Chapter 1
Security Awareness in the Internet of Everything

Viacheslav Izosimov
Semcon Sweden AB, Sweden

Martin Törngren
KTH Royal Institute of Technology, Sweden

ABSTRACT

Our societal infrastructure is transforming into a connected cyber-physical system of systems, providing numerous opportunities and new capabilities, yet also posing new and reinforced risks that require explicit consideration. This chapter addresses risks specifically related to cyber-security. One contributing factor, often neglected, is the level of security education of the users. Another factor, often overlooked, concerns security-awareness of the engineers developing cyber-physical systems. Authors present results of interviews with developers and surveys showing that increase in security-awareness and understanding of security risks, evaluated as low, are the first steps to mitigate the risks. Authors also conducted practical evaluation investigating system connectivity and vulnerabilities in complex multi-step attack scenarios. This chapter advocates that security awareness of users and developers is the foundation to deployment of interconnected system of systems, and provides recommendations for steps forward highlighting the roles of people, organizations and authorities.

INTRODUCTION

Joe[1] was driving a long-hauler on his way to Michigan. Suddenly, the truck electronics started acting crazy showing speeds above 90 mph, lots of failures on the display, beeping all over. He pulls off the truck onto the sideway. That day most of the trucks stopped all over the country, not possible to fix or repair on a short notice... This led to goods not being delivered, with empty supermarkets, empty gas stations, stopped production plants, and other economically negative consequences. What was the reason for these events? A good friend recommended installing a great app for fuel consumption monitoring.

DOI: 10.4018/978-1-6684-3554-0.ch001

Joe did and so did many drivers. The app was helpful until the very last update… Luckily, some trucks were still operational and the reserve vehicles were put to help.

The system will not be more secure than the knowledge in security of its creators. Security knowledge and awareness of engineers that implement or install a system can be as critical as the choice of a crypto algorithm and a proper key management infrastructure. Security-awareness of system users and operators are critical to ensure that the system is not compromised. Irrespective of the technical quality, any solution becomes effectively unsecure if the user leaks out passwords or blindly accepts installation of malicious software.

The focus of this chapter will be on smart cyber-physical systems (CPS) in Internet of Things (IoT) that provide services critical for society. Examples of these smart systems include connected passenger cars, intelligent transportation systems, smart household appliances and alike. This chapter considers them together with their drivers, operators, installation engineers and other persons directly and indirectly involved into their creation and during operation. These systems live in the Internet or exist as part of an era of connectivity and dependencies represented by infrastructures such as 3G/4G/5G, global navigation and positioning systems, providing and requesting services. The IoTs are nowadays part of infrastructures in healthcare, energy, transportation and many others. The level of interaction in these infrastructures has increased substantially with advances in development and enhancement of “clouding”, connecting to and making use of cloud computing services. This type of connectivity nowadays raises concerns for robustness and trustworthiness. A fault or a malicious attack on one of system’s components, even the least critical at first glance, may affect other, critical, ones. A trend is, thus, emerging towards “edge computing”, as a way to decentralize the cloud and reduce some of the risks associated with the clouding. For example, Satyanarayanan et al. (2013) advocate for cloudlets as a viable connectivity alternative to clouds in hostile environment, ultimately considering the whole Internet or its parts as possibly hostile, e.g. in the event of a cyberwar, natural disaster or during military operations.

The chapter will also look into examples of “not yet smart” systems and will advocate that they must be designed with the same level of security requirements as those connected to the Internet. Otherwise, these “not yet smart” systems pose potential serious threats to society when they unintentionally find their ways to the connected world, in situations often unexpected. In a modern society, it is nearly impossible to avoid these connections, due to actions of users, due to system complexity and sometimes due to security negligence of system developers.

According to the Roundtable on Cyber-Physical Security, Peisert et al. (2014), developers and users are responsible for security of an embedded product. Tariq, Brynielsson & Artman (2014) studied the problem of users’ security awareness in where they conducted a number of semi-structured interviews in a large telecommunication organization.

The authors of this chapter decided to use a similar approach to evaluate security-awareness of developers, engineers and academics, by conducting a number of interviews and surveys. The chapter will give some insight into the study of user awareness in a user-centric survey.

To evaluate state of practice in security of existing systems, authors conducted two practical attacks feasible, in particular, due to security-unawareness of system developers and users. The attacks involve a connected smart product, a modern commercial vehicle, e.g. Joe’s truck, and an off-line critical facility.

The objectives of this chapter are to:

- Present background and relevant literature on cyber-physical security and security awareness;