21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

CIGRE US National Committee
2021 Grid of the Future Symposium

Prevent Cyber-attacks: Know Your Network

S.R. KNUDSEN
KeyLogic Systems, Inc.
USA

SUMMARY

The internet was envisioned as a way to connect people from anywhere to anyone. This is great for a company with international ambitions, but malware and cyberattacks have become an affliction, arguably reaching the debilitating level in 2021.

This uber-connectivity works on the business side of an enterprise, for marketing products, taking orders, and delivering goods, but the internal core of business, the operational technology (OT) of making, manufacturing, customizing, and finishing the "stuff" that is to be sold is exposed to cyber threats from around the world.

As networks scale in size, the common sense concept of "Know Your Network" becomes difficult to attain. Engineering and system administration is necessary for monitoring the network and controlling access. From a larger perspective, complex networks, a common terminology is derived from the 5 NIST cybersecurity criteria. However, the NIST criteria are action-oriented (identify, protect, detect, respond, recover), whereas what is known about the network is pre-decisional, and based on knowledge using the language of ontology (what the network is or can do, prior to what it does). So improved cybersecurity depends on useful knowledge of the system and the human resources, vision and determination to act. The paper will also examine inexpensive test beds (using Arduino, Raspberry PI) to build simple networks including data diodes and discrete mathematical methods for examining network paths. Part of knowing a network is scanning for unknown nodes, and so Shodan and similar scanning tools will be considered as well.

The paper concludes by showing why air-gapping energy systems is impossible without crushing impediments to productivity. To do so, we define and explain how raw materials (such as energy) at sufficient scale can't get to consumers without IT talking to OT, that is, there is no complete air-gapping of OT from the internet.

A testbed allows the enumeration of all communication paths, allowing insights to be applied to larger systems so at risk and vulnerability can be minimized. Novel technology like data diodes may also help, but they don't change the essential two-way nature of network paths. Along with data diodes, biometric authentication with hardware tokens[1] should be investigated as a way to monitor or throttle network flow.

KEYWORDS

NIST criteria, information technology (IT), operational technology (OT), ontology, cyber testbed

[1] CDW, «https://www.cdw.com/content/cdw/en/articles/security/hard-tokens, What Are the Differences Between Hard Tokens and Soft Tokens?," https://www.cdw.com/content/cdw/en/articles/security/hard-tokens-vs-soft-tokens.html

steve.knudsen@keylogic.com

Cyber-attacks and Networks

The internet was envisioned as a way to connect people from anywhere to anyone. This is great for a company with international ambitions, but malware and cyberattacks have been an affliction, arguably reaching the debilitating level in 2021.

This uber-connectivity works for marketing products, taking orders, and delivering goods, but securing the internal core of business, the operational technology (OT) of making, manufacturing, customizing, and finishing the "stuff" that is to be sold is more obscure. Organizations with sloppy cybersecurity don't consider the connection between their IT and their OT, but even thoughtful business strategies leave holes for attacks. For instance, the Solarwinds hack of 2020 and the Kesaya[2] attack of 2021 were software supply chain attacks, which are hard to grasp or locate and led to finger pointing. The alternative to broadly available IT software is to build it oneself, which takes time, money, and potentially opens up other vulnerabilities. This reduces business value arguably as much as an infrequent cyberattack. Hardware supply chain attacks are even more difficult to find, and both kinds of supply chain attacks require testbeds to identify and locate.

Software/services used for business live on IT and OT networks. In the past, OT systems were air gapped, which provided a natural protection against foreign meddling by states or individuals. A little thought shows that for raw materials, including energy, this is no longer possible. Each unit moved does so in response to being ordered, and is invoiced. In addition, notification emails are sent upon ordering and upon delivery. The sensor measuring the units moved (flow) must by necessity be connected to the IT system unless communication is done manually. Thinking far back in time, business processes were done with paper, and air-gapping could be complete because humans moved information, not computers.

Now, far beyond the age of paper, the Colonial Pipeline attack fit the rubric of a raw goods delivery company which has no realistic way of separating IT and OT functions. The process of ordering a product, physically connecting for transfer of the product, disconnection and invoicing are subject to surveillance and attack, a process that must be carefully examined via red team attacks and penetration testing (PenTest).

Cyberattacks usually involve compromising user login information (remote privilege access), then escalating privileges[3] from user to administrator to have the "keys to the kingdom" of the network. Risks include ransomware, data loss or compromise, and network unavailability. Cyber defense strategies depend on in depth knowledge of system administration, operating systems and software, and strategy. These are applied according to the rubric of the NIST Cybersecurity Criteria. Also, the Electric Power Research Institute (EPRI) has provided a detailed guidebook on the "what" and how[4] of protecting EDS. In particular, the section "Identify: Future States and Gap » (p. 4) is about knowing the business and operations from the standpoint of the network and its services.

Information and Operational Technologies (IT and OT)

Information technology (IT) refers to using computation for storing, retrieving, and sending information. It also involves a level of computation, for databases and manipulation as necessary. IT supports users for all their information needs, as controlled by the system

[2] NPR, A 'Colossal' Ransomware Attack Hits Hundreds Of U.S. Companies, A Security Firm Says https://www.npr.org/2021/07/03/1012849198/ransomware-cyber-attack-revil-attack-huntress-labs, accessed 7/19/2021

[3] Enterprise Utility Attack Types, part of a Full Circle Group industry reference model, 8/15/2021

[4] Electric Power Research Institute (EPRI), Cyber Security Vision For 2030, https://www.epri.com/research/products/000000003002022715, accessed 8/20/2021

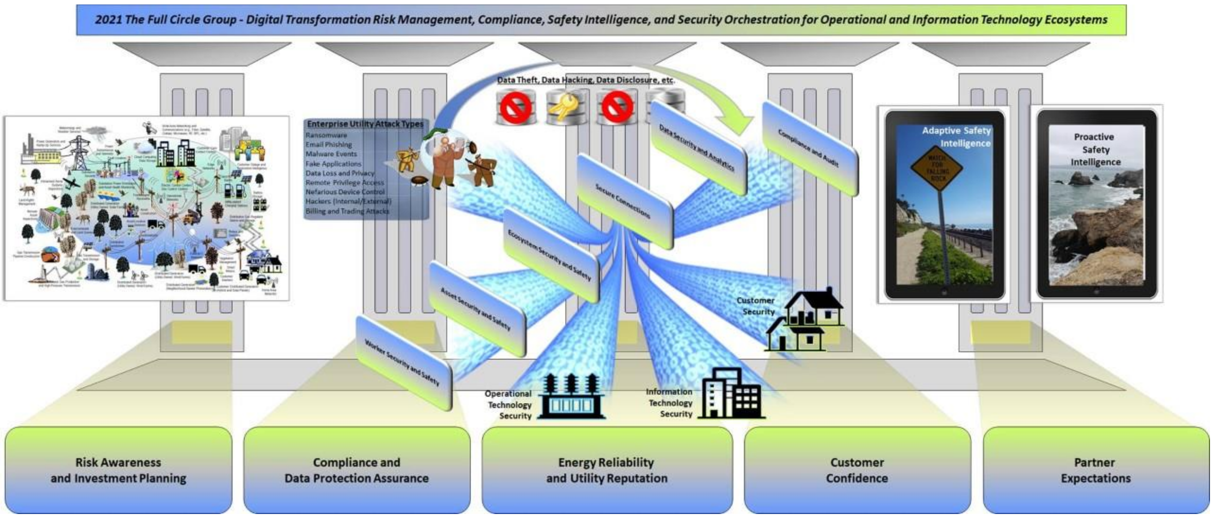
administrator. At its base, IT doesn t DO anything, it just facilitates. However, it took just a short step for IT to get into transactions (think Amazon or Ebay).

Communications are done via « signals », and this is the language used to indicate when a communication leads to (« causes ») something to happen. Suddenly, IT enabled internet (or cellular) connected security systems (think « Ring »), TV on demand and the smart electric grid. This is called the internet of things (IoT).

Digging deeper, there is a world of control systems using a blizzard of protocols/modalities, including RS-232 (connecting computer and its peripheral devices to allow serial data transfer), USB, Modbus, etc. These systems can interface to business systems through one or more layers of internet based equipment. The switches and programmable logic controllers (PLC) and field programmable arrays (FPGA) make up the world of operational technology (OT).

These operational technologies are the devices and services that monitor and control transformers, breakers, generators, etc. Figure 1 shows a digital transformation slide about how IT and OT interrelate, with the « real world » on the middle left and cybersecurity concerns ot its right. Safety here is considered to be in a yin-yang relationship with security.

As an example with OT technologies, the substation automation, protection, and control network should be clearly separated from any external network. This can be achieved by using firewalls to control data access to the control network.


2021 The Full Circle Group - Digital Transformation Risk Management, Compliance, Safety Intelligence, and Security Orchestration for Operational and Information Technology Ecosystems

Enterprise Utility Attack Types
Ransomware
Email Phishing
Malware Events
Fake Applications
Data Loss and Privacy
Remote Privilege Access
Nefarious Device Control
Hackers (Internal/External)
Billing and Trading Attacks

Data Theft, Data Hacking, Data Disclosure, etc.
Data Security and Analytics
Compliance and Audit
Secure Connections
Ecosystem Security and Safety
Asset Security and Safety
Worker Security and Safety
Customer Security
Operational Technology Security
Information Technology Security
Adaptive Safety Intelligence
WATCH FOR FALLING ROCK
Proactive Safety Intelligence
Risk Awareness and Investment Planning
Compliance and Data Protection Assurance
Energy Reliability and Utility Reputation
Customer Confidence
Partner Expectations

Figure 1 Digital Transformation, Safety, and Security[5]

The language of cybersecurity: NIST Criteria

Energy delivery systems (EDS) cyber-security can be understood with the help of the National Institute of Science and Technology (NIST) criteria.[6] These five criteria can be understood as:

- Identify -- manage cybersecurity risk to systems, people, assets, data, and capabilities. For EDS, this is identifying threats, vulnerabilities and maintaining situational awareness.

[5] Courtesy of the Full Circle Group, 8/25/2021, http://www.fullcirclegrp.com/, see Reference [3]

[6] NIST Cybersecurity Framework, https://www.nist.gov/cyberframework, accessed 7/19/2021

- Protect – implement appropriate safeguards to ensure delivery of critical services. Authentication, authorization (include role-based access control), and physical security are key here.
- Detect – identify/detect the occurrence of a cybersecurity event, using an intrusion detection system (IDS).
- Respond – take appropriate action regarding a detected cybersecurity incident. For EDS, that means either closing a network connection or shutting down a machine, or some sort of automated or pre-planned/program response. There may be relevant “safe-modes” which are intermediate states between full operation and shutoff.
- Recover -- Develop and implement appropriate activities to restore any capabilities or services impaired due to a cybersecurity incident. The time span for this is ranges from 2.0 seconds (spin down time out of synchronization for generator) to days to months.

There is a way to use “old-school” methods such as human operators and an alternative to electronic communications to secure systems. Concepts such as biometric authentication and access tokens for opening sessions for transfer of information to/from IT/OT system is one. Use of randomized USBs for low throughput systems is another. One promising approach is data diodes, but using these effectively requires network design skills as round-trip communications are necessary for successful business value generation.

Returning from Global to Local

The “cat’s out of the bag”, so to speak, regarding the global reach of networks. Air-gapped generators and plants are no longer possible because of the expense of personnel and the costs of paper records. Below are several suggestions for virtual air-gaps at key parts of the industrial infrastructure:

Access tokens with biometric authentication

Since the internet reach is worldwide, devices and codes tied to devices (“tokens”) can narrow access to a subsystem/sub-network to the locality of the company employees. The two factor authentication used for banking or by employees uses numerical codes, but these are tied to a physical device, usually a smartphone. This is closer to a hard token, as opposed to challenge questions, which are soft tokens.

One-Way Data Diodes

Unidirectional data transfer creates a boundary between trusted and untrusted networks through a one-way, physically secure communication channel. The approach uses optical technology in place of electrical signals to send data from one secure network to another, allowing data to enter but not exit. Data diodes are simple to deploy and require little or no ongoing maintenance. And they can help organizations comply with requirements such as North American Electric Reliability Corp. (NERC) guidance on diodes. But while they’re highly effective in situations that need only one-way data transfer, they’re not appropriate for IT-OT connections that require two-way communication. In addition, they do not validate data.

Although data diodes are for one way data transfer, systems can be engineered to separate IT from OT by using circular communication paths (see figure 2). This does not stop a malware or mal-control signal into the loop, and, indeed control/communications nodes are needed to separate data transmission from reception. In this figure, the computer providing this choke/throttle/broker service is indicated wedged onto a “V” representing the IT (top half) and OT portions. The manufacturing operations with all their control and data are represented as a dot in the lowest part of the “V”.

Four network principles

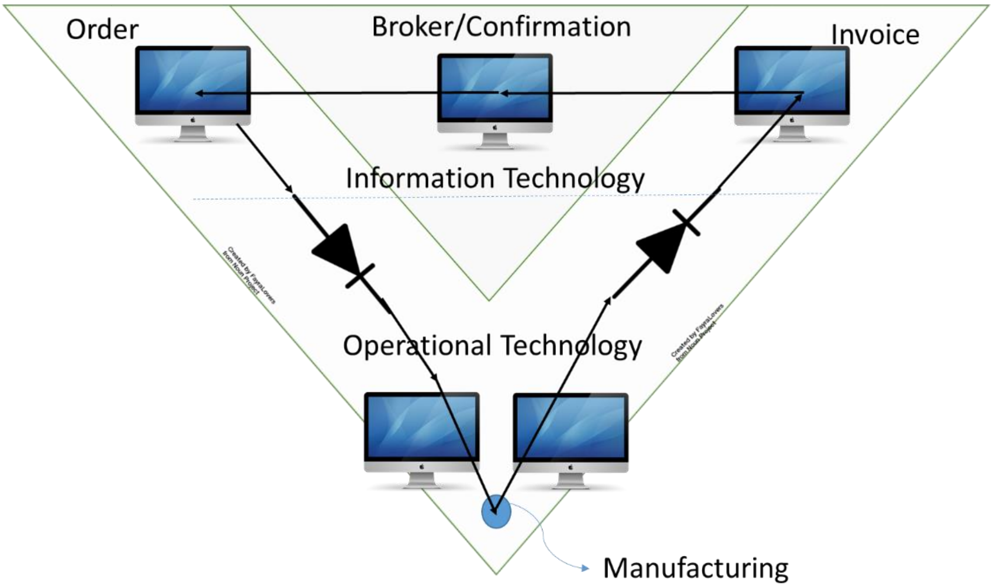
Multi-layered Defense Architecture – Principle #1—Slowing the attacker down
A single layer of defense is rarely enough as any security mechanism may be overcome by an attacker. The system architecture should ensure that the most sensitive parts of the system are protected by

multiple rings of defense that all must be breached by an attacker in order to get to the “crown jewels”. The NIST five categories apply, with protection and detection mechanisms in focus. This includes both technical measures, such as intrusion detection systems, as well as procedural measures, such as review of log files or access rights.

Least-privilege Approach – Principle #2 – Need to Know
The concept of “need to know” can be expressed as “least privilege”. No user or process should be able to do more in the system than what is needed for the job. This principle is not only key to preventing malicious attacks but also very important in preventing “accidents or missed patching opportunities.” For instance, spreading of a virus that sits on the laptop of an authorized user can be limited if the user only has minimal access to the system and network.

Network Segmentation – Principle #3 –Splitting the network into zones
Any computer network should be divided into different zones depending on the criticality of the nodes within each zone. In a typical substation automation environment, separate zones could be envisioned for bay level devices and for the station level devices and computers. Depending on the size of the substation, having separate zones for bay level devices for each bay might make sense. Zones should be separated by data diodes, firewall application gateways or similar devices.

Secure Substation and Command Center Communications – Principle #4
Network communication, both within a substation automation system and with external networks, should be protected using encryption and/or message integrity protection, using lightweight cryptographic algorithms as necessary to ensure performance. For external connections, the use of VPN (Virtual Private Networks) is recommended for both operational as well as maintenance and engineering connections. For engineering and maintenance in substations access, security protocols such as HTTPS or SSH should be used[7].



diode symbol by FayraLovers from the Noun Project

Figure 2 Network segmentation, with data diodes

[7] These four principles developed in collaboration with the Full Circle Group, 8/26/2021, http://www.fullcirclegrp.com/

Ontology: Knowing everything about the network and its interfaces

An ontology is a formal representation of the (full) domain of knowledge, including properties defining relationships, restrictions and interdependencies. This is a fancy way to express knowing a network and what it can do. The key is that, theoretically at least, the network can be completely understood, its configuration, the services that can run on it, and what constraints they have.

The ontology is the network of nodes and directed edges together with metadata. An edge with two way communication in principle can in actuality have its "ports" blocked by a firewall, with this constraint being some of the metadata recorded in the ontology. One or more nodes can refer to entities outside a company's system, such as a generating plant connected to a transformer on a distribution or sub-transmission grid.

The set of all communication paths and actions can be computed in principle from the ontology.
If data diodes are used, circular paths become even more important, because a clockwise or clockwise information flow is forced. It's possible for the Konigsberg bridge problem[8] to become relevant here, an introductory topic in discrete math. One might ask why this is relevant. If there is a path through a network with the concept that each edge crosses a "river" on its way to "land", then, if an attacker can get into the loop, the attacker will move till it reaches a port that is blocked. Note that the attacker can seek to elevate privilege or use Windows zero day flaws, etc., so this notion of a circular path through a network is non-trivial. The circular path involves a business transaction, the production of goods, and their delivery, along the circle. The relationship of this discrete math problem to cybersecurity was published in 2013 and is likely still not fully appreciated[9].

Action: Knowing and Doing (Execution)

There are business books about execution, but it's a mystery how things go from thoughts to actions, and, certainly, companies need to take thoughtful action on cybersecurity now, not just plan it!

The decision/transition matrix for knowledge of a system (ports, services, communications, etc.) and executing, in this case executing protective measures, is given below (Tableau 1).

Tableau 1Knowledge vs. Execution

Knowing and Protecting	(Yes) Know	Don't Know
Apply protection	Case 1	Case 2
Business as Usual (no protection)	Case 3	Case 4

We discuss the cases one by one:

Case 1: Prompt attention to knowledge about one's network is ideal. Fixing Window's flaws, and scanning with tools like Shodan reduce risk to one's system.

Case 2: Patch update management allows you to protect against threats not known to plant personnel because the protection is outsourced to a vendor. If hackers target your system, it only makes sense to pool resources with others to protect everyone.

Case 3: Knowing what's right and not following through sounds like the depths of hypocrisy, but learned helplessness from poor management techniques and a culture of cost cutting (the urgent over the important) puts even « good » people in this predicament.

Common information models: INDL

[8] Boza and Munoz, « (In) Security in Graph Databases, Analysis and Data Leaks », https://www.scitepress.org/Papers/2017/64190/64190.pdf, accessed 8/24/21
[9] LANL, https://www.lanl.gov/discover/publications/1663/2013-july/graphic-math.php

Case 4 : If 2021 taught us anything, it’s that blissful ignorance is no longer an option. Malware as a service (a sort of « software as a service ») is making complacency and ignorance deadly to system health and the bottom line.

Even the most prepared system can be attacked. Whitelisting (deny by default) and trimming privileges (« need to know ») is a start towards securing systems.

Developing an ontology seems simple until one realizes that all possible behaviors and states should be in principle derivable from the ontology. To get started making an ontology, realize that common information models are necessary for successful development of ontologies for large networks. An example is the « Infrastructure and Network Description Language » (INDL). Along with the expected nodes and links, there are ports and services: A node (vertex) is a machine part of the network, such as a router, or just a regular PC . A port limits the permissions for the node’s connection to the network. A link is the connection between two ports and a service defines the capabilities of a Node or Port; examples are a SwitchingService, or an AdaptationService respectively.

Services are computer programs or apps that can modify the network or user data and are therefore of great interest to hackers, system administrators, and network security specialists. These services can become malware in the wrong hands. Services can be infinitely complex, and so simplifying and restricting possible services is a key cybersecurity strategy.

Network Topology

Available topologies for network include Ring, star, bus, mesh, tree[10], where mesh is the most general, a sort of amorphous network that allows unlimited connectivity (up to all to all as a limit). The topology is a security consideration but the sub-networks corresponding to all domains of the business (OT, IT, etc.) must allow information in and out. This is what makes the system vulnerable.

Network and device Protocols

A Protocol is a “set of rules that govern how systems communicate. For networking they govern how data is transferred from one system to another[11]”

Because we speak of a network as having edges and vertices, or links and nodes, devices are implied on a network. But they deserve special interest here. They obey certain protocols in communication, or are intended to, and so malware and bad commands will come over the network targeting the devices in « their own language ».

TCP/IP

TCP/IP is formally known as the Internet Protocol Suite. One can learn about this online, but the important part is that you should know that when one goes online or onto social media, it’s the “internet” or more archaicly the “world wide web.[12]” The big deal about Netscape was that it was a browser that could efficiently find information on the WWW. The internet can be thought of more broadly as not just information but also capabilities to request services or even do command and control. This means that if your OT network is connected to the internet, it has world wide reach and even into space due to GPS and other satellites. Remote access from anywhere in the world is conceivable.

[10] Types of Network topology, https://www.geeksforgeeks.org/types-of-network-topology/, accessed 8/15/2021

[11] Steve’s Internet Guide, http://www.steves-internet-guide.com/internet-protocol-suite-explained/

[12] WWW is still appropriate, but hypertext and information systems are a subset of the idea of the internet as the ability to “connect everything”, see Ben Segal, Internet prehistory at CERN, https://home.cern/news/opinion/computing/internet-prehistory-cern

This world wide reach of the internet is the foundation for the attempts outlined in this paper to narrow the reach for OT subsystems.

Software defined networking.

Software defined networking (SDN) is the physical separation of the network control plane from the forwarding plane, with the control plane controlling several devices[13]. By design, this allows for no direct connection of devices to the network with external internet (TCP/IP) access. This moves the battle to the “services”, i.e. software using the OpenFlow® protocol so the focus on protection can move there. SDN controllers replace a bunch of device controllers using multiple, vendor-specific device commands and protocols.

The OpenFlow® protocol separates the network and data planes. Data is associated with a device, because it’s the device that monitors current and voltage, switches power on and off to other devices and equipment, measures temperature and other physical variables, and does other control actions. SDN allows fine control over which data can get onto the network, which improves cybersecurity.

An analog is the “plug and play” nature of computer peripherals[14], with a simple USB protocol for connecting devices. However, in the plug and play case, cybersecurity is an aspiration whereas interoperability is the goal, while with OpenFlow, cybersecurity is the animating principle, with interoperability as a prominent secondary goal.

Remote Access :

As mentioned above, remote access from anywhere in the world is conceivable if a corporate system is connected to the internet. It makes sense for an executive to have access from Eastern Europe to company email and some databases. However, in the extreme risk environment we are in, it may make more sense for the executive to need to connect to an employee who will provide only the needed information. This is like “need to know” referencing not only who may know something but how much they may know. This may lead to hurt feelings, but all employees need to get used to a consistent (not uniform) application of security protocols.

Software defined radio

Software defined radio (SDR) is a form of SDN that is wireless and therefore extends beyond plant boundaries. In fact, remote access is a feature of SDR, not a bug. To understand its value, imagine a physical attack on a plant with hostages. SDR can be used from the outside to secure system resources. This requires more scenario building and use cases than a naïve “whitelisting” approach would take, i.e. remote access should be restricted, not eliminated.

Furthermore, maintaining substations and remote generation sources requires SDR for efficiency purposes. The radios have a large range, with this S&C Electric offering having a distance range of about 40 miles[15]. Given that some radio broadcasts travel thousands of miles, it’s possible for a radio to have too much range, causing a security problem, but 40 miles seems fine.

Case study : The Colonial Pipeline Attack.

Certainly an IT based attack which branches into the OT is the worst nightmare for a company. Indeed, during the Colonial Pipeline episode, the company closed down the pipelines (on the OT network) for a couple reasons. First, it would take a couple days to figure out if OT software and networks were breached. But also, the company could not invoice for the gasoline delivered without IT and OT functions being exposed to each other. One might ask why not just deliver the gasoline

[13] SDN Overview, Open Networking Foundation, https://opennetworking.org/sdn-definition/

[14] Interesting discussion at Wikipedia, “Plug and Play”, https://en.wikipedia.org/wiki/Plug_and_play

[15] S&C SpeedNet™ SDR Software Defined Radio, https://www.sandc.com.br/globalassets/sac-electric/documents/sharepoint/documents---all-documents/descriptive-bulletin-1075-30.pdf?dt=637652648808663752

manually and settle the invoices later. This is what happened, but the number of personnel were limited and they had to get to the pumping and control locations. Indeed, there was a misleading article suggesting it would take 15 days to restore service to New York because of the flow rate of gasoline. This never happened due to manual operations.

But panic did happen. Panic buying along with reduced pipeline deliveries led to many gas stations running out of gasoline. Many people, though, did not believe assurances that there would soon be gas, and this worsened the crisis. This is an example of a lack of resilience of faith in government, but resilience is more generally making sure that all pieces of the system work together to produce business value.

To this end, the following cases for attacks on the IT/OT can be considered:

1. IT failure only, OT left intact
2. OT failure only, IT left intact
3. Leakage of failure from IT to OT (the Colonial Pipeline situation)
4. Leakage of failure from OT to IT

The data diode approach with circular subnetworks with biometric authentication can prevent #3 and #4, but the rare case still exists that both IT and OT could have been attacked simultaneously. If the company used the same philosophy to build its OT and IT networks, such as using TCP/IP and common servers, attacks on each subsystem might use Windows operating systems and be subject to the same classes of Windows flaws.

Business resilience is holistic, that is, it depends on each subsystem. So cases #1 and #2 can be devastating to the bottom line. In the case of the Colonial Pipeline episode, it appears that it was in category #1. This is the sort of attack we are familiar with, for example, with data encrypted, and ransoms required to decrypt the data.

Developing a Test bed for resilience to cyber-attack of OT or IT.

Each business system for communications and operations is different. However one simple example can point the way to more complicated ones. Because this system stands in place of the actual business system, this is an example of a cybersecurity test bed.

The OT business subsystem should be able to provide information to, and take commands from, the IT business subsystem. An inexpensive way to do that is to represent the OT subsystem by an Arduino microcomputer, which costs less than $100 with supporting documentation and cables and simple circuit elements such as LED bulbs. At the simplest level, the in-built LED or the external LED can turn on when raw material is “flowing” or manufacturing is “taking place.”

The IT business subsystem can be simplistically indicated as a web page, https://mylink56.com (dummy address) for example. “Mylink56” can push data or a command to the OT microcomputer, or it can pull data from it. The symmetrical consideration applies to the Arduino (OT micro), which can push or pull commands or data. Insertion of the data diode can be done conceptually by closing a port.

The business flow is:

- The business, “Emove” with site “Mylink56” can allow customer “C01” to make a username and a password, which is validated by information provided early by C01. That is, C01-account is not anonymous, as we have been accustomed to expect for accounts with social media or email.
- Customer “C01” orders product, which is then processed by Emove and prepared to send to the Arduino for production.
- Emove then prepares and/or manufactures product and delivers it.
- Emove invoices C01 via the site Mylink56.
- Emove is now able to receive payment and confirm it.

Current work on cybersecurity for EDS is being done through DOE's "Cyberforce Program[16]." The relevant low cost testbed work was started by CybatiWorks™ and been taken over by IntelliGenesis[17] .

Supply Chains

The Solarwinds attack was technically at supply chain attack because it compromised a vendor. It's hard to imagine avoiding supply chain attacks by building all solutions in house, but a zero trust approach would involve testing all software purchased on a replica of the IT/OT system. Testbeds provide a practical way to induce and check devices mimicking supply chain attacks. Rootkits, FPGAs with malware and other subtle attacks can be tested.

Conclusion

The Colonial Pipeline attack demonstrated leakage of data across the OT/IT divide, or the possibility of it, which forced the company to shut down most networks temporarily and run the system manually. This demonstrates the need for resilience (reversion to manual operation) but also to "know your network" in such a way that deficiencies and insufficiencies could be addressed in a timely manner.

Network segmentation and detailed ontologies of the network are two ways to harden the system and conceivably make it more resilient. At key points, data diodes can further control the movement of information, but biometric authentication can effectively blunt the effect of the world-wide nature of IT networks on the particular OT network. In all these cases, test beds can help the system administrators and other security staff explore potential vulnerabilities and solutions. Making OT systems (network + services) effectively and in essence local rather than global is the goal of "know your network", i.e. developing a system ontology.

BIBLIOGRAPHY

[1] Kamis, George, Powermag, Zero-Trust Gateways: A New Strategy for Protecting Critical Infrastructure, https://www.powermag.com/zero-trust-gateways-a-new-strategy-for-protecting-critical-infrastructure/

[2] T. Seppa "Fried Wire?" (Public Utilities Fortnightly, December 2003, pages 39-41)

[3] Figure 1 provided by Phil Wilkerson of Full Circle Group, contact pwilkerson@fullcirclegrp.com

[16] DOE Cyberforce Program, https://cyberforcecompetition.com/, accessed 8/24/21

[17] CybatiWorks taken over by IntelliGenesis, https://intelligenesisllc.com/cybati-is-now-part-of-intelligenesis/, accessed 8/24/21