Securing Operational Technology (OT) networks

Implementing zero trust and managing supply chain risks to prevent cyberattacks on critical infrastructure

KPMG in Singapore
September 2021

Contents

Preface

Operational Technology (OT) networks are computerised systems used to control physical industrial operations and are found across a broad range of asset-intensive sectors. They perform a wide array of tasks, ranging from monitoring critical infrastructure to controlling robots on a manufacturing floor.

As efforts to modernise critical infrastructure are ramped up, the risks of cyberattacks on OT networks are amplified. Traditionally, OT systems were separated from the Internet but increasing digitalisation has led to greater IT and OT integration. Unfortunately, this also means hundreds of millions of OT and Internet of Things (IoT) devices, such as medical and power equipment, are now vulnerable to attacks.

The number of OT vulnerabilities discovered and reported annually by the US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has increased at an estimated rate of 16 per cent year-on-year from 2017 to 2020, according to the Singapore Cyber Landscape 2020 report by the Cyber Security Agency of Singapore.

> “Cyberattacks on OT systems can have serious and highly damaging consequences, as attackers may incapacitate critical infrastructure such as water plants, fuel pipeline facilities and power grids. This explains why business leaders have identified cybersecurity risk as the greatest threat to their organisation’s growth.”

The COVID-19 pandemic has further blurred the lines between the physical and digital worlds, exposing fault lines in cybersecurity infrastructure and unravelling a host of new challenges.

In the post-pandemic context, workforce shortages on site are one such challenge. One of the key reasons for the lack of personnel at sites is that companies are adopting hybrid work arrangements and split teams amid COVID-19 related restrictions. This often leads to extended maintenance cycles and workarounds like contractor remote service support. As a result, supply chain risks have also heightened.

In many cases, companies have started deploying Virtual Private Networks (VPNs) to enable remote access. But this can be a double-edged sword, as VPNs are potential targets for attackers to gain unauthorised access to the company’s IT and OT network.

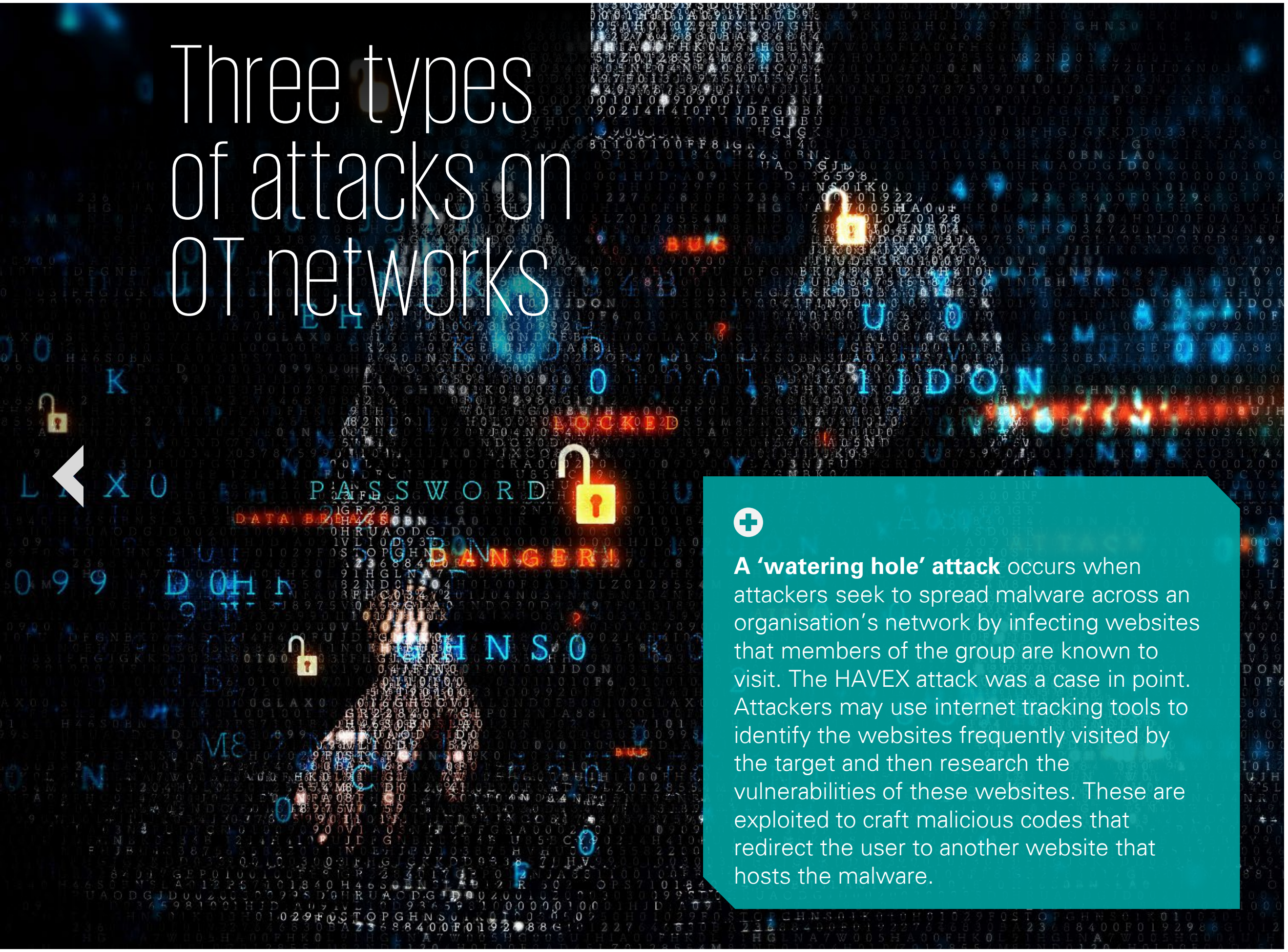
Cyberattacks on OT systems can have serious and highly damaging consequences, as attackers may incapacitate critical infrastructure such as water plants, fuel pipeline facilities and power grids. This explains why business leaders have identified cybersecurity risk as the greatest threat to their organisation’s growth over the next three years, according to KPMG’s 2021 CEO Outlook Pulse Survey.

Therefore, it becomes important to understand the nature and routes of attack on operating systems to build robust defences. Businesses need to understand how attackers are gathering intelligence on specific systems. Is it via open-source intelligence (OSINT) or other discovery methods? Are they reverse engineering protocols or developing customised tools? Have they tested them in a simulated environments before carrying out attacks?

This report examines the key challenges OT practitioners face and seeks to chart a clear roadmap for securing OT systems in a rapidly evolving threat landscape.

Eddie Toh
Partner, Cyber, Advisory
KPMG in Singapore

Three types of attacks on OT networks



A 'watering hole' attack occurs when attackers seek to spread malware across an organisation's network by infecting websites that members of the group are known to visit. The HAVEX attack was a case in point. Attackers may use internet tracking tools to identify the websites frequently visited by the target and then research the vulnerabilities of these websites. These are exploited to craft malicious codes that redirect the user to another website that hosts the malware.

Broadly, organisations today face three types of attacks: direct attacks, indirect attacks, and reconnaissance attacks. All of these attacks may expose vulnerabilities in crucial supply chains that could cripple an organisation's normal operations. In extreme situations, it could shut down a critical sector which many people depend on.

- **Direct attacks** are executed to inflict damage to a specific target OT system. Among the examples of hackers using remote connections to launch such attacks are the recent incidents at a power grid in Europe and a water plant in the US.

  Once systems are breached, attackers may insert malicious codes into the system causing it to malfunction by modifying its control logic. This is what happened when a malware dubbed Triton took remote control of a safety control workstation at an energy plant. Investigators found that a Safety Instrumentation Systems (SIS) engineering workstation (EWS) was the first to be compromised. Then, the EWS interacted directly with the SIS controllers using UDP protocol.

Four binaries were uploaded to the controllers – two embedded in a compiled Python script along with two other files targeting a specific SIS controller. This is how the SIS triggered a system shut down in this attack.

- **Indirect attacks** are also on the rise. They do not directly impact OT systems, but may still lead to serious consequences, such as disruption to services and damage to the environment, threats to process safety and human lives. Among the recent examples are ransomware attacks on a fuel pipeline in the US and on a university hospital in Europe.

  In both cases, hackers originally targeted IT systems, rather than OT networks, but operations were still brought to a standstill causing substantial damage. The gas pipeline attack was linked to a criminal group which specialises in crafting ransomware and selling it to affiliates for a cut, known as Ransomware-as-a-Service (RaaS). This breached the organisation's IT system through harvested credentials and deployed ransomware which was reported to have affected the company's billing systems by locking down endpoints and exfiltrating terabytes of confidential data. Consequently, the company had to shut down 5,500 miles of pipelines supplying while it investigated how deeply its systems had been infected. The outage may be compared with the fallout from natural disasters such as hurricanes that often force segments of pipelines and refineries to shut down for days or weeks.

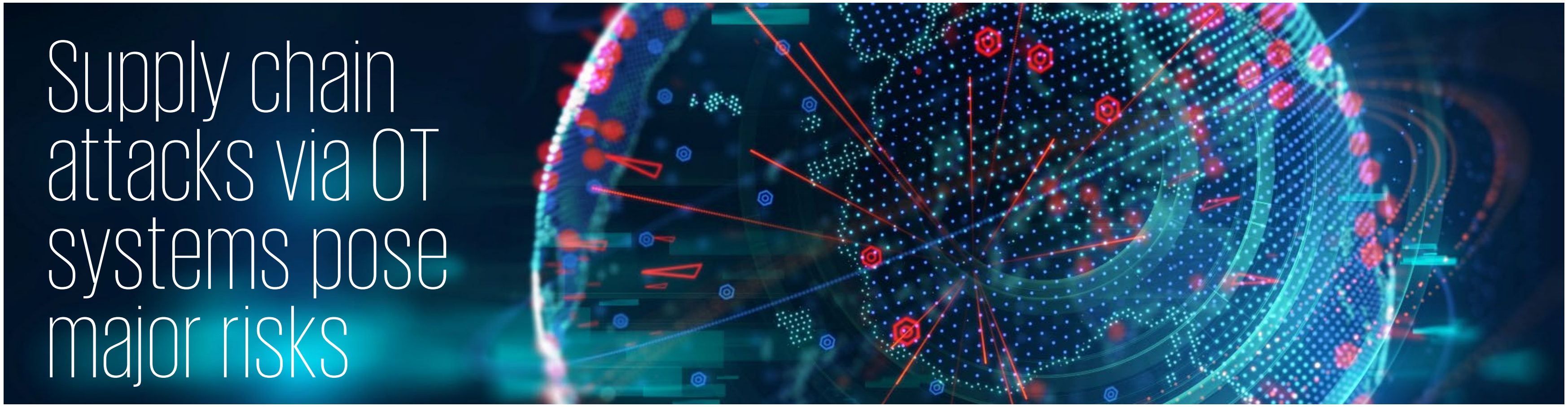
  The university hospital attack in Europe showed how human lives are also at stake. In this attack, a malware dubbed Doppel-Paymer gained access to the system through a software vulnerability. One patient seeking emergency treatment lost her life because the ambulance carrying her was turned away after the malware infected more than 30 endpoints at the hospital crippling normal operations. These examples reveal how vulnerable we are to indirect consequences from attacks on IT systems.

- **Reconnaissance attacks** do not lead to immediate disruptions. Attackers may lurk in an environment to gather information, exfiltrate sensitive data and perform cyberespionage.

  One of the well-known examples is the HAVEX attack, carried out by an advanced persistence threat (APT) group. This attack involved a remote access trojan (RAT), downloaded from OT vendor websites.

  The RAT then used Open Platform Communication (OPC) to scan for devices on ports commonly used by OT devices. The information that was collected was sent back to the attacker's Control and Command (C2) server.

Supply chain attacks via OT systems pose major risks



✚

Understanding how security architecture in OT networks are set up can help identify gaps that need to be filled and protect supply chains from cyberattacks.

As highlighted in the previous section, all three types of attacks may be exposed to supply chain vulnerabilities. To disrupt supply chains, attackers may choose to target different phases of the system life cycle from design, development, distribution to maintenance and disposal.

Supply chains are often targeted via malicious content disguised within reputed or trusted products. This method offers attackers a route to reach many targets. In one of the most well-known examples, the source code was injected with a malicious code just before the final build of the software patch.

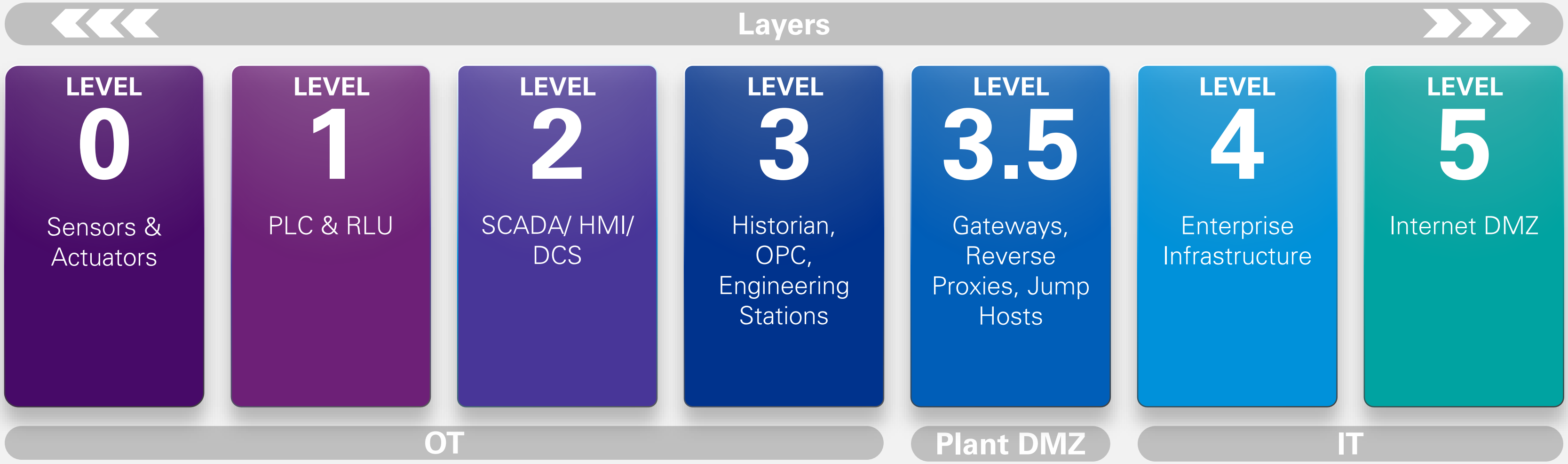
The infected patches hit more than 20,000 end users including government agencies and private organisations. By hijacking updates, undermining code signing and compromising open-source code, attackers may abuse trust in procured software and hardware.

More recently, a managed security provider (MSP) platform vendor was hit by an attack affecting more than 1000 companies including a major Scandinavian grocery chain.

Segmenting OT networks

As cyber threats rise in the turbulent wake of the COVID-19 pandemic, organisations are recognising the need to segment their networks to protect OT systems. While most OT systems have hardened perimeters with gateways, firewalls and diodes, many legacy OT systems are still unsegmented flat networks internally. This allows attackers to move laterally into other systems in the network after breaching initial entry points. Therefore, the traditional approach to address this issue is network segmentation. The Purdue Model and IEC 62443 Standards, depicted below, have been built to address security issues in industrial automation and control systems (IACS) and OT.

The Purdue Model



Layers

LEVEL 0 Sensors & Actuators

LEVEL 1 PLC & RLU

LEVEL 2 SCADA/ HMI/ DCS

LEVEL 3 Historian, OPC, Engineering Stations

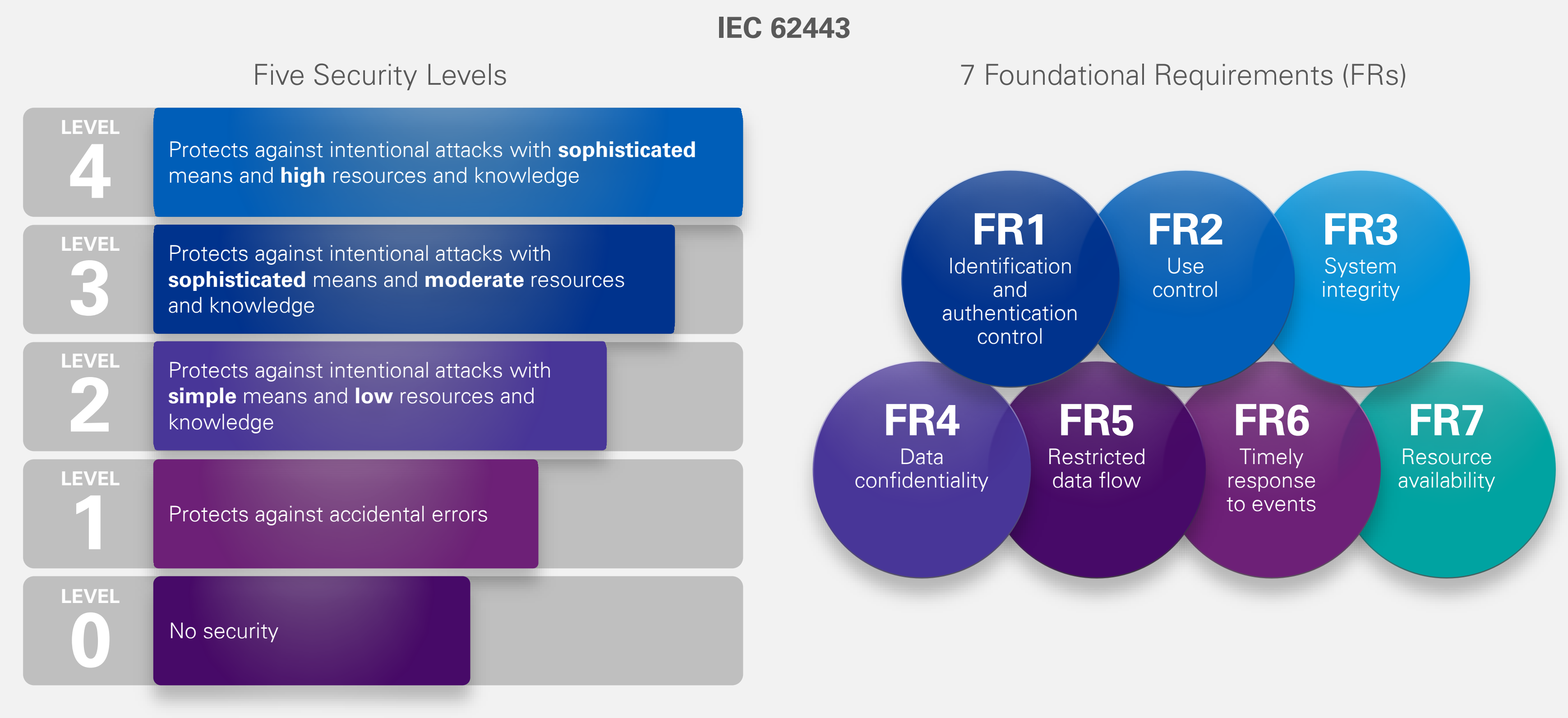
LEVEL 3.5 Gateways, Reverse Proxies, Jump Hosts

LEVEL 4 Enterprise Infrastructure

LEVEL 5 Internet DMZ

OT | Plant DMZ | IT

This model defines IACS into several levels – level 0 field devices, level 1 field controllers, level 2 system control and data acquisition (SCADA), level 3 plant local area network (LAN), level 3.5 plant de-militarised zone (DMZ), level 4 enterprise zone, level 5 enterprise DMZ. Each level should have its own layered defence or defence-in-depth



IEC 62443

Five Security Levels

LEVEL 4 – Protects against intentional attacks with **sophisticated** means and **high** resources and knowledge

LEVEL 3 – Protects against intentional attacks with **sophisticated** means and **moderate** resources and knowledge

LEVEL 2 – Protects against intentional attacks with **simple** means and **low** resources and knowledge

LEVEL 1 – Protects against accidental errors

LEVEL 0 – No security

7 Foundational Requirements (FRs)

- FR1 Identification and authentication control
- FR2 Use control
- FR3 System integrity
- FR4 Data confidentiality
- FR5 Restricted data flow
- FR6 Timely response to events
- FR7 Resource availability

Set by the International Electrotechnical Commission, this series of standards covers general guidance on securing OT systems, policy and procedures, system technology and design, as well as component requirements. IEC 62443 recommends that OT networks are segmented into zones and conduits and defines five Security Levels (SL) (0 to 4) with seven foundational requirements (FR), shown in the figure below. SLs are assigned by assessing FRs implemented in each zone and how well inter-zonal chokepoints are secured.

Shifting towards zero trust in OT

Even though the Purdue Model and IEC 62443 are both well-established frameworks, the concept of zero trust is gaining popularity. And for good reason, given the growing number of incidents in which attackers have abused the victims' trust in procured software and hardware.

A zero-trust security architecture is a relatively new model that assumes that authenticated identities or even the network itself may already be compromised — even if they aren't. This approach treats every user, device, and interaction as a potential threat, and as such, every single connection or condition needs to be continuously validated to ensure that it is legitimate. Zero trust is broadly built on the following tenets:

- **The distinction between trusted and untrusted zones is removed** since all zones are considered untrusted.
- All data sources and computing services are **considered as resources.**
- Any human user, application or device accessing resources must **be authenticated and authorised.**
- **Decisions on access are independent of locality in the network.** In other words, hosts sitting in the same zone do not inherently trust on another.
- There are **no zones and conduits**, only a control plane, which processes requests for access to protected resources, and a data plane, where everything else resides.
- **Never trust, always verify.**

The tenets of zero trust were originally conceived for enterprise. However, as OT evolves to be more interconnected and digital, some elements of the zero-trust model should be adopted in OT too.

Zero trust removes the burden of safeguarding passwords. Multifactor authentication ("what you have" and "who you are") is used, instead of "what you know" credentials.

What you need to know

In a zero-trust framework, role-based access control is practised, and access control matrices are created following the principle of least privilege, i.e. a user only has just enough rights to carry out his function. Furthermore, strict session management is implemented so that all sessions are immediately terminated once the user completes the necessary function; if a session is idle for too long, it is also terminated.

Encryption is an important consideration for zero trust in OT. But OT communication is traditionally unauthenticated, and protocols are unencrypted in transit. There is a great deal of potential to employ encryption in OT protocols like Secure Modbus, Open Platform Communication Unified Architecture (OPC UA), and Generic Object-Oriented Substation Event (GOOSE). These are described in IEC 62351, Power Systems Management and Associated Information Exchange – Data and Communications Security.

Zero trust avoids default policies and configurations. Therefore, historical user behavioural data and current user actions are sent for analysis to an analytics engine on the control plane. Confidence scores are provided against a baseline, and policies are then developed, deployed and enforced. This method is described in the US Department of Defense's Zero Trust Reference Architecture publication.

While perimeter defences like gateways and diodes are still important, there is less emphasis on technologies like VPNs, which are often the target of attackers. As part of the zero-trust approach, the entire network is micro-segmented to the application level, and a mechanism of whitelisting is implemented whereby some identified entities are allowed to access a particular privilege, service, mobility, or recognition. Meanwhile, next generation firewalls (NGFWs) carry out deep packet inspection (DPI) of North-South traffic, while East West traffic is monitored with high granularity.

Overcoming the challenges of migrating OT systems to zero trust

As zero trust is adopted in OT systems, manual implementation is seen as impractical because it is costly and time consuming. Capabilities like computing power and log storage capacity need to be designed so that monitoring, analytics, encryption, key management, and auditing can be automated to reduce overheads.

Some OT practitioners think that migration to zero trust architecture is just too costly as it requires organisations to tear down and rebuild legacy infrastructure. But we have a different view — this process doesn't need to be expensive. The US National Institute of Standards and Technology (NIST) special publication 800-207 on Zero Trust Architecture charts out a roadmap to implement zero trust in an OT system as a journey, rather than a wholesale replacement of infrastructure. It proposes the following steps:

1. Identify who are the subjects e.g. users, administrators in the system;
2. Identify objects e.g. assets, devices, services etc. in the system;
3. Identify key processes and evaluate risks associated with executing the process;
4. Identify a candidate process for zero trust architecting;
5. Formulate policies for the candidate process;
6. Initial deployment, monitoring and feedback; and
7. Expanding the zero-trust architecture.

Strengthening supply chain risk management

What we believe you should do about it

As discussed in the earlier sections, the rise of attacks on OT systems has exposed global vulnerabilities in supply chains. These attacks have also intensified the spotlight on the need for zero trust in cyber supply chain risk management (C-SCRM) for OT. In Singapore, the CSA is expected to publish its Critical Information Infrastructure (CII) Supply Chain Programme. At the heart of this programme are three guiding principles to manage supply chain cybersecurity risks, namely – assurance, transparency and accountability.

At the same time, it is important to understand the different kinds of risks at play. Supply chain risks can be broadly categorised into hardware risks, software risks and vendor risks. Key security controls to mitigate them include:

1. Understanding your inventory well. This involves creating a bill of materials for both hardware and software, and knowing each item’s function, source, and how to verify their integrity.
2. Practising security by design. Like the software design life cycle, this requires pre-production vulnerability and risk assessment, penetration testing and thorough code review.
3. Specifying cybersecurity requirements for vendors and products to fulfil as part of contract. Organisations should verify by reviewing certificates and providing for right to audit.

An increased focus on managing supply chain cybersecurity threats in OT networks has culminated in the development of a couple of well-known frameworks that aim to address these risks.

NIST publications on C-SCRM

The US NIST commissioned the NIST C-SCRM Project in 2008 to improve supply chain risk management among the industry. Among its major reports is NIST Special Publication (SP) 800-53, Security and Privacy Controls for Information Systems and Organizations.

NIST SP 800-53 lists the recommended 20 control families including access control, awareness and training, configuration management, as well as supply chain risk management. Within the supply chain risk management control family, there are 12 controls along with its control enhancements. This serves as an excellent reference for establishing a framework for organisational C-SCRM. What is even better is that related controls are linked to each supply chain control. For example, Supply Chain (SR) Control 10 - Inspection of Systems or Components, links to Awareness and Training (AT) Control 3 - Role Based Training, which ensures competency during inspection.

MITRE's Technical Report

Aside from NIST, organisations may also consider the approach described in MITRE's technical report titled, "Supply Chain Attack Framework and Attack Patterns" to address and guard against supply chain vulnerabilities.

The diagram on pg. 13 explains how users can zero in on specific types of supply chain attacks that can harm their systems.

Attack on Locations

According to this technical report, there are four types of supply chain attacks can occur - hardware, software, patch / firmware and system data / information.

Following the technical report, points where attacks can occur are mapped towards each vulnerable location - primary production (hardware/software); hardware/software integration; sub-contractor; prime contractor; program office.

Attacks on Linkages

After attacks on locations are mapped, points where attacks can occur are also mapped towards each vulnerable linkage - logistics (physical flow via processing, packaging and distribution); information and data flow (via networks and internet connectivity).

Product Lifecycle Phase Attacks

In addition, there are five phases of a product lifecycle that may be attacked - material solution analysis, technology development (TD), engineering and manufacturing development (EMD), production and deployment (P&D), and operations and support (O&S). Attacks are mapped to the phase where compromise is likely to be occur.

Cataloguing Possible Attacks

1. Attack ID (unique ID number) e.g. A1, A2, A3 etc.
2. Attack Point (supply chain location or linkage)
3. Phase Targeted (acquisition lifecycle phase)
4. Attack Type (malicious insertion of SW, HW, FW, or system information/data)
5. Attack Act (the "what")
6. Attack Vector (the "how")
7. Attack Origin (the "who")
8. Attack Goal (the "why")
9. Attack Impact (consequence if successful)
10. References (sources of information)
11. Threat (adversarial event directed at supply chain)
12. Vulnerabilities (exploitable weaknesses)

Analysing potential attacks

Mapping each attack against vulnerable locations and lifecycle phases allows controls to be implemented in order to reduce supply chain risks.

Use-Case Scenario Attacks for Consideration

Critical component targeted for malicious insertion	Phase targeted	Number of applicable attacks	Specific attacks																		
Hardware	TTD	5	A2		A6		A8										A29				A36
	EMD	13	A2	A5	A6	A7		A9	A10		A15	A22		A24			A29	A31	A33		A36
	P & D	12	A2	A5	A6	A7				A11	A15	A22		A24	A25		A29	A31	A33		
	O & S	10		A5	A6	A7			A10		A15		A23	A24		A28				A34	A36
Software	TTD	5					A13	A18				A27			A36	A38					
	EMD	15	A1	A3	A4	A5	A13	A18	A19		A26	A27	A32		A36	A38	A39	A40	A41		
	P & D	9		A3	A4	A5			A19		A26	A27	A32			A38	A39		A41		
	O & S	11		A3	A4	A5	A13			A21				A35	A36	A38	A39	A40	A41		
Firmware	TTD	1							A29												
	EMD	8	A4	A7	A10		A15	A20	A29	A33	A41										
	P & D	8	A4	A7		A12	A15	A20	A29	A33	A41										
	O & S	6	A4	A7	A10		A15	A20			A41										
Sys Info/Data	MSA	3	A14	A16	A17																
	TTD	4	A14	A16	A17	A18															
	EMD	3	A14			A18		A31													
	P & D	3					A30	A31	A37												
	O & S	2					A30		A37												

Example: Critical component focus is software

Review these supply chain attacks of malicious insertion for applicability

Use-case example: Consider attack A3

[Source: MITRE Technical Report on Supply Chain Attack Framework and Attack Patterns, by John F. Miller, 2013]

The future of OT security

OT threats are expected to increase in intensity and complexity, as organisations embrace new technologies. Some examples include data analytics and machine learning, distributed control systems (DCS) virtualisation, and SCADA as a service (SCADA hosted on cloud). Such virtual machines and cloud models represent workloads that also require zero trust security.

Meanwhile, quantum computing comes as a mixed blessing for OT systems. On one hand, it enhances system performance and speed, while on the other, it allows adversaries to crack traditional encryption with greater ease.

Finally, blockchain technology also represents a new frontier, giving OT practitioners a great deal of food for thought. While blockchain is still in the nascent stages of adoption in OT systems, there will likely be several new use cases going forward. For example, the ability of a blockchain ledger to remain unchanged holds promise for authentication of host-to-host transactions in OT systems.

Only time will tell how OT security will evolve, but what is clear is that businesses must be prepared to adapt quickly to stay ahead of ill-intentioned adversaries.

No matter where you are on your cyber security journey, KPMG in Singapore can help you reach your destination: a place of confidence in which you can operate without crippling disruption from a cyber security event – and at the budget you feel most comfortable with. Our highly experienced professionals will also help you work through strategy and governance, organisational transformation, cyber defense, and cyber response, among other areas.

From penetration testing and privacy strategy to access management and cultural change, KPMG in Singapore takes a hands-on approach to helping you every step of the way.

Contact us

Eddie Toh
Partner, Cyber, Advisory
KPMG in Singapore
E: eddietoh@kpmg.com.sg
T: +65 6213 3028

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.