FORTINET

WHITE PAPER

Cybersecurity Considerations in IoT Ecosystems and Services

Executive Summary

Organizations are heavily investing in the Internet of Things (IoT), which has a growth outlook for 2023 of 18.5% to $238 billion worldwide.[1] To reap the potential benefits of IoT, businesses rely on an entire ecosystem of vendors and solutions to cover everything from the IoT devices' hardware and software to connectivity, data storage and analysis, and more. IoT is fast becoming a complex ecosystem that is difficult to realize, maintain, and manage.

Telecommunication service providers (Telcos) play an increasingly important role in providing IoT ecosystem components, from devices to IoT ecosystems, IoT applications, and related services.

The importance of a secure IoT solution cannot be overestimated. Security is often considered to be the factor most likely to inhibit both the development of IoT services as well as their adoption. The potential impact of a successful cyberattack on an IoT ecosystem could cause critical services and industries to fail and even physical danger to individuals and the environment. IoT solution providers must provide IoT services and capabilities that are secure by design.

IoT Security Needs

Internet-of-Things solutions encompass many layers, including the devices themselves, but also on-premises gateways, mobile and fixed access networks, service platforms, application servers, and internet access gateways. Attacks come in many forms, and any of these components could be a target itself, or a stepping stone to a higher-valued target. Internet-of-Things security must be a multilayered solution that encompasses everything from the initial boot of the device to distributed denial-of-service (DDoS) protection at the network edge.

A significant hurdle in protecting IoT environments is having visibility of devices, applications, and traffic. This is the basis for any anomaly detection but also allows teams to verify that all is well in the network. Visibility can be best described in two parts:

- An inventory of the devices themselves, including vendor, device model, and firmware version.
- Details of the protocols and applications being used by each device. This can be delivered via application control capabilities and should include support of industrial protocols for Industrial-IoT (IIoT) applications. If device data is being encrypted, inline decryption should be performed (if this is possible) to verify the device data.

Internet-of-Things cybersecurity solutions must be able to detect signs of an attack and act immediately. This includes two major components: the IoT device itself and the IoT platform.

If an attacker does manage to gain control over a device, there are several possible actions that could be taken to cause disruption or denial of service:

- **Disable the IoT device**: This may be considered a simple denial-of-service (DoS) or could also be more sinister if the device is part of a physical process.
- **Destroy the device**: Via increased battery usage, for example.
- **Use the device to move laterally in the network**: A device may be used as a launch point, having potential access to other devices, the IoT platform, and other internal resources.
- **Recruit the device into a botnet**: The effectiveness of IoT botnets was exemplified in 2017 with Mirai, where up to 2,000,000 IoT devices were used to stage the largest-ever recorded DDoS attack.

Device Protection

The IoT devices themselves may be attacked. Generally, they will have limited connectivity and communicate with a small number of destinations (the IoT platform and maybe some application servers providing other services, such as firmware upgrades or data storage). This means that the attack possibilities are limited. But, it should always be assumed that the IoT platform or any application servers may become compromised and an attack could be launched from inside the local network. Such attacks may consist of:

Malware: Expected to grow as threat actors realize better return on investment (ROI) for choosing to attack IoT.

Exploits: Some IoT devices have limited functionality, and consequently the probability of vulnerabilities is reduced. Internet-of-Things device functionality is often custom developed, which may introduce bugs that wouldn't be present in general-purpose components. Also, the sheer breadth of device types means that an agricultural soil monitor must be considered very differently from an autonomous vehicle, for example, even though they may both be labeled IoT. No matter what the device, exploits must be expected, and protection put in place.

DoS: If traffic can be sent to a device by an attacker, it may be possible to conduct a DoS attack, especially for constrained devices.

Protecting the IoT Platform

The IoT platform is the critical heart of any IoT service, and in larger networks may be implemented as a hierarchy of platforms. All signaling and data will normally pass through one or more platform nodes, so protecting them against attack is imperative. The common types of attacks are:

- **Vulnerability exploits** originating from software vulnerabilities
- **Scanning and exploiting unused services**, resulting from exposed unused services or ports
- **Denial of Service** via externally facing interfaces, or from the IoT devices themselves
- **Hidden attacks** caused by a compromised IoT device using an encrypted connection to hide malicious traffic

Securing IoT Ecosystems and Services with Fortinet

Telcos must embrace security as part of their IoT solutions and services to meet three main objectives:

1. Secure the entire IoT ecosystem to ensure service continuity

2. Deliver IoT security service-level agreements (SLAs) to encourage IoT services adoption and acceptance

3. Deliver revenue-generating IoT cybersecurity services

Fortinet IoT Security capabilities are delivered via the most comprehensive range of network security products in the industry, interconnected, and integrated with the Fortinet Security Fabric platform to deliver end-to-end IoT ecosystem security. Fortinet IoT Security capabilities are delivered mainly via:

- FortiGate Next-Generation Firewalls (NGFWs)
- FortiWeb application firewalls (WAFs)
- FortiGuard Labs IoT Threat Intelligence Services
- Security operations center (SOC) tools for early detection, response, and automation (FortiAnalyzer, FortiSIEM, FortiSOAR, FortiEDR, and more)

FortiGate segmentation and stateful firewalling

In many cases, the traffic patterns of an IoT device are very predictable, and a FortiGate stateful firewall can block any traffic that is addressed to nonauthorized destinations, as well as raise an alert that the device is behaving abnormally. In a typical IT environment, traffic to unauthorized destinations may be common due to many reasons, and typically such communications would simply be dropped. But in IoT and other machine-to-machine networks, such communications are usually a sign of misconfiguration or compromise. For this reason, specific negative rules should be configured with appropriate action to ensure that an alert is generated, or automatic remediation is triggered.

FortiGate Intrusion Prevention

The FortiGate Intrusion Prevention Service is designed to detect and block a wide range of different IoT attacks, including:

- **Exploits**: This includes any attack on a vulnerability and will typically be used either to cause a DoS (by causing crashes or extra work within the software) or local code execution that often results in a second-stage attack, such as transferring a malicious executable.
- **Scanning attacks**: These include looking for open Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports, or looking for known software or protocol versions. Usually, the goal of reconnaissance attacks is to identify vulnerable targets or to identify high-value targets.

- **Fuzzing attacks**: This is another method of finding vulnerabilities. It is usually done locally in a controlled environment but can be used as a blunt-instrument attack on a live network. Examples include deliberate protocol anomalies or the use of extremely long fields, or invalid or unusual data. All of these techniques are designed to trigger programming errors. The goal is to find vulnerabilities or simply to cause disruption.

These attack types and more are covered by the FortiGate Intrusion Prevention System (IPS) function, which contains more than 30,000 rules, including an optional industrial package. Rule packages are automatically updated daily to ensure that protection is constantly up to date.

Fortinet IPS also can define rate-based rules, and because many IoT devices have a predictable packet rate, this can be used to detect unusual activity, possibly caused by malfunction or compromise, and remove such devices from the network. There is a general trend in all areas of networking toward data encryption, and this is also true for IoT, where data is often private. Transport layer security (TLS) is most often used here, and IPS can perform TLS inspection to allow attacks to be detected over such secure links.

FortiGate Application and Protocol Control

The Application Control feature can be used to monitor or limit the protocols that can be used by the IoT device. Any unauthorized protocols can generate an alert and optionally be blocked. Application definitions include more than 4,000 application rules in 24 categories. All commonly used IoT protocols such as MQTT, AMQP, HTTP, and CoAP are covered. As for IPS, TLS inspection can be used with the appropriate configuration. A wide range of industrial protocols is also available for IIoT solutions.

FortiGate Antivirus

Fortinet has an industry-proven antivirus solution underpinned by FortiGuard Labs research and artificial intelligence (AI)-based processing. In conjunction with intrusion prevention, most malicious files will never make it to their target. Antivirus is important today mainly for the IoT infrastructure, such as the platform or web servers. But researchers anticipate that malware attacking the devices themselves—such as in the case of the Mirai IoT malware, perhaps the most famous recent example—will become more prevalent in the years to come. FortiGuard Labs has almost 20 years of experience defending against malware of all types, and even though device-targeted malware is not common today, the needed research is already underway to ensure that protection of the highest quality will be ready.

FortiGate Anti-Botnet

Any botnet activity, whether detected by destination address, domain, or protocol, can generate an alert and be blocked. Additionally, connections to other known bad destinations as detected by the FortiGuard Indicators of Compromise Service can generate a compromised alert. FortiGuard Labs maintains an updated list of known botnet destination address/port combinations that are checked against all outgoing sessions. Botnets that use fast-flux domains (in which a domain continually changes its IP address mapping) can be checked against the domain itself by intercepting and checking the Domain Name System (DNS) request. Finally, even if the destination address and domain are unknown, many botnets can be detected by their command-and-control protocol. By using these three methods in parallel, Fortinet ensures the best chance of detecting botnet-infected devices.

Application-level protection with FortiWeb

Web applications are the target for data and information from IoT devices and platforms. They can control the devices and their behavior and be used as an entry point to the entire IoT platform and ecosystem. FortiWeb provides machine learning (ML)-powered web applications protection that includes anomaly detection, bot mitigation, suspicious URL and data-type patterns, application vulnerabilities, and more.

API protection with FortiWeb

Application programming interfaces (APIs) are used in multiple areas in IoT networks. The interactions between devices and IoT platforms are done via APIs, usually involving protocols, such as MQTT, HTTP, and CoAP, and using either JSON or XML as data encoding, with binary encodings, such as CBOR used for high-compression, low-bandwidth environments. APIs are also used to communicate between applications and the IoT platform, usually using HTTP. Fortinet has a very strong API protection function in FortiWeb, allowing a wide range of constraints to be defined, from simple rules such as maximum header and field lengths, all the way to schema validation and enforcement, focused on HTTP with JSON or XML. Both generic attacks and those focused on attacking representational state transfer (REST) APIs and web front ends can be mitigated with FortiWeb API protection.

SoC tools

Fortinet has a comprehensive SOC management and automation framework and tools that allow visibility and a wide range of triggers to be linked to actions, such as alerting, removing rogue devices from the network, or making API calls to other devices. For example, any of the above detections can cause a device to be quarantined and blocked from further communications until the cause is established and remedial action is taken. These tools include:

- FortiManager and FortiAnalyzer security management and analytic tools for powerful and simplified orchestration, automation, and response for on-premises, cloud, and hybrid environments.
- FortiEDR provides endpoint security for the IoT platform components and applications with real-time visibility, analysis, protection, and remediation.
- FortiSIEM security information and event management tool provides real-time event data analysis, allowing for early discovery of breaches and targeted attacks.
- FortiSOAR security orchestration, automation, and response provides SOC case management, automation, and orchestration, to unify operations, and reduce alert fatigue and the mean time to respond to incidents.

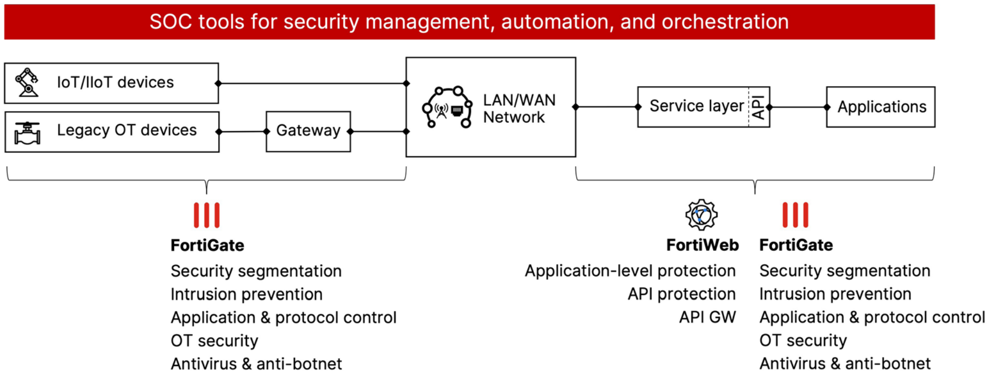

Figure 1: Fortinet cybersecurity solutions for the IoT ecosystem

Conclusion

IoT devices are part of a larger, complex IoT ecosystem. The growing use of IoT and the use cases it enables emphasizes the IoT ecosystem as a critical set of services and environments that must be safeguarded.

As enterprises embark on the IoT journey, they turn to service providers for devices, services, IoT platforms, management, and additional value add. Integrating the appropriate cybersecurity as built-in components or as a managed service, Fortinet enables service providers to deploy different levels of security solutions to ensure their IoT service and platforms—from the device level, the mobile, and fixed network connectivity, the IoT platform, and onto the applications.

[1] Philip Wegner, "IoT Analytics' Global IoT Enterprise Spending Dashboard," IoT Analytics: Market Insights for the Internet of Things, Feb 7, 2023.

February 15, 2023 5:03 PM
1822655-0-0-EN