Applying Zero Trust Principles to Secure Industrial Control Networks

Eduardo Marsola do Nascimento

Petrobras – Petróleo Brasileiro S/A
Rio de Janeiro – RJ – Brazil

edunasci@yahoo.com

Abstract. *The defense in depth principles, normally used by industrial control networks (ICN), may no longer be adequate in an industry 4.0 scenario, which the sensors, actuators and supervisory systems needs to communicate directly to the cloud. The Zero Trust Architecture is raising as de facto standard for securing cloud application and can be used to protect an ICN, but normally it is applicable only by replacing existing applications and network gears. This preliminary work presents an option to apply the Zero Trust principles on ICN, maintaining the existent systems and network.*

Resumo. *Os princípios de segurança em profundidade, normalmente utilizados para proteger as redes de controle industrial (ICN), podem não ser mais adequados em um cenário de indústria 4.0, no qual os sensores, atuadores e sistemas supervisórios precisam se comunicar diretamente com a nuvem. A Zero Trust Architecture surge como padrão de fato na proteção de aplicativos em nuvem e pode ser utilizada para proteger uma ICN, mas normalmente ela aplicada somente pela substituição de aplicações e equipamentos de redes existentes. Este trabalho preliminar apresenta uma opção para aplicar os princípios de Zero Trust em uma ICN, mantendo sistemas e redes existentes.*

1. Introduction

The industrial control systems (ICS), like SCADA and DCS, are used to control processes on a plethora of industries like electrical, oil and gas, discrete manufacturing, transportation and many more. An ICS contains several components like actuators, sensors, programable logical controllers (PLC), intelligent electronic devices (IED), remote terminal units (RTU), human machine interface (HMI), engineering workstations and data historian. These systems have different security requirement from the IT system and networks. While on a typical IT system the confidentiality and integrity are the main concerns, on an industrial control system human safety and fault tolerance to prevent accidents are more important [ICS-CERT 2016]. The life cycle is another difference, which is 2-3 years on IT compared to 10-20 years on industrial control assets. To protect the ICN the NIST [Stouffer et al. 2015] and the ANSI/ISA 62443-3-3 recommend the defense in depth principles when defining the security boundaries of an ICS. If the principle were correctly applied, no ICS component would be accessible through Internet but Andreeva [Andreeva et al., 2016] had estimated that multiple ICS components, over 172,000 hosts, are accessible externally and vulnerable to known exploits or to insecure protocols. As the systems evolve to the industry 4.0 or Industrial Internet of Things (IIoT), where it is possible to have sensors and actuators connected directly to the Internet and

the ICS on the cloud, this situation may deteriorate very fast. One reason as concluded by [Leander et al, 2019] is the difficult to hold boundaries because of the IIoT system dynamics. An alternative to secure this new environment is the use of the Zero Trust Network (ZTN) concept. Some cloud providers like Microsoft [Beraud et al., 2019] and Google [Ward, Beyer, 2014] already pointed the advantages of this approach. The ZTN considers the network is not trustable and before accessing any resource it is necessary to identify and authenticate the device, user, application or network flow. Other characteristics are the application of the least privilege concept and full visibility. This way even if a device is compromise, the malicious traffic is detected before causing any damage. The main problem to implement Zero Trust on an Industrial Control Network (ICN) is the need to replace network gears and devices. The Zero Trust Architecture (ZTA) draft document from NIST [Rose et al., 2019] shows about the need to wholesale replacement of technology to transition to a ZTA. This paper presents an option to avoid the replacement of all components by working with an overlay based in open software and low-cost hardware.

1.1. Related works

In his master thesis, Tommey [2018] points out that a ZTA can obtained by using only explicit data flow configuration on a Software Defined Network (SDN). That work evaluates how the SDN, and consequently some zero-trust principles, can improve the cybersecurity of the OT network. The work from Bobba [Bobba et al., 2014] had already identified the cybersecurity gaps on conventional networks that can be addressed by SDN use. The use of SDN on ICN is also a vast research area. A comprehensive survey about its use on Smart Grid networks, which is an ICN, was presented by Rehmani [Rehmani et al., 2019]. A new work is the effort from NIST [Rose et al., 2019] to define Zero Trust Architecture (ZTA). There is also an ongoing project on the National Cybersecurity Center of Excellence (NCCoE) about implementing ZTA [Kerman et al., 2020]. This work is different from the formers because it considers applying Zero Trust principle without replacing all existent network. It also allows the coexistence of old and new ICS, which is necessary because the longer life cycle of many ICS components.

2. Zero Trust Network

According to Gilman and Barth [2017], "a ZTN is built upon five fundamental assertions: the network is always assumed to be hostile; external and internal threats exist on the network at all times; network locality is not sufficient for deciding trust in a network; every device, user, and network flow is authenticated and authorized; policies must be dynamic and calculated from as many sources of data as possible". Comparing a traditional network to a ZTN, using their definition, while on the former, a device usually accepts any connection from the internal network without extra validation, on the later, the network is considered always hostile and no communication should be allowed without authenticating the device, the user, and the data flow. Every device should be identified, and a security score calculated before allowing any communication, which is encrypted to avoid eavesdropping.

In a similar way, Rose [Rose et al., 2019] considers that a ZTA must be adhering to the following tenets: all data sources and computing services are considered resources; all communication is secure regardless of network location; access to individual enterprise resources is granted on a per-connection basis; access to resources is

determined by policy, including the observable state of user identity and the requesting system, and may include other behavioral attributes; the enterprise ensures all owned and associated systems are in the most secure state possible and monitors systems to ensure it; user authentication is dynamic and strictly enforced before access is allowed. The work lists as core components for a ZTA: Policy Decision Point (PDP) - responsible for granting decisions - and the Policy Enforcement Point (PEP) – that enable, monitor and terminate the connection. The PDP uses supporting components like Continuous Diagnostics and Mitigation (CDM) System(s), Industry Compliance System, Threat Intelligence Feed(s), Data Access Policies, Enterprise Public Key Infrastructure (PKI), ID Management System, Security Incident and Event Management (SIEM) System to make the decision about an access. An SDN controller can perform the function of the PDP. The PEP can be a switch, a router, a firewall, a reverse proxy, a security gateway or any other software/hardware component that block or allow the communications. Other works from cloud providers like Microsoft [Beraud et al., 2019] and Google [Ward, Beyer, 2014] make similar considerations.

In summary, a Zero Trust Network is an implementation that consider the following principles: the network perimeter does not exist or is limited to a very few devices; full visibility of the network and its data flows; encrypted communication is the default on the network; least privilege – all access must be explicitly granted and should be minimum; all devices, users and data flow are authenticated.

3. Comparing Zero Trust Network and Defense in Depth model

A network based on defense in depth model considers perimeters to segregate the security zones. A simple configuration may have four security zones: Internet, corporate, ICN DMZ and ICN. This was made considering that a threat always come for outside, so to affect the most secure zone it would need to break several layers of security.

Table 1. Data flow permission in a network with four security zones

	ICN	ICN DMZ	Corporate	Internet
ICN	Unrestricted	Filtered	Forbiden	Forbiden
ICN DMZ	Filtered	Unrestricted	Filtered	Forbiden
Corporate	Forbiden	Filtered	Forbiden	Filtered
Internet	Forbiden	Forbiden	Filtered	Not Controlled

There are rigid rules on defense in depth model, by example the devices on the ICN communicate among them and to servers on the DMZ but they never communicate to devices at the corporate network or Internet. When the data flows from one security zone to another, it is filtered with explicit permissions. With this model, a simple anti-virus pattern update is a complex process. The client on ICN download the AV pattern downloads from a server on the DMZ, which downloads from the corporate network, which downloads from the Internet. To setup this infrastructure, at least two servers would be necessary and three sets of rules in two different firewalls would need to be created. If a ZTN approach is used, it is only necessary to create one rule allowing communication from the client on the ICN to the cloud. Auditing is also easier, only the central controller needs to be checked for logs and configuration.

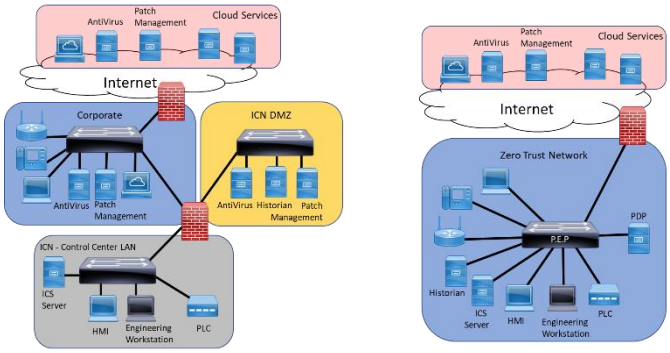

Figure 1. Defense in Depth with four security zones compared to a ZTN.

Many protocols used on the ICS are clear text and an attacker may intercept and modify packets without been detected. The encryption principle on the communication avoid this kind of attack. The admission control prevents a rogue device connection on the network to gather information of the ICN. If all switches on the ICN supports SDN, which permits packet forwarding and discarding rules creation, the ZTN principles can be applied directly. The PDP function is performed by the SDN controller. Normally, it is only obtained if legacy network equipment is replaced.

4. Overlay and Underlay Approach

In this approach, it is possible to provide a ZTN without replacing the legacy equipment. The PDP function can still be performed by SDN controller, but the PEP will be performed by a security gateway (SG). Every device creates a secure encrypted communication to the SG. There may be as many SG on the network as need to support the network traffic and provide redundancy. A future work should detail and standardize this communication.

The underlay is a simple L2 or L3 network, hardened to avoid lateral attacks. This layer provides basic infrastructure services, like DNS and DHCP, and allow communication between the devices and the SG. This layer should have an admission control to prevent successful attacks like DHCP starvation or network traffic interception by spoofing the MAC address. The underlay may be a wireless network like a corporate WiFi, Ethernet radios, LoRa or even a 4G or 5G Internet connection.

The overlay is provided by a piece of software installed on the device. It is used to create a communication to the SG providing a microsegmentation. The device must be configured to use the physical network adapter only to communicate to the SG and DHCP/DNS server. This measure protects the device if the underlay is an Internet or insecure connection. The device must use a strong authentication like digital certificates to avoid Man in the Middle attacks. All data will be encrypted using secure algorithms like AES using an IPSEC configuration on each host or a TLS based client like the OpenVPN client. Fritsch [2019] has found that agent-based microsegmentation have lower complexity and high flexibility than network-based architecture. Some devices like PLCs may not support the software agent and a low-cost hardware, like a raspberry pi, can be used in between the PLC and the switch or the WLAN network to provide the overlay connection. Due the industrial environment this hardware may need to support extended temperature ranges and dust protection.

The main function of the SG is to be the Policy Enforcement Point. It will receive

the communication rules from the PDP and apply on its logical interfaces to enforce the network policy. A firewall software or an OpenVSSwitch software can be used to enforce these rules using the approach described by Tsuchiya [Tsuchiya et al., 2018]. The SG is also responsible for collecting information to provide the full visibility of the network. All network flow and the blocked communications information, can be used on an inspection software, using machine learning or signature, to detect unusual and malicious behaviors. The result should be used to increase or decrease the security score of a device or user. This information is used by the PDP to decide if block or allow futures flows.
The SG can be constructed using open source software and off the shelf hardware or it may be commercial product like a firewall with IPS/IDS integrated. The number of security gateways needed will depend the network traffic, time delay restrictions and high availability. The quantity ranges from having only one security gateway on the Cloud to have a security gateway for every switch. The security gateway could run on a low-cost computer or a high-performance virtual server, it all depends on the performance needed. An initial proof of concept experiment, with a SG and three clients, was created. The clients were hardened to allow communication only through the SG. The policy was created manually on the SG using iptables firewall. After it, although the clients were in the same subnet, they could only communicate if policy explicitly allowed. A notebook was connected behind a raspberry pi to emulate a device that do not support the client. All communication flows were collected on the SG.

5. Conclusion and Future Works

The Zero Trust Network implementation on Industrial Control Network will bring better security and will simplify the overall administration. To avoid the replacement of legacy network equipment on existent Industrial Control Systems, a Software Defined Network using an overlay/underlay architecture, as describe on this paper, can be used. Even in a new ICS implementation, there are still gaps on the standardization of how the Zero Trust Network components communicate among them. A complete ZTN ecosystem must be defined using open standards to avoid proprietary solutions. This showed the need to expand the studies of Zero Trust Networks (ZTN) on the industrial control environment. It also detected the need to standardize API interfaces among Zero Trust components. The lack of open standards may cause a vendor lock-in [Rose et al., 2019] which is not desirable.

The proposal for the continuation of this work is to define an ecosystem for a ZTN, using open components. It will be done as comprehensive research project which after identifying the actual state of art of Zero Trust Architecture components determine the gaps on open standards and propose solutions. A functional ZTN system based on open standards, including the policy decision point and policy enforcement point components, will be implemented. It should describe in detail each component and creating a functional implementation of an ICN using ZTN principles.

References

Andreeva, O., Gordeychik, S., Gritsai, G., Kochetova, O., Potseluevskaya, E., Sidorov, S. I. and Timorin, A. A. 2016. “Industrial Control Systems and Their Online Availability”. URL: <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/07/07190427/KL_REPORT_ICS_Availability_Statistics.pdf >. Access Date: Mar 29th 2020.

ANSI/ISA-62443-3-3 (99.03.03)-2013. 2013. “Security for industrial automation and control systems Part 3-3: System security requirements and security levels”. ISBN: 978-0-876640-39-5.

Beraud, P., Grasset, J., Jumelet A. 2019. "Implementing a Zero Trust approach with Azure Active Directory". URL: <https://download.microsoft.com/download/8/2/7/8271584F-A6D6-419A-B262-C37E5FFAB593/Implementing-a-Zero-Trust-approach-with-Azure-Active-Directory.pdf>. Access Date: Jan 8th 2020.

Fritsch, J. 2019. "Architectures and Paradigms of Microsegmentation Products". URL:<https://www.gartner.com/document/3913602?ref=solrAll&refval=245593753>. Access Date: Feb 01st 2020.

Gilman, E. and Barth, D., 2017. "Zero Trust Networks". O'Reilly Media, Incorporated.

ICS-CERT - Industrial Control Systems Cyber Emergency Response Team. 2016. "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies". URL: <https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf>. Access Date: Mar 29th 2020.

Kerman, A., Borchert, O., Rose, S. 2020. "Implementing a Zero Trust Architecture". URL:<https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/zt-arch-project-description-draft.pdf>. Access Date: Apr 4th 2020.

Leander, B., Čaušević, A. and Hansson, H., 2019, August. “Applicability of the IEC 62443 standard in Industry 4.0/IIoT”. In Proceedings of the 14th International Conference on Availability, Reliability and Security (pp. 1-8). URL: <https://doi.org/10.1145/3339252.3341481>. Access Date: Mar 29th 2020.

OpenVPN INC. 2020. "A Business VPN to Access Network Resources Securely". URL:<https://openvpn.net/>. Access Date: Apr 5th 2020.

Rose, S., Borchert, O., Mitchell, S. Connelly, S. 2019. "Draft NIST Special Publication 800-207 - Zero Trust Architecture". URL:< https://doi.org/10.6028/NIST.SP.800-207-draft >. Access Date: Dec 11th 2019.

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M. and Hahn, A., 2015. "NIST Special Publication 800-82 - Revision 2 - Guide to Industrial Control Systems (ICS) Security". URL: <http://dx.doi.org/10.6028/NIST.SP.800-82r2>. Access Date: Mar 29th 2020.

Tommey, C.R., 2018. "Implications of Implementing Software Defined Networking to Improve Cybersecurity for Operational Technology Networks". Master Thesis. Utica College.

Tsuchiya, A., Fraile, F., Koshijima, I., Ortiz, A. and Poler, R., 2018. Software defined networking firewall for industry 4.0 manufacturing systems. Journal of Industrial Engineering and Management (JIEM), 11(2), pp.318-333. URL:<https://doi.org/10.3926/jiem.2534>. Access Date: Apr 5th 2020.

Ward, R. and Beyer, B., 2014. “Beyondcorp: A new approach to enterprise security”. URL: < https://www.usenix.org/system/files/login/articles/login_dec14_02_ward.pdf>. Access Date: Jan 8th 2020.