Introduction

William Hurst* and Nathan Shone

Department of Computer Science,
Liverpool John Moores University,
Byrom Street, Liverpool, L3 3AF, UK
Email: W.Hurst@ljmu.ac.uk
Email: N.Shone@ljmu.ac.uk
*Corresponding author

Biographical notes: William Hurst is a Senior Lecturer in the Department of Computer Science at the Liverpool John Moores University (LJMU). He completed his PhD studying critical infrastructure protection and previously worked as a Research Assistant in the PROTECT research centre at the LJMU. Prior to this, he received his MSc with distinction in Web Computing from the Liverpool John Moores University. His research interests include critical infrastructure protection, cyber security, data classification, simulation and 3D graphics.

Nathan Shone is a researcher and currently working as part of the PROTECT research centre in the Department of Computer Science at the Liverpool John Moores University (LJMU). He received his BSc (Hons) in Computer Forensics from the LJMU in 2010. He also holds a PhD in Network Security, and studying misbehaviour detection in complex system-of-systems, which was awarded by LJMU in 2014. His research interests include complex system security, security monitoring, IoT security and digital forensics.

Modern society is increasingly dependent upon a wide variety of interconnected critical infrastructure systems that govern many aspects of our daily lives, including energy, manufacturing and governmental sectors. The roles of these critical infrastructure systems are changing; as they are becoming more ubiquitous within society. Increasing demands are forcing these traditionally offline and reticent systems to integrate growing levels of end-user accessibility, functionality and controllability. Hence, many of our critical services now incorporate a diverse range of digital technologies, such as online portals, mobile apps and social media integration. Whilst this provides a greater level of real-time user control, the effect on the system is an augmented vulnerability to digital threats and an increased concern over the potential damage resulting from targeted attacks and cyber warfare. It is therefore imperative that new technology is developed to maintain a high standard of both security and functionality within critical infrastructure systems.

Critical infrastructure preservation was traditionally focused upon protecting system against environmental threats. Now however, the focus has changed, as infrastructures have become significantly more complex, interconnected and linked to the internet. They are facing a more difficult and clandestine plethora of threats posed by cyber-attacks, and the potentially devastating consequences they entail. The increased exposure of critical systems has created a greater number of attack vectors. This leaves them directly vulnerable and increases the chances of a successful cyber-attack taking place.

Additionally, the growing integration of wireless communications, within such systems, has further exacerbated the situation. Security is an issue facing all critical systems, especially those considered as part of a critical infrastructure.

With state-sponsored cyber-attacks and the rise in organised hacking groups, it is of no surprise that novel and increasingly sophisticated threats are constantly emerging. Alongside this, is the recent spate of attacks and weaknesses discovered in critical-infrastructure systems; thus, emphasising their vulnerability and the importance of developing improved security techniques.

As critical-infrastructure systems are at the heart of most modern societies, they are prime targets. Such attacks can have catastrophic consequences, including loss of critical services, physical damage, loss of utilities or even human injuries and fatalities. There are also other far-reaching side-effects to be considered, such as impacts upon governmental, social and economic stability. Launching a cyber-attack against a critical infrastructure is a relatively easy method of causing disruption to as many people as possible. It also provides criminals with a level of anonymity, making it difficult to trace the real source of an attack.

Cyber-attacks are usually financially motivated, whether this is payment received from offering attacks as a service, using stolen financial information (e.g., through spear-phishing attacks) or through ransom payments. Paid-for cyber-attacks are usually in the form of distributed denial of service attacks, which normally operate as a Botnet. These attacks are used to incapacitate public-facing servers by attacking applications, network protocols or by bombarding networks with huge volumes of traffic. However, spear-phishing attacks rely on human error and a lack of threat awareness to be successful. Their aim is to trick the victim into thinking an e-mail-based scam is legitimate by ensuring the information inside is specific to that person or organisation. As a result of successful spear-phishing attacks, numerous military and private industry systems have been breached in recent years. Each penetration is the direct result of lack of understanding about the nature of the attack, which leads to sensitive information being disclosed.

The future for modern critical-infrastructure security lies with the ability to adapt to suit the needs of the constantly changing digital landscape. By embracing innovative security techniques, existing methods can built upon to provide well-structured defence-in-depth. The significant weaknesses of existing security measures combined with the increasing complexity and susceptibility of critical systems highlights the necessity for effective protection methods. It is for these reasons, that in this special issue, the focus of discussion is on current state-of-the-art solutions into cyber-security and existing cutting edge research on technological infrastructures. Emphasis is placed, in particular, on the smart grid and critical infrastructure technologies, which are predominantly vulnerable to threats from the digital domain.