Applying Lessons from Cyber Attacks on Ukrainian Infrastructures to Secure Gateways onto the Industrial Internet of Things

Chris. W. Johnson DPhil, Maria Evangelopoulou and Tanya Pavlova

School of Computing Science, University of Glasgow, Glasgow, UK.

Keywords: Industrial Internet of Things, Modbus, Profibus, Switches, Safety, Cyber Security.

Abstract

Previous generations of safety-related industrial control systems were 'air gapped'. In other words, process control components including Programmable Logic Controllers (PLCs) and smart sensor/actuators were disconnected and isolated from local or wide area networks. This provided a degree of protection; attackers needed physical access to compromise control systems components. Over time this 'air gap' has gradually been eroded. Switches and gateways have subsequently interfaced industrial protocols, including Profibus and Modbus, so that data can be drawn from safety-related Operational Technology into enterprise information systems using TCP/IP. Senior management uses these links to monitor production processes and inform strategic planning. The Industrial Internet of Things represents another step in this evolution – enabling the coordination of physically distributed resources from a centralized location. The growing range and sophistication of these interconnections create additional security concerns for the operation and management of safety-critical systems. This paper uses lessons learned from recent attacks on Ukrainian critical infrastructures to guide a forensic analysis of an IIoT switch. The intention is to identify and mitigate vulnerabilities that would enable similar attacks to be replicated across Europe and North America.

Introduction

In the past, Industrial Control Systems (ICS) were isolated from conventional, digital networks. Specialist protocols, including Modbus and Profibus, were used to communicate between devices provided by many different suppliers. Over time this 'air gap' between industrial and conventional networks has gradually been eroded. There has been an increasing convergence between ICS networks and Internet technologies. Protocols, such as Modbus TCP/IP, provide interfaces that enable users to interact with ICS applications using conventional computer networks. The PROFINET industrial Ethernet protocol provides real time extensions to TCP/IP over Wireless Local Area Networks (LANs). These innovations not only increase the flexibility of ICS but also provide significant cost savings. They also enable monitoring and control applications to be run on mass-market equipment. Industrial gateways/switches also help companies to monitor and control distributed resources without duplicating existing network infrastructures. Operators can carry network enabled, mobile control devices in a flexible manner, close to the point of need rather than being tied to a systems engineering desk. From a management perspective, enterprise planning and decision making tools can be informed by real-time process data delivered over their office newtorks to support collaborative situation awareness (Ref. 1).

The development of industrial interfaces to conventional networks also creates potential vulnerabilities if attackers can exploit these mechanisms to gain access to safety-critical applications. In other words, the convergence of industrial Operational Technology (OT) and conventional Information Technology (IT) has increased the potential attack surface. These concerns have been exacerbated by the relative lack of progress in improving the cyber security of ICS applications. Many industrial, serial protocols have well known vulnerabilities. Messages are typically unencrypted and provide only weak means of authenticating their sender. There are more robust variants; for instance Modbus Secure and EtherNET/IP Secure. However, these are not yet widely used and can be difficult to integrate into legacy applications without incurring significant costs, especially in terms of the safety assessments that might be triggered by the introduction of these more secure protocols.

There has only been limited adoption of the International Society of Automation (ISA) cyber-security recommendation (Ref. 2) or of evolving standards such as IEC 62443: Network and system security for industrial-process measurement and control. Such guidance encourages a lifecycle approach from development through to the

operation and maintenance of secure ICS applications. However, the lack of documented case studies and the perceived costs associated with their adoption dissuades many companies from benefitting from these techniques. In consequence, many ICS remain vulnerable, misconfigured, and available over TCP/IP. These vulnerabilities have numerous root causes, most of which do not stem from technical limitations. Network management is often out-sourced to companies with limited experience in security- or safety-critical engineering.

The Internet of Things

There are strong parallels between the increasing connectivity of industrial control systems and the growth of what has become known as the Internet of Things (IoT). The IoT refers to physical objects – including domestic products such as fridges, televisions and microwaves but also buildings and vehicles that are embedded with sensor/actuators and with processing capability, which can be addressed through network interfaces. A strong theme in the development of the IoT is the blending of the physical and the virtual. Control actions on digital representations will have effects on their physical counterparts. Things can be identified, interrogated and controlled across distributed computer networks creating interconnections across cyber-physical systems. This has significant benefits in terms of the coordination and optimization of resources and of production processes. It also offers remote monitoring capabilities and potential for novel forms of automation that can minimize the need for direct human intervention.

Key application areas for the IoT include home automation where users can control heating, lighting, power systems from remote applications. They can also program domestic appliances to react in particular ways when they sense changes in their environment. For example, fridges may use Internet connections to schedule food deliveries when particular items have been exhausted. On a wider scale, smart-city applications can sense congestion and respond by changing the timing of traffic control software. They may also automatically schedule additional public transport services when video cameras detect large numbers of passengers waiting for a bus or light rail service. These applications rely on a high degree of interoperability. Data can only be exchanged between sensors and their control applications if there are common protocols.

Another requirement is that participants in the IoT must be able to handle significant amounts of senor data. Inferences about potential actions typically depend on identifying patterns across these senor values. The ability to store and analyze heterogeneous data sources creates a range of privacy and security concerns. There is an expectation that companies will take active measures to secure IoT devices and applications – this can include encryption by default and the anonymization of sensitive data. It is also important that companies seek explicit consent from the data subjects if information is shared with other organizations. Finally, companies should only collect the data that is needed for the intended use and hold it only as long as it is needed. Concerns include the use of IoT data by criminals to time burglaries to coincide with periods when sensors show that a house is unoccupied. Other scenarios include disclosing health-related information through the data obtained from personal health monitoring systems.

Many of these IoT security concerns also have implications for safety-related systems. Novel sensing technologies are being used to automate and optimize traffic control, to inform and personalize health related decisions, to support ‘just in time’ distribution processes. These services rely on integrated, networked data sources that are increasingly providing the digital foundations for safety-related infrastructures.

Progress in the Industrial Internet of Things

As mentioned, the Internet of Things refers to physical objects that are embedded with sensor/actuators, which can be addressed through network interfaces. By extension the Industrial Internet of Things (IIoT) depends on the ability to access distributed ICS resources through conventional networks, typically over TCP/IP links. This offers huge potential benefits – including the development of so-called ‘smart’ manufacturing and distribution systems; where processes can be automatically scheduled to respond to a customers needs or where distributed control systems can be used to optimize production systems around the globe through information integration. Specific examples include ‘smart grid’ power systems where generation and distribution are precisely matched to consumer requirements; enabling the integration of novel and renewable sources. The ‘digital oilfield’ enables operators to

control massively distributed resources from a single control room. It also enables engineers to hand-over centralized control to another location in response to changing operational requirements; for instance, to increase resilience to infrastructure failures.

The IIoT creates a number challenges. In particular, it is hard to achieve the levels of interoperability that characterize the conventional IoT. Traditional serial protocols were designed for ICS environments that only required limited connectivity (Ref. 3, 4). It was never envisaged that safety-related processes might require thousands of programmable components. In consequence, engineers have to resolve address limitations; Modbus by default only supports 254 devices on one data link. Such limitations have to be resolved before existing ICS protocols can support the level of connectivity envisaged in the IIoT (Ref. 5). There are further concerns. Modbus and the other serial protocols were also designed for relatively predictable interaction with industrial control systems. They exploit traditional client/server architectures. The master must explicitly poll each of the networked devices. Components cannot raise asynchronous alerts in response to changing operating conditions. The simplicity of the master/slave architecture has significant advantages for the timing and reliability analyses that are required during safety assessments. However, such models of interaction are less easy to integrate with more conventional TCP/IP networks that are intended to support asynchronous interaction.

These ICS serial protocols were also originally developed to support communication between a relatively homogeneous array of devices, including Programmable Logic Controllers (PLCs) and sensor/actuators. In consequence, Modbus only supports data types that are recognized by PLCs. It cannot support the arbitrary binary objects that are used within more conventional network architectures. Data objects are not supported by any meta-data. The semantic information needed to understand and use an object has to be embedded within each client. If new forms of data are transmitted across a serial interface then every client may potentially have to be updated – raising significant cost pressures. As we shall see, these device updates may also create possible attack vectors.

A number of techniques have been developed to address these limitations of traditional ICS networks. These include message queuing to support a publish/subscribe model. Nodes register their interest in particular messages with a centralized broker. These brokers will forward-on information of a particular type when polled by the device. The approach is effective because it filters unnecessary broadcast communication that might overwhelm the limited processing power of many ICS devices. It provides limited asynchronous operation and a means of interfacing serial protocols with more conventional TCP/IP environments. The storage of messages by the broker also helps provide a degree of resilience across networks with very different bandwidth and speed. These message queuing gateways can also offer translation services to ensure the transmission of compatible data types into the OT networks.

Security Concerns in the IIoT: Impact on Ukrainian Infrastructures

Previous sections have argued that the Internet of Things raises a host of security and privacy concerns. The ICS counterparts in the IIoT share many of these issues. However, the potential consequences of attacks on safety-critical infrastructures means that such concerns are increasingly placing limits on the development of innovative network enabled applications. Regulators and investors are concerned about their risk exposure as complex, distributed systems are interfaced with public data networks. These concerns are not simply theoretical. The potential threats have been illustrated by recent attacks on a number of Ukrainian companies as part of the on-going conflict there. One of these cyber-attacks was triggered on the 23rd December 2015 when a third party compromised regional electricity distribution systems (Ref. 6). The attackers appear to have gained access more than six months prior this date. They were able to cut the power supply by undermining a range of ICS devices. The outages affected three different distribution companies affecting some 225,000 customers.

The subsequent investigation revealed that the attackers had exploited spear phishing emails to compromise the Ukrainian accounts. These were carefully targeted attacks that used social engineering to encourage the recipients of the emails to open a malicious attachment; in most cases a Word document with harmful macro extensions. Once an account had been compromised, they used this access to gain further logon credentials from the business network and to conduct an extensive reconnaissance of the associated ICS systems. They were able to target directory service infrastructure to directly manipulate and control the authentication and authorization system. They were also able to exploit the connectivity provided by IIoT applications; using legitimate VPN access to bridge between the

corporate IT and industrial OT/ICS environments. The attack was assisted by external suppliers listing some of the equipment used in the Ukrainian infrastructures, such as Remote Terminal Unit (RTU) vendors and versions. It was the IIoT serial to Ethernet gateways, described in previous sections, which enabled the direct reconnaissance to take place before the attack was launched.

Once the attack was triggered; a number of different ICS components were affected. Initially, the human machine interfaces were compromised. This prevented operators from issuing commands to the underlying systems. Their commands were further undermined by the attackers' ability to upload malicious firmware for the serial to Ethernet gateways that are core components of IIoT applications. This ensured that once the operator workstations were restored, remote commands could not be issued to bring the substations online. At the same time, the attackers were able to generate thousands of telephone calls to prevent legitimate customers from contacting the companies' call centers. The attackers were also able to undermine Uninterruptible Power Supplies so that when their attack disrupted the distribution network; the company itself lacked sufficient power to maintain its own computational infrastructure. This illustrates how attackers can use IIoT infrastructures to sustain long-term reconnaissance of ICS networks and then to execute highly synchronized, multi-stage, multi-site attacks on safety-related systems.

Defending the IIoT

A number of lessons have been learned for the cyber-security of safety-related IIoT applications in the aftermath of the attacks on the Ukraine. There was no two-factor authentication to protect the VPNs that were used to bridge from the office environment into the ICS networks. Two-factor authentication is a means of establishing a user's credentials using two independent mechanisms. A bank cash machine can be used to illustrate this approach. The user presents a card (something they possess) and a Personal Identification Number (PIN) (something they know). Even if an attacker learns the PIN, this is useless without access to the card. In VPNs it is possible to use a similar card and reader to generate a one-time session key that would be hard for a remote attacker to obtain. Such techniques are not foolproof but they raise the barriers to any intrusion between the conventional and ICS networks.

The Ukrainian firewalls enabled the attackers to use administrative privileges to perform remote configuration tasks on the serial to Ethernet gateways. These vulnerabilities were exacerbated by a lack of monitoring on ICS networks. This is surprisingly common – given the bandwidth limitations within many industrial systems and also the potential need to demonstrate that the monitoring itself does not undermine safety. However, the lack of such intrusion detection facilities helps to explain why the attackers remained undiscovered for up to six months.

First Check Known Vulnerabilities. We must learn from such incidents if we are to defend the growing array of applications across the Industrial Internet of Things. This relies on a clear understanding of existing vulnerabilities. We, therefore, established an ICS forensic lab described at last year's conference (Ref. 4). Initially, our work focused on a forensic analysis of 'air gapped' systems including PLCs and sensor/actuators that were entirely isolated. We then began to consider industrial protocols separated from more conventional networks by a physical 'gap'; i.e., there was no direct connection. Over the last eighteen months, we have extended our test environments to support almost a dozen different protocols, which are interfaced with TCP/IP networks. For security reasons, we do not make these networks more widely visible over the public Internet; we do not want others to access our devices nor do we want some of the techniques we have developed to affect other legitimate applications. Some of the software we test has the potential to affect safety-related systems connected to these wider networks; equally we need to protect some of the devices that we examine from external discovery.

Within one line of analysis, we are working to discover the strengths and vulnerabilities of the industrial switches and gateways that provide access between the more specialist ICS protocols and conventional TCP/IP networks. Further details about particular devices can be provided by contacting the authors at the address given in the biographies at the end of this paper. We work with a range of industrial sponsors who identify the classes of devices that we investigate. The aim is both to assess and then address the vulnerabilities of existing devices but also to help inform subsequent procurement decisions.

Table 1 illustrates the starting point. For most ICS components, there are publically available lists of known vulnerabilities. The table summarizes the concern and provides a Common Vulnerability Scoring System (CVSS) assessment. CVSS is a standard mechanism for assessing the severity of security vulnerabilities in a range from 0 to

10, where 10 is the most severe. In Table 3, the impact of an attack using these means on this particular IIoT switch should be apparent from the scoring.

When our sponsors provide a new device to assess, we use the published vulnerabilities to guide an initial security assessment. Most, but not all of these concerns, are addressed in subsequent software/firmware updates distributed by the vendors. However, these patches are seldom applied in critical applications because of the additional verification and validation costs that are required to demonstrate any modification does not compromise safety requirements. 'If it ain't broke, don't fix it'. While this may be appropriate in terms of a safety assessment, it is no longer sustainable from a security perspective. It is dangerous practice in a world where state-sponsored attackers have focused on vulnerabilities in firmware, distributed over compromised network connections.

ICS Computer Emergency Response Team (CERT) Number	Description	Vulnerability	CVSS Score
CVE-XXXX-XXXX	Error log message which is displayed when a remote connection to the device fails, can identify an authentication pathway	DoS Authenticate	8.6
CVE-XXXX-XXXX	Maliciously crafted packets could cause a restart	DoS Restart	8.6
CVE-XXXX-XXXX	Corrupt the information in the local DNS cache using a malicious response message	DoS Restart	9.9
CVE-XXXX-XXXX	Specially crafted packets sent on port 4786/TCP could cause a memory leak	DoS Memory Leak	8.6

Table 1 – Known Vulnerabilities in an IIoT Switch (Ack: ICS-CERT, Computer Emergency Response Team)

Looking for Configuration and Access Control Vulnerabilities. The high-level architecture of an IIoT switch was introduced in previous paragraphs. These devices can store messages sent using Profibus or Modbus. They can also inject messages from external TCP/IP networks. They may filter some of this traffic – for instance to exclude erroneous types of data that would not be expected within an ICS environment. For example, email traffic should not be routed into the industrial domain. The detailed operation, including the filtering mechanisms, of an IIoT switch can be controlled through configuration parameters. These may only be read or written if a user can provide appropriate access credentials. Similar forms of authentication restrict administrative access, which has the additional ability to create or delete configuration accounts. The device considered in this paper is widely used and was provided by industrial co-sponsors of this work. It is accessed through a device manager interface, broadly similar to those available for domestic routers. Read-only access can be used to query the state of the switch including how many packets have passed through a port, its temperature etc. In addition, administration accounts can make changes to the configuration of the switch. On the device we received, the default password was still enabled as 'Admin'. With this particular switch, the initial configuration required the user to reset the default password. Hence it must be inferred that the initial recipient of the device chose to deliberately re-use the default Admin password. This seems to be standard practice amongst many engineering teams even in safety-related systems where multiple people require access to critical devices. Following the Stuxnet/Olympic Games and Ukraine attacks it is extremely important that such practices are identified and stopped immediately.

Further analysis showed that the plaintext user names were stored together with an MD5 hash of the passwords and the associated access permissions in a configuration file. Hashing is not a form of encryption – it cannot be used to recover the plain text but provides a characteristic value that can be used to check if any given text is similar to the stored hash value. For example, an overly simplistic hash function might be the number of characters in a file. If a character was added then the hash value would increase by one and a recipient of the file could detect the change.

Any alteration that added one character and deleted another could not be detected; this problem is known as hash collision. The MD5 algorithm suffers from a large class of known vulnerabilities and CMU's Software Engineering Institute describes it as "unsuitable for further use" (Ref. 7). Further concerns stem from the use of a weak, proprietary encryption algorithm to protect the switch's administration account. This is retained in addition to MD5 so that the switch can exchange plaintext credentials over legacy protocols including Telnet, which in most cases should have been explicitly disabled for IIoT applications. Telnet does not encrypt traffic, including passwords; hence anyone with a packet analyzer and access to the network can potentially gain credentials for these gateways and switches. If Telnet is being used elsewhere on the network then a compromised IIoT gateway can be used in a recursive manner to analyze the packets being sent to other networked devices. This enables the attacker to pivot through the network incrementally gaining more and more access privileges. By default, the IIoT switch used the hypertext transfer protocol (HTTP) to communicate with its device manager application running on a workstation. The credentials were again passed in clear text.

The device supports access control lists. These can be used to specify which IP addresses can communicate through particular ports on the device. This creates the potential for implementing thresholds that might be associated with particular ports – to limit an external source from overwhelming or flooding the switch and thereby interrupting valid communication through other ports. However, such potential security techniques raise questions for system safety engineers to identify appropriate values. If a valid application exceeded the threshold then it would be denied access to the switch. If the thresholds are set too high then they provide only limited protection against an attack. In safety-related applications these values should be supported by detailed arguments that demonstrate it is acceptably safe to cut off communication above the particular values that are used to configure the device. In contrast, an attacker with admin rights could set the cut-off values to zero and deny access to safety-related devices. This provides a further example of the need for safety and cyber security to be closely integrated in the detailed engineering of IIoT infrastructures.

More Aggressive Forensic Attacks. In previous papers, we have coined the term 'forensic attack analysis' – this goes beyond penetration testing and is intended to identify defenses as well as forensic techniques that can be used in the aftermath of a potential attack (Ref. 4). In the case of the IIoT switch, we began to conduct a form of remote packet capture to learn as much about the network and the device as possible. This stage of our analysis confirmed our concern about the vulnerability of the legacy protocols that were enabled on the switch. One particularly useful source was packets sent using the proprietary protocol developed by the device manufacturer; our analysis tools were configured to filter these from the rest of the traffic so we could focus on this data. They were weakly encrypted and it was straightforward to extract the IP number as well as the user credentials for the device. We were also able to monitor responses from the device to the configuration application, sent using HTTP GET – including a GIF with the temperature, which is updated every 60 seconds as well as the SHTM for the web page, JavaScript and CSS code.

Once an adversary has the credentials for an authorized account and the device details, including the firmware version from the proprietary device protocol, they can begin to develop an attack vector. The manufacturer's website provides a host of additional information about the architecture of the switch. Second-hand devices are easily obtained from Internet marketplace sites; enabling adversaries to refine their techniques. From then on, an attacker can replicate the events that played out across the Ukrainian energy infrastructures.

For each of the vulnerabilities described above there are numerous defenses. For instance, audits help to ensure that patches are applied. This requires technical support and organizational commitment. It also requires communication and coordination between the teams that are responsible for safety and for cyber security. Safety engineers must understand the consequences of failing to apply a security patch. Security managers must understand that there can be significant costs to ensure that a patch does not compromise safety.

Conclusions and Further Work

The 'air gap' that isolated previous generations of Industrial Control Systems (ICS) has been eroded. Gateways and switches now provide a bridge between specialist protocols, including Modbus and Profibus, and more conventional TCP/IP networks. This creates external communications links with safety related process components including a vast array of PLCs, sensors and actuators. Senior management use these links to monitor production processes and

inform strategic planning by connections between operational process technology and enterprise information systems. On a larger scale, this has led to the development of the Industrial Internet of Things (IIoT). IIoT applications offer huge benefits where global industries can coordinate distributed just-in-time production from a small number of centralized control rooms. Smart grid infrastructures provide one example. Others include 'digital oilfields' and a host of urban applications that synchronize public services to meet user needs that are identified through remote monitoring technology.

This paper focuses on the interactions between the safety and the cyber security of IIoT applications; illustrated by recent attacks on Ukrainian critical infrastructures. We summarized the techniques that were used to undermine a portion of their energy distribution systems. These included a prolonged period of surveillance after an initial penetration using spear phishing emails that encouraged individuals to open compromised attachments. Once inside the enterprise information systems, the attackers gained valid VPN credentials to bridge into the ICS environment. When the attack was launched they disabled the industrial Human Machine Interfaces. After the defenders restored these devices, they found that their TCP/IP switches had been compromised because the attackers had used the compromised network connections to install invalid firmware updates. Techniques that can be used to defend against this form of attack are addressed in a companion paper for this conference[1]. These exploits were exacerbated by a simultaneous attack on VOIP communications systems.

Later sections of this paper used the insights from the attacks on the Ukraine to focus our defensive analysis of an IIoT switch; used to interface between TCP/IP and serial protocols, including Modbus or Profibus. Safety-related industrial sponsors provided the device. The analysis began by demonstrating that some already publicized vulnerabilities continued to affect our version of the device even after patches had been applied. In other cases, the operators of safety-related infrastructures have deliberately chosen not to patch their devices because of the additional verification and validation costs, even though this leaves them vulnerable.

We exposed security concerns around access control, authentication and configuration of the IIoT switch. With recent products, it is possible to disable many of the legacy features and to address these concerns over authentication – however; our cooperation with infrastructure providers has shown that this has not been done in many existing systems. Finally we have used a number of hacking tools and network analysis techniques to build plausible attack vectors from the vulnerabilities identified in previous stages of our analysis.

There are many directions for further work. When devices are procured, in national critical infrastructures, teams need to be competent in what we term 'forensic attack analysis'. In other words, they need to know where to find potential vulnerabilities in configuration – especially in the use of hashing and legacy communication protocols. Increasingly in the IIoT we see devices that can be secured but only if the companies who supply them know what they are doing. In Glasgow, we have developed a set of procurement criteria that can be used to guide this process. They extend existing reliability, dependability criteria to include cyber-security requirements. We are using these within the context of UK critical infrastructures to provide informed guidance to our sponsors. However, this information remains commercially sensitive and carries strong implications for national security hence it is unlikely to appear in the public domain.

The closing aim of this paper has been to encourage safety engineers to undertake at least an initial course in cyber security.

References

1. S. McLaughlin et al., "The Cybersecurity Landscape in Industrial Control Systems," in Proceedings of the IEEE 2016. doi: 10.1109/JPROC.2015.2512235. Available at http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7434576&isnumber=7456363, last accessed May 2017.

[1] C.W. Johnson, M. Saleem, M. EVangelopoulou, M. Cook, R. Harkness and T. Barker, Defending Against Firmware Attacks on Safety-Critical Systems, in this volume.

2. UK Centre for the Protection of National Infrastructure (CPNI), Good Practice Guide – Process Control and SCADA Security, Centre for the Protection of National Infrastructure, London, UK, 2008. Archived by the National Cyber Security Centre (www.ncsc.gov).

3. C. W. Johnson, Securing the Participation of Safety-Critical SCADA Systems in the Industrial Internet of Things. In C. Sandon, R. Piggin, M. St. John Green, P. Casely and C. Johnson (eds.), Proceedings of the 11th International Conference on System Safety and Cyber Security, Savoy Place, London, 11-13th October 2016, The IET, Savoy Place, London, 2016.

4. C.W. Johnson, R. Harkness and M. Evangelopoulou, Forensic Attack Analysis and the Cyber-Security of Safety-Critical Systems. In Proceedings of the 34th International System Safety Conference, Orlando, USA 8-12 August 2016, International System Safety Society, Unionville, Virginia, USA, 2016.

5. N. Mor, B. Zhang, J. Kolb, D.S. Chan, N. Goyal, N. Sun, K. Lutz, E. Allman, J. Wawrzynek, E.A. Lee, J. Kubiatowicz, Toward a Global Data Infrastructure. IEEE Internet Computing. 20(3):54-62, May 2016.

6. Electricity-Information Sharing and Analysis Centre (E-ISAC), Industrial Control System-Sharing and Analysis Centre (ICS-SANS), Analysis of the Cyber Attack on the Ukrainian Power Grid, Defense Use Case, Washington DC USA, March 18, 2016. Available at: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

7. C.R. Dougherty, Vulnerability Note VU#836068 MD5 Vulnerable to Collision Attacks. *Vulnerability notes database*. US Computer Emergency Response Team (US CERT), Carnegie Mellon University Software Engineering Institute/Department of Homeland Security, USA. December 2008.

Biography

Chris Johnson, DPhil, School of Computing Science, University of Glasgow, Glasgow, Scotland, G12 8RZ, Scotland, U.K., telephone – +44 (141) 3306053, facsimile – +44 (141) 3304913, email – Johnson@dcs.gla.ac.uk.

Chris Johnson is Professor and Head of Computing Science at the University of Glasgow in Scotland. He leads a research group devoted to improving the cyber-security of safety-critical systems. He has developed forensic guidance on behalf of the UK civil nuclear industry and helped develop European policy for the cyber-security of aviation – including ground based and airborne systems.

Maria Evangelopoulou, School of Computing Science, University of Glasgow, Glasgow, G12 8RZ, Scotland, U.K., telephone – +44 (141) 330-6053, facsimile – +44 (141) 330-4913, e-mail – Maria.Evangelopoulou@glasgow.ac.uk.

Maria Evangelopoulou is a Research Assistant working on a joint FAA/US Navy project in Glasgow University, looking at safety and security analysis of network data. She attained her MSc in Intelligence and Security Informatics from the University of Abertay and a BSc Technology Management from University of Macedonia in Greece. Maria's current research is concerned with the investigation of Cyber Situation Awareness Methods and Techniques in Cloud Networks and other kind of systems.

Tanya Pavlova, School of Computing Science, University of Glasgow, Glasgow, G12 8RZ, Scotland, U.K., telephone – +44 (141) 330-6053, facsimile – +44 (141) 330-4913, e-mail – tanyushapavlova@gmail.com.