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:

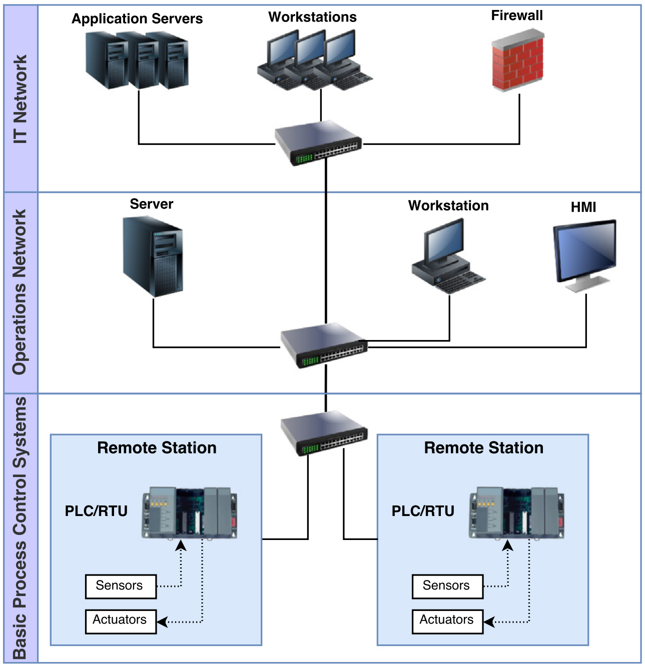

Fig. 1. A typical SCADA system.

- 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. anti-virus) 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