International Institute of Humanitarian Law
Institut International de Droit Humanitaire
Istituto Internazionale di Diritto Umanitario

42nd ROUND TABLE ON CURRENT ISSUES OF INTERNATIONAL HUMANITARIAN LAW ON THE 70th ANNIVERSARY OF THE GENEVA CONVENTIONS

"Whither the human in armed conflict? IHL implications of new technology in warfare"

Sanremo, 4-6 September 2019

Casualties caused through computer network attacks: the potential human costs of cyber warfare

Marina KROTOFIL
Senior Security Engeneer, BASF

Summary

Industrial Control Systems (ICS) threat landscape has changed dramatically over the past few years. New threats have emerged to challenge the shock created by Stuxnet, malware used to disrupt Iranian nuclear program in 2010. Industrial Control Systems are frequently called Cyber-Physical Systems (CPS) because they consist of software and network components deeply embedded into the physical world. Examples of such systems include water treatment, electricity generation/distribution, manufacturing, (petro)chemical production and other processes. Correspondently, attacks on CPS are called cyber-physical attacks. This talk presents the evolution of the ICS exploits and tactics to picture ongoing „Race-to-the-Bottom" trend between ICS threat actors and defenders. There are two conclusions which follow this talk: (1) Traditional IT security approaches are not enough to defend against cyber-physical attacks and defenses should additionally include process- and control-engineering

methods, (2) Due to the potential of cyber-physical attacks to have kinetic effect and cause casualties, it is urgent and of utmost importance for the international community of IT security specialists, governments and humanitarian lawyers to have a conversation about how to regulate the deployment of cyber-physical attacks.

Introduction

In the Information Technology (IT) domain, increasingly there is a gap between the attacker and defender capabilities. The attackers embraced firmware modifications and supply chain rootkits a decade ago while the defense community has recently embraced data diodes and application whitelisting. Current IT security defense technologies are not matched to offensive capabilities of threat actors and the gap keeps increasing, slowly becoming hard to close. It is highly likely that similar pattern will repeat for industrial control systems, and it is hoped that understanding the historical trends of the IT security industry will provide a discussion point when anticipating threats and planning defense strategies for Industrial Control Systems against cyber-physical attacks.

History of IT security

Security is a moving target. At first the security was introduced into the network to prevent hackers from stealing passwords and impersonating communication parties or Man-in-the-Middle (MITM) attacks. Later the security moved into the computer and the operating system (OS). As the attackers became practiced in exploiting OS, security controls had to expand into software applications, resulting in such solutions as sandboxing and hypervisors. However, even these technologies are no longer enough.

The fundamental flaw in the modern defensive computer security is the assumption that a personal computer (PC) is only a single computer running a single operating system. The fact is that nearly every hardware component that used to be “dumb” has been replaced with a “smart” component. For example, network cards now have own firmware (own OS), built-in web server and perform complex cryptographic tasks. The main CPU of a computer system requests these other “computers” for access and data. Modern computer is not just one computer anymore!

The advantage for the attacker is that these other computers lack almost all of the security protections built into modern operating systems. It is currently less labor intensive to write and maintain a rootkit for a firmware than to maintain the same rootkiting functionality in the main operating system.

In the hacking community it is sometimes called *Race-to-the-Bottom*. As soon as security is introduced at some layer of computer or network architecture abstraction, the attackers are placing their exploits one layer down. While Windows has gotten its own firewall not long ago, the attackers are already mastering their skills in exploiting silicon microchips.

Current trends in ICS security

Industrial control system (ICS) is a collective term used to describe different types of control systems and associated hardware instrumentation, software applications and communication infrastructure, which are used to automate and operate industrial processes. Some of the industrial processes are called critical infrastructures because they are critical to the wellbeing of the population (e.g., water and power distribution utilities).

Industrial automation has followed IT hardware development path. What used to be a simple analog sensor is now an IP-enabled smart transmitter with complex firmware, multiple wired and wireless communication modes, a large number of configuration possibilities, and even a web-server so that maintenance staff could calibrate and configure the device without approaching it.

The sensors used in ICS are also becoming more distributed than ever before with new types of sensors being introduced continuously. Tank farms are frequently placed in safer locations away from the main production plants. Weather sensors are placed outside the plant fence. Predictive maintenance systems with additional sensors are being integrated into assets that were previously only mechanical machines. We should take a look at the current trends in ICS exploitation to see whether industrial controller and smart field instrumentation (smart sensors and actuators) could become an attacker target any time soon.

The major difference between IT and cyber-physical attacks is the attacker's end goal. While in IT domain the ultimate goal of the attacker is to get access to certain data, in the ICS domain attacker's goal is to cause impact in the physical world. Besides Stuxnet (https://www.langner.com/wp-

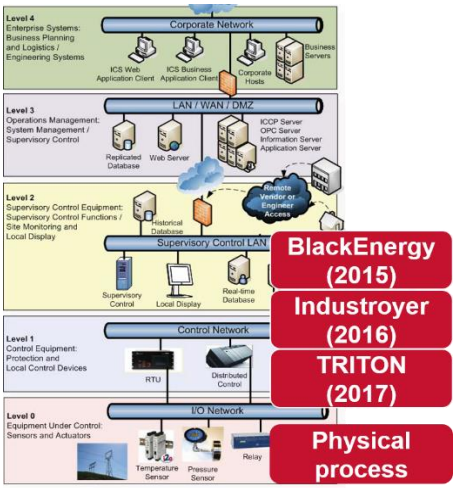
content/uploads/2017/03/to-kill-a-centrifuge.pdf), there were three other cyber-physical attacks in the past years:

Attacks on three power substations in Ukraine, 2015; malware family – BlackEnergy3, (https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pd);

Attack on power substation in Ukraine, 2016; malware family – Industroyer (https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf);

Attack on Safety Instrumented System (SIS) in a Saudi Arabia refinery, 2017; malware family – TRITON (https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html)

If we map these attacks against the Purdue reference model of the Industrial Control Systems network architecture, we will notice that with each attack threat actors are moving their exploits one network layer lower. Thus, the first attack on Ukrainian power grid in 2015 (BlackEnergy3) was executed at the level of Human Machine Interface (HMI) by taking control over operator's screen. In the second attack (Industroyer), threat actor moved one layer lower and launched their exploits at the level of industrial control protocols. In the TRITON attack, threat actors attempted to inject malicious code directly into the memory of Programmable Logic Controller (PLC) belonging to Safety Instrumented System (SIS), thus placing themselves very closely to the I/O cards and field instrumentation (sensors and actuators). It means, that the attackers have moved their exploits to the immediate proximity of the physical processes. This is because majority of embedded systems (controllers and field instruments) are currently lacking any exploit mitigation capabilities and defenders have little experience in



performing compromise assessment and forensic analysis on these systems.

To date, it is unclear how to evaluate these attack from the legal perspective. During the attack on Ukrainian power grid in 2015, around 250k people were left without power supply for an hour. At that time no national government condemned the execution of this attack and as a result, attacks on critical infrastructures were silently accepted as a "new normal" (this phenomenon is sometimes called "normalization of deviance"). A similar attack on the Ukrainian power grid in 2016 affected 225k people and was similarly left undiscussed from the legal standpoint. Situation became more critical in 2017, when the attackers targeted Safety Instrumented Systems with TRITON exploit. SIS are designed to guard civilians in the hazardous facilities from e.g. toxic releases or explosions and are meant to prevent casualties. By targeting these systems, the threat actors are willingly putting human lives in danger and denying their right for being safe. This is why it is of utmost importance to regulate deployment of cyber-physical attacks by the means of international laws.

Miscellaneous

Cyber-physical attacks are not the only attacks which can put human lives in danger. On June 27th, 2017, a massive cyberattack (NotPetya ransomware) hit Ukraine on the eve of Constitution Day. The attack payload was distributed via the updates of the most popular tax-filling software in Ukraine. Once delivered to the organization's network, the malware spread rapidly across all reachable computer systems. Cash counters in the grocery stores, bank's ATMs, medical facilities, metro ticket sales points, critical infrastructures, industrial production enterprises, governmental organizations – all these systems were paralyzed by the malware. The life in the country has almost entirely came to holt in less than 24 hours since the time of attack initiation.

In Ukraine, the country's Minister of Health, Ulana Suprun, told BBC Future that her office was taken back in time about 30 years. "We're working by pen and paper again," she says. "There are so many things we can't do because we're down," says Suprun.

For example, her ministry centralizes the distribution of medicine across the vast territory of Ukraine's 24 regions. When hospitals in those regions run low on medications for patients, they contact the ministry to source

medicine. Either the ministry has them, or they locate them in other regions and send them to the region in need.

"But we can't relay those messages right now, except for by phone, so imagine how crippling that is to us," says an exasperated Suprun. "What used to require one email, copied to the 24 regions now requires 24 separate phone calls before we can find the drugs. Ukrainians can't get medical documents because our internal system is down. I can't pull up statistics for a meeting I have this week about Aids. I couldn't even tell you which hospitals went down because they can't reach us." https://www.bbc.com/future/article/20170704-the-day-a-mysterious-cyber-attack-crippled-ukraine

Through the globally interconnected systems, NotPetya rapidly propagated worldwide, causing significant downtime and financial losses to such multinational companies as Maersk, pharmaceutical giant Merck, FedEx's European subsidiary TNT Express, French construction company Saint-Gobain, food producer Mondelēz, manufacturer Reckitt Benckiser and many others. Currently, the world has very little understanding of such international IT infrastructure interrelationships and dependencies. Maersk has suffered 300 million in recovery costs due to NotPetya attack (https://www.reuters.com/article/maersk-results-idUSL8N1L21HM).

It is critical to understand that at the time of national or global crisis the speed of the infrastructure recovery will be dependent on the number of available professionals to perform these tasks. Typically, companies rely on external service providers for recovery operations. At the time of crisis when multiple organizations are affected, the amount of trained work force will become a major bottleneck. Additionally, majority of organizations have weak backup policies and processes, which may result in unavailability of backups. This, in turn, will lead to significant delays in recovery and return to operational state.

Exploitation of embedded systems (industrial equipment, IoT and mobile devices, automotive systems and others) once used to be an exotic skill. These days, cyber-criminals and state-sponsored threat actors demonstrate advanced skills in exploiting these systems. An example includes VPNFilter attack (2018), in which more than 500,000 SOHO (small and home office) routers of diverse makes/models worldwide were targeted by sophisticated modular malware with a multistage payload (http://blog.talosintelligence.com/2018/05/VPNFilter.html).

Moreover, as the attackers becoming more skilled, it is getting easier for them to exploit large organizations such as vendor or service provider to get access to a small number of intended targets. E.g., in a recent example, attackers subverted ASUS software update process to distribute their malicious code. It turned out, that the adversaries were merely interested in about 600 specific MAC addresses of ASUS laptops or in another words – in only 600 intended targets (https://www.wired.com/story/asus-software-update-hack/). In general, usage of staging targets such as equipment vendor or trusted service providers became a preferable method of the attackers to get access to their intended targets. In 2018 USA and UK governments have issued security advisories (https://www.us-cert.gov/ncas/alerts/TA18-074A and https://www.ncsc.gov.uk/news/joint-us-uk-statement-malicious-cyber-activity-carried-out-russian-government) to warn industrial control systems and critical infrastructure operators about state-sponsored attacks with the goal of intrusion and establishing persistence in the infrastructure, possibly for future needs.

Conclusions

While the world has not discovered a disruptive attack code being hidden in the smart field instrumentation yet, it does not mean that threat actors are not capable of exploiting these systems or fitting complex exploitation code into resource-constrained devices. Thus, the numbers of attacks on various embedded systems has exploded in the past years. Also, researchers have already shown that it is possible to embed the entire code for sophisticated physical damage attack into the firmware of a smart transmitter.

Following IT domain trends, the ICS defenders mount firewalls and harden the systems to prevent the attackers from reaching lower layers of industrial control networks. In response, the attackers are searching for alternative exotic pathways into control network, where supply chain, external maintenance laptop and subcontractors' remote access are being just few examples. Overall, supply chain compromise is becoming one of the most serious threats to industrial environments with limited opportunities for proactive detection and prevention of these attacks.

The origin of one of the TRITON attack was narrowed down to Central Scientific Research Institute of Chemistry and Mechanics in Moscow, Russia. This is a previously unseen modus operandi for offensive operations, when an intrusion team was moved closer to the team of technologists (engineers) and indicates a formation of multidisciplinary teams when

conducting cyber-physical attacks. Note, that other national states has previously claimed their capability to disrupt civilian and critical infrastructures by the means of cyberattacks at the time of political or military crisis.

Defending against a sophisticated attacker require sophisticated defense methods. In addition to canonical IT security protections, it is important to include engineering approaches from the process- and control-engineering domain. E.g., forged sensor readings can be detected via plausibility and consistency checks – the same methods, which are used for detecting faulty sensors. Predictive maintenance algorithms could be used for spotting early signs of process or equipment degradation so that operators could take corrective actions in a timely manner and prevent an attacker from completing their destructive mission.

Due to the potential of cyber-physical attacks to have kinetic effect and cause casualties, it is urgent and of utmost importance for the international community of IT security specialists, governments and humanitarian lawyers to have a conversation about how to regulate the deployment of cyber-physical attacks to prevent potential humanitarian crises.