Chapter 21
Enterprise Security: Modern Challenges and Emerging Measures

Manish Shukla
TCS Research, Tata Consultancy Services, India

Harshal Tupsamudre
TCS Research, Tata Consultancy Services, India

Sachin Lodha
TCS Research, Tata Consultancy Services, India

ABSTRACT

As we increasingly depend on technology, cyber threats and vulnerabilities are creating trust issues for businesses and enterprises, and cybersecurity is being considered as the number one threat to the global economy over the next 5-10 years. In this chapter, the authors explain this phenomenon by first describing the changing cyber ecosystem due to extreme digitalization and then its ramifications that are plainly visible in the latest trends in cyber-attacks. In the process, they arrive at five key implications that any modern enterprise needs to be cognizant of and discuss eight emerging measures that may help address consequences of those implications substantially. It is hoped that these measures will play a critical role in making enterprise security more proactive, cognitive, automated, connected, invisible, and risk aware.

INTRODUCTION

Due to the extensive digitalization in the last decade, the cost of entry into cyberspace has rapidly come down. Importantly, it has induced major changes in the enterprise and in its operating environment as manual and paper oriented processes are being replaced with software. Large scale digitalization has also made it possible for enterprises to better analyze their performance, cost drivers, customer behavior and associated risks. With the emergence of Internet of Things (IoT), there is now an explosion of interconnectivity that has led to the rapid blurring of the boundaries between virtual and physical worlds.

DOI: 10.4018/978-1-6684-3698-1.ch021

Information flows that originally were within the digital spaces are now flowing into physical spaces, leading to numerous benefits and several concerns, especially with regards to safety, security and privacy.

Indeed, a cyber threat is a possibility of an attack, via cyberspace, targeting the cyberspace of an organization for the purpose of disrupting, disabling, destroying, maliciously controlling a computing environment or stealing sensitive information (Kissel, 2011). According to 'The Global Risk Report 2019' by World Economic Forum, cyber threat is ranked 5th in terms of likelihood and ranked 7th with respect to overall impact (World Economic Forum, January 15, 2019). A large majority of respondents (82%) expect increased risk of data and money theft, and disruption in critical services (80%). The survey results clearly show the perception of new risks due to increased digitalization. This belief is substantiated by the fact that cyber threats can come from any direction, as shown by a massive distributed denial of service (DDoS) attack by IoT devices which were infected by Mirai botnet starting in 2016 (Antonakakis et al., 2017). Similarly, Meltdown (Lipp et al., 2018) and Spectre (Kocher et al., 2018) hardware vulnerabilities in modern processors allow malicious programs to steal data which is being processed on the vulnerable computer. Additionally, there are threats which are equally applicable to software and hardware, for example, ransomware attacks (Shukla, Mondal, & Lodha, 2016). The current generation of cyber threats are getting more sophisticated and have the ability to spread rapidly due to high interconnectivity between systems.

CHANGING CYBER ECOSYSTEM

To better understand the explosion of cyber-attacks, we have to look at the changes in the cyber ecosystem due to digitalization and hyper interconnectivity.

1. **Increase in Attack Surface:** Traditionally, attack surface of a system is defined as the exposure of an application, its interfaces and objects to an attacker (Heumann, Keller, & Turpe, 2010). However, from an enterprise perspective, a system consists of a combination of hardware and software assets and the humans using them.

It has been demonstrated multiple times that even if the software is bug free, yet it is possible to steal personal and sensitive data by exploiting hardware vulnerabilities (Lipp et al., 2018; Kocher et al., 2018). In a recent paper, researchers have shown systematic degradation in deep-neural-networks (DNN) under bitwise errors that are induced by hardware fault attacks (S. Hong, Frigo, Kaya, Giuffrida, & Dumitras, 2019). According to (Ornes, 2016), only 5 million IoT devices went online in 2016 and it is estimated that 20-50 billion devices will be online by 2020. Thus, the hardware part of attack surface is growing at a rapid pace, and, that too, without security bedded into it.

Typically, software creation process involves multiple people with varying level of skills in information security, which results in buggy software. Attacks on software can be broadly divided in two classes: a) exploitation of benign software, and b) threat from malicious software. Both of these classes are fairly prominent, for example, authors in (Evtyushkin, Ponomarev, & Abu-Ghazaleh, 2016) have shown an attack on branch predictors to bypass address space layout randomization (ASLR). Similarly, authors have demonstrated exploitation of web-applications for mounting cross-site scripting (XSS) attacks and performing parasitic computation on victim's system (Eskandari, Leoutsarakos, Mursch, & Clark, 2018; Steffens, Rossow, Johns, & Stock, 2019). The other class of attacks using software is well-known, for