KICS The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com

ScienceDirect

ICT Express 4 (2018) 42–45

www.elsevier.com/locate/icte

Cyber security of critical infrastructures

Leandros A. Maglaras[a,d,*], Ki-Hyung Kim[b], Helge Janicke[a], Mohamed Amine Ferrag[c], Stylianos Rallis[d], Pavlina Fragkou[e], Athanasios Maglaras[f], Tiago J. Cruz[g]

[a] *School of Computer Science and Informatics, De Montfort University, Leicester, UK*
[b] *Ajou University, Republic of Korea*
[c] *Department of Computer Science, Guelma University, Algeria*
[d] *General Secretariat of Digital Policy, Athens, Greece*
[e] *Department of Informatics, T.E.I. of Athens, Greece*
[f] *Department of Electrical Engineering, T.E.I. of Thessaly, Larissa, Greece*
[g] *Department of Informatics Engineering, University of Coimbra, Portugal*

Received 2 January 2018; accepted 2 February 2018
Available online 21 February 2018

Abstract

Modern Supervisory Control and Data Acquisition (SCADA) systems are essential for monitoring and managing electric power generation, transmission and distribution. In the age of the Internet of Things, SCADA has evolved into big, complex and distributed systems that are prone to be conventional in addition to new threats. Many security methods can be applied to such systems, having in mind that both high efficiency, real time intrusion identification and low overhead are required.

Keywords: SCADA systems; Security

1. Introduction

Industrial Control System (ICS) is an umbrella term that refers to a group of process automation technologies, such as Supervisory Control and Data Acquisition (SCADA) systems and Distributed Control Systems (DCS), which unfortunately have been subject to a growing number of attacks in recent years [1]. As they deliver vital services to critical infrastructure, such as communications, manufacturing and energy among others, hostile intruders mounting attacks represent a serious threat to the day to day running of nation states [2].

ICS have unique performance and reliability requirements and often use operating systems, applications and procedures that may be considered unconventional by contemporary IT professionals [3]. These requirements typically follow the priority of availability and integrity, followed by confidentiality and include the management of processes that, if not executed correctly, pose a significant risk to the health and safety of human lives, damage to the environment, as well as serious financial issues such as production losses [4]. Unavailability of critical infrastructure (e.g., electrical power, transportation) can have economic impact far beyond the systems sustaining direct and physical damage. These effects could negatively impact the local, regional, national, or possibly global economy.

2. Security of ICS

Despite the apparent risk to critical infrastructure, the security of ICS is not considered a significant investment area. Authors in [5] argue that the costs involved in ICS security

* Corresponding author at: School of Computer Science and Informatics, De Montfort University, Leicester, UK.
E-mail addresses: l.maglaras@gsdp.gr, leandrosmag@gmail.com (L.A. Maglaras), kkim86@gmail.com (K.-H. Kim), heljanic@dmu.ac.uk (H. Janicke), Mohamed.Amine.Ferrag@gmail.com (M.A. Ferrag), strallis@gmail.com (S. Rallis), pfragkou@tieath.gr (P. Fragkou), maglaras@teilar.gr (A. Maglaras), tjcruz@dei.uc.pt (T.J. Cruz).
Peer review under responsibility of The Korean Institute of Communications Information Sciences.

https://doi.org/10.1016/j.icte.2018.02.001

are prohibitive, especially within critical systems, when the perceived risks to an organisation or infrastructure cannot be adequately quantified and a business case not satisfactorily articulated. This often leads to an underdeveloped incident response capability in the deployed operational ICS, in particular within the SME supply chain. Larger infrastructures suffer from the insufficient understanding of the deployed components such as Programmable Logic Controllers (PLC) or similar Intelligent Electronic Devices (IED), Remote Terminal Units (RTU) and input/output (I/O) devices that are used to manage electromechanical equipment in either local or distributed environments. This unique environment, that combines large scale, geographically distributed, legacy and proprietary system components presents significant challenges to Security Operation Centers (SOCs) and Cyber Emergency Response Teams [6].

In the past, ICS were operated as separated networks unconnected to public communication infrastructures, but as businesses have turned to exploit the services and data provided by the Internet, such isolation that protected these systems has declined [7]. The benefits afforded by real time monitoring, peer to peer communications, multiple sessions, concurrency, maintenance and redundancy have enhanced the services provided for consumers and operators. Moreover, this interconnectedness will grow with the implementation of smart grids and execution of the Internet of Things (IoT) [8]. Hence, the previously isolated systems have become increasingly exposed to a range of threats [9], regarding which, Byres et al. [10] cite that formerly isolated ICS now average 11 direct connections across networks with weak network segmentation.

IT security is generally focused on protecting networked computer assets with clear, shared attributes, but Zhu [11] argues that for securing ICS there needs to be a combination of conventional computer security and communication networking with control engineering. However, since current ICS have recently taken up IP based communications, where traditional IT security, communications security and protection of control systems have their boundaries, their efficiency remains unclear. Luallen [12] reports that for a survey of 268 respondent organisations, most did not report critical ICS assets and relied on staff to detect issues, not tools.

3. SCADA systems

SCADA systems have traditionally been associated with a subset of ICS referred to as Wide Area Control systems (see Fig. 1).

As aforementioned, security in SCADA systems is more salient than with most other computer systems owing to the potential severity of the outcomes due to a degrading of service, as well as the disruption to day to day life. With older computer systems, reliability was the key concern and security was much further down the list. Today, with greater connectivity [13], security is now high on the agenda. Moreover, SCADA systems are not only becoming more connected to the internet; the communications within them operate through shared Internet Protocol (IP) infrastructure. A number of concerns in relation to implementing security in SCADA have been raised in the current research:

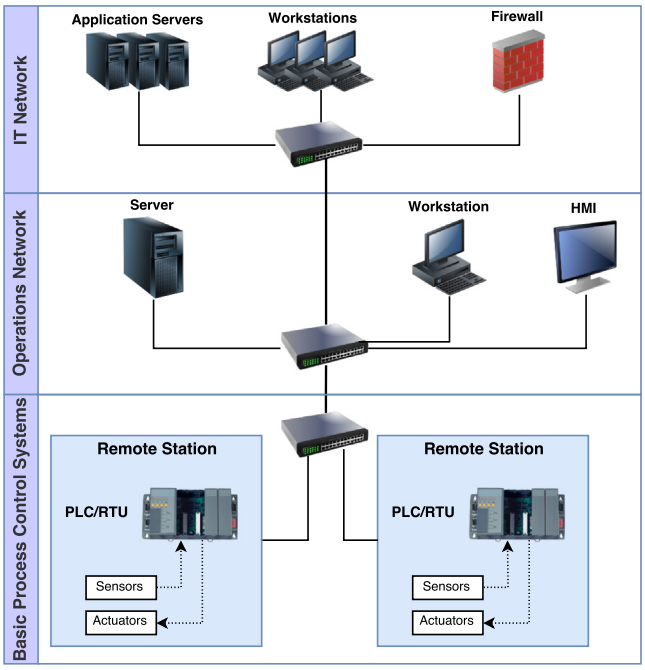

Fig. 1. A typical SCADA system.

- System reliability regularly takes precedence over threats to security and can result in high security vulnerability.
- Absence of encryption in earlier communication protocols (plain text is often utilised).
- The common used well-documented protocols and off the shelf hardware solutions can threaten to undermine obscurity [14]. Whilst this is not a mechanism of security per se, the loss of it can lead to attacks becoming easier.
- The operation of SCADA has to be ongoing, which makes it very hard to apply updates, perform patching or to modify system components.
- Today's systems are lasting longer than in the past, which means that hardware and software are operating beyond their supported lifespan [15].

The aforementioned specific characteristics and constraints in relation to SCADA mean that a domain specific approach is necessary. In-line security mechanisms (e.g. traditional network IDS utilisation) or security tools at the host level (e.g. antivirus) are not recommended owing to possible latency impact or the occurrence of single points of failure along the vital communications path. Further, given the increasing sophistication of attacks, cyber-security no longer can depend on supervised, pattern-based detection algorithms to guarantee continuous security monitoring. There needs to be approaches that handle rogue threats, which provide a suitable balance between maintenance and detection power [16].

4. Real-world attacks

Among others, the STUXNET worm infection [17] perfectly represents the frailty of the regulatory systems devoted

to control critical infrastructures. First isolated in mid-June 2010, STUXNET was a computer virus specifically designed for attacking Windows based industrial computers and taking control of Programmable Logic Controller (PLCs), influencing the behaviour of remote actuators and leading to instability phenomena or even worse. The paradox is that critical infrastructures massively rely on newest interconnected (and vulnerable) Information and Communication Technology (ICT) technologies, while the control equipment is typically old, legacy software/hardware. Such a combination of factors may lead to very dangerous situations, exposing the systems to a wide variety of attacks. The lesson the CIIP (Critical Information Infrastructure Protection) community has learned from the spread of the STUXNET worm is that, in order to effectively react to a specific low level menace, there is the need to consider both the global and local perspectives. In fact, besides obtaining a wider perspective on the state of the System of Systems, there is the need to increase the intelligence of equipments and devices that are used to influence the behaviour of the system, such as RTUs, valves, etc.

Moreover, as emphasised by several episodes [18], another effective way to paralyse a SCADA system via cyber attack is to saturate the bandwidth of the carrier used for the communication (this was, for example, the way in which the SLAMMER worm operated in 2003 to affect the SCADA of two United States (US) utilities and a nuclear power plant). Indeed, as emphasised also by the ANSI/ISA.99 (American National Standards Institute/International Society of Automation), availability is the most crucial attribute of information security. The lack of timely information to/from the field may cause dramatic consequences because the field is unable to receive the adequate command, hence even trivial episodes may provoke dramatic impact, as shown by the US black-out.

In an evaluation of the Mariposa botnet infection in an ICS organisation, the US Department of Homeland Security [19] explained that they found that the infection occurred when an employee used a USB drive to download presentation materials to a corporate laptop. When the user connected the laptop to the corporate network upon returning to work, the virus spread to over 100 hosts.

The security of SCADA communications is becoming more complicated because the decision has been taken to link the SCADA networks with IT networks to allow better and faster communications. But these new features have increased the threats and risks on SCADA communications. There are presently no convinced solutions to enforce the security of SCADA communications in that perspective. The idea to add intelligence to the field is not new; electro-valves for gas pipelines are available on the market that, in the case they receive a rapid sequence of open-close commands, do not perform them in order to avoid the consequence of the mechanical shock. A number of EU (European Union) projects such as the FP6 SAFEGUARD and FP7 CRUTIAL (CRitical UTility InfrastructurAL Resilience) have explored the technical feasibility to improve cyber security of SCADA system by improving the smartness of the field devices.

5. Discussion

Further complication arises because it is known that a large percentage of attacks are induced by inside attackers. Thus perimeter defense alone cannot defend the system. In such cases, the question that one is confronted with is whether there is enough indication of an ongoing attack in the dynamics of the system itself [20]. Despite this range of activities, it has been proven that half of these have human error at their core [21]. Therefore, there should be increased empirical and theoretical research in to human aspects of cyber security based on the volumes of human error related incidents in order to establish ways in which mainstream cyber security practice can benefit.

Security measures tend to neglect that persistent attackers will eventually gain access whatever that perimeter protection may be. One main objective from modern security solutions would be to develop novel methods that could detect and disturb the activities of the attackers once they have gained access inside the system. Special care should be given to the implementation of new strategies that can detect, prevent and mitigate data exfiltration attacks, since intrusion detection/prevention strategies are now deemed to be inadequate for data protection [22].

In order to strengthen the security of SCADA systems, one solution is to deliver defence in depth [23] by layering security controls so as to reduce the risk to the assets being protected. By applying multiple controls on top of the information asset (in this case the SCADA and ICS configuration and management data) the architect introduces further barriers, which a threat actor has to overcome. For the more competent threat actors this will slow them down. Within the time it takes to get through some of the controls, the protective monitoring service should have alerted someone to the attack, which will allow further action to be taken (such as dropping the threat actors connection). Defence in depth ensures there is no single point of failure from threats to assets by providing differing barriers (controls) in a layered approach.

6. Conclusions

The synergy between the ICS and the IoT has emerged largely bringing new security challenges. We have identified key security issues for ICS and current solutions. Future work should primarily focus on the balance between holistic approaches that can deal with a wide variety of attacks, real time identification of intruders with high accuracy and solutions that impose low overhead to the communication and performance of SCADA/ICS systems.

References

[1] Eric D. Knapp, Joel Thomas Langill, Industrial network security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems, Syngress, 2014.

[2] Adrian Pauna, K. Moulinos, Matina Lakka, J. May, T. Try-fonas, Can we learn from SCADA security incidents? in: White Paper, European Union Agency for Network and Information Security, Heraklion, Crete, Greece, 2013.

[3] Allan Cook, Helge Janicke, Leandros Maglaras, Richard Smith, An assessment of the application of it security mechanisms to industrial control systems, Int. J. Internet Technol. Secured Trans. 7 (2) (2017) 144–174.
[4] Robert Mitchell, Ing-Ray Chen, A survey of intrusion detection techniques for cyber-physical systems, ACM Comput. Surv. 46 (4) (2014) 55.
[5] Martin Naedele, Addressing IT security for critical control systems, in: System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference, IEEE, 2007 115–115.
[6] Ehab Al-Shaer, Mohammad Ashiqur Rahman, Smart grids and security challenges, in: Security and Resiliency Analytics for Smart Grids, Springer, 2016, pp. 3–13.
[7] Tiago Cruz, Luis Rosa, Jorge Proença, Leandros Maglaras, Matthieu Aubigny, Leonid Lev, Jianmin Jiang, Paulo Simões, A cybersecurity detection framework for supervisory control and data acquisition systems, IEEE Trans. Ind. Inform. 12 (6) (2016) 2236–2246.
[8] Mohamed Amine Ferrag, Leandros A. Maglaras, Helge Janicke, Jianmin Jiang, A survey on privacy-preserving schemes for smart grid communications, 2016. ArXiv preprint arXiv:1611.07722.
[9] Grigoris Tzokatziou, Leandros Maglaras, Helge Janicke, Insecure by design: Using human interface devices to exploit SCADA systems, in: 3rd International Symposium for ICS & SCADA Cyber Security Research, 2015.
[10] Eric Byres, P. Eng, I.S.A. Fellow, Using ANSI/ISA-99 standards to improve control system security, White paper, Tofino Security, 2012.
[11] Bonnie Zhu, Anthony Joseph, Shankar Sastry, A taxonomy of cyber attacks on SCADA systems, in: Internet of things (iThings/CPSCom), 2011, 4th International Conference on Cyber, Physical and Social Computing, IEEE, 2011, pp. 380–388.
[12] M. Luallen, Breaches on the rise in control systems: A sans survey 2014, 2014.
[13] Ahmad-Reza Sadeghi, Christian Wachsmann, Michael Waidner, Security and privacy challenges in industrial internet of things, in: Proceedings of the 52nd Annual Design Automation Conference, ACM, 2015, p. 54.
[14] Andrew Nicholson, Tim Watson, Peter Norris, Alistair Duffy, Roy Isbell, A taxonomy of technical attribution techniques for cyber attacks, in: European Conference on Information War-fare and Security, Academic Conferences International Limited, 2012, p. 188.
[15] Tiago Cruz, Jorge Proença, Paulo Simões, Matthieu Aubigny, Moussa Ouedraogo, Antonio Graziano, Leandros Maglaras, A distributed IDS for industrial control systems, Int. J. Cyber Warfare Terrorism 4 (2) (2014) 1–22.
[16] Leandros A. Maglaras, Jianmin Jiang, Tiago J. Cruz, Combining ensemble methods and social network metrics for improving accuracy of ocsvm on intrusion detection in scada systems, J. Inf. Secur. Appl. 30 (2016) 15–26.
[17] Robert McMillan, Siemens: Stuxnet worm hit industrial systems, in: Computerworld, Vol. 14, 2010.
[18] Sandro Bologna, Roberto Setola, The need to improve local self-awareness in CIP/CIIP, in: Critical Infrastructure Protection, First IEEE International Workshop on, IEEE, 2005, p. 6.
[19] Prosenjit Sinha, Amine Boukhtouta, Victor Heber Belarde, Mourad Debbabi, Insights from the analysis of the mariposa botnet, in: Risks and Security of Internet and Systems, CRiSIS, 2010 Fifth International Conference on, IEEE, 2010, pp. 1–9.
[20] Sandeep K. Shukla, Cyber security of cyber physical systems: Cyber threats and defense of critical infrastructures, in: 15th International Conference on Embedded Systems, VLSID, IEEE, 2016, pp. 30–31.
[21] Mark Evans, Leandros A. Maglaras, Ying He, Helge Janicke, Human behaviour as an aspect of cybersecurity assurance, Secur. Commun. Netw. 9 (17) (2016) 4667–4679.
[22] Awais Rashid Dr, Rajiv Ramdhany, Matthew Edwards, Sarah Mukisa Kibirige, Ali Babar, David Hutchison, Ruzanna Chitchyan, Detecting and preventing data exfiltratio, in: Security Lancaster, Lancaster University, 2014.
[23] Andy Wood, Ying He, Leandros Maglaras, Helge Janicke, A security architectural pattern for risk management of industry control systems within critical national infrastructure, Int. J. Crit. Infrastruct. (2016).