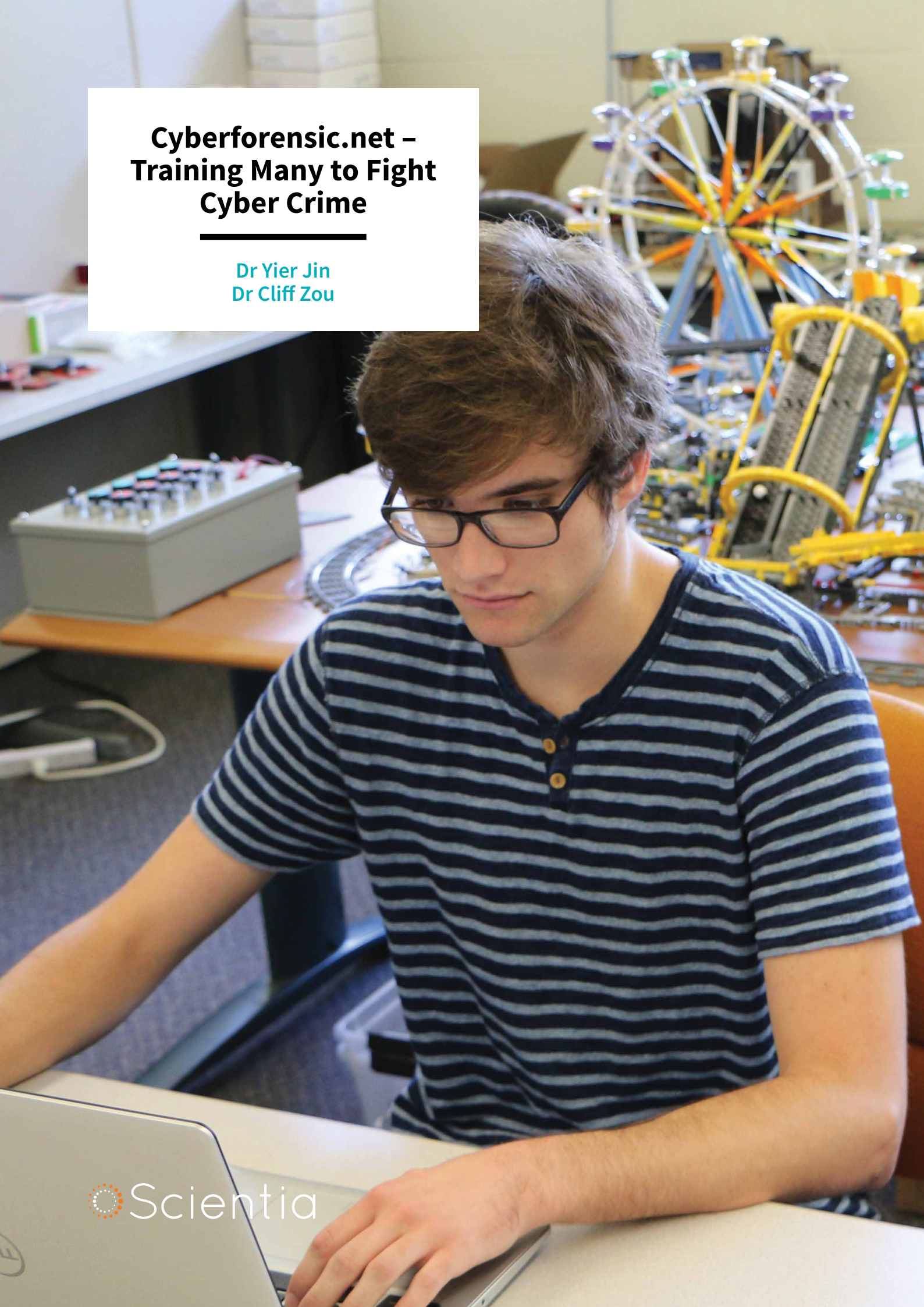


Cyberforensic.net – Training Many to Fight Cyber Crime

Dr Yier Jin
Dr Cliff Zou

Scientia

CYBERFORENSIC.NET – TRAINING MANY TO FIGHT CYBER CRIME

People are sharing more personal information online than ever before. It is essential, therefore, that robust security and privacy systems are in place to protect it. Furthermore, experts in the field of cybersecurity are essential. Drawing on their extensive research experience in the field of internet security, **Dr Yier Jin** of the University of Florida and **Dr Cliff Zou** of the University of Central Florida have created cyberforensic.net. This website aims to enrich the cybersecurity workforce by providing training in the areas of digital forensics and internet security.

The Promise & Pitfalls of the IoT

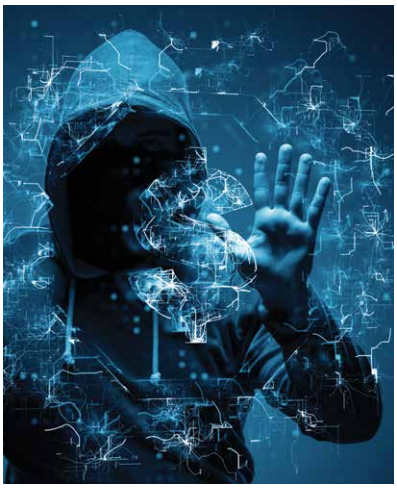
The Internet-of-Things (IoT) has revolutionised the way we interact with society and the world. Briefly, the term 'Internet-of-Things' refers to the collecting and sharing of information between computers, electronic devices and humans by means of the internet. It may involve anything from mobile phones to jet engines. If it can transmit useful and beneficial information between device and user through the internet, it is part of the IoT.

The IoT is already having a huge impact on our lives. Most companies, government agencies and ordinary people rely on the cyber world for information and data management, processing and exchange. For example, many of us use our devices to pay bills and buy groceries. Many use devices to monitor the performance of systems remotely. And of course, most of us use the internet to communicate with others.

However, the dependence on IoT-based systems introduces challenges. Given the personal nature of the information exchanged by these means, maintaining security and privacy is of utmost importance. Consider, for example, online fraud – the act of deception over the internet for financial gain. According to estimates, some $16.8 billion was stolen in 2017 by way of fraudulent activity. As a result, the call has gone out to greatly strengthen our cyber-defence systems to better respond to attacks.

Part of this involves skilling up individuals who, using their newfound expertise, can improve and implement enhanced digital security systems. To get the ball rolling on this, Dr Yier Jin of the University of Florida and Dr Cliff Zou of the University of Central Florida have created cyberforensic.net – a website that aims to enrich the cybersecurity workforce by providing training in the areas of digital forensics and IoT security.

During the website's creation, Dr Jin and Dr Zou were able to draw on their wealth of research and development experience in these fields. Examples of their previous contributions are discussed below.



A Fraud Detection Mechanism for Online Merchants

As the use of online marketplaces and digital transaction technologies becomes more customary, acts of fraud by these means are frighteningly common. There has never been a greater need, then, to protect every individual's financial data. This is especially true as many retailers move towards so-called 'Card Not Present', or 'CNP' schemes, where transactions can be made without presenting an actual credit or debit card at the time of purchase.

‘The development of an online digital forensics program will reshape current cybersecurity education practices and improve related outcomes. It does this by providing a more comprehensive and thorough atmosphere in which students and professionals can study and build their expertise in the field cybersecurity, and ultimately, prevent cybercrime.’

While CNP offers several benefits for consumers, the absence of face-to-face contact means that merchants cannot positively ascertain the cardholder’s identity. Moreover, merchant security systems themselves are far too simplistic and easy for hackers to bypass. They are often based on the merchant’s own history of fraudulent activity, and so are not adaptable to emerging methods of fraud. Remember too, there is time lag between when a fraudulent transaction occurs and the time when it is reported by the cardholder.

To fight against this type of fraud, Dr Zou, Dr Jin and their colleagues developed an innovative fraud detection model that can be implemented by online merchants. Their model directly interacts with the buyer’s electronic purchasing device (a computer or a smartphone) and combines it with a statistical concept known as a buyer’s ‘diversity index’. The technology essentially assesses a buyer’s previous purchasing patterns and looks for anomalies that may indicate fraudulent activity.

The team’s proactive anti-fraud technique has proven to be incredibly effective. In the associated paper, they highlighted, ‘our method has been tested against real transactional data and yielded exceptional results with the ability to detect even previously undetected fraudulent transactions.’ Armed with this approach, online merchants may be able to significantly reduce instances of fraud.

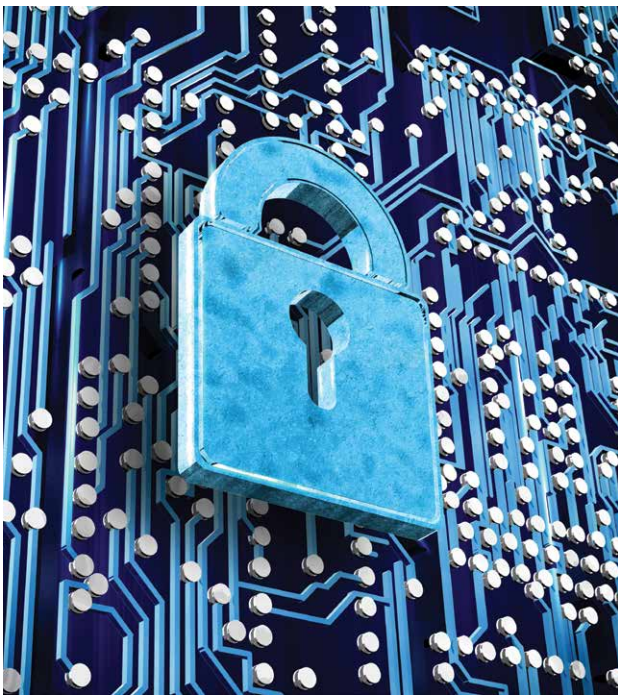
How Attackers Can Get Around Traffic Shaping

Traffic shaping, or packet shaping, refers to the practice of regulating network data transfer speeds, to maintain certain levels of internet performance. Traffic shaping is often employed to control usage over free Wi-Fi connections, such as those offered by fast food restaurants, coffee shops, hotels, and airports. Limiting speeds prevents a single user from overloading the hotspot and pushing out others. However, hackers can bypass traffic shaping systems and essentially steal internet speed.

To investigate this practice, Dr Zou, Dr Jin and a colleague assumed the role of ‘attacker’ – investigating the methods by which traffic shaping systems can be overcome. Their approach involved creating multiple wireless clients that emulate separate wireless devices. They then combined all of these into one physical wireless interface card. The result was an amalgamation of multiple connections and a significant increase in internet speed. The team concluded that a would-be attacker could achieve a 16-fold increase in internet speed using this technique.

The Cyber Attack & Defence Relationship

Cyberattacks are, in a sense, warfare – an interaction between attackers and defenders. And like warfare, the associated interactions are dynamic. However, in a research paper published in 2018, Dr Zou explained that current models of cyber-attack behaviour often do not recognise this fact: ‘Most of the cybersecurity research focus[es] on either presenting a specific vulnerability or proposing a specific defence algorithm to defend against a well-defined attack scheme… Few have paid attention to the dynamic interactions



between attackers and defenders, where both sides are intelligent and will dynamically change their attack or defence strategies...'

Understanding that cyberwarfare is a dynamic process is vital when developing cyber defence algorithms and strategies. It offers deeper insight into attacker behaviour. So, the goal of Dr Zou's research was to design a cyberwarfare framework that considers this fact. In summary, their model was indeed able to better predict the progression of cyber-attacks and offered much more insight than typical fixed-strategy defence systems.

Training the Next Generation of Cyber-Crime Fighters

As the IoT continues to grow, and we share more personal information online, we will need a skilled up cybersecurity workforce. This in turn, creates a demand for effective training. With their invaluable experience in the field, that's exactly what Dr Jin and Dr Zou are working towards. 'The development of an online digital forensics program will reshape current cybersecurity education practices and improve related outcomes,' says Dr Jin. 'It does this by providing a more comprehensive and thorough atmosphere in which students and professionals can study and build their expertise in the field cybersecurity, and ultimately, prevent cybercrime.' And so, the duo launched cyberforensic.net in February of 2018.

Cyberforensic.net is a teaching and learning resource that imparts practical cybersecurity skills to students. There are several courses available. For example, it offers courses in incident response technologies, cyber operation and penetration testing, and malware and software vulnerability analysis. Each of these courses is supported with relevant lectures, notes and assignments. Another notable feature is the IoT and security related 'labs', or practical sessions. These have been developed to expand digital forensic training beyond traditional personal computers to include emerging devices such as smart phones.

IoT training packages are also available to K-12 students. A series of so-called 'IoT Smart Car Labs' guides students through the basic principles of the IoT by way of hands-on, interactive activities. In the IoT Smart Car Lab 1, for example, the goal is to introduce young students to the IoT through a fun and interactive lab. 'A car will be constructed and equipped with motors and sensors,' says Dr Jin. 'The car can [be driven] over Wi-Fi from the student's laptop and the sensors can be read remotely as well.'

A Sharing of Cybersecurity Expertise

The cases discussed in this article are really just the tip of the cybersecurity iceberg, as it were. It is certainly an area that needs constant attention. Dr Zou and Dr Jin are developing an action plan to meet this challenge. Not only are they at the forefront of cyber-related trends and theory, they also aim to ensure that we have skilled individuals at our disposal to deal with cyber threats.

When asked about future aspirations, Dr Zou explained, 'the online digital forensics program will be offered to all graduate and undergraduate students majoring in computer science, computer engineering, and information technology at the University of Florida and the University of Central Florida.' And after a successful trial, they intend to expand the program by collaborating with other universities. 'The final goal,' Dr Zou relates, 'is to make the online digital forensics program available to all universities and community colleges nationwide.'

Meet the researchers

Dr Yier Jin
Department of Electrical and Computer Engineering
University of Florida
Gainesville, FL
USA

Dr Yier Jin received his PhD in Electrical Engineering from Yale University, Connecticut, USA in 2012. After some time at the University of Central Florida, he became Associate Professor at the University of Florida's Department of Electrical Engineering and Computer Science, where he currently serves. His research interests include: The Internet of Things (IoT) and related security, Cyber-Physical System (CPS) design, resilient high-performance computing platforms, hardware-software co-design for system level security and protection, functional programming and proof writing for trusted IP cores, and trustworthy SoC architecture. He and his colleague, Dr Cliff Zou, have also created cyberforensic.net – an online cybersecurity training resource.

CONTACT

E: yier.jin@ece.ufl.edu
W: http://jin.ece.ufl.edu

Dr Cliff Zou
Department of Computer Science
University of Central Florida
Orlando, FL
USA

Dr Cliff Zou received his PhD in Electrical and Computer Engineering from the University of Massachusetts at Amherst in 2005. After completing his PhD, he moved to the University of Central Florida's Department of Computer Science, where he currently serves as Associate Professor and Program Coordinator for the Digital Forensics MS program. His research interests include: computer and network security, computer networking and network modelling, and performance evaluation. He and his colleague, Dr Yier Jin, created cyberforensic.net as a means of sharing their expertise, and educating others.

CONTACT

E: czou@cs.ucf.edu
W: http://www.cs.ucf.edu/~czou/

FUNDING

National Science Foundation (NSF)
Cyber Florida at the University of South Florida

UF UNIVERSITY of FLORIDA

University of Central Florida