iKSP Journal of Emerging Trends in Basic and Applied Sciences
http://iksp.org/journals/index.php/ijetbas/index

Cyber security for Industrial Control System – A Survey

Hafiz Muhammad Attaullah*[1], Rahat Ali Khan[1], Shaheryar Mughal[1]
[1]Department of Telecommunication Engineering, Faculty of Engineering and Technology, University of Sindh, Pakistan

Abstract - The prevention of PCs, servers, cell phones, electronic frameworks, systems, and knowledge from noxious assaults is known as cyber security. This paper contains a thorough Cyber Security for Industrial Control Systems (ICS), secondly, during this paper, we review the characteristics and reference models of commercial system and analyze security status of commercial system. Moreover, we discuss the key works, ICS and SCADA and Industrial IOT. A compromise to ICS can result in enormous physical harm and danger to human live. During this work, we've an in depth take a look at vulnerability in a form of Operational Dark trace Technology involving the passive observation, Visibility Into ICS, Dark trace proof of values and Coordination of sensors and actuators used to track and control physical processes. Furthermore, we discussed about defensive properties, active safety and passive tracking security policies for these security issues. Lastly, explicitly we center on examining and evaluating the various sorts and structures of an ICS, security necessities, various dangers assaults, and existing answers for secure Industrial control frameworks. By this review, we want to give an away from of security issues in ICS and explain the diverse exploration issues to solve later on.

Keywords: Cyber security, network security, security and solutions for ICS, Industrial security systems, Industrial IOT.

INTRODUCTION

Industrial Control Systems (ICS) support singular organizations around the world in National Vital and Critical Infrastructure. They retain ownership of intensity stations and atomic plants, water appropriation structures and local assembly. Today they are frequently centered by digital assailants aiming to keep an eye on these relationships, negotiate and hurt them. Truly, modern systems were kept separate from corporate systems, however critical productivity gains and an expansive pattern for computerized interconnectivity with have driven an intermingling between the Operational Technology (OT) and Information Technology (IT) frameworks. The appropriation of modern developments in control and the implementation of the Industrial Internet of Things (IIoT) are also widening the unpredictability and interconnectedness of conventional OT circumstances and situations (Khan et al., 2020).

The matter of digital security has been changed drastically in approximately previous not many years, introducing a critical test to supervisory groups over all enterprises and business areas. A Cyber Security Research Group study found that in recent time, 67 percent of organizations with a basic platform encountered at least one digital attack and 78 percent expected their ICS and Supervisory Control and Data Acquisition (SCADA) systems to be exploited in the next two years (Fellows & Stockdale, 2019).

[1]*Corresponding author:
Email: attaullahshafiq10@gmail.com (H. M. Attaullah); Email: rahat.khan@usindh.edu.pk (R. A. Khan); Email: shaheryarmughal209@gmail.com (S. Mughal)

We see an increasing trend towards IT security groups taking on greater responsibility and duty to ensure that the OT systems need different technical skills and working with practices. This social with specialized combination will bring a lofty expectation to absorb information that must be survived. Progressively presented to a similar assault vectors utilized in most of digital assaults, OT gadgets inside ICS and SCADA situations are innately harder to make sure about, however their trade off can prompt huge physical harm and peril to human life. The basic idea of ICS situations additionally makes making sure about these gadgets more testing than in IT conditions. Since the time the Stunned malware was generally detailed in 2010, dangers to modern frameworks have developed quickly in both number and capacity. That was clarified in, among others, the 2014 trade off of a German steel factory that made enormous harm an impact heater and the 2015 and 2016 assaults against the Ukrainian force network).

Progressing malware crusades are effectively obtaining basic information about control frameworks, while discreetly keeping up persevering access (Byres & Cusimano, 2012). Existing guards, for example, firewalls have over and again demonstrated deficient all alone, particularly against insiders who as of now have special access. The security network is progressively going to the accord that we are entering another time of genuine OT digital danger, with consistently rising quantities of weaknesses being found in charge framework gadgets.

Dark trace's Industrial Immune System is an essential development that sees information from an ICS organize progressively, and sets up an advancing 'example of life' for administrators, workstations and robotized frameworks. Dark trace utilizes AI and AI calculations to distinguish and react to digital dangers that get past border controls and avoid decide based methodologies that can just recognize beforehand observed dangers. Dark trace's Industrial Immune System innovation is conveyed across both OT and IT situations to give full inclusion of an association.

SCADA AND ICS

ICS (Byres & Cusimano, 2012) is an umbrella term that encompasses several different types of control structures, such as SCADA (Supervisory Control and Data Acquisition) and DCS (Distributed Control Systems), for example.

They are a type of operational technology, otherwise referred to as IACS (Industrial Automation and Control Systems), including the supervision and coordination of control gadgets, sensors and actuators sent to the screen and physical procedures. Media distributions also use "SCADA" reciprocally with "ICS," technically speaking (Babu et al., 2017). Corporate Information Technology (IT) frameworks and Industrial Control Systems have various destinations, in any event, while working inside a similar association. While OT and IT regularly communicate in various dialects, digital assaults across the two conditions have kept on advancing to turn out to be more focused on and dangerous (Murray et al., 2017).

With regards to ICS, wellbeing and unwavering quality are the essential worries as aggressors plan to upset the basic administrations clients depend upon. OT and IT frameworks are joining, driven basically by monetary weights coming about because of globalization and escalating rivalry, alongside the advantages and possible upper hands that originate from the reconciliation of these orders. Such advantages include: cost decrease, expanded control, improved execution and business advancement. The cost of remediating a system is ultimately higher than identifying a digital danger early, in time and cash, but also in well-being and notoriety.

The intermingling of OT and IT, having been normally separate spaces, represents just as specialized an organizational and key test for associations. A structured security technique includes CISOs to reshape current security rehearsals as well as build new technologies and capabilities for OT defense. Progressively responsible for both OT and IT stability, CISOs have had to assume responsibility for the protection of ICS conditions without having clear OT capabilities in essence.

This hierarchical change takes steps to introduce another scope of progress the board and innovative dangers. In this condition, improvement of a viable bound together way to deal with security procedure will turn into an earnest operational need. The engineering changes that follow intermingling, however, may offer an opportunity to improve OT security. Sharing a traditional system engineering will open the door to joint observation and detection strategies in both OT and IT fields, as well as the extension of current IT traffic control methods for dealing with ICS systems (Ali et al., 2018). "Recognition of malware based on Mark is dead. A quantum leap forward is needed for digital security. It needs to rely on man-made consciousness based on AI." James Scott, Senior Fellow, Institute for Critical Infrastructure Technology.

Industrial Internet of Things (IIOT)

Despite the progress made through assembly, the reach of Operational Technology is widening into traditional ICS conditions with the receipt of Internet of Things gadgets. Through the implementation of new gadget classes, the Internet of Things is causing wide-spread shift across all forms of arranged exchanges (Mouratidis & Diamantopoulou, 2018). The accessibility of brilliant, small form factor gadgets is steadily driving a transition from solid stages to deeply expressed hubs in production without ceasing. The Industrial Internet of Things (IIoT) in modern space refers to the choice of IoT structures and gadget forms under control conditions extending PLC-based systems with transmitted sensor matrices (Bakhshi et al., 2018).

The structure and protection of control situations have important consequences for this new worldview. Drastically increased sensor lattices coordinate unpredictability and the amount of associated gadgets. These gadgets are ordinarily associated in remote geographies, with preparing and examination disseminated near the last mile in "edge" and "haze" figuring plans (Stouffer et al., 2011). This extends the possible attack surface of the ICS into a significant number of client homes in Smart Grid organizations.

Cyber security Issues of ICS

ICS situations face various digital security danger vectors with differing degrees of possible misfortune, extending from resistance to disturbance of tasks which could bring about demolition of property and likely loss of human life (Babu et al., 2017). Instances of potential ICS-related dangers include; Advanced Persistent Threats (APTs), Unintended overflow of corporate system settles, Disruption of voice and information organize administrations, Coordinated physical and digital assault Insider damage, Hacktivist assaults Supply chain interruption or bargain and Catastrophic human mistake.

In reality, mechanical control conditions were typically isolated from the corporate system and the web by distributed denial of service (DDoS). Be that as it may, PC infections and various forms of cyber-attacks have been known to conquer any obstacle by misusing security openings associated with removable media care, or simple human error. Although protection is an advantage of providing an effectively shut or segregated structure, the disadvantages include restricted access or powerlessness to access diverse information from large companies or to enable control specialists to screen frameworks from different systems. In addition, autonomous offices such as force, oil and gas pipelines, water appropriation and wastewater assortment structures are routinely incorporated by ICS, among various others, where the structure is difficult to truly ensure. Although viably intended to be interoperable and scalable, ICS frameworks are not always easy to make sure of with the number of conations between ICS structures, corporate systems and the internet, combined with the change from exclusive developments to progressively structured and transparent arrangements, they are becoming increasingly vulnerable to the kind of system assaults that are all the more commonly discovered under IT conditions. Digital security specialists are especially worried about the foundational absence of validation in the plan, arrangement and activity of some current ICS systems and the conviction that they are totally secure essentially on the grounds that they are truly secure (Yang & Zhao, 2014). It has become evident that any conceivable association with the web can be misused, regardless of whether it isn't immediate. ICS-explicit conventions and exclusive interfaces are currently all around reported and effortlessly misused. The utilization of a Virtual Private Network (VPN) is additionally might not adequate security for ICS clients as this can be inconsequentially avoided with physical access to organize

switches and never gives start to finish inclusion. Gracefully chain dangers and distant access necessities from sellers and administration supplies present a regularly obscure degree of hazard for in any case isolated situations (Drias et al., 2015).

VULNERABILITY

Although all things considered the rundown of realized tradeoffs is evolving, multiple assaults are never discovered to people in general (Lou & Tellabi, 2019). The disclosure of the Stuxnet attack in June 2010, a "weaponized" form of malware, was the most prominent event that ostensibly pushed the vulnerability of ICS into standard knowledge. A few high-profile assaults were seen from that point forward against producers and utilities, as described in sections below.

Shutdowns with Sabotage

In addition, ICS systems have been adversely affected as unintentional reactions to issues starting with corporate systems that have abused increased availability (Mugavero et al., 2018). In any case, this has been openly attributed to three problems at major power stations; the Davis Besse Atomic Force Station (Ohio, USA) where security mechanisms have been disabled by the Slammer worm; The Browns Ferry Atomic Force Station (Alabama, USA) is physically scrambled due to an exceptional rise in organized traffic, and the Hatch Atomic Force Station (Georgia, USA) due to an erroneous programming change on a company organizing machine that spoke to the control device (Franck et al., 2018).

As unintended responses to problems starting in corporate systems that violated increasing accessibility, ICS systems were also harmed. In any case, three problems at large power stations have been unreservedly related to this; the Davis Besse nuclear power plant (Ohio, USA) where security systems have been compromised by the Slammer worm, the Browns Ferry nuclear power station (Alabama, USA) has been genuinely scrambled as a result of a phenomenal increase in mastermind traffic, and the Hatch nuclear power station (Georgia, USA) due to an increase in mastermind traffic (Pogliani et al., 2019).

Additionally, the 2017 Want to Cry-ransom product assault that influenced the IT frameworks of associations over numerous verticals and topographies made extreme interruptions Honda's assembling offices. At the finish of 2014 programmers assaulted on Germany steel factory this focused on the Advanced Persistent Threat (APT) agreement, starting with a spear phishing attack that engaged software engineers to improve early access to the steelworks' working climate. Starting there, they had the option to properly explore the mechanisms of the association and over long-term control and upset the structures of development. Disappointments with individual control components quickened, causing an impact heater to be unable to shut down, causing "enormous" damage to the establishment. Through using an extraordinarily strong 'watering-gap' attack, Havex was oriented against ICS customers, where the assailants traded off three authentic ICS merchant sites and supplanted genuine programming refreshes with variants previously containing the malware.

In 2015 and 2016 the Ukraine encountered the principal known occasions of conscious digital assault focusing on the force network these ambushes utilized advanced malware proposed to deal SCADA conditions, known as Black Energy, and Industroyer such scenes show that atypical compromise stances as colossal a peril to operational circumstances as viable concentrated on attacks against ICSs.

Insiders Threat

Danger from 'believed' insiders is a significant thought for OT conditions. Over the long lifecycles associated with the structure and usage of foundation and assembling gear, countless various people, including both lasting staff and transient contracted pros, will as a rule have interfaced with control frameworks. Huge numbers of them will have had benefits that permit them to adjust arrangements or the hidden programming and equipment. Verifying and preparing staff can diminish however not dispose of the danger of insider episodes from happening. These occurrences can be inadvertent because of a mix-up or planned easy route that puts something significant in danger, or a purposeful demonstration by a repelled or ideologically inspired person. The expanded access and hierarchical nature that insiders have implies their vindictive activities can

be very much focused on and viable at upsetting tasks. They likewise have a more prominent capacity to meddle with observing or take on the appearance of others, making their exercises harder to distinguish and property (Lou & Tellabi, 2019). Insider chance is a genuine test regularly thought little of in expansiveness. At the point when flexibly chains or temporary workers are included, it gets difficult to draw a perfect line among 'inside' and 'outside'. We have to confide in individuals in our all-inclusive associations with the entrance and benefit that they require in carrying out their responsibilities, yet we likewise need systems to recognize when something is turning out badly and should be revised. For example, customary device fringe barriers, firewalls play out a significant capacity in a full digital protection scheme, but insiders are a key case of their confines. In order to accomplish the vast majority of their probable targets, insiders do not need to go through fringe protections, meaning that those guards have little ability at all to forestall or identify their activities. It is important to start from a full understanding of what is usual for the specific environment by monitoring complex networks. It will only then be able to recognize the emerging trends and correlated behavior that indicate a hazard (Ngufor, 2020).

DTS: A NEW APPROACH

New vulnerabilities are emerging at a rate that is difficult to remain aware of, and it is an unsatisfactory technique for operationally critical circumstances to look only for distributed authentic assault forms. Darktrace does not involve conditions or hazards from the earlier assumptions, and can discern the 'obscure' hazards that are up to now unidentified, either because they are novel or have been custom-fitted to a particular safeguard along these lines. Throughout its entire organization, Dark trace engineering continues to evolve and self-learn. This ability to change means that Dark trace cannot avoid any new or modified risk. The Industrial Immune System identifies deviations from the informed 'life example' at whatever point an anomalous shift in behavior occurs within the earth and alerts the association to the conceivable risk. In Darktrace's radical understanding of ordinariness, improvements that are not real risks are consolidated. Within Darktrace, the propelled science makes it exceptionally suitable for vital possible hazards without covering them under various immaterial or rehashing cautions. Undeniably in excess of a lot of basic principles applied to arrange traffic, it can associate numerous inconspicuous markers isolated by type or time into solid proof of a genuine developing danger, implying that security investigators are not overwhelmed with bogus positives (Fellows & Stockdale, 2019). The Threat Visualizer interface of Darktrace can be used to triage and analyses these identifications, but it is also conceivable to attempt the return to the existing Security Information and Event Management (SIEM) system of an association to integrate with procedures and strategies set up. "The machine learning approach of Darktrace is unparalleled. We are now finding anomalies that would have taken us weeks, or even months, to find on our own in real time."

Proof of values for Darktrace

Darktrace's Proof of Value (POV) enables associations to specifically experience the potential of the Industrial Immune System to identify already inconspicuous hazards and atypical activities within the state of a client. In addition to the POV, Darktrace offers access to our Threat Visualizer for use during the POV, just as its community of digital security pros have generated Threat Intelligence Reports week after week. A few organizations want Darktrace to affirm the aloof and safe operation on their corporate IT structures before interacting with the establishment of ICS systems (Solms & Niekerk, 2013).

ICS Visibility

ICS models and their operating systems are often recorded to a degree that surpasses corporate reciprocals, but these apparently constant situations are misunderstood and may have undergone multiple progressions over their lifespan by different individuals on a regular basis. It can be a true test to know and understand what actually happens within the earth (Wegner et al., 2017). By analyzing, dissecting and capturing correspondences alongside their associated metadata, Dark trace answers this examination. Despite its central recognizable evidence of irregular movement and conceivable trade off, the Threat Visualizer interface of Dark trace interestingly demonstrates this rich data in an instinctive 3D dashboard that enables the administrator to obtain a true and constant diagram of what is happening. This can be used to explore whether the genuine

action of the control mechanism co-ordinates the planned plan (Wegner et al., 2017). Under ICS conditions, the isolation and zoning of the device is a fundamental safety regulation, particularly given the normal natural absence of protection inside endpoint gadgets. In such situations, it is important to consider the proper progression of device information and how it looks to planned conductors and examples of correspondence. The Threat Visualizer allows OT security groups within the Industrial Framework to see continuous data on information sources, and to think about this against planned and proposed designs. The Industrial Immune System of Dark trace retains the entirety of Dark trace's capabilities in the technical workplace and would ideally be sent to observe both the ICS and corporate structures. The IT agreement is the most likely attack vector for ICS negotiations. The guard from top to bottom of the control structure is restricted by seeking dangers when still within the corporate environment. It also includes classified details on the control system installed on corporate servers that could include comprehensive organizational descriptions, subtleties of gadgets or performance and well-being reports (Wegner et al., 2017).

CONCLUSION

Organizations face numerous difficulties as we move into a period of consistently expanding network. Those seeking to ensure mechanical control mechanisms are far less safe than their corporate partners, just as corporate structures face additional and substantially different problems, as the gadgets used are far less reliable. There is accessible evidence of the growth of motivation and potential of dangerous entertainers towards control structures, a trend responsible for proceeding in recent years and brought into sharp concentrate by the assaults. The vast majority of these assaults were best used in class strategies to enter focus regulation systems with limited political or ideological essentiality, a combination that has not been seen recently. Retaking a chance with the OT condition is an unending test requiring new innovations that will convey consistent understanding and give early admonition of both unpredictable and focused on bargain.

All out anticipation of bargain appears to be viably outlandish for a long time to come, yet counteraction of emergencies is an attainable objective across both corporate IT and operational innovation situations. It needs another approach that can track incidents in corporate IT and OT before they become an operational emergency. With Darktrace's invulnerable self-learning system, associations will continually recognize and respond to rising hazards. AI calculations will identify inconspicuous, novel or custom-fitted attacks even beforehand, whether or not they launch or navigate in the corporate IT or OT areas.

With ICS organizations across oil and gas, assembly and transport divisions in 5 countries, fundamental platform suppliers currently rely on Dark trace to protect their control environment against all forms of cyber threats. The Industrial Immune System has become the main AI and AI breakthrough for modern digital security, with long periods of experience protecting extremely perplexing and different control mechanisms.

ABBREVIATIONS

ICS Industrial Control Systems
OT Operational Technology
IT Information Technology
IIoT Industrial Internet of Things
APT Advanced Persistent Threats
DDoS Distributed Denial of Service
VPN Virtual Private Network
DCS Distributed Control System
AI Artificial Intelligence
POV Proof of Value
3D 3 Dimensional
SIEM Security Information and Event Management

REFERENCES

Ali, S., Balushi, T. Al, Nadir, Z., & Hussain, O. K. (2018). ICS/SCADA System Security for CPS. In *Cyber Security for Cyber Physical Systems* (pp. 89–113). Springer, Cham.

Babu, B., Ijyas, T., & P, M. (2017). Security issues in SCADA based industrial control systems. *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*.

Bakhshi, Z., Balador, A., & Mustafa, J. (2018). Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models. *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, 173–178.

Byres, E., & Cusimano, J. (2012). *7 Steps to ICS and SCADA Security*.

Drias, Z., Serhrouchni, A., & Vogel, O. (2015). Analysis of cyber security for industrial control systems. *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*.

Fellows, S., & Stockdale, J. (2019). *A cyber security appliance for an operational technology network* (Patent No. 16/278,953).

Franck, S., Cédric, E., Eric, Z., & Jean-Marie, F. (2018). From ICS Attacks' Analysis to the S.A.F.E. Approach: Implementation of Filters Based on Behavioral Models and Critical State Distance for ICS Cybersecurity. *2018 2nd Cyber Security in Networking Conference (CSNet)*. https://doi.org/10.1109/CSNET.2018.8602960

Khan, R. A., Xin, Q., & Roshan, N. (2020). RK-Energy Efficient Routing Protocol for Wireless Body Area Sensor Networks. *Wireless Personal Communications*.

Lou, X., & Tellabi, A. (2019). Cybersecurity Threats, Vulnerability and Analysis in Safety Critical Industrial Control System (ICS). In *Recent Developments on Industrial Control Systems Resilience. Studies in Systems, Decision and Control*. Springer, Cham.

Mouratidis, H., & Diamantopoulou, V. (2018). A Security Analysis Method for Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, *14*(9), 4093–4100.

Mugavero, R., Abaimov, S., Benolli, F., & Sabato, V. (2018). Cyber Security Vulnerability Management in CBRN Industrial Control Systems (ICS). *International Journal of Information Systems for Crisis Response and Management (IJISCRAM)*, *10*(2), 49–78.

Murray, G., Johnstone, M. N., & Valli, C. (2017). The convergence of IT and OT in critical infrastructure. *He Proceedings of 15th Australian Information Security Management Conference*, 149–155.

Ngufor, F. A. (2020). *Understanding the Perspectives of Information Security Managers on Insider Threat: A Phenomenology Investigation*.

Pogliani, M., Quarta, D., Polino, M., Vittone, M., Maggi, F., & Zanero, S. (2019). Security of controlled manufacturing systems in the connected factory: the case of industrial robots. *Journal of Computer Virology and Hacking Techniques*, *15*, 161–175.

Solms, R. von, & Niekerk, J. van. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102.

Stouffer, K., Falco, J., & Scarfone, K. (2011). *Guide to Industrial Control Systems (ICS) Security*.

Wegner, A., Graham, J., & Ribble, E. (2017). A New Approach to Cyberphysical Security in Industry 4.0. In: Thames L., Schaefer D. (eds) Cybersecurity for Industry 4.0. In *Springer Series in Advanced*

Manufacturing. Springer, Cham. https://doi.org/https://doi.org/10.1007/978-3-319-50660-9_3

Yang, W., & Zhao, Q. (2014). Cyber security issues of critical components for industrial control system. *Proceedings of 2014 IEEE Chinese Guidance, Navigation and Control Conference*.