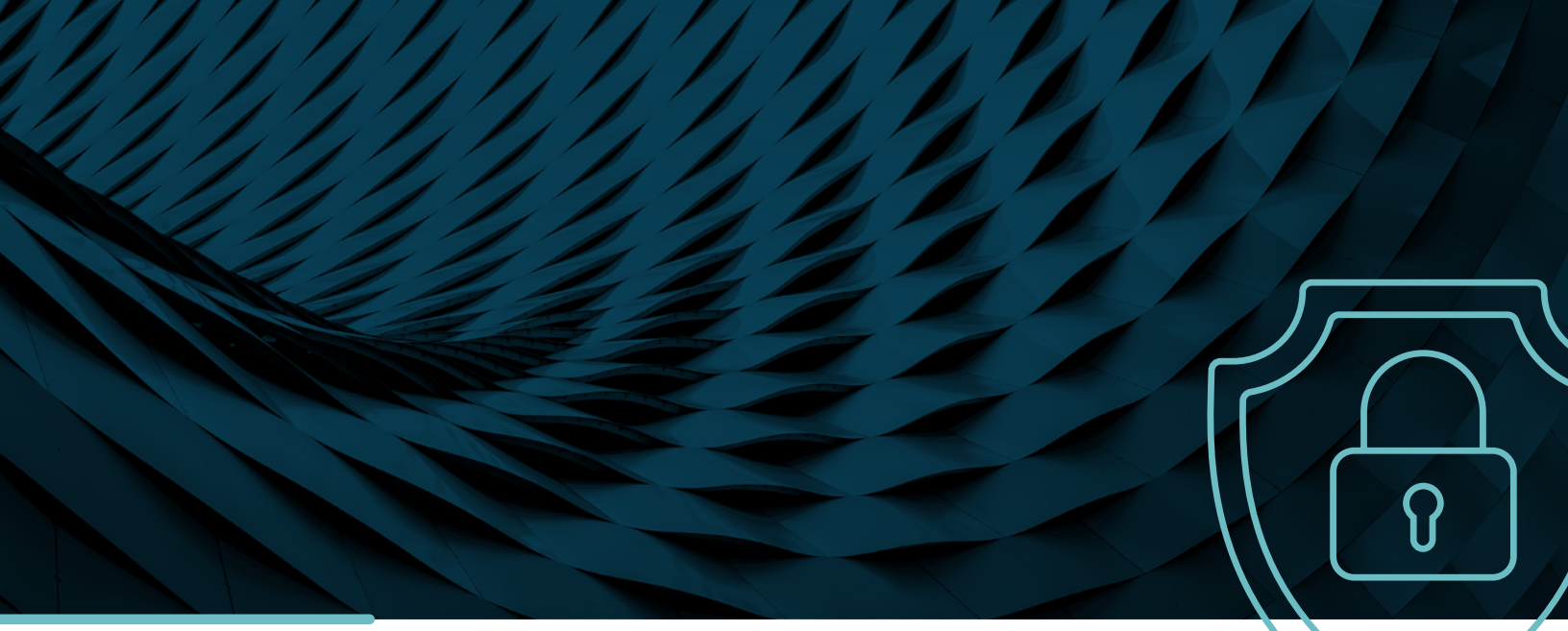
CISO Guide to **Operational Technology (OT) Security**

By Dr. Bill Anderson

Managing Partner at MarketR



Cybersecurity INSIDERS



The State of Security for Operational Technology

Industry 4.0 designs and new smart Internet of Things (IoT) devices promise to allow all the components of industrial production to be seamlessly interconnected, increasing visibility, productivity and efficiency. OT systems used to be effectively air-gapped from the world, but to achieve these new capabilities operational technology (OT) is being connected with information technology (IT) systems.

While integrating IT and OT environments offers substantial business benefits, it also inadvertently expands the attack surface of the highly-critical OT environment. Without adequate security measures, interconnecting IT and OT environments can prompt adversaries to exploit an IT access point or cloud vulnerability to break into internet-facing OT/Industrial Control Systems (ICS).

OT extends beyond the usual network perimeter boundaries into many types of environments that might include robots on the manufacturing line, in smart commercial buildings, traffic intersections, agriculture fields, hospitals or even space. Many of these environments present unique challenges for managing security, due to the difficulty of securely communicating with the device in the field.

The Risks Ahead

Perimeter-based security controls such as firewalls are no longer enough to protect OT systems against sophisticated attacks. With manufacturing, electric utilities, and oil and gas companies around the world digitizing their infrastructure we are seeing OT exploits emerging as a significant threat to business today. Operations rely on increasingly complex devices made up of bundles of hardware, software and firmware, and it's becoming increasingly difficult to ensure that all these components are secure and can be trusted.

Industrial cybersecurity threats are becoming increasingly common and can have a significant financial and reputational impact on businesses. Trend Micro's 2022 Industrial Cybersecurity report found a **tangible financial, and reputational impact on organizations.** In the past 12 months 72% of industrial customers were disrupted at least 6 times, at an **average financial cost of $2.8 million per incident.**

Customer Demands

Industrial customers are demanding security solutions from their OT vendors. The top factors leading to customer action are:

42% Security audits or penetration tests reveal vulnerabilities

30% Experience with a recent breach leading to a board mandate to prevent future incidents

29% Requests from customers and partners

22% Incidents at competitor sites

Hardware Root of Trust

Many semiconductor vendors offer variants of their products with hardware security options. The most capable include an isolated cryptographic processing engine, and secure key storage. These can be found integrated into a system on chip (SoC) or as a standalone security module. Better known examples include the Trusted Platform Module (TPM) found in most laptops, ARM Trustzone, and Secure Element solutions found in most smartphones. Companies like RAMBUS produce a wide variety of excellent chips for these tasks.

Finding the right option for an OT device requires understanding the threat environment where the device will operate and the value of the assets at risk, then factoring in unit cost, development and maintenance expenses. It makes sense to have security expert support through the design phase at least.

Attacks on OT Systems

Cybersecurity attacks can be highly creative, sophisticated, and targeted to the weaknesses of a specific system. Successful attacks chain a number of small weaknesses together to build the access needed to exploit the system.

One example of a particularly strong and effective attack was the STUXNET "worm" reportedly developed by the U.S. and Israeli intelligence services to disrupt Iranian nuclear weapon development.

It was specifically intended to destroy centrifuges used to enrich uranium. This was a hard target, but it was achieved through exploits of a series of Windows vulnerabilities and knowledge of the embedded software running on the programmable logic controllers for the centrifuges. As a result, over 2000 expensive centrifuges were rendered inoperable and the Iranian program was set back over 2 years.



What is Machine Identity?

A machine identity allows you to confirm some basic facts about the device without it being physically present. A machine identity would typically tell you the manufacturer, make, model, firmware version, a unique serial number for the device. Much more information may be included, including the assigned location and current owner.

The trouble is, all this information can be spoofed by an attacker. False information could be injected to data in transit, or be copied and stored in a counterfeit device.

How can any identity be trusted if the data can be easily spoofed? The solution comes from modern cryptography, which enables a digital signature. Trustworthy devices contain a unique private key that is locked into the device and protected. This allows a device to digitally sign data in a way that allows other parties to verify that it could only have come from that device. Similarly, the manufacturer signs and publishes the machine identity data so that other parties can compare and confirm they are talking to the legitimate device.











If a strategic and protected target like this can be breached, so can other OT systems. OT attacks generally fall into these categories:

Protocol Attacks:

In OT environments, devices communicate using industrial control system (ICS) protocols which are often not designed with security in mind. Attackers can exploit weaknesses in these protocols to manipulate the communication between devices or control units, leading to operational disruptions or malfunctions.

Firmware Modification:

Many OT devices have firmware that is rarely updated. This can make them susceptible to attacks where the firmware is modified to include malicious code. Once infected, these devices can cause havoc in the OT environment, from subtle changes in process control to complete shutdowns.

Device-Level Attacks:

Attackers may physically tamper with devices, alter configurations, or interfere with readings to disrupt normal operations. For example, tampering with a sensor's reporting could result in unsafe conditions in a manufacturing process.

Input/Output Spoofing:

By gaining access to the control network, an attacker can mimic or "spoof" regular commands, leading to equipment being turned on or off, or safety measures being bypassed. This can be particularly damaging in environments where precision and timing are critical, like in chemical plants or power stations.

Unauthorized Access Through Maintenance Ports:

Many OT systems have maintenance ports that are intended for troubleshooting or software updates. However, these can often be left open and unprotected, allowing an attacker to gain access to the system.

We see combinations of these attack vectors used in effective attacks, including big ones like STUXNET. The impacts of attacks are significant, including disruptions to operational processes, safety incidents, environmental damage, and financial loss due to downtime or damaged equipment. In many industries, such as utilities or manufacturing, these impacts can also have broader societal effects, such as power outages or pollution incidents.

Preventing OT System Attacks

Not every facility will be subject to the combined efforts of the best nation-state attackers, but almost every OT system can and will be targeted by some adversary. Safety comes from reducing the weaknesses an attacker can use for a successful exploit. If you can take away just one link in the attack chain, you can keep OT systems safe.

OT OEMs need to respond to customer needs for better security, while simultaneously delivering competitively priced solutions in a reasonable timeframe. Given the threat environment, OT systems need a security approach that is highly flexible, time-tested, and standardized for maximum security and interoperability.

Automotive Systems, a Cautionary Tale

Automotive systems have a distinct challenge resulting from OEMs' long-established practice of farming out significant parts of their vehicles to a large ecosystem of parts suppliers. The auto companies combine hundreds of sub-systems to make a finished product.

In a recent interview Ford CEO Jim Farley addressed the issue of software interactions and compatibility in their vehicles:

"We farmed out all the modules that control the vehicles to our suppliers, because we can bid them against each other [for price]...We have about 150 modules with semiconductors all through the car. The problem is that the software is written by 150 different companies. And they don't talk to each other.

150 different modules represents about 149 opportunities for attackers to find exposed features, improperly authenticated or unsecured communications, read/write access to critical data, and potential for injecting new functionality. Given that vehicles are increasingly connected to open data networks (over 5G), the opportunities for attackers are significant.

The automotive example is similar to what you may see in a large operational technology environment where multiple generations of OT equipment is connected and stitched together with everything from ancient (dumb) controllers to the latest in internet connectivity. You can bet that adversaries have already been mapping these systems, finding the gaps, access points, incompatibilities and weaknesses in substantial industrial operations.

These goals can be met with three key security capabilities:

01 Authentication for secure network access.

OT devices mostly connect to servers to report data, receive control signals, and updates. It's important to be able to uniquely identify OT devices before communicating with them. OT systems should ideally start with identity-based security in every OT node. The system can thereby recognize trusted devices and exclude imposters. This reduces the attack surface available. Each node can enforce basic protection by refusing to interact with potentially dangerous outside systems.

Authentication means every device and server in a customer system can be properly validated every time they request network access.

02 Secure machine-to-machine communications.

OT systems are largely focused on generating actionable data and sending it to where it can be put to use. OT data often has proprietary value or is subject to regulations requiring that it be protected, but the networks available to OT devices can not be trusted to be secure. OT systems must provide their own encryption solution to protect their data. Designers need to safeguard data by providing end-to-end data encryption. This helps ensure the data stored in OT systems and the communication between IT and OT systems remain insulated from attacks.

Encrypting communications also helps meet compliance requirements. Regulatory bodies, such as the NERC, FERC, NIST, and U.S. President Biden's recent executive order on cybersecurity all require encryption.

There are several well-established security protocols, including TLS and IPSec, that if properly implemented ensure data-in-transit is reliable and confidential. Proprietary security protocols should be highly discouraged as they are much more likely to contain unexpected weaknesses than openly-reviewed and standardized systems.

03 Data and Software integrity.

Unreliable data or control signals could render the OT device useless, or worse, a liability to the customer. OT systems must be designed to prevent unauthorized changes to code or data. Ensuring the firmware in OT systems is safe and free of corruption is crucial to avoid software supply chain attacks. OT vendors need to secure their firmware to help organizations verify the identity of the supplier and confirm that the received firmware hasn't been altered since its signing.

It can be a challenge to find and implement technology needed for OT data integrity at an appropriate price point. Ideally, every OT device would include a hardware root-of-trust - a secure computing and secure storage space protected against physical and electronic tampering. In practice, it can be enough to design each OT device to have just enough secure storage to hold the trusted root public key from the manufacturer (for validating incoming communications and commands) and to hold a secret private key for the device (for signing outgoing communications).

OT Security Design Challenges

OT devices deployments are very different from traditional IT systems. The OT environment characteristics make security harder and must be factored into the design. For example, here are a few of the details that must be addressed:



OT Environments can be **risky and unsupervised:** physically accessible to public, but also potentially remote and inaccessible to operators. Devices must designed to be remotely accessible and still secure.



Connectivity: Devices might use one or more of Ethernet, Bluetooth, WiFi, Cellular, NFC, LoRa, and other short range protocols, which may not be always available. Security designs must account for sporadically disconnected endpoints.



Computation and power capabilities can be very limited on IoT devices due to cost constraints and operating environments. Security design choices must account for constrained environments.



Machine to Machine paradigm. When there is never a human in the loop, provisioning, updating, renewal and recovery operations must be made automatic. Setup schemes that use usernames and passwords, or send out-of-band codes by SMS are just not appropriate.



Availability and reliability are more important because no humans are there to troubleshoot. These systems must be able to resolve most issues without human intervention.



About the Author

Dr. Bill Anderson is managing partner at MarketR *(marketr.services)*, a consulting firm that helps cybersecurity product companies solve product management, marketing, strategy and sales problems. Bill is a security industry expert with experience founding, operating and funding a series of high-growth cybersecurity companies.