Securing the Industrial Internet of Things for Critical Infrastructure (IIoT-CI)

John O'Raw
Department of Computing
Letterkenny Institute of Technology
Letterkenny, Ireland
john.oraw@lyit.ie

David Laverty
School of Electronics, Electrical Engineering and Computer Science
Queen's University, Belfast
Belfast, Northern Ireland
david.laverty@qub.ac.uk

D. John Morrow
School of Electronics, Electrical Engineering and Computer Science
Queen's University, Belfast
Belfast, Northern Ireland
Dj.Morrow@qub.ac.uk

Abstract— The Industrial Internet of Things (IIoT) is a term applied to the industrial application of M2M devices. The security of IIoT devices is a difficult problem and where the automation of critical infrastructure is intended, risks may be unacceptable. Remote attacks are a significant threat and solutions are sought which are secure by default. The problem space may be analyzed using threat modelling methods. Software Defined Networks (SDN) provide mitigation for remote attacks which exploit local area networks. Similar concepts applied to the WAN may improve availability and performance and provide granular data on link characteristics. Schemes such as the Software Defined Perimeter allow IIoT devices to communicate on the Internet, mitigating avenues of remote attack. Finally, separation of duties at the IIoT device may prevent attacks on the integrity of the device or the confidentiality and integrity of its communications. Work remains to be done on the mitigation of DDoS.

Keywords—IIoT-CI, SD-WAN, SDN, Software Defined Perimeter, SD-Node

I. INTRODUCTION

Around ten years ago, the authors concluded that in the context of IT usage in critical infrastructure, conventional technology and practices were broken; that critical infrastructure protection (CIP) was an intractable problem and that it required new approaches. The domain of interest was critical infrastructure machine-to-machine (M2M) communications. The term Internet of Things (IoT) was not yet in use, but the issues were the same as are currently faced. The primary domain of interest was the electricity industry, where the use of common-of-the-shelf (COTS) equipment and systems was becoming common and the systems were often no more secure than a domestic PC. Statements like this were considered sweeping and unjustified back then, they can now be made without expectation of serious challenge [1].

Since the early 1980s and the dawn of distributed computing, the tools and methodologies to create secure and reliable systems have lagged the churn of new technology. The security issues with the first waves of IoT devices were just a new iteration of a systemic problem which emerged almost forty years ago.

Business success in technology is driven by being early to market with the newest technologies whether those technologies are yet fit for purpose. There are no serious limiting factors on manufacturers or on the enterprise, historically the cost of a breach has been less than the cost of implementing secure systems [2] and any calculation of risk results in unpunished risky behaviours where others pay the price [3]. Good for rapid innovation, good for short term business returns, potentially devastating in the long term, especially for critical infrastructure. Perhaps GDPR may begin to address this?

The architectural choices behind the design of the modern PC/Server are based on a rapid design project carried out in IBM almost forty years ago; the enhancements in this design have in some cases introduced new families of vulnerabilities [4] which are also intractable. Attempts at mitigation for recently revealed architectural problems with CPUs may involve a serious performance impact.

Software development is a relatively young field and there are still a limited number of studies to give an empirical backing to the efficacy of common development methods [5]. There can be few other fields of human endeavour where terms of use deny all responsibility for the implications of using the product. Most contemporary End User License Agreements (EULA) of any common software platform will verify this claim. With software, "...*the problem is both the absence of standard metrics and a generally accepted organization that could conduct assessments* [6]. Although processes like Common Criteria [7] exist, where system design can be quality assured to Evaluation Assurance Levels (EALs), very few commercial devices meet standards beyond EAL 4+; the same level as Microsoft's Windows Operating System.

Global communications are another issue; legacy systems were accessible for perhaps 500m, modern systems are unbounded if they are Internet connected. The communications protocols commonly used originated perhaps forty years ago and were not designed for security. The ubiquity of Wi-Fi makes a system's perimeter porous; even the local area network (LAN) is unbounded.

In this environment, the authors set out take an aerial view and look at the problems in terms of first principles. Threat modelling was carried out to understand vulnerability, the actors who could exploit that vulnerability and the mitigations which could prevent it. Other risks such as mis-configuration were also considered.

But the intention was to go further; not to patch a problem with a slightly better kludge, but to develop a family of solutions which were *secure by default from remote attack*. Many available technologies were reviewed, including technology in use by security agencies; this was considered where it was available and in the public domain. Where technologies were not available to mitigate vulnerabilities, new approaches were taken or developed.

The term Industrial Internet of Things (IIoT) has emerged to describe the pervasive M2M devices used in Industrial Automation and Control Systems (IACS). Although the original intention was to address these solutions for critical infrastructure M2M applications and COTS equipment, they

978-1-5386-4980-0/19/$31.00 ©2019 IEEE

apply equally to the world of IoT. The IoT solutions are of interest as they allowed the authors to consider hardware changes to secure the underlying architecture, an option not available with solutions based on COTS.

This paper discusses concepts evaluated to secure IIoT for Critical Infrastructure (IIoT-CI) communications on the LAN, the WAN and in the design of the individual nodes.

II. Characterizing attack vectors

Before identifying the priority of technical solutions required, it is necessary to understand the vulnerabilities (the weaknesses in a system), the threats (the agent which will exploit the vulnerability), and the consequences should the vulnerability be exploited. Knowledge of existing controls (countermeasures) and their effectiveness is also required.

A. Risk Control

General risk analysis is a mature field; terminology has been standardized by [8], but the Latin verb *riscare*, meaning *to dare*, well describes its origin. Insurance is one of the oldest strategies for mitigating risk and doctrines for risk management and insurance (or bottomry) date back at least to 3950 BCE.

Modern risk management theory for ICT seems to date to the 1950s and it has always had a basis in the insurance industry and actuarial science. One of the earliest discussions was "*Risk Management: New Phase of Cost Control*" by Russell Gallagher. This is interesting wording that quantified risk in terms of direct financial loss. This may be one of the greatest criticisms of using standard risk modelling for critical infrastructure. The loss experienced by an operator in the event of a critical infrastructure failure may not be significant compared to the consequential losses experienced by others. There are many normative sources on risk management, ISO 31000:2018 (Risk Management) is new. ISO 31010:2009 considers risk assessment techniques and ISO/IEC 27005:2011 deals with information security risks.

ISO 31000 establishes a framework "to assist organisations in integrating risk management" and defines risk as "the effect of uncertainty on objectives". In addition to the guidance of these standards, a detailed methodology with controls is still required and even following that, detailed analysis methods such as threat modelling. The final step is to identify mitigation or in the language of risk control, treatment. Some work has been done on applying these standards to IIoT [9].

B. Attack Trees and Graphs

System security is penetrated all the time, often not in a manner considered by the designers. To analyze security, a starting point may be to use Attack Modelling Techniques (AMTs), such as attack trees, graphs or nested lists. As in so many aspects of ICT, there are the common practices to be found in books and journal articles, but there are very few empirical studies that consider the efficacy of any of these techniques [10].

In 2002, Bill Gates issued a memo [11] which is often quoted as a turning point for Microsoft from a security perspective; Trustworthy Computing. This is of interest, as much of Microsoft's following work was in the public domain, including the evolution of their Secure Development Lifecycle (SDL) [12]. Microsoft's Threat Modelling Tool emerged from this work and is still one of the few free and open tools which allows for threat and attack graph modelling.

Attack trees are a useful way to diagrammatically model potential attacks vectors. Some users prefer to use a written outline, as complex trees become unmanageably large. At the root of the tree is a successful compromise. Each child node must be satisfied before the root can be satisfied. Each child node has leaves, which may themselves have child nodes [13]. Fault Trees are normally modelled with Boolean values using logical operations like AND, OR and XOR and there can be thousands of branches and levels in the tree. After the tree is built, any attack path that is considered infeasible or improbable is marked as such. In some models, costs or probabilities are used to represent the likelihood of attack. Controls and mitigation strategies may also be noted. It is challenging to fully capture the meta-data relating to an attack vector and to represent it in a simple logical structure. What is the cost of each event to the attacker and what is the least cost path through the tree? What are the consequences of that event to the asset owner? What are the pre-requisites or tools required for each event? Is it possible to calculate probability values and to integrate tools like Bayes Algorithm and Markov chains? This is an active research field [14].

III. The many applications of "Software Defined"

In the age of analogue telephones, hacking was easy and pervasive; it was called phone phreaking. Because the network used audio frequencies for control and users could also inject audio frequencies (voice), it was very easy for any user equipped with a "little blue box" to make free trunk calls [15]. By the time phone systems were digitized and Signalling System No. 7 (SS7) was introduced in 1975, it was known that for security and flexibility, user data and control signals needed to be separated. This lesson was not considered with the fundamental communications protocols of data infrastructure; Ethernet and Internet Protocol (IPv4) or with routing protocols such as IS-IS, OSPF or BGP.

A. The first potential solution: Secure the LAN and implement Intrusion Detection/Prevention by default

Several attempts were made to develop intelligent networks [16] but by 2008, the concept of a Software Defined Network (SDN) emerged to mean a network where control signals and data signals were separated, and Open Flow emerged as an initial configuration protocol [17]. Heterogenous data flows were divided into a data plane, a control plane and a management plane, and it became possible to tailor network connections precisely; switches became programmable. The authors developed methodologies for using this technology in CIP as applied to electrical substations [18].

1) On connection to the network: No traffic flows as no rules have been provisioned, the network is secure by default. Each node is documented in the asset management register.

2) Learning: To baseline the node it is "sandboxed" (isolated), traffic is allowed to flow freely and the characteristics of the node are identified by the SDN Controller, they are documented and validated.

3) Operations: These valid flow rules are added to the network and the device communicates with other devices according to its baseline. No other communications can occur, Intrusion Detection and Protection (IDS/IPS) are provided at the controller and not reliant on the resource constraints of IIoT devices. Any attempted new or unknown data flow is flagged as a security event; the flow does not complete, the network fails-safe.

In these circumstances, the attack surface for remote vulnerability is removed. There is a potential remote attack vector to the SDN controller and this can be mitigated by isolating it. Within the limitations of the use-case, nodes are secured from remote attack and can only be accessed by other secured nodes, over well defined ports. IDS/IPS is implicit and fail-safe and is not dependent on the end nodes. Some attack vectors using MAC address impersonation still exist, but require physical access to the network. These may be mitigated using existing technologies like IEEE802.1x implemented as an SDN application [19] or by device attestation technology.

In earlier work, the authors experimented with data diodes and one-way data flows for M2M communications. Methodologies were developed for one-way flows and applied to the C37.118 protocol for Synchrophasors in the electrical industry targeted at a specific IIoT-CI device, the OpenPMU [20]. SDN gave much more flexibility, ease and economy of application for one way data flows. In addition to improvements in security, the automation of network configuration and its integration with other engineering processes has the potential to assist with change management and reduce configuration error, another source of vulnerability [21]. The application of SDN to IIoT is an active area of research [22].

B. The second potential solution; secure the WAN and make it highly available.

Software Defined came to mean more than the separation of control and data planes; it came to mean programmable, configurable and intelligent. Where multiple paths exist across an automation data network, dynamic routing protocols are used to find the best path using simple metrics like shortest number of router hops, or cheapest in terms of some significant metric. Protocols like RIP, OSPF, IS-IS and BGP date back to simpler times when processing power was limited, and security, availability and performance were less critical. The software-defined WAN (SD-WAN) has emerged as the replacement for these legacy technologies.

Consider an intelligent router which measures every path in real-time and determines its performance across a range of significant metrics; jitter, latency, packet loss, financial cost. this intelligent router further considers every traffic type which must transit the network and runs an optimization algorithm to pass traffic down the most appropriate link, dynamically changing paths in real-time. Segmentation, the isolation of one traffic stream from another, is a fundamental principle in network security. Imagine this intelligent router could extend segmentation of traffic across the wide area, that traffic could be classified and passed in separate streams, as it would on a LAN. Modern cryptography can be applied to secure this wide area data traffic and with all this intelligence, the behaviour of this router can be policy based and the reporting and alerting can be exceptional. This is one interpretation of SD-WAN, device based. SD-WAN can be approached a different way, by encapsulating all this functionality in a carrier's dedicated network; SD-WAN in the cloud. This summary is based on work done in 2018 to evaluate the use of SD-WAN technology for the future of a national research and education network (NREN) [23].

In many applications, IIOT devices use either redundant connections or Ethernet ring topologies such as High-Availability Seamless Redundancy (HSR) and Parallel Redundancy Protocol (PRP) [24]. Applying the philosophy of SD-WAN to layer 2 may provide a new way of looking at very low latency reliable communications for safety applications such as protective relays. For less demanding applications which use layer 3 (TCP/IP), the features of SD-WAN can be applied directly to give the best possible performance over redundant paths, with performance telemetry and better situational awareness than any other technology evaluated by the authors.

C. The third potential solution; make the IIoT-CI devices in the cloud effectively impervious to remote attack

Techniques like SDN and SD-WAN offer the potential to reduce any organisation's attack surface for any device. They eliminate much of the attack tree for devices in closed networks, but they do not address the vulnerabilities associated with remotely accessible devices over public networks; a new paradigm was needed. Without this, connectivity from IIoT devices to the cloud will always be vulnerable. Conventional design uses perimeter technology to secure sites and services; however, firewalls, network access control (NAC) and virtual private networks (VPNs) are all subject to vulnerability, exploitation and attack. These legacy approaches will not secure cloud services on the public Internet.

Work done by the Defence Information Systems Agency (DISA) c. 2007 [25] established the concept of a Black Cloud, an application infrastructure which can be connected to from the Internet, but which cannot be detected and has no exploitable attack vector. Anecdotal information suggests some intelligence agencies may be using this approach for secure systems. The key characteristic is that authentication and authorization occur prior to network access. There is a Software Defined Perimeter (SDP) working group and the first publications on the work from the Cloud Security Alliance (CSA) occurred around 2013; SDP specifications were released in April 2014 [26] and an open source

reference implementation is available [27]. The authors were working on similar principles (Kerberos in the Cloud) and this has contributed key design points; CSA terminology is used in parenthesis and diagrams are based on CSA SDP.

Any IIoT-CI device (initiating host or IH) must authenticate to an authorization server (SDP controller) before it can access any application servers (accepting SDP host or AH), this is the control plane of the SDP (Fig 1). Conventional/multifactor authentication could be used [28] and new standards for device attestation have emerged recently [29]. Geo-location could also be used, as could client posture (patching, anti-malware, policies). The authorization server provides the client with a list of services and matching application servers. This can be done on a per client basis, where the controller has a policy-based list of resources that the client can access.

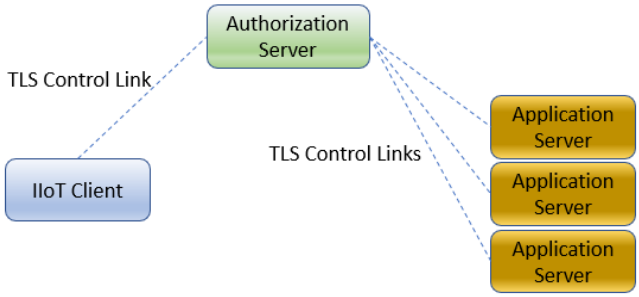

Fig. 1. IIoT device authenticates to controller

All application servers are black, they cannot be detected; they have no DNS entries and give no response to port-scanning, the application servers only accept connections at the request of the authorization server. The first interaction between an IIoT client and an application server is when the IIoT client raises a connection with the application server and authenticates using the ticket it has obtained from the authorization server, using HMAC single packet authentication [30] or similar schemes. Unless the IIoT client knows where to find the application servers and has an admission ticket, the application server does not respond. The application servers have been pre-notified by the authorization server to accept the connection but bound only to specific IIoT clients and applications; this is the data plane of the SDP and it is implemented with mutual (two-way) TLS authentication, mTLS. Device validation also takes place; the IIOT client has both an admission ticket and is confirmed to be the original client which was granted the ticket (Fig 2).

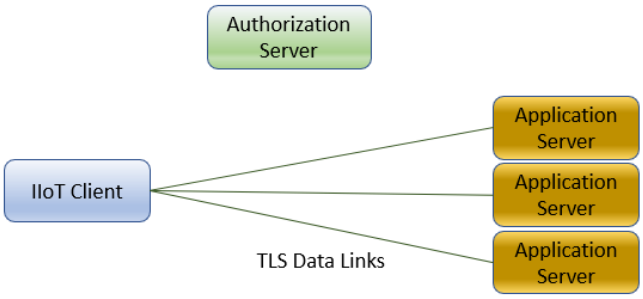

Fig. 2. IIOT device mutually authenticates to services

Public connectivity may also be to proxy servers, with the actual application server one step further removed from the perimeter; these act as a dynamic firewall with a default DENY ALL rule. There are a range of further security enhancements which could be applied here. Which topology to use is dependent on scale, number of services, etc. (Fig 3).

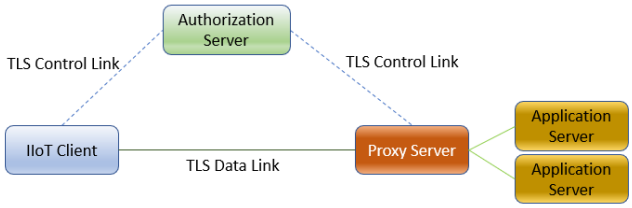

Fig. 3. Mutual authentication occurs via a proxy

A few examples of technology which use SDP are commercially available and some independent evaluation of its efficacy has been completed. By the SDP specification, there are five separate layers of security in this model.

1. Single Packet Authorization
2. Mutual TLS
3. Device Validation
4. Dynamic Firewalling
5. Binding tunnels to applications

In a five-day public international hackathon in 2014, there was no penetration of even the first layer, the single packet authorization protocol [31].

IV. The Fourth Potential Solution: SD Node

Many of the remaining vulnerabilities in the attack tree relate to the endpoints. At the risk of making a sweeping statement, systems of hardware and software will always have vulnerabilities, this truism also applies to the firewalls and VPN concentrators that conventional security practice deploys at the perimeter. Whatever additional solution is applied must mitigate this risk. The solution is to apply the original principles of SDN, separate the data from the control plane and the communications channels, but do it at the device level. As a simple example, consider four conventional personal computers arranged as shown in Fig. 4.

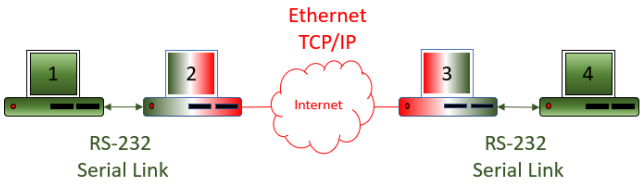

Fig. 4. A simple explanation of SD-Node

Computer 1 (client) is considered secure and has data to transmit to computer 4 (server). Computer 1 encrypts the data using conventional algorithms and passes it over a data-only link to Computer 2. If we consider a traditional RS-232 serial link with all handshaking disabled, there is no vector for attack between the two computers. Computer 2 receives the encrypted data payload (which it cannot decrypt) inserts it into a conventional frame/packet and forwards it to Computer 3. Computer 3 strips the data payload (which it cannot decrypt) and forwards it to computer 4 over a data-only serial link which once again, has all handshaking

disabled and present no attack surface. Computer 4 can decrypt the payload.

Assume that despite black cloud techniques, computer 2 and 3 could be attacked from the Internet. They can be considered sacrificial; they cannot decrypt the data and they have no attack vector to Computers 1 and 4. Computer 2 and 3 should only receive traffic which can be decrypted by Computer 1 and 4, which holds the decryption keys and can read/write the payload. Any packet which cannot be decrypted is a security event, an attempted intrusion, intrusion detection is implicit. There is no remote attack which compromises the data, or the integrity of the secure client and server.

This is the simplest way of explaining the notion of SD-Node, the separation of the subsystems which hold and encrypt data and the exposed subsystems involved in communications, with a data-only path between the sub-systems. This is very easy to model using virtual machines and allows for easy development and evaluation.

Embodying this in an IIoT device is more complex and remains a project. The present scheme envisages three separate internal hardware modules, similar in function to many other small memory devices, but with a unique partitioning scheme.

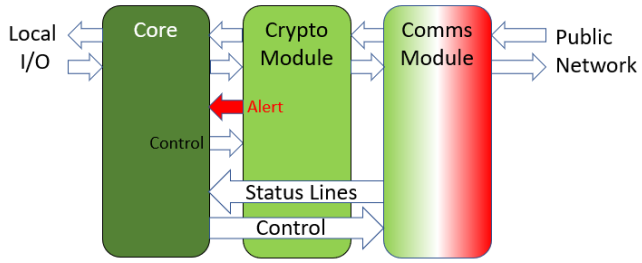

Fig. 5. A hardware reference implementation for IIOT-CI

1) Core: the core is the conventional computer component of the device, containing a CPU, main memory, a boot device/persistent storage and I/O. The nature of the I/O depends on the nature and function of the IIoT device, but will typically be digital inputs and outputs, analouge inputs and outputs, pulse inputs and outputs. Alternatively, it may connect to a process data bus.

2) Crypto Module: data from the core is encrypted using conventional algorithms. In security models which require a separate security component, this will serve. In standards which require dedicated hardware components like TPM, an additonal module will be required.

3) Comms Module: the comms module is the only component which is exposed to remote attack. It is configured by the core through a one-way, data only path. The current design envisages a limited number of status lines, but the only restriction on the status path is that it can carry status data only, that there is no vulnerability exposed.

The Core configures the Crypto Module with initial keying information and for a functional system, a status return is optional. The Crypto Module contains no persistent configuration data, it is wholly reliant on the Core.

Once the Comms and Crypto Modules have been configured, the Core can begin to encapsulate and send frames of plaintext data. The Crypto Module creates ciphertext and forwards it to the Comms Module. The Comms Module inserts the ciphertext as its data payload and forwards the packet to a similar node. On receipt of a valid frame, the ciphertext data is extracted and sent to the Crypto Module. If the frame is invalid due to data corruption, the frame is dropped by the Comms Module and TCP should take care of retransmission. If the data payload deciphers correctly, then it is validated as having originated with a valid device and it is forwarded as plaintext to the Core. If the data payload does not decipher, it is an intrusion attempt and a security event; IDS and IPS is by default. The remaining attack vector is a data channel attack from the trusted server or client.

Data passing to and from the Comms Module is encrypted, it is completely opaque. As the data is encrypted, a compromised Comms Module cannot decipher the data stream. The Comms Module looks after packaging the data into frames/packets and sends them via the best path, it implements SD-WAN functionality and provides granular link performance data.

The path from the Crypto Module to and from the Comms Module is data only, there are no control signals, a compromise of the Comms Module cannot lead to an attack on the Crypto Module. Any attempt at data injection from the Comms Module to the Crypto Module will be an immediate indicator of compromise and an alert status line can be raised by the Crypto Module.

Data will flow to and from the Core to an identical peer device elsewhere on the public network. The Core has a list of root authentication devices in the black cloud and can initiate an authentication session with a black cloud authentication server. A secure method is required to update this server list. On successful authentication, the black cloud authentication server provides a list of authorised black cloud application servers along with a service granting ticket. The Core configures the Comms Module with the correct network information and receives a status acknowledgement. The Core can receive new keys and root lists once connected. A Single Packet Authentication is then initiated to the application server or proxy.

V. Conclusions

The attack tree was designed to consider remote attacks on IIoT devices; most paths through the tree may be eliminated by the techniques discussed. In analysing the class of attacks mitigated, remote attacks which can compromise the integrity or confidentiality of the devices or the data communications are eliminated.

With an isolated controller, remote attacks on the LAN are eliminated using SDN. The techniques of SD-WAN offer potential gains for availability and performance and yield very detailed data relating to link performance. SDP removes the reliance on firewalls, perimeters and zones and offers the potential of a ubiquitous solution for IIoT and its interaction with public cloud services. Finally, SD-Node

ensures that the underlying device and its communications are inviolate and cannot be compromised. A technology designed to enforce security must accept that attacks will take place and intrusion detection must be included in any design consideration. If part of a system is compromised, it must fail-safe and protect the integrity of the system, intrusion prevention must be implicit from the design. The combination of technologies discussed in this paper meets these requirements.

As packets pass through routers, although the payload may be encrypted, the IP address of source and destination nodes are visible. For an attacker in the middle, these addresses are discernible; even through a node is black, an attacker now knows it is there. This can be mitigated with SD-WAN in the Cloud.

Although attacks on availability are mitigated, they cannot yet be eliminated; Denial of Service (DDoS) attacks may still be achieved. Work is on-going in the IETF to find standards-based ways of mitigating DDoS attacks and draft Distributed-Denial-of-Service Open Threat Signalling (DOTS) Architecture documents have been released. DOTS includes a signal channel with which an IIoT device could inform upstream devices (routers, switches) that it is receiving inappropriate traffic; the traffic can be blocked upstream to the device. When standardized, this functionality can be added to any of the proposed solutions. Work on DDOS mitigation is also on-going within the Cloud Security Alliance and the SDP Working Group. Some of the difficulties which prevent conventional IoT devices identifying malicious traffic do not apply to the SD-Node architecture; every inappropriate frame is flagged.

This work was intended to address remote attacks only. The physical design of the device, its operation and update, and the cryptographic strategies taken all need to be addressed to create a final IIoT-CI device which aspires to be unconditionally secure by default.

REFERENCES

[1] Online: ISACA Journal, Volume 4 2018, “The Price of a Data Breach” https://www.isaca.org/Journal/archives/2018/Volume-4/Pages/the-price-of-a-data-breach.aspx. Accessed 9th December 2018

[2] Online: ISACA Journal, Volume 5 2018 “Why We Failed”, https://www.isaca.org/Journal/archives/2018/Volume-5/Pages/why-we-failed.aspx. . Accessed 9th December 2018

[3] Online: Equifax Breach Aftermath Report, 2018. https://www.idtheftcenter.org/wp-content/uploads/2018/08/ITRC_Equifax-Breach-Aftermath-Report-2018-2.pdf. Accessed 9th December 2018

[4] Canell et al. “A Systematic Evaluation of Transient Execution Attacks and Defenses”, November 2018, arXiv:1811.05441

[5] Estler, HC., Nordio, M., Furia, C.A. et al. Agile vs. Structured Distributed Software Development: A Case Study (2013), Springer US

[6] National Academy of Sciences Report. National Academy Press; 1998. “Trust in Cyberspace”.

[7] ISO/IEC 15408:2009, Information technology, Security techniques, Evaluation criteria for IT Security.

[8] ISO Guide 73:2009, "Risk management. Vocabulary."

[9] E. T. Nakamura and S. L. Ribeiro, "A Privacy, Security, Safety, Resilience and Reliability Focused Risk Assessment Methodology for IIoT Systems Steps to Build and Use Secure IIoT Systems," 2018 Global Internet of Things Summit (GIoTS), Bilbao, Spain, 2018, pp. 1-6.

[10] H. S. Lallie, K. Debattista and J. Bal, "An Empirical Evaluation of the Effectiveness of Attack Graphs and Fault Trees in Cyber-Attack Perception," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 5, pp. 1110-1122, May 2018.

[11] Online: B. Gates, “Trustworthy Computing”, https://www.wired.com/2002/01/bill-gates-trustworthy-computing/, accessed: 9th December 2018.

[12] Online: https://www.microsoft.com/en-us/securityengineering/sdl/, accessed 10th December 2018

[13] B. Schneier, Attack Trees, Dr. Dobb's Journal, December 1999.

[14] Online: The TREsPASS Project, https://www.trespass-project.eu/, accessed 10th December 2018

[15] Online Secrets of the Little Blue Box, R. Rosenbaum, http://explodingthephone.com/hoppdocs/rosenbaum1971.pdf, accessed 11th December 2018

[16] RFC 3746, Forwarding and Control Element Separation (ForCES) Framework, April 2004.

[17] Casdao et al. “Ethane: Taking Control of the Enterprise”, SIGCOMM’07, August 27–31, 2007, Kyoto, Japan.

[18] J. O’Raw, D. M. Laverty, D. J. Morrow, “Software Defined Networking as a Mitigation Strategy for Data Communications in Power Systems Critical Infrastructure”, presented at PESGM, Boston 2016

[19] F. Hauser, M. Schmidt and M. Menth, "Establishing a session database for SDN using 802.1X and multiple authentication resources," 2017 IEEE International Conference on Communications (ICC), Paris, 2017, pp. 1-7.

[20] D. M. Laverty, R. J. Best, P. Brogan, I. Al Khatib, L. Vanfretti and D. J. Morrow, "The OpenPMU Platform for Open-Source Phasor Measurements," in IEEE Transactions on Instrumentation and Measurement, vol. 62, no. 4, pp. 701-709, April 2013

[21] J. O'Raw, D. M. Laverty and D. J. Morrow, "IEC 61850 substation configuration language as a basis for automated security and SDN configuration," 2017 IEEE Power & Energy Society General Meeting, Chicago, IL, 2017, pp. 1-5.

[22] R. Chaudhary, G. S. Aujla, S. Garg, N. Kumar and J. J. P. C. Rodrigues, "SDN-Enabled Multi-Attribute-Based Secure Communication for Smart Grid in IIoT Environment," in IEEE Transactions on Industrial Informatics, vol. 14, no. 6, pp. 2629-2640, June 2018

[23] Unpublished MSc Research, Khalid Said Abdullah AL Shereiqi, J. O’Raw 2018

[24] H. Heine and D. Bindrich, "Designing reliable high-performance IEC61850 substation communication networks based on PRP and HSR topologies," 22nd International Conference and Exhibition on Electricity Distribution (CIRED 2013), Stockholm, 2013, pp. 1-4Department of Defense Global Information Grid Architectural Vision, Vision for a Net-Centric, Service-Oriented DoD Enterprise, 2007

[25] Department of Defense Global Information Grid Architectural Vision, Vision for a Net-Centric, Service-Oriented DoD Enterprise, v1.0, June 2007

[26] Online: CLOUD SECURITY ALLIANCE SDP Specification 1.0, April 2014, accessed 1st December 2018

[27] Online: https://github.com/WaverleyLabs/fwknop, accessed 10th December 2018

[28] Online: Enabling Network Access for IoT devices from the Cloud, July 2019, accessed 10th December 2018

[29] 802.1AR: IEEE Standard for Local and metropolitan area networks–Secure Device Identity

[30] RFC 4226, HOTP: An HMAC-Based One-Time Password Algorithm

[31] Software Defined Perimeter Working Group, SDP Hackathon Whitepaper, April 2014