FORTINET

WHITE PAPER

Security Considerations for the IoT Ecosystem

The Promise of IoT

Businesses are expected to spend over $1 trillion on Internet-of-Things (IoT) projects in 2023.[1] This investment is yet more evidence of the growing value of IoT as a means of gathering information and controlling a multitude of physical systems, and the impact of IoT technology on how businesses innovate, stay competitive, and remain environmentally sustainable.

But 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. This is why at least 75% of organizations plan to turn to solution providers such as system integrators and managed service providers to handle IoT integration, development, management, and support.[2]

Security Is Key for the IoT Ecosystem

The importance of a secure IoT solution cannot be overestimated. It 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 may result in failure in critical services and industries and even physical danger to individuals and the environment. It is therefore important that IoT solution providers demonstrate a commitment to providing a service that is secure by design.

IoT Security Needs

IoT solutions encompass many layers, including the devices themselves, but also on-premises gateways, 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. Security, then, is not simply a hardened device operating system (OS) or an encrypted access link. It is a multilayered solution that encompasses everything from the initial boot of the device to distributed denial-of-service (DDoS) protection at the network edge.

Delivering IoT Network Visibility

A significant hurdle in protecting IoT environments is having visibility of devices 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.** The exact information available depends on many factors and will vary from device to device.
- **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, in-line decryption should be performed (if this is possible) in order to verify the device data.

Compromised Device Detection

In general, the goal should be to stop attacks before they are able to compromise the device. But in cases where an attack gets through defenses, IoT security solutions must be able to detect signs of the infection and act immediately.

If an attacker does manage to gain control over a device, there are a number of next-step possibilities:

- **Disable the device:** This may be considered as simple denial-of-service (DoS), or could also be more sinister, if for example a device is monitoring a critical value such as tank pressure or temperature in an industrial context. Critical applications may have other protections against such an attack, but this should never be assumed.
- **Destroy the device:** Some attacks have shown that in some cases, a device could be permanently destroyed by a cyberattack. A simple example could be causing increased battery usage, to the point of exhaustion, in a device whose battery is otherwise intended to last the lifetime of the device.

- **Use the device to launch attacks:** A device may be used as a launch point, having potential access to other devices and to the IoT platform and other internal resources.
- **Recruit the device into a botnet:** The effectiveness of IoT botnets was shown in 2017 with Mirai where up to 2,000,000 IoT devices (mainly cameras and DVRs) were used to stage the largest ever recorded DDoS attack.

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 and so protecting them against attack is imperative.

The types of attacks that may be expected are:

Exploits: IoT platforms may have vulnerabilities just like any other software. In most cases, they will consist of coding bugs allowing buffer overflows and other memory corruptions, as well as unhandled corner cases. In addition, most IoT platform signaling is via some kind of application programming interface (API), so typical API attacks should be considered. Finally, data received by the platform will often result in a read or write to a database, so SQL attacks should also be covered.

Scanning/exploiting unused services: As in any service platform, care must be taken to expose only the minimum services, and not to leave unused services running (as they may be by default). For example, Server Message Block (SMB) services are often enabled by default and are also a common vector for attack. Open ports should be checked and any unnecessary services should be disabled or removed from the system.

Denial of Service

Denial-of-service attacks could come via externally facing interfaces (if indeed there are any), or from the IoT devices themselves. A simple device malfunction causing a cyclic registration can result in a massive DoS attack if there are a large number of devices behaving this way at the same time.

Hidden Attacks

When communications are protected end-to-end with transport layer security (TLS), there should be at least one security device that is decrypting the traffic to ensure that the protected traffic is as expected. If this is not the case, a compromised IoT device could use the encrypted connection, and the malicious traffic would be hidden from the operator. If the security device is colocated with the IoT platform, then it may offload the TLS processing and send decrypted traffic directly to the platform. Otherwise it should reencrypt the traffic to ensure that eavesdropping is not possible.

Device Protection

The IoT devices themselves may also be attacked. Generally, they will have limited connectivity and communicate with a small number of destinations (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 launched from inside the local network. Such attacks may consist of:

Malware: Although IoT malware is not prevalent today, it will become more so 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. However, at the same time, IoT 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, 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. Since traffic levels are typically low, relatively simple rate-limiting rules should be effective against such an attack.

Conclusion

IoT already plays a key role in driving automation, efficiency, and innovation in many industries. These connected devices are just the tip of the iceberg in terms of the uses and benefits IoT creates. But enterprises and communications service providers must prioritize the robust security of this ecosystem—including devices, connectivity, and the IoT platform's data and applications—for IoT to reach its full potential.

[1] "Worldwide Internet of Things Spending Guide," IDC, August 2020.

[2] "IDC FutureScape: Worldwide IoT 2020 Predictions," IDC, October 2019.

FORTINET

www.fortinet.com

October 26, 2020 8:25 PM

785704-0-0-EN

D:\OneDrive\Desktop\wp-FA-security-considerations-for-the-iot-ecosystem-10262020\wp-FA-security-considerations-for-the-iot-ecosystem-10262020