Secure Technology Alliance Response: NIST “IoT Security and Privacy Risk Considerations” Questions

April 26, 2018

The Secure Technology Alliance IoT Security Council is pleased to submit our response to the NIST invitation for stakeholder input outlined in the NIST “IoT Security and Privacy Risk Considerations” document (posted at https://www.nist.gov/sites/default/files/documents/2017/12/20/nist_iot_security_and_privacy_risk_considerations_discussion_draft.pdf).

Members of the IoT Security Council reviewed the draft NIST document; our answers to the questions posted by NIST are below.

Q1: Is a network connection to an external network required for devices to be considered IoT?

In general, we would like devices to be connected in two virtual planes – the control plane and the application plane. The application plane is related to the functions that the device is intended to do. For instance, a connected industrial robot can measure and take actions on its local environment, responding to commands and configuration from a human-operated console. The control plane refers to the configuration, diagnostics, maintenance and other lifecycle-related information and commands that must be supplied to the connected industrial robot. Typically, the manufacturer of the connected industrial robot plays an important role in the control plane. The industrial robot may be connected to the external network for the purposes of maintenance by the manufacturer.

In summary, it is not required for devices to be connected to an external network for normal operations. However, if application plane or control plane operations necessitate the device to be connected to an external network, then we can consider the device an IoT device.

Q2: NIST selected the term “devices” over terms such as “objects” and “things” as there does not seem to be consensus among technology, security, and privacy professionals on the preferred term. Which term would be best for future guidance?

The other term that is also widely used is “end point.” However, in the case of IoT, real end points may be realized and deployed using IoT edge gateways, therefore diluting the term “end point” between the edge gateway and the actual end device. However, in this case, both are classes of connected devices and the more generic “device” seems to fit the connected IoT device paradigm.

The “device” concept should also encapsulate the notion of a “digital twin,” which has become a common way to manage IoT devices. A “digital twin” represents the canonical properties of an IoT device typically used for active remote management or for capturing the last known state of the actual IoT device. An example of this is for devices that attach to a network and send/receive data at very seldom intervals. The device is then represented on the IoT platform through its “digital twin” and all management actions are done on the digital twin, which is synchronized with the actual device the next time it attaches to the network.

The other notion that the concept of “device” needs to encapsulate is “hypallage.” As an example, by connecting a small IoT device to the OBD-II port of an automobile, we transfer the notion of the “device” to the entire automobile, and not just the small IoT device anymore.

Q3: Our expected focus for the guidance is security and privacy risks for two types of IoT ecosystem components: integrated IoT devices with built-in sensors and/or actuators, and composite IoT devices. Are these the areas where organizations need more guidance? Are there any others NIST should focus on?

While these seem to be broadly applicable, there are some use cases where we need to apply it judiciously. For instance, in fleet-tracking use cases, we attach a device to a car/truck, thus making the car/truck connected. In this case, an IoT device (e.g., accelerometer, GPS, cellular data connection, CAN bus connection) is attached to the car to make it connected. The actual IoT device is a hybrid device, having characteristics of both integrated and composite IoT devices.

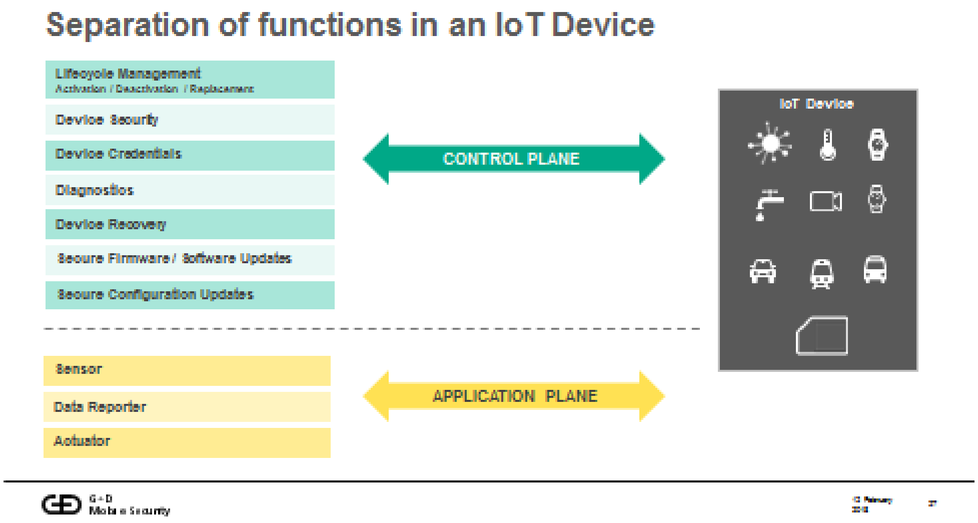
We would need to consider a hybrid device that has both integrated and composite IoT device characteristics.

Beyond thinking about individual components, guidance should also be provided around the clustering or segmentation of components. For example, how might an organization protect an environment that has a combination of greenfield and brownfield components? When might there be a need to segment a subset of devices (for example, older connected devices that have gaps in their security functionality)?

Q4: Are there any gaps in the capabilities list? (See page 3 of NIST document)

The capabilities listed are typically what we claim to be in the application plane, except for the software usage and management part. For classification purposes, we separate device characteristics into application plane and control plane. The control plane provides diagnostics, lifecycle management enablement, credentials enabling identity and security and secure configuration, and software updates.

The graphic below helps to illustrate the control plane and application plane distinction.


Separation of functions in an IoT Device

Lifecycle Management
Activation / Deactivation / Replacement
Device Security
Device Credentials
Diagnostics
Device Recovery
Secure Firmware / Software Updates
Secure Configuration Updates

CONTROL PLANE

Sensor
Data Reporter
Actuator

APPLICATION PLANE

IoT Device

G+D
Mobile Security

Q5: What use cases would best document interactions between IoT capabilities?

In a broad sense, IoT device capabilities fall into three areas – sensing, communicating, and actuating. IoT devices can have one or more of those capabilities built into them. The security risk is unique for each of those capabilities. Some devices have all three capabilities built into them. Several use cases that are common examples are highlighted below.

- In a timber logging plant, the hardness of the logs is related to the ambient temperature and the temperature of the log. The device sensing the temperature also has to actuate the right amount of force for cutting and sawing the logs.
- Another example is in IoT devices used for electric power optimization in electric grids – a field known as Volt Var Optimization (VVO). In these cases, the devices on the electric grid have to sense the current and voltage on the lines, make an assessment of the load factor, and actuate transformer step changes to keep the electric grid in balance. These devices are sensing, reporting and actuating, and are also connected to SCADA control buses so that commands can be sent to them by human technicians.
- We might also consider use cases around medical devices. For example, there may be edge devices collecting patient vitals such as heart rate or blood pressure. Those devices may feed into a base station that then aggregates that information and shares it across a broader network, such as a hospital system or insurance company.
- Another use case that should be considered is with consumer IoT devices. For example, consumers use IoT devices to sense, monitor and control their home environment. These devices often are a mix of many different manufacturers and vendors, so security relies solely on the security of the home WiFi network.

Q6: How could risk assessment and response processes be adjusted to take IoT characteristics into account?

Many security principles that are applicable to traditional information security and IT do not apply to the IoT.

Perimeter

Traditional notions of IT security include a well-defined perimeter which defines and separates trust zones. Devices and network elements inside the perimeter are trusted entities, and only application security is handled on a session basis.

Point-to-point encryption

The other common technique used in IT security is point-to-point encryption in the form of VPN, IPSec tunnels and similar approaches. These use strong encryption between devices and networks or enterprise edge elements and are totally agnostic to the actual data being carried through those tunnels. This is perhaps the best current practice to thwart man-in-the-middle attacks independent of the applications.

Human interaction

The other key aspect of IT security involves the human factor. While perimeters and tunnels can keep out malicious actors, the end user of the device can still be the weakest link in the security chain. End users are subject to phishing attacks to easily hand over key login or authentication credentials making it easy to get past any other security measure. Two- and three-factor authentication schemes help to mitigate against these threats.

Identity

The concept of identity is stored in directory servers in traditional IT systems. IoT systems miss this concept of identity for the various devices and sensors that comprise an IoT environment.

A traceable and well-managed device identity should be used in IoT devices to provide authentication within networks and to services existing in cloud infrastructure. For solutions in which authenticated command and control is critical, asymmetric public key encryption should be used to both provide devices with traceable identity and provide for signing of data which is transported and stored in the cloud. For systems in which life and safety critical physical systems are affected, hardware-based secure credentials should be deployed to ensure trusted device integrity through the entire deployed lifecycle.

IoT security challenges

Security for IoT challenges all four of these well accepted principles. IoT devices are remote and far flung and challenge the concept of a traditional security perimeter that is enclosed within the physical perimeter of the enterprise. The IoT makes the security perimeter virtual and extends it far beyond the physical premises of the enterprise.

The virtual security perimeter leads to a “zero trust” environment where every device or element has to mutually authenticate with every other device it is communicating with. This challenges the notion of application agnostic point-to-point encryption and makes application-level security paramount for all devices that are communicating with each other.

Lastly, IoT devices, being completely autonomous, do not rely on humans to login for normal operations. Hence instead of authenticating a human through identities such as username/password and other related schemes, the IoT device must be authenticated using very strong identity credentials that are derived from a “root of trust.” This root of trust needs to be immutable and will provide the basis for irrefutable identity credentials for the device. Since the identity credentials are derived off the root of trust, it provides for lifecycle management of the device and allows for the flexibility of attaching policy and other actions needed to administer the device.

About the Secure Technology Alliance

The Secure Technology Alliance is the digital security industry’s premier association. The Alliance brings together leading providers and adopters of end-to-end security solutions designed to protect privacy and digital assets in payments, mobile, identity and access, healthcare, transportation and the emerging Internet of Things (IoT) markets.

The Alliance’s mission is to stimulate understanding, adoption and widespread application of connected digital solutions based on secure chip and other technologies and systems needed to protect data, enable secure authentication and facilitate commerce.

The Alliance is driven by its U.S.-focused member companies. They collaborate by sharing expertise and industry best practices through industry and technology councils, focused events, educational resources, industry outreach, advocacy, training and certification programs. Through participation in the breadth of Alliance activities, members strengthen personal and organizational networks and members take away the insights to build the business strategies needed to commercialize secure products and services in this dynamic environment.

About the Secure Technology Alliance IoT Security Council

The Secure Technology Alliance IoT Security Council was formed to develop and promote best practices and provide educational resources on implementing secure IoT architectures using “embedded security and privacy.” The Council focuses on IoT markets where security, safety and privacy are key requirements and leverages the industry expertise and knowledge gained from implementing embedded security technology for payment, identity, healthcare, transport and telecommunications systems to provide practical guidance for secure IoT implementations. The Council provides a unified voice for the industry to the broader IoT ecosystem.