Security Challenges Analysis of IoT

Abhishek Mishra
Oct 11, 2016

Example of few risks

1. Fitness tracker devices can be hacked to completely monitor a person's schedule.
2. Smart homes can be hacked resulting into many accidents and possible thefts.
3. Services that a person avails like car washing on service centres can be used by a hacker by accessing the data the owner carries on his IoT ID.
4. Links to a pacemaker can be fatal.

Security techniques at our disposal

1. Application-aware/Packet-filtering firewalls
2. Intrusion detection and prevention systems (IDS/IPS), and security incident and event management (SIEM) solutions.
3. Signature matching and blacklisting for malwares or whitelisting for more sophisticated security.
4. Virtual private networks (VPN) or physical media encryption, such as 802.11i (WPA2) or 802.1AE (MACsec).

New constraints, threats and challenges

1. Applying these same practices or variants of them in the IoT world requires substantial re-engineering to address device constraints.
2. Blacklisting, for example, requires too much disk space to be practical for IoT applications.
3. Embedded devices are designed for **low power consumption**, with a **small silicon form factor**, and often have **limited connectivity** They typically have only as much processing capacity and memory as needed for their tasks And they are often headlessthat is, there isnt a human being operating them who can input authentication credentials or decide whether an application should be trusted; they **must make their own judgements and decisions** about whether to accept a command or execute a task.
4. The endless variety of IoT applications poses an equally wide variety of security challenges.

Building an overall secure system

Security must be addressed throughout the device lifecycle, from the initial design to the operational environment:

(a) **Secure booting:** When power is first introduced to the device, the authenticity and integrity of the software on the device is verified using cryptographically generated digital signatures In much the same way that a person signs a check or a legal document, a digital signature attached to the software image and verified by the device ensures that only the software that has been authorized to run on that device, and signed by the entity that authorized it, will be loaded

(b) **Access control:** Next, different forms of resource and access control are applied Mandatory or role-based access controls built into the operating system limit the privileges of device components and applications so they access only the resources they need to do their jobs If any component is compromised, access control ensures that the intruder has as minimal access to other parts of the system as possible

(c) **Device authentication:** When the device is plugged into the network, it should authenticate itself prior to receiving or transmitting data

(d) **Firewalling and IPS:** The device also needs a firewall or deep packet inspection capability to control traffic that is destined to terminate at the device. The device neednt concern itself with filtering higher-level, common Internet traffic the network appliances should take care of thatbut it does need to filter the specific data destined to terminate on that device in a way that makes optimal use of the limited computational resources available.

(e) **Updates and patches:** Once the device is in operation, it will start receiving hot patches and software updates Operators need to roll out patches, and devices need to authenticate them, in a way that does not consume bandwidth or impair the functional safety of the device.