Integrated security mechanisms

Increasing networking of devices with the Internet makes the devices vulnerable and poses a risk to operational reliability. Analog Devices explains how to achieve data security at the edge of the IIoT network.

A spoof masquerades as a known node to a gateway (Source: Analog Devices)

The complete article is published in the September issue of the CAN Newsletter magazine 2020. This is just an excerpt.

IoT (Internet of Things) sys- tem attacks are making headlines and continue to showcase the security vulnerabilities of networks, edge nodes, and gateways. A recent Mirai botnet infected over 2,5 million IoT nodes by logging into devices running telnet servers in which the default password had not been changed. [1] Mirai later was able to invoke a denial of service for servers that disrupted Internet access for a large portion of the world. The Reaper Botnet attacked over a million IoT devices by exploiting software vulnerabilities and infecting them. An Internet-connected fish tank provided the entry point into a casino's net- work, leading to the theft of 10 GiB of data. Smart televisions have been exploited and used for espionage and surveillance.

Embedded sensor systems are just starting to be connected and exposed to the Internet. As part of the Industrial Internet of Things (IIoT), these sensors lack the past two decades of evolution that web servers have had in this hostile environment. Hence, the industry is witnessing many of the attacks commonly seen in the 1990s and earlier in these systems. The lifecycle of an IIoT system is often much longer than one in traditional computing. Some devices may continue operating for decades after they are deployed, and with unknown maintenance schedules.

While servers and PCs are complex enough to allow for security provisions, IIoT nodes are usually low in power consumption and processing power. This leaves a small power budget for intentional security measures. Security is largely a tradeoff, as there are development costs involved. Although IIoT may have higher costs than consumer IoT, it will still face challenges in cost for scalability. If security is ignored there are hidden impacts that will arise after products are deployed, and these costs will eventually need to be addressed.

Sensors and actuators allow IIoT devices to inter- act with the physical world. Cyber attacks have been mostly limited to the loss of data, although an IIoT hack allows potential entry into the physical world easier than it has in the past. Attacks now have the potential to cause physical harm. This is even more significant in IIoT, where a failure could potentially shut down or destroy a multimillion-dollar industrial process or lead to a life-threatening situation.

A connected world

IIoT devices are generally connected to some network and often the Internet. This connectivity is what exposes them the most to an attack. Similar to the realm of epidemiology, infection is spread by contact with other machines. Attack vectors exist where systems interact with the outside world. Attackers are able to interact with systems strictly due to their connected access. The first system design security question to be asked is: "Does the device really need to be connected to a network?" Connecting it to a network dramatically increases the security risk.

The best way to secure a system is to prevent it from connecting to a network or limiting it to a closed net- work. Many IIoT devices are connected to networks solely because they can be without much reason. Does the benefit of having the device connected to a network outweigh the security risks associated with it? In addition, any other legacy systems that interact with the Internet facing system can also be put at risk.

In many cases, an otherwise secure network and secure nodes must also interoperate with a legacy incumbent network that could be far inferior in its own security. This poses a new problem in that the weakest security risk could be outside the influence of the IIoT system. In that case, the IIoT system also needs to protect itself from within the network.

Security considerations at the node [2]:

- Confidentiality—protection from data disclosure to unauthorized people, such as from a spoof attack
- Authentication—use of digital certificates to validate the identity between two machines
- Secure boot—ROM bootloader storage validates authenticity of second-stage bootloader
- Secure firmware updates—only authorized code from the manufacturer is permitted
- Authorization—only authentic nodes should be able to gain network access
- Integrity—protecting data from being altered
- Accounting—proper accounting of data, node counts, and timestamps can help prevent unwanted access to IIoT networks
- Secure communication—encrypted protocols that can reside on a low power node
- Availability—ensuring users have access when they need it
- Nonrepudiation—assurance that authentic communication requests cannot be denied
- Reliability—even in harsh electrical environments, access needs to be reliable

Isolation

Isolating systems from each other can reduce the attack surface and limit the spread of malware. Isolate systems that do not require network connectivity from systems that are exposed to networks. Consider setting up a separate air-gapped or tightly monitored network that is separated from other networks for high risk systems. Ideally, critical systems should be completely isolated from the outside world [3].

The infotainment system of a connected car can expose the vehicle to many new attack vectors not previously seen before. The main engine control unit (ECU) has nothing to do with the infotainment system and there should be no way to interact with it through the infotainment system. Though there are typically two separate CAN net- works in vehicles separating the most critical systems from the rest, they are still connected together in some way. It is still possible to compromise one and gain control of the other. If there is total isolation between these networks, the risk of compromise would be reduced from potentially life threatening to something far less serious.

Many IIoT systems connect to a cloud server that collects and processes information sent to it by the device and also manages the device. As the number of devices scales to large numbers, the cloud can have difficulty keeping up with all of them. Many systems are moving processing out to the edge on the IIoT devices to reduce the amount of traffic to the cloud.

We often think of data as an asset. Data is mined and sold to find hidden patterns in large data sets. However, the bulk of collected data is usually not very useful, though it may be useful to an attacker. Sensitive data creates a target for attackers and creates a liability. Collected data should be filtered down to only what is needed, and the rest should be deleted as soon as possible. This not only improves security, but also the utility of the collected data.

Various types of malware that can potentially infect an IIoT system (Source: Analog Devices)

It is important to identify potentially sensitive information and eliminate or limit its collection. Processing data at the edge can reduce the amount of data sent and exposed to the cloud. The more locations data is sent, the more difficult it is to keep it confidential. Each new node is another potential compromise where data can be leaked. The attack surface can grow exponentially.

Keeping sensitive data contained at the edge can limit the attack surface specifically on confidential data. If it is confined to one edge node, it is less likely to be stolen. A parking occupancy sensor that detects and only reports the presence of a vehicle through a binary signal after image processing will not stream video. It eliminates the large amount of unnecessary data contained in an image. This reduces the burden on the receiving server so that it cannot be reused maliciously for surveillance.

Similar to consumer IoT systems, industrial IoT systems also have proprietary and confidential information that must be maintained:

- Proprietary algorithms
- Embedded firmware
- Customer information
- Financial information
- Asset location
- Equipment usage patterns
- Competitive intelligence
- Access to a larger network

Some IIoT devices still lack the power and performance to be edge-based. Another topology emerging, the fog model, is a hybrid between cloud- and edge-based systems. In the fog model, the edge nodes first connect to a gateway that receives data and does some processing before sending it to the cloud. There may be one gate- way for many IIoT devices. The gateway does not need to operate on battery power, can afford a much higher bud- get in processing power, and costs more than constrained IIoT devices.

The fog has risen more from scalability issues, but could also come to play a role in security. The gateway device could help protect vulnerable edge nodes that may be too constrained to provide security on their own, but it may be better to provide some level of protection instead of none. The gateway can be used to help manage all the nodes underneath it instead of managing each individual node directly. The fog model can also allow for incident response in IIoT while avoiding disruption of service. For example, security may respond by interacting with the gateway instead of shutting down a mission critical manufacturing line.

Among the greatest challenges in IIoT is the deployment and management of large numbers of devices. Wide reaching IIoT systems are notoriously difficult to set up and configure. With the long lifecycle of IIoT, systems may be deployed by one team and still be operational years later when yet a different team supports it.

IIoT systems are often insecure with weak authentication mechanisms by default. As seen with the Mirai botnet, most users never log into IIoT devices to configure them. They may even be unaware that they are supposed to be configured. Most IIoT users assume things just work out of the box. Systems must be made secure by default. A system expectation should be set that the user may never configure the device other than the default. Weak default passwords are a common mistake.

A Man-in-the-middle attack inserts a malicious access point between a node and a gateway (Source: Analog Devices)

Network security

While the edge receives most of the focus in IIoT, it is important to not neglect the cloud or the server side of a sys- tem. Test for common server side vulnerabilities such as cross-site scripting, SQL injection, and cross-site request forgeries, and review APIs for vulnerabilities ensure that software running on the server is patched promptly.

Data in transit across the network needs to be secured, or it could be intercepted and modified maliciously. Secure cryptographic protocols such as TLS or SSH are used to protect data in transit. Data should ideally beend-to-endprotected.

The perimeter boundary of an IIoT network can often be blurry. IIoT sensor nodes often spatially reside on the periphery of their network. However, they also provide an easy portal into a larger industrial network through a fixed gateway [4]. Proper authentication of these devices to the help prevent traffic from being tampered by a malicious third party.

Securing network data traffic involves the use of a secure communications protocol. The best practices should be to use standard protocols that are known to be secure. Security on an Ethernet LAN can be provided using IEEE 802.1AE Macsec. Wireless LANs tend to be a higher risk since they are more accessible and ubiquitous. WPA2 provides security for IEEE 802.11 wireless networks. The low power IEEE 802.15.4 standard, often used within wireless IIoT solutions, offers its own suite of security protocols. However, these are layer-2 protocols used on the data link layer and only secure traffic on the LAN.

Securing traffic that needs to be routed outside the LAN, for example over the Internet, requires higher layer protocols that provide end-to-end security. TLS (transport layer security) is commonly used to secure Internet traffic and provides end-to-end security. While TLS uses TCP (transmission control protocol) and many IoT devices communicate using UDP (user datagram protocol), there is DTLS (datagram transport layer security), which works over UDP. While IoT devices are constrained in power and memory, it is possible to implement TLS for most constrained applications with minimal effort. For even more tightly constrained devices, there is currently a new protocol, constrained application protocol (CoAP) in development by the IETF.

Endpoint security

While securing data in transit is important and necessary, attacks are more often targeted at the endpoints. Network facing interfaces need to be hardened against vulnerabilities. One approach to IIoT security is to build protection directly into the sensor node device. This provides a first critical security layer, as the devices are no longer dependent on the corporate firewall for their sole protection. This can be especially critical for mobile corporate devices and IIoT sensors that are deployed in remote locations.

A security solution for IIoT devices must provide protection against a wide range of cyber attacks. It must ensure that the device firmware has not been tampered with. Additionally, it hast to be able to secure the data stored within the device, be able to secure inbound and outbound communications, and it must be able to detect and report any attempted cyber attacks [5]. This can only be achieved by including security in the early stages of design.

There can never be a one-size-fits-all security solution for embedded devices. Solutions are available that provide a general framework for OEMs (original equipment manufacturers). However, a complete security framework must consider the core capabilities required to protect specific devices, net- works, and entire systems. There must be also the flexibility to customize a solution to any specific requirements, while also ensuring that critical security capabilities are included.

In medicine, sterilization of surgical tools is essential to allow their reuse while preventing the spread of disease. The autoclave is the gold standard for sterilization. It quickly sterilizes instruments with superheated steam at high pressure. It obliterates all bacteria and returns the instruments to a known good state. This allows a surgeon to use a scalpel for surgery and safely reuse the scalpel after sterilizing it.

If you would like to read the full article you can download it free-of-charge or you download the entire magazine.

cw