Abstract

The topic of kinetic threats and Industrial Internet of Things (IIoT) cybersecurity has become matters of importance among academia and practitioners, as these buzzwords appear on front-page news in trade journals and media. The academia world has brought awareness to IT security, such as kinetic threats and industrial IoT cybersecurity solutions. Kinetic threats, identified as a class of attacks, both directly or indirectly, causes any form of destruction through the exploitation of exposed, vulnerable networks and infrastructure. These threat agents target cyber physical systems (CPS), including IIoT, which includes physical machinery with software and networked sensors across power grids, telecommunications and transportation networks. A recent study revealed that industrial IoT cybersecurity attacks will impact software, hardware, national infrastructure, defense, and daily operations of individuals and organizations. Traditional security solutions are outdated and have vulnerabilities, which are exposed to hackers, who gain unauthorized access to unprotected interfaces, hardcoded backdoors, and unencrypted connections. This paper presents the current status and trend of attacks such as kinetic threats and industrial IoT cybersecurity. Then, it discusses various kinetic threats and real-world issues. Five recommended solutions will be proposed.

Keywords

Cyber-physical systems (CPS), Cybersecurity, Internet of Things (IoT), Industrial Internet of Things (IIoT), Industrial Control Systems (ICS), Kinetic Threats.

I. INTRODUCTION

Kinetic threats and industrial Internet of Things (IoT) cybersecurity have become the buzzwords in today's IT security world, appearing on front-page news in trade journals and media. Kinetic threats exist as threat agents that target cyber physical systems (CPS), including IIoT, which pertains to physical machinery with software and networked sensors within industrial industries such as manufacturing, logistics, oil and gas, transportation, energy, utilities, mining, and aviation (Alguliyev et al., 2018; Youssef and Labeau, 2018). Kinetic threats fall under a class of attacks, both directly or indirectly, that cause any form of destruction through the exploitation of exposed, vulnerable networks and infrastructure. The 2018 Symantec Internet Security Threat Report showed alarming statistics: a 600% increase in IoT attacks in 2017, and the number of ICS vulnerabilities increased 29% in 2017 (Symantec, 2018). This leads to Cerf's proposed question, "what if a device is adopted that's corrupted, and it has a backdoor allowing remote access to a residential network of devices?" (Cerf, 2018).

Recent research on challenges to cybersecurity (Sen, 2018) have pointed out that cybersecurity incidents will impact software, hardware, national infrastructure, defense, and the daily operations of individuals and organizations. Traditional security solutions have shown weaknesses and unreliability, with hackers accessing vulnerable interfaces, perimeter defense device, hardcoded backdoors, and unencrypted connections which are not enough to protect entities from industrial IoT cybersecurity attacks. A recent report by the Identity Theft Resource Center identified 1,138 breaches as of December 5, 2018 (Identity
Theft Resource Center). Supervisory control and data acquisition (SCADA), a part of industrial control system, span a large geographic area, including big three utilities (water, power, and gas) control systems.

Today’s issues relating to kinetic threats and IoT cybersecurity requirements are in the spotlight: privacy, data security, data transfer, as challenges revolve around the complexity of defective IoT devices. As organizations face increased inadequate data protection, with data transmitted over networks and IoT devices, this can pose to be a greater concern, which is why resilience is crucial. Resilience is a fundamental networking concept and a matter of reducing in the volume and severity of damage and loss as well as staying in business or on mission (Rothrock, 2018). This resilience is an entity’s ability to conduct business in a proactive manner in today’s intensively interconnected environment -- while taking a defensive stance against challenges such as cyberattacks and financial loss. The purpose of this paper is to describe the current status and trend of attacks such as kinetic threats, and industrial IoT cybersecurity; to discuss various kinetic threats and real-world issues; and to propose some solutions.

II. CURRENT TREND OF CYBERKINETIC ATTACKS

Over the past decade, attackers have targeted cyber-physical systems (CPS) such as the Aurora Generator, the Stuxnet computer worm and power blackouts. The cyber-physical systems ecosystem includes the world of Internet of Things (IoT) and Industrial Control Systems (ICS). Within the rapidly evolving IoT ecosystem, IoT devices are often unmanaged and insecure by design, as devices are deployed quickly and convenience is prioritized over security. Unmanaged IoT refers to individual devices that are connected and managed by individual end users (U.S. Chamber of Commerce, 2017). With a tremendous rise in cyber attacks against these unprotected/unmanaged IoT devices, the list of IoT attacks grows daily: data breaches, IoT ransomware, distributed denial of service (DDoS) attacks, vulnerable and unpatched IoTs, and attacks on cyber-physical systems.

Thus, this leads to a compromise on every level of the organization, including information exchanged within the networks, especially as the mean time to identify the source of a data breach reached 197 days (Ponemon Institute, 2018a). With the supply chain as a backbone for most corporations’ business operations, defective IoT devices are more at risk than ever before.

The tangible threats have exponentially grown for CPS, including IoT and industrial control systems (ICS). This literature survey, while not exhaustive, presents cyber kinetic attacks limited to technical professional journals (IEEE), trade journals, magazines, and news from 2007 to 2018. Figure 1 shows a timeline of major kinetic attacks over the past decade. Table 1 presents a compilation of cyber kinetic attacks, which highlights widespread kinetic threats and ransomware attacks on various industries. In sum, IoT security solutions need to be interdisciplinary; nations are building armies of trained cyber warfare specialists.

Figure 1. Cyber Kinetic Attacks Timeline
### Kinetic Threats and IoT Cybersecurity

#### Table 1. Kinetic Attacks and Descriptions

<table>
<thead>
<tr>
<th>Industry</th>
<th>Kinetic Attacks Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media</td>
<td>Iran Cyber Army used a DDoS attack on Baidu, China’s top search engine</td>
<td><a href="www.newsweek.com/chinese-hackers-cyberwar-us-cybersecurity-threat-678328">www.newsweek.com/chinese-hackers-cyberwar-us-cybersecurity-threat-678328</a></td>
</tr>
<tr>
<td>Transit</td>
<td>San Francisco transit system was slammed by a ransomware attack</td>
<td><a href="www.reuters.com/article/us-california-cyber-idUSKBN13N1LN">www.reuters.com/article/us-california-cyber-idUSKBN13N1LN</a></td>
</tr>
<tr>
<td>Residential</td>
<td>Hackers use DDoS attack to cut heat to buildings</td>
<td><a href="www.theregister.co.uk/2016/11/09/finns_chilling_as_ddos_knocks_out_building_control_system/">www.theregister.co.uk/2016/11/09/finns_chilling_as_ddos_knocks_out_building_control_system/</a></td>
</tr>
<tr>
<td>Medical</td>
<td>WannaCry Ransomware infects 200,000 medical devices in 150 countries</td>
<td><a href="www.idtheftcenter.org/global-wannacry-ransomware-attack-inflicts-more-than-200k-users">www.idtheftcenter.org/global-wannacry-ransomware-attack-inflicts-more-than-200k-users</a></td>
</tr>
<tr>
<td>Auto</td>
<td>Remote carjacking exposed -- research hackers control every part of the car’s lifeline</td>
<td><a href="www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/">www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/</a></td>
</tr>
</tbody>
</table>

#### III. RECOMMENDED SOLUTIONS

The quest continues in combating cybersecurity threats, as entities are being armed with implementations. In Ponemon Institute’s report, 66% of respondents (out of 3,836 IT security practitioners surveyed) say their organizations have no or low ability to secure their IoT devices and apps (Ponemon Institute, 2018b). The following five recommended solutions are advised for entities looking for protective measures against kinetic threats and IoT cybersecurity.

First, analyze network traffic to detect potential security threats (e.g., IoT applications, malware infections, intrusion attempts, and sensitive data). Protect endpoint security platforms (network accessed by remote devices) focusing on mobile device management and security; enterprise app, prompt patch, user rights management; and secure enterprise file sharing. Numerous devices exist in the market with weak default passwords, as many IoT manufacturers launch devices quickly in the name of convenience. Aside from setting stronger passwords, authentication and intrusion detection system (IDS), especially radio-frequency-based distributed IDS (Shekari et al., 2019) are strongly advised.

Also, safeguard connected devices and networks via more restricted certifications, compliance and regulatory requirements, and internal audits to identify IoT devices as a vulnerable point. More restricted compliances, certified IoT devices, and internal audits should be identified, tested, and implemented. Taking into account the creation of agility, reliability, security, and compliance, expanding DevOps to DevSecOps and/or DevSecComOps is critical and essential (Kim, Humble, Debois, & Willis, 2016). Identifying what the attackers might gain from unauthorized access to either the network or the device is an important first step when designing protections, since security should be programmed in beginning stages, not in late stages to avoid DDoS, which would lead to vulnerable and unpatched devices.

Secondly, fix misconfiguration issues and implement a disaster recovery process to be performed as a protection requirement if other security precautions fail. Secure rigorous and harden configuration for network devices, such as firewalls, routers, and switches are needed and should be conducted depending on the procedures. There are published IoT Security Guidelines for IoT service and endpoint ecosystem, and for network operators by the GSM Association. The guidelines direct critical, high-priority, medium-priority, and low-priority recommendations. In addition to best practices documented in various standards or framework (e.g., National Institute of Standards and Technology (NIST) Cyber Security
Framework, International Organization for Standardization (ISO) 27001, following comprehensive IoT security guidelines is a viable solution (GSMA, 2017).

Thirdly, establish policy and regulation on cyberattacks against a power grid and remote hacking of connected cars, along with rigid technical standards. Schneier set out detailed solutions along with developing standards, funding research, and maintenance and upkeep (Schneier, 2018). On a national level, the federal government should establish a Federal Cybersecurity Commission (“FCC”). Various scenarios of cybersecurity attacks should be analyzed to find new solutions and piloted to prepare for proactive rather than reactive responses, such as: strengthening cybersecurity measures through supplementation of policies and laws; strengthening cooperation between businesses and the government; supporting the government's cybersecurity business; introducing innovation in the cybersecurity industry; and strengthening continuous improvement of privacy laws.

Fourth, grant customers (consumer and industrial) the right to sue IoT vendors when things go wrong (Schneier, 2018). Traditional security solutions are susceptible to attacks with its vulnerable interfaces, hardcoded backdoors, and unencrypted connections. Advocacy groups have asked major retailers to voluntarily adopt “a list of standards for Internet-enabled products, including that they use encrypted communications and adopt hard-to-crack passwords” (Kochman, 2019). The major retailers’ responses will pave the way for future of IoT cybersecurity, should the retailers respond favorably. When it comes to legality and litigation risks, the question arises -- who takes responsibility in these legal issues?

Finally, linking artificial intelligence (AI) to cybersecurity solutions will be a viable defensive approach. Since AI and machine learning (ML) find patterns of threats, attacks and malicious activity, AI and ML-based cybersecurity solutions can be complementary to IoT vulnerabilities and kinetic threat solutions. While AI offers a response speed that surpasses that of human analysts, human judgment could deliver intuition and insights in replicating a hacker’s thoughts via out-of-the-box solutions and creativity that AI may not be able to replicate.

IV. CONCLUSION

Kinetic threats and IoT cybersecurity continue to be a focal point where IoT devices and industrial control systems (ICS) encounter exposure to cyber-attacks. For example, malwares such as botnets “Mirai”, "Hajime", or "Satori", based on IoT devices, took the Internet by a storm in late 2016 (Krebs, 2016). Likewise, the distributed denial of service (DDoS) attack on Dyn (a major DNS provider) that shut down large parts of the Internet in USA in 2016, largely came from IoT devices. We, as members of a digital society, must act individually and collaboratively to increase the resilience of the networks we control directly as well as those to which we connect (Rothrock, 2018). To put it another way, developers, security professionals, and operations team should collaborate not only on cybersecurity threats, where the security team can assist developers in detecting and fixing vulnerabilities within the networks, but also to educate consumers on cyber security threats. Consumers who do not download security patches potentially put the whole Internet at risk of additional disruptions (Krebs, 2016; Shim, Avital, Dennis, Rossi, Sorensen, French, 2019).

Kinetic threats have real, dire consequences. Governments and businesses have taken steps to combat the undesired consequences of these kinetic threats. Although much of the infrastructure technology susceptible to kinetic threats are outdated, precautionary measures can be taken to combat these cyberattacks. Businesses are taking steps to train employees on how to confront these cyberattacks. Governments are proposing regulation reforms that would make it mandatory for manufacturers to disclose potential cyber threats of a device or machine. These initiatives will create a more proactive stance against these invisible threats that lurk in the digital world.

Like any other security solution, a holistic approach, comprised of technical, business, policy and regulation perspectives, should be conducted when identifying kinetic threats and cybersecurity solutions, instead of a silo approach. Thus, the security community should begin to take these types of threats seriously and address vulnerabilities associated with cyber-physical systems (Applegate, 2013). Since cybersecurity complexity is one of our biggest vulnerabilities and threats, all aspects of society will benefit from an interwoven approach that weaves in technical, business, managerial, and policy perspectives to
counter kinetic threats and industrial IoT cybersecurity. Lessons learned (e.g., how to detect, respond, and restore from previous cyberattacks) will be critical to detect and prevent ransomware and cyberattacks in cyber-physical systems and industrial IoT.

REFERENCES


Schneier, B. 2018. Click Here to Kill Everybody: Security and Survival in a Hyper-connected World, Norton.


