwn ac rydym ni'n parhau i adeiladu ar yr arbenigedd trawiadol sydd eisoes yn bodoli ar draws y rhanbarth rhwng y byd academaidd, llywodraeth a busnes.

Mae ein hethos ymchwil dwys, sy'n seiliedig ar effaith, yn hanfodol i'n llwyddiant yn y maes hwn, ac fel Canolfan Ragoriaeth, mae'n ein galluogi i feithrin talent ifanc a datblygu'r genhedlaeth nesaf o weithwyr proffesiynol ym maes seiberddiogelwch.

Yr Athro Pete Burnap
Cyfarwyddwr Canolfan
Ymchwil Seiberddiogelwch

For more than a decade Cardiff University has been at the forefront of cybersecurity research earning a world-leading reputation for our expertise. The University was named as an Academic Centre of Excellence in Cyber Security Research by the UK's National Cyber Security Centre (NCSC) in 2018.

We are proud to be the first institution in Wales given this status as we continue to build on the impressive expertise that already exists across the region between academia, government and business.

Our research intensive, impact driven ethos is fundamental to our success in this area, and as a Centre of Excellence allows us to nurture more young talent and foster a pipeline of the next generation of cyber security professionals.

Professor Pete Burnap
Director of the Centre for
Cybersecurity Research

Mae cydnabyddiaeth gan y Ganolfan Seiberddiogelwch Genedlaethol yn dilysu arbenigedd y Brifysgol sy'n arwain y byd, ac yn dangos effaith ein hymchwil yn y byd real ar draws y DU.

Mewn cyfnod sydd â bygythiadau i'n seilwaith hanfodol na welwyd eu tebyg erioed, mae'n arbennig o galonogol gweld ymchwil Prifysgol Caerdydd yn cyfrannu at ymdrechion i ganfod ac atal ymosodiadau seibr.

Yr Is-Ganghellor, yr Athro Colin Riordan

The recognition afforded by the National Cyber Security Centre is validation of the University's world-leading expertise in this area, and further demonstrates the real-world impact that our research has on the UK as a whole.

At a time when threats to our critical infrastructure have never been greater, it's particularly encouraging to see Cardiff University research contributing to efforts to detect and deter cyber-attacks.

Vice-Chancellor Professor Colin Riordan

Canolfan Rhagoriaeth Academaidd mewn Ymchwil Seibr-ddiogelwch (ACE-CSR)

Mae Prifysgol Caerdydd yn ***un o ddim ond 19*** ACE-CSR yn y DU, a'r un cyntaf a'r unig un yng Nghymru.

Ariannu

Ers 2012, mae Prifysgol Caerdydd wedi derbyn ***mwy na £10 miliwn*** mewn cyllid i gefnogi ymchwil seibr-ddiogelwch.

Prosiectau

Ar hyn o bryd, rydym yn gweithio ar ***ystod eang o brosiectau*** gyda chyllid gan gyrff Ymchwil ac Arloesedd y DU (UKRI), megis yr Cyngor Ymchwil Peirianneg a Gwyddorau Ffisegol (EPSRC) a Chyngor Ymchwil Economaidd a Chymdeithasol (ESRC), ynghyd â'r diwydiant a'r llywodraeth.

Prosiectau Cydweithredol

Rydym yn gweithio gydag ***ystod eang o bartneriaid diwydiannol*** gan gynnwys Admiral Insurance, BAE systems, BT, HSBC, IBM, Thales a Toshiba.

Arbenigwyr

17 academydd a dros 40 o ymchwilwyr o bob rhan o cyfrifiadureg, seicoleg, troseddeg a'r gyfraith.

Academic Centre of Excellence in Cyber Security Research (ACE-CSR)

Cardiff University is ***one of only 19*** ACE-CSRs in the UK, and the first and only ACE-CSR in Wales.

Funding

Since 2012 Cardiff University has received ***more than £10m*** in funding to support cyber security research.

Projects

We are currently working on a ***wide range of projects*** with funding from UK Research and Innovation (UKRI) bodies, such as the Engineering and Physical Sciences Research Council (EPSRC) and Economic and Social Research Council (ESRC), industry and government.

Collaborations

We work with ***many industry partners*** including Admiral Insurance, Airbus, BAE systems, BT, HSBC, IBM, Thales and Toshiba.

Experts

17 academics and more than 40 researchers from across computer science, psychology, criminology and law.

UKRI Engineering and Physical Sciences Research Council

Academic Centre of Excellence in Cyber Security Research

ACE-CSR in association with National Cyber Security Centre

Centre for Cyber Security Research

Canolfan Ymchwil Seiberddiogelwch Prifysgol Caerdydd

Research themes

- Risk assessment and modelling
- Risk communication, governance and collective decision making
- Data-driven human and software behavioural analytics and threat intelligence
- Motivations, dynamics and social factors of cyber-crimes
- Security and privacy of emerging technologies

Grand Challenges

Automated cyber defence and security operations

The use of data science and AI methods, combined with expertise in criminology, psychology and international relations, to better utilise and interpret the vast volumes of data being produced on a daily basis for prediction and real-time automated responses to emerging cyber threats. This includes robustness testing of AI algorithms, better visualisation and explainability of AI algorithmic decisions, and communication of threats between interdependent people and processes.

Future of secure manufacturing

We aim to transform the future of manufacturing using data-driven technologies while retaining security via the integration of our research on automatic monitoring and control in safety critical systems. Our team are leading the safety critical systems theme in the National Centre of Excellence for the Internet of Things Cybersecurity (PETRAS).

Governing online harms

The Internet and Web are core ecosystems for launching cyber attacks. Do we have to accept they are not governable given their international reach? We aim to better understand the routine interactions in cyber space to allow us to use data to model and observe cause and effect in cyber attacks in an era of international political unrest.

Centre for Cyber Security Research

Canolfan Ymchwil Seiberddiogelwch Prifysgol Caerdydd

AI for cybersecurity

"Artificial Intelligence is at the heart of the UK government's industrial strategy and we are working to innovate with AI to improve automated cyber threat intelligence and support decision making and policy responses to make the UK more secure for individuals, businesses and the government."

Cybercrime costs the world almost £460bn a year with businesses worldwide incurring increasing losses as a direct result of cyber attacks.

The work we carry out at the Centre for Cyber Security Research (CCSR) focuses on the interdisciplinary fusion of artificial intelligence and cybersecurity, a concept we call Cyber Security Analytics.

We developed the first machine learning models to predict cyber attacks on online social networks such as Twitter, and desktop PCs you would see in every home and office.

This has allowed us to make in-roads into proactively blocking and preventing attacks, rather than reacting and repairing at a later date.

Our cutting-edge research and expertise in this area has also led to our partnership with Airbus - the European aerospace corporation - to develop new ways of detecting cyber attacks using Artificial Intelligence. This partnership has been awarded funding to enhance the adoption of automated detection and response capabilities by finding and testing new ways to 'explain' how the AI has decided there is a malicious presence on the network to security operations experts.

Our leading research on securing AI has led to new knowledge on testing the resilience and attack susceptibility of AI-powered defence systems, by providing an understanding of the limitations of current AI-deployed implementations and informing security by design considerations. Part of this work has been funded by the Alan Turing Institute.

AI for Cybersecurity contact:

Professor Pete Burnap – *BurnapP@cardiff.ac.uk*

Dr Tingting Li – *LiT29@cardiff.ac.uk*

www.cardiff.ac.uk/centre-for-cyber-security-research

Centre for Cyber Security Research

Canolfan Ymchwil Seiberddiogelwch Prifysgol Caerdydd

Cloud Security

"Our research aims to improve transparency and trust between users of online services and the service providers."

With increasing take up of externally provisioned and managed services (from government, finance, entertainment), often hosted over Cloud computing infrastructure, there is a realisation that on-line electronic services can involve an interlinked range of providers. However, from a user's perspective, trust in the use of these services remains limited. Although billions of people use smartphones and the Internet now, many still do not use that connectivity for shopping, banking, and other important transactions due to limited trust in on-line providers.

The ongoing EPSRC-funded project *PACE: Privacy-Aware Cloud Ecosystems*, addresses security and privacy requirements of environments where multiple Cloud computing providers need to work collaboratively to offer services to a user.

Users of these services only interact with a Web interface rather than the larger, distributed service ecosystem, and are often unfamiliar with the "ecosystem" of providers that are involved in offering them a particular capability. Their visibility beyond the first service provider is often missing, requiring them to "trust" the provider in handling and managing their data.

We propose a mobile software "container"-based solution that will ensure that all provider accesses to user data are securely logged in a Blockchain. This will improve transparency, enable an audit trail of providers and facilitate greater trust between users and service providers.

Our industrial partners in this research are Airbus, FlexiOPS Limited, Muckle LLP Solicitor, Simudyne Limited and T-Systems North America Inc, and our academic partnerships are with Newcastle University and UCL.

Cloud Security contact:

Professor Omer Rana – *ranaof@cardiff.ac.uk*

Centre for Cyber Security Research

Canolfan Ymchwil Seiberddiogelwch Prifysgol Caerdydd

Cyber in Organised Crime

"We have been combining social media data and social network analysis to identify successful strategies to disrupt criminal activities."

Over the years, organised crime has become a significant threat to societies around the world. International organised hacker groups that are skilled in developing hacking tools have cost financial services over €1bn across 40 countries by carrying out cyber-enabled attacks such as ransomware, distributed denial of service attacks, payment card fraud, etc.

To stop or reduce the harm from these organisations, government and law enforcement agencies worldwide seek ways to disrupt criminal groups effectively, preferably at an early stage.

Our work on Cyber in Organised Crime focuses on modern slavery, the sale of illicit drugs, the propagation of malware and money laundering, including 'money muling'. The research on malware propagation focuses on the spread of malware via social media platforms.

It aims to identify malware that are produced by an organised entity and to differentiate them from those which are the result of a single individual. Perhaps more importantly, we examine the impact of different strategies aimed at disrupting the diffusion of malware on social network platforms such as Twitter.

Our solutions can support law enforcement authorities, policy makers, private and third sector organisations to respond more effectively to organised crime, as we provide tested strategies to disrupt criminal organisations resorting to online technologies and to reduce harm to vulnerable people.

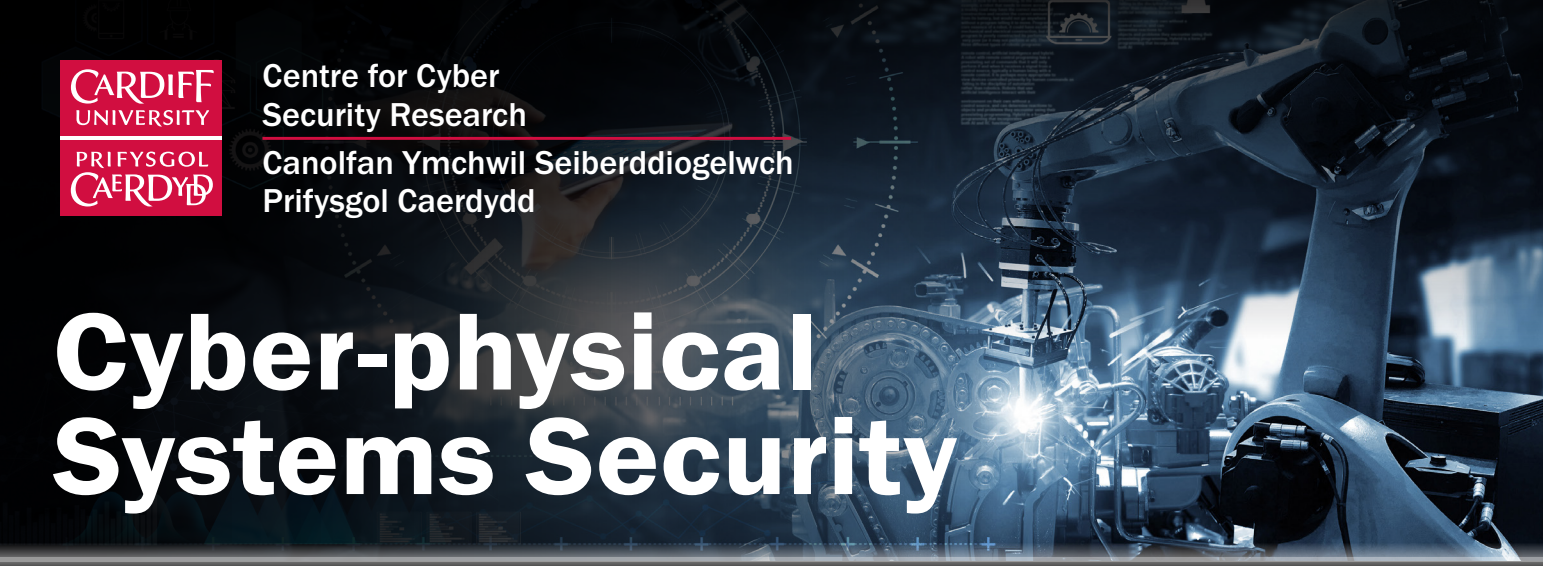
Our team works with private and public sector bodies, including fraud prevention organisation CIFAS, professional services firm Deloitte, South Wales Police and the Crown Prosecution Service (CPS).

Cyber in Organised Crime contacts:

Dr Luca Giommoni – *giommonil@cardiff.ac.uk*
Dr Amir Javed – *javeda7@cardiff.ac.uk*
Professor Mike Levi – *levi@cardiff.ac.uk*
Professor Matt Williams – *williamsm7@cardiff.ac.uk*

Centre for Cyber Security Research

Canolfan Ymchwil Seiberddiogelwch Prifysgol Caerdydd



Cyber-physical Systems Security

"Attacks on cyber-physical systems can have catastrophic consequences for life and the economy. We are working on securing these systems by developing novel ways of detecting and mitigating risks and attacks."

Cyber-physical systems in Critical National Infrastructure, in industrial settings, and in the home environment are increasingly being attacked by state actors and international cyber-criminals. The key characteristic of these systems is that they interact with the physical world. Successful attacks cause serious harm, including loss of human life and severe economic damage to entire supply chains.

At the Centre for Cyber Security Research (CCSR) we are developing methods for securing cyber-physical systems by detecting attacks, identifying risks, and predicting their potential impact.

We have a particular focus on Industrial Control Systems - detecting indicators of compromise and mitigating the impact of attacks through cyber incident-response and lightweight security solutions. We have conducted extensive research into risk assessment in cyber-physical systems.

We have translated our research on monitoring physical symptoms into a commercial solution supported by an Innovate UK start-up grant, while our work has also received funding support for securing smart grid systems.

Our collaborations with Airbus and Thales' National Digital Exploitation Centre (NDEC) brings our expertise to the real world.

Cyber-physical Systems contacts:

Dr Philipp Reinecke – *reineckep@cardiff.ac.uk*

Dr Neetesh Saxena – *saxenan4@cardiff.ac.uk*

Centre for Cyber Security Research

Canolfan Ymchwil Seiberddiogelwch Prifysgol Caerdydd

Human factors of cybersecurity

"We do not believe that humans should be the weakest link in cyber security: in fact humans have the capabilities to be the strongest line of defence and our cutting edge research is based upon this ethos. We are developing innovative methods to harness our unique human cognitive capabilities, while also better understanding our limitations, evidenced under certain conditions."

Understanding the nature of human behaviour is a key way in which challenges to cyber security can be addressed in order to suggest ways of safeguarding individuals, companies and institutions.

The Human Factors Excellence (HuFEx) Research Group Defence and Security theme has a key focus on Cyberpsychology as does the Human-centred Technologies and Society theme of the Cardiff University Centre for AI, Robotics and Human-Machine Systems (IROHMS).

With more than £1m cyberpsychology-related funding over the past two years from the likes of Airbus, CREST, Endeavr Wales, ESRC and NCSC, our research includes systematic studies investigating human susceptibility to cyber-attack techniques. Our work focuses on the development of methods to combat this significant national and international threat.

In addition to research at Cardiff University, HuFEx Director and IROHMS Director of Research Professor Phil Morgan is currently leading a new Airbus Accelerator in Human-Centric Cyber Security in a bid to better understand human cyber strengths, vulnerabilities, and methods of securely interacting with digital systems within organisations. Findings and initiatives are being developed and tested and will be rolled out across Airbus through existing training and awareness schemes, and also shared with partners in an attempt to drive a step change in thinking for the cyber security community.

Human factors contact:

Professor Phil Morgan – *MorganPhil@cardiff.ac.uk*

CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD

Centre for Cyber Security Research

Canolfan Ymchwil Seiberddiogelwch Prifysgol Caerdydd

Privacy by design

"We have been designing rigorous statistical and multi-objective optimisation methods to anonymise and obfuscate the data in a way that balances best between making useful inferences while hiding sensitive data."

There are clear advantages to living in a world in which the collection and storage of data is so prevalent, such as using the information to improve existing services or create entirely new ones via Deep Learning, Machine Learning and AI techniques.

However, there are also clear downsides when this same data can be sensitive (eg. medical records) or it can be used to make sensitive inferences about people when it comes to web browsing data, purchase history, location and mobility data.

The same can be said for Internet of Things (IoT) applications which typically collect and analyse personal data that can be used to derive sensitive information about individuals, but privacy concerns have not been explicitly considered in software engineering processes, partly due to a lack of tools, technologies and guidance.

Our work in privacy by design and in machine learning and cloud aims to find a balance at which both the user and the collector are as happy as possible with the amount and type of data being shared. We provide solutions that extract as much use out of the data that the user consents to provide, or to protect privacy as much as possible while guaranteeing a utility level. We are currently aiming to protect against sensitive disclosures from published machine learning models.

Privacy contact:

Dr George Theodorakopoulos
theodorakopoulosg@cardiff.ac.uk

Centre for Cyber Security Research

Canolfan Ymchwil Seiberddiogelwch Prifysgol Caerdydd

Airbus Centre of Excellence in Cyber Security Analytics

Cardiff University's expertise in cybersecurity analytics has led to a unique collaboration with Airbus - the European aerospace corporation - to create cutting-edge cybersecurity risk mitigation tools that have transformed the company's global digital security strategy.

The successful partnership was first established through Airbus Endeavr Wales, a joint research programme between Airbus and the Welsh Government. Our involvement centred on the quantification of risk in industrial manufacturing systems. The research outcomes produced were transitioned by Airbus into a functional tool that combines risk assessment, dependency modelling capability, and impact analysis for manufacturing systems and industrial supply chains.

Following the first publication of our early research into behavioural modelling of malware, Airbus recognised the innovation potential and our team was tasked with exploring novel malware detection methods incorporating machine learning for cyber-attack detection across the global Airbus IT and manufacturing network.

This key research was led exclusively at Cardiff University in collaboration with Airbus between 2016 and 2019, with the initial unique innovation aiming to distinguish malicious from trusted behaviour on computer networks using machine learning. Airbus then funded a PhD studentship to explore the concept further, and this work subsequently enhanced detection methods to include a world-first in predicting attacks during the early stages of execution, both from the Web and via desktop computing environments (eg. ransomware).

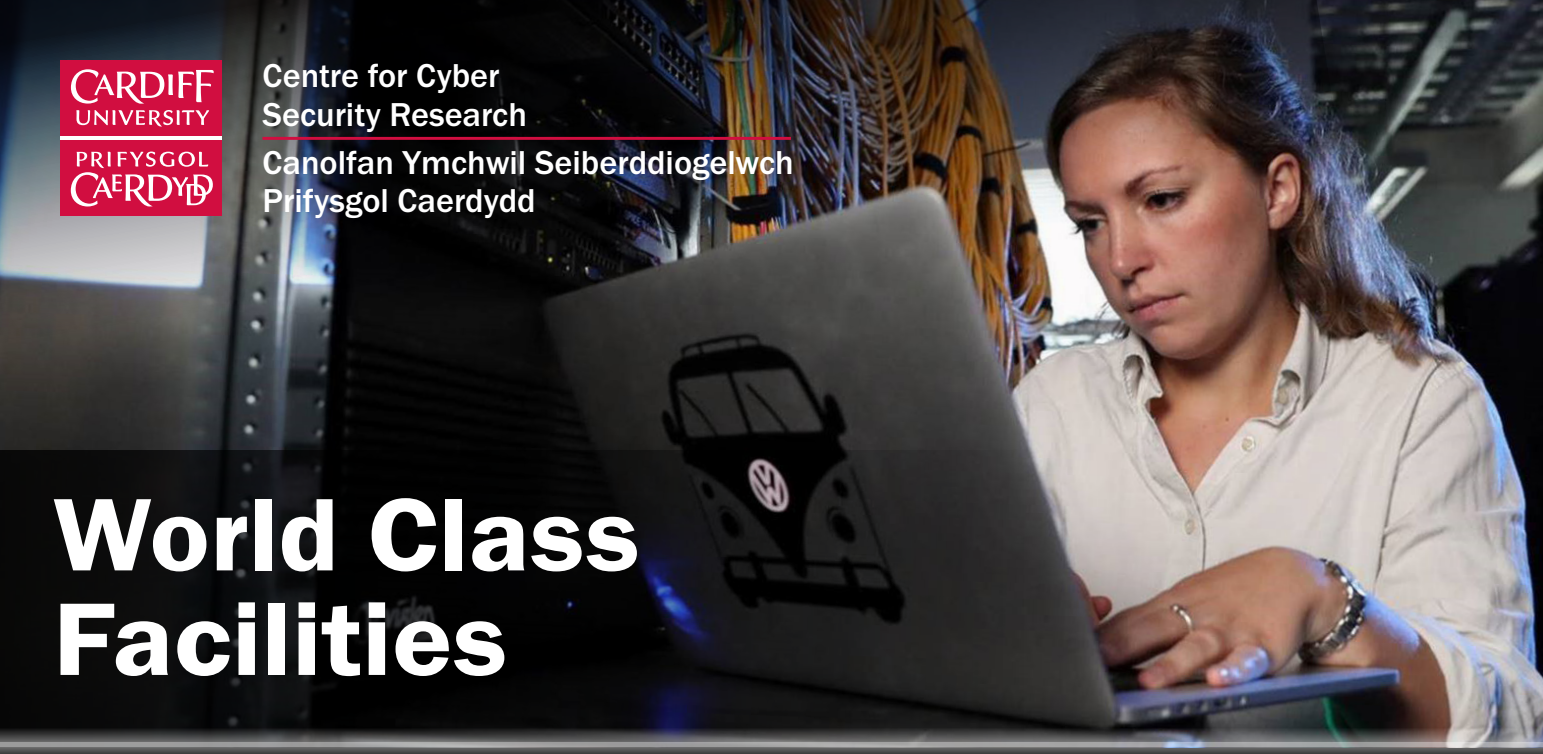
Airbus have directly invested more than £1.5m in collaborative research activity with our team, who are now providing leadership roles within the new £8m Welsh Government and Airbus-funded Cyber Lab that will research the next generation of cybersecurity solutions.

Airbus Centre of Excellence contact:

Professor Pete Burnap – *BurnapP@cardiff.ac.uk*

Centre for Cyber Security Research

Canolfan Ymchwil Seiberddiogelwch Prifysgol Caerdydd



World Class Facilities

We have invested millions of pounds in research infrastructure for cyber security, including a state-of-the-art cyber range and immersive cyber-attack and defence lab in the across the School of Computer Science and Informatics; and a new cyber security control centre zone, 6m x 6m Igloo dome, transport simulator with autonomous capabilities, cognitive robotics zone and a VR/AR space in the School of Psychology.

The facilities in both labs underpin experimental research for human and technical aspects of cybersecurity and developing evidence-based knowledge and understanding of next-generation cyber threats including:

- vulnerability testing a range of large next-generation virtualised infrastructures by threat hunting to identify where cyber-attacks could impact them
- determining the optimum approaches for ensuring security by design - ie. ensuring the threats are mitigated before the digital environment is rolled out in the real-world
- developing and testing novel automated cyber-attack and defence solutions
- training and skills development in both technical cyber-attack and defence methods, and human factors surrounding susceptibility to attack and communication/decision making responses to attack stimuli and cyber intelligence under stress while exposed to attack.

www.cardiff.ac.uk/centre-for-cyber-security-research

Centre for Cyber Security Research

Canolfan Ymchwil Seiberddiogelwch Prifysgol Caerdydd

The National Software Academy

"Our ethos is centred on giving students "real life" projects to work on throughout their studies and providing opportunities to engage with experienced software engineers from industry."

The National Software Academy is a centre of excellence for software engineering in Wales, which was established to address the shortfall of qualified, industry-ready software engineers.

A partnership between Cardiff University, the Welsh Government and industry leaders, the National Software Academy (NSA) aims to produce sought after graduates with industrial experience who will be recognised as leaders in their field.

We deliver innovative Software Engineering degrees at both undergraduate and postgraduate level, and our course content has been designed with input from leading organisations to ensure students gain experience in hands-on software development using current commercial tools and techniques.

Cybersecurity is a key aspect of the curriculum we deliver as it lies at the heart of developing quality software. Our undergraduate program covers cryptography, database security, web-application security and risk assessment giving our students a solid foundation in cybersecurity. Our students also work on penetration testing and reducing vulnerabilities in real-world web-applications.

Our work has been highlighted as a key element of Cardiff University's involvement in the Institute of Coding, a £20m initiative set up to tackle the UK's digital skills gap by training the next generation of digital specialists, bringing together universities, businesses and industry experts to equip people of all ages with the digital skills they need.

We are also proud to have been given a Collaborative Award for Teaching Excellence (CATE) by Advance HE as a recognition of our outstanding commitment to teaching in the UK higher education sector.

National Software Academy contact:

Matthew Turner – *TurnerM1@cardiff.ac.uk*

www.cardiff.ac.uk/centre-for-cyber-security-research

Centre for Cyber Security Research

Canolfan Ymchwil Seiberddiogelwch Prifysgol Caerdydd

The Data Science Academy

"Our vision is to import and combine skills, knowledge and ideas across disciplines to deliver world-class education in the fields of data science, cyber security and AI."

The Data Science Academy (DSA) has been established to ensure that Wales produces highly-skilled and employable graduates in some of the fastest growing and in-demand areas, from Data Science and Artificial Intelligence to Cybersecurity. The DSA offers a core suite of Master's degree programmes boasting a cutting edge curriculum, real-world projects, industry connections and career support.

Our postgraduate portfolio of degree offerings currently consists of MSc Data Science and Analytics, MSc Artificial Intelligence and MSc Cybersecurity. The MSc Cybersecurity features projects around building secure systems and securing systems (IoT, Cloud), dealing with attacks (remediation, forensics), detecting attacks, and evaluation of security in practice (effectiveness and efficiency of SIEMs, choice of appropriate security policies).

Students are given "real world" experience by working on team-based, client-facing projects. This is to expose them to a broad range of techniques for understanding data and use these to apply innovative analytical methodologies.

There are a range of opportunities for partners to get involved. You can:

- provide live client projects for students to develop and acquire skills
- mentor students both face-to-face and virtually
- present guest seminars or skill sessions
- provide summer placements and graduate opportunities for students
- provide sponsorship and bursary opportunities for students
- sponsor a prize/incentive for students

Data Science Academy contact:

Matthew Turner – ***TurnerM1@cardiff.ac.uk***

Centre for Cyber Security Research

Canolfan Ymchwil Seiberddiogelwch Prifysgol Caerdydd

EPSRC Doctoral Training Partnership Hub in Cyber Security Analytics

Our cyber security analytics PhD training Hub focuses on the fusion of AI, cybersecurity and risk – which considers the applications and implications of new and emerging technologies across these three lenses from both a human and algorithmic perspective.

Here at Cardiff University, we are one of the foremost authorities in this area. Future industrial leaders in this area will need to be critical and innovative in designing new technology-driven systems, recognising that cybersecurity and AI are human-centred challenges that cannot be achieved with technology alone.

Our unique programme provides a holistic training perspective that aims to develop future leaders who can communicate (and debate) the best ways to address the challenge of fusing cybersecurity, AI and risk, to the benefit of future generations. Without this cohort-based training environment, we argue that future leaders will miss opportunities to co-create a world with a much richer interdisciplinary understanding of AI and cyber threats from a systems and human perspective.

This would result in new technologies containing inherent exploitable vulnerabilities that will have an exacerbated impact as we become more dependent on interconnected autonomous systems. The interdisciplinary co-creation of new research that leads the way in addressing these topics sits at the core of the research goals in the hub.

We expect our graduates to take up employment across a range of sectors where the cybersecurity of new technologies such as AI is critical. Expected roles where the advancements of new technologies are vital include:

- strategic research directors
- legal and governance practitioners
- social policy officers
- technology developers
- data scientists
- human factors experts.

Fully funded scholarships are available from October 2021.
Please get in touch to find out more.

Doctoral Training Partnership Hub contact:

Professor Pete Burnap – *BurnapP@cardiff.ac.uk*

www.cardiff.ac.uk/centre-for-cyber-security-research