Chapter 98
A White Hat Study of a Nation's Publicly Accessible Critical Digital Infrastructure and a Way Forward

Timo Kiravuo
Aalto University, Helsinki, Finland

Mikko Särelä
Aalto University, Helsinki, Finland

Seppo Tiilikainen
Aalto University, Helsinki, Finland

Jukka Manner
Aalto University, Helsinki, Finland

ABSTRACT

The developed society depends on many critical infrastructure processes, such as power generation, water treatment, many types of manufacturing, and smart buildings. These processes need control and the automation industry has embraced the Internet to connect all these controls. However, the controlling devices thus opened to the world do not always have adequate safeguards to withstand malicious users. Many automation systems have default passwords or known and unknown backdoors. Also, often those systems are not updated to close security weaknesses found after original installation. The authors argue that while the industry is familiar with the notion of safety of equipment and processes, it has not focused enough on IT security. Several years ago the Shodan search engine showed how easy it is to find these control devices on the Internet. The authors followed this research line further by targeting one nation's IP address space with Shodan and found thousands of control systems, many of which represent models and versions with known vulnerabilities. Their first contribution is presenting these findings and analyzing their significance. Their study started in 2012 and the most recent results are from the end of 2015. To gain further knowledge, they have built a prototype scanner capable of finding industrial control systems. This lets the authors evaluate the possibility of performing routine scans to gauge the vulnerability of a nation. Their second contribution is to present a template for a national Internet scanning program. The authors discuss the technology, performance, and legality of such a program. Based on their findings and analysis they argue that nations should continuously monitor their

DOI: 10.4018/978-1-7998-2466-4.ch098

own Internet address space for vulnerabilities. The authors' findings indicate that the current level of vulnerabilities is significant and unacceptable. Scanning a nation's critical infrastructure can be done in minutes, allowing them to keep a tight control of vulnerabilities. Yet, in addition, the authors need to extend current legislation and the rights of government officials to bring more security in national critical infrastructures; this discussion is their third contribution. The cyber-space has become a playing field for criminals, terrorists and nation states, all of which may have a motive to disrupt the daily life of a nation, and currently causing such disruptions is too easy.

1. INTRODUCTION

The World Economic Forum describes in their Global Agenda how our society is moving towards the fourth industrial revolution. The first revolution was the shift to water and steam power to enhance production, and the second revolution used electric power to further extend mass production. The third revolution brought in electronics and information technology to automate production even further. Now we are moving towards an intertwined world where everything from single small sensors to huge power plants and production facilities are networked, building the fourth industrial revolution. Thus the critical functions of a modern, high-technology society are becoming tightly linked.

The information infrastructure is at the heart of the fourth revolution, fusing formerly independent systems together: distribution of electricity is as dependent on communications networks as communication networks are dependent on electricity. Disturbances in some elements of the critical infrastructure can have massive ripple effects to other parts of the infrastructure, and towards the entire society.

The vulnerability of this critical digital infrastructure has been pointed out in recent years by several authors (Byres 2004, Lewis 2006). One of the most efficient tools to visualize how vulnerable the developed economies are, is the Shodan search engine that can be used to find cyber-physical devices on the Internet (Matherly 2009). The need for inside information or detailed knowledge about the systems is increasingly not needed anymore to compromise Industrial Control Systems (ICS) (Byres 2004, Weiss 2010). We decided to use Shodan and self-developed tools to evaluate the situation in Finland.

Our first contribution is that we ran a study from 2013 up to end of 2015, looking at targets in Finland. In the early phases, the number of potential critical targets increased at an alarming rate, but in late 2015 the numbers dropped significantly. This seems to imply that our initial work that was reported to the authorities lead eventually to a higher level of system protection. There have been other published similar studies, yet our work is a long-time effort to study one specific country in detail.

As the second contribution, we built and measured a prototype for a national scanning service, capable of analyzing all IPv4 addresses of a country in order to find ICS systems that might be vulnerable to an attack. Our measurements and calculations show that it would be very much feasible to scan all of a nation's IPv4 hosts even every hour in order to proactively find critical systems that need to be better protected.

Finally, even though we can show that proactive scanning is possible to implement, at least when IPv6 becomes more wide-spread, scanning all possible IP addresses will be impossible, simply due to the sheer number of potential IPv6 hosts. Thus, we need to understand the role of government officials and the industry players at large, and what responsibilities we can see given to each of them. The discussion of how to enable a more secure country, what responsibilities we can envisage, is our final contribution.