**IoT Security Overview**

The Internet of Things is the wave of the future, offering businesses immediate and real-world opportunities to reduce costs, increase revenue, and transform their business. Many businesses, however, are hesitant to deploy IoT in their organizations due to concerns about security, privacy, and compliance. A major point of concern comes from the uniqueness of the IoT infrastructure, which merges the cyber and physical worlds together, compounding individual risks inherent in these two worlds. Security of IoT pertains to ensuring the integrity of code running on devices, providing device and user authentication, defining clear ownership of devices (as well as data generated by those devices), and being resilient to cyber and physical attacks.

Then, there’s the issue of privacy. Companies want transparency concerning data collection, as in what’s being collected and why, who can see it, who controls access, and so on. Finally, there are general safety issues of the equipment along with the people operating them, and issues of maintaining industry standards of compliance.

Given the security, privacy, transparency, and compliance concerns, choosing the right IoT solution provider remains a challenge. Stitching together individual pieces of IoT software and services provided by a variety of vendors introduces gaps in security, privacy, transparency, and compliance, which may be hard to detect, let alone fix. The choice of the right IoT software and service provider is based on finding providers that have extensive experience running services, which span across verticals and geographies, but are also able to scale in a secure and transparent fashion. Similarly, it helps for the selected provider to have decades of experience with developing secure software running on billions of machines worldwide, and have the ability to appreciate the threat landscape posed by this new world of the Internet of Things.

Protecting IoT solutions requires that businesses ensure each of the following:

* secure provisioning of devices
* secure connectivity between these devices and the cloud
* secure data protection in the cloud during processing and storage

Working against such functionality, however, are resource-constrained devices, geographic distribution of deployments, and a large number of devices within a solution.

https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-ground-up

https://www.microsoft.com/en-us/internet-of-things/security

https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-architecture

<https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices>

**IoT Threat Modeling**

In this topic, you'll learn:

* The definition of a threat model
* How threat modeling applies to IoT security
* How to develop your own threat model

**IoT Security**

As we've seen in previous lessons, planning for security in an IoT solution is not only essential but it can get complicated very quickly. IoT solutions involve data-collecting devices, cloud services (which includes storage and analytics), and can involve personal or sensitive data (a lot of it). Each of these can represent “soft targets” for hackers or others with malicious intent so understanding how a solution can be vulnerable should be an integral part of any IoT architecture.

Intel, in their IoT Platform Reference Architecture document [what they refer to](https://www.intel.com/content/www/us/en/internet-of-things/white-papers/iot-platform-reference-architecture-paper.html) as the “security layer” in their architecture. They describe it this way:

Robust hardware- and software-level protection are essential for ensuring world-class security, which is a foundational IoT tenet. Security is more like a process than a product because it depends upon evaluating the threat model for specific use cases and addressing each possible threat. A layered security approach is highly recommended since it establishes multiple defense mechanisms against hackers.

Let's look more specifically at how this layered approach to security works in an IoT architecture.

**Threat Modeling**

When designing a system, it is important to understand the potential threats to that system, and add appropriate defenses accordingly, as the system is designed and architected. The objective of threat modeling is to understand how an attacker might be able to compromise a system and then make sure appropriate responses and repairs are in place.

The movie *The Big Short* includes a quote (falsely attributed to Mark Twain) states, “It ain’t what you don’t know that gets you into trouble. It’s what you know for sure that just ain’t so.” In the context of IoT security, this means that we can get in the most trouble when we confidently assert that something won't (or will) happen. Part of threat modelling is planning for the things you can't plan for or anticipate. This might be as radical as taking a server offline or sending technicians to collect devices from the field if there's a breach. But it could include a lot of much less dramatic measures to ensure that data is safe and hackers are thwarted.

You should threat model the solution as a whole and also focus in the following areas:

* The security and privacy features
* The features whose failures are security relevant
* The features that touch a trust boundary

Three rules of thumb to keep in mind when building a threat model:

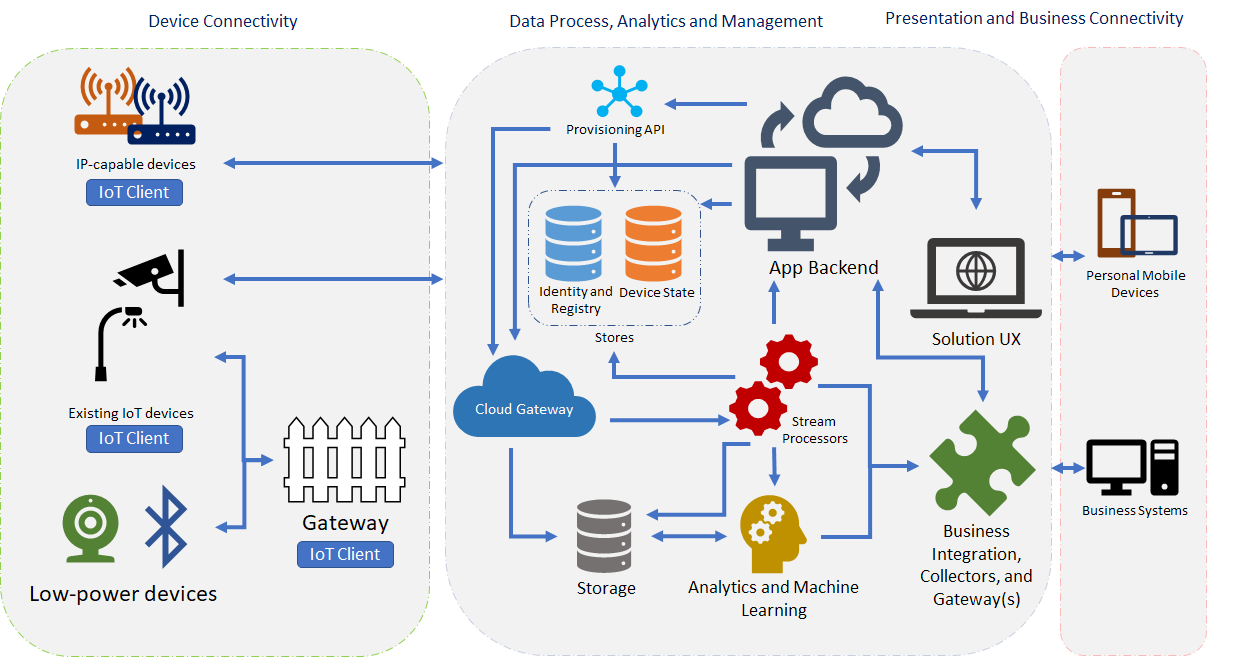
* Create a diagram out of reference architecture.
* Start breadth-first. Get an overview, and understand the system as a whole, before deep-diving. This approach helps ensure that you deep-dive in the right places.
* Drive the process, don’t let the process drive you. If you find an issue in the modeling phase and want to explore it, go for it! Don’t feel you need to follow these steps slavishly.

**Threat modeling and IoT architecture**

Microsoft's [guidance on threat modeling](https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-architecture) includes four main areas of focus. Each of these will have specific needs and involve particular “threat vectors” (ways the area can be attacked). They include:

* Devices and Data Sources
* Data Transport
* Device and Event Processing
* Presentation

The diagram below illustrates an IoT architecture with each of these areas designated. The blue arrows indicate paths the data can take through the system. While this looks complex, it's important in a threat model to understand where your data is coming from and *every possible place it can go*. Missing just one path can create a serious vulnerability.



**Attack Vectors to Consider**

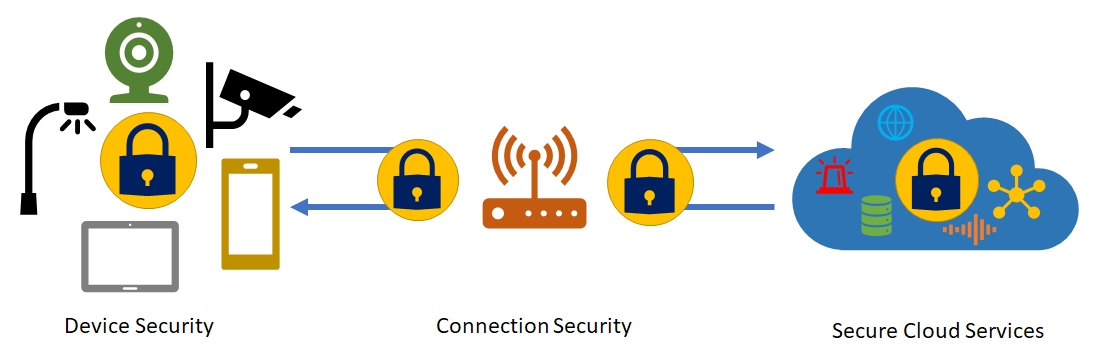
Again, an attack vector is simply a particular way that a hacker or person with malicious intent could compromise your IoT system. Microsoft documentation [lists many possible options](https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-architecture) and we'll summarize a few of the most important here.

1. **Spoofing**. Device spoofing takes place when an analogous device or virtual device takes the place of an intended device without the system knowing a switch was made. Spoofing can happen with services, APIs and other parts of an IoT system. Certificates can help reduce spoofing but an IoT architecture should have mechanisms in place to ensure that the devices and services deployed to the solution are the ones you intend to be there.
2. **Denial of Service**. Denial of Service (DOS) attacks are something we hear about in the news every so often because they can negatively affect our ability to reach a web site or service provider. One type of DOS attack involves overwhelming a service or device with garbage data or requests so the service or device can't operate normally. General a DOS attack is any hack where the device or service designed to perform a particular function is rendered useless. These types of attacks (besides being annoying) can prevent critical data from reaching a destination or enable hackers to attack other parts of an IoT installation.
3. **Elevation of Privilege**. This type of attack causes a device or service that has a set of capabilities that are limited by permissions or function (e.g. an automobile accelerator that has a mechanism that prevents the car from exceeding a certain speed) to function beyond their imposed limitations. You can imagine an API or device that has permission to collect or store impersonal data being tricked into collecting or storing personal data that could cause harm if it got into the wrong hands (e.g. credit card information).

As mentioned above, there are many other attack vectors to consider and a threat model should include mitigations for as many as possible.

**A Secure Ecosystem**

As you think about the security of an IoT solution, it can help to break down each aspect of the problem into functional categories. In the threat model we considered above, we saw four areas of focus. We can abstract these even more to help us build a threat model. In an [article for *Network World*](https://www.networkworld.com/article/3266375/internet-of-things/best-practices-for-iot-security.html), author Dean Hamilton echos the guidance that we'll be looking at in this module. He recommends that IoT architects focus on securing devices, the network, and data. We'll talk about security in three primary areas: **devices**, **connection and communication**, and **cloud services**. We'll call this our secure IoT Ecosystem.



In the next three lessons, we'll look at each of these categories in turn.