Security of Things in a Connected World

According to Gartner, by year 2020, there will be more than 25 billion connected devices. These devices would connect with the cloud (and other devices) *without any human intervention.*

What used to be dumb machines, devices, sensors, automobiles etc. would now turn intelligent with added computing and network capability. Systems and assets which used to be isolated from external networks would get connected to the Internet.

What do all these imply in the context of cybersecurity? And public safety?

Well, the relevance and impact of cybersecurity are no less disruptive in this connected ecosystem.

In today’s internet a security breach in a bank datacenter would result in huge loss of private data and account information. It can trigger financial losses and theft of identity of customers and employees. This is bad enough.

However, in case of an IOT security breach, the impact could be much worse.

A smart door operator, for example, allows you to control access into your house even while you are miles away, by using cloud based apps over the Internet. It also allows you to control your home appliances such as, thermostat, oven, boiler etc. If this door operator is hacked – you are not only exposed to chances of burglary. The hacker can remotely take full control of your home, manipulate appliances to dangerous levels and even be a threat to those living there.

In the aviation and transportation industry, connected sensors and cloud based control is on the rise. It allows jet airliners and long distance trains to operate with greater efficiency. General Electric, using its Predix platform can monitor and analyze the enormous volume of data generated by these sensors, and precisely predict when a jet-engine is due for its next maintenance. Hacking and tampering the sensor data of an in-flight jetliner can lead to enormous loss. Not just financial but it can cost several lives. Similar impact may result in the case of a cybersecurity breach in a nuclear plant or smart energy grid.

In the IT world, if your PC is hacked you may lose your credit card and other personal information. That’s not good. But in IOT, because of a cybersecurity hack somebody may die.

Given this degree of impact, IOT cybersecurity cannot be an afterthought. It has to be built into the design process. IOT specific security measures are needed for the connected sensors, devices and appliances. And also in the gateways, routers and servers which are central to IOT-enabled applications and services.

The threat scenarios for various applications must be analyzed in advance. And risk and mitigation measures put in place.

Described below are some new threats and security challenges in IOT deployments.

A Wi-Fi enabled Appliance added to a Local Area Network (LAN)

An IOT appliance, for example, a "smart" refrigerator with standard TCP/IP protocol stack is added to the LAN. If this smart refrigerator is not equipped with enterprise-level security protocols, there can be serious risks.

Because now we have allowed a potentially malicious endpoint behind the LAN firewall.

Firewalls and NATs are designed to prevent outside direct attacks on the host. It filters and controls inbound data traffic, but outbound traffic is always trusted. Otherwise it would be hard to use such appliances. Since our smart fridge is already behind the firewall, it can send any outbound requests and data.

Unlike Windows and Apple operating systems, the OS embedded in such IOT devices is not as robust. Without built-in security, if malicious code is injected in the chip, this fridge can connect to external malicious servers across the firewall. This process, known as "Reverse Tunneling" enables the device behind the firewall to open a socket connection with a remote endpoint to initiate malicious traffic *(Add illustration?)*

IOT device manufacturers and network operators must factor in such exploits during the design phase itself.

Applying Software Upgrades and Security Patches to IOT Devices

Security involves continuous learning. It is a journey. As new threats get exposed and resolved, patches are released to prevent proliferation of similar attacks. This works well with IT systems like PCs and laptops. Microsoft and Apple issue regular security patches for newly exposed security exploits. With automatic upgrades in place, these patches get added to our PCs on a regular basis. These upgrades may cause, at the most, a 15 minutes service disruption.

Well, this is not going to work quite as easily in case of connected systems and appliances. Currently there is no mechanism or infrastructure in place that can automatically "push" patches and upgrades to IOT devices. Even if the device manufacturer releases a patch for an exposed vulnerability, how is the patch to be dispatched to users? What degree of downtime and manual intervention would that require?

And how easy would it be to introduce such upgrades? Would customers be required to reboot their oven, car, or pacemaker and maneuver through an upgrade process? Or the updated software be only available in the next release of the physical product?

An upgrade scheme which can be easily adopted across the industry is needed to overcome this challenge.

Exposing Private and Encrypted Data in the Chip

IOT appliances have low memory resources. They often operate on low power. Mission-critical operational data is usually embedded in the chip itself. Take the example of a driverless car. It has numerous embedded sensors and control systems. If a hacker can get access to the encrypted data over a USB port or a debugger interface, they may be able to gain access and take over the control of similar devices from the same manufacturer.

Access control from external sources is another security challenge we must mitigate.

Navigating IOT Security landscape with Smart Mitigation Strategies

Innovations in IOT are unfolding enormous potential for the future. However to make these benefits sustainable, iron clad security measures must be integrated all along the device and solution lifecycles. From initial design and planning to real-world operational environments.

Some mitigation strategies are described here.

Securely powering up devices

When the device is powered up, the authenticity and integrity of its software is verified using cryptographically generated digital signatures. This is similar to signing a check or legal document to prove its authenticity. Signature verification during boot phase confirms that the software running is indeed the correct one. That it is verified by the device by utilizing authorized root of trust. This is a foundational step to secure the boot process.

Minimizing the impact of a security breach through access control

The principle of least privilege restricts software applications to access only those memory and processor resources which are barely needed for that application to function properly. Once an application authenticates, it gets role-based authorization. This concept is similar to how users are granted access to a secured network.

This principle of authorizing resources based on role and necessity can also be extended to other hardware components within the IOT ecosystem.

Authenticating IOT devices before granting network access

Before connecting to a secured network, users are authenticated using their username and password. Similarly IOT devices must also be authenticated before they can access other network resources.

In a real-world IOT deployment, these devices can be deeply embedded in various locations that limits any human intervention. What is needed is a scalable solution that allows devices to automatically authenticate themselves using encrypted credentials and a root of trust.

Iron-clad Security using Firewall and IPS

When smart physical objects are connected in a given industrial application, they communicate using protocols proprietary to that industry. For instance, the smart energy grid has its own set of protocols governing how devices talk to each other. These are different from enterprise IT protocols. While this renders the devices immune to internet traffic, malicious packets injected for these industry protocols is still a big risk. Industry specific firewalls and deep packet inspection capabilities can be used a mitigation strategy.

As IOT applications mature and gain mainstream popularity, the relevance to keep these applications and assets secure are also mounting. Industry consortiums, product developers and adopters have a equal stake in making things secure and sustainable.