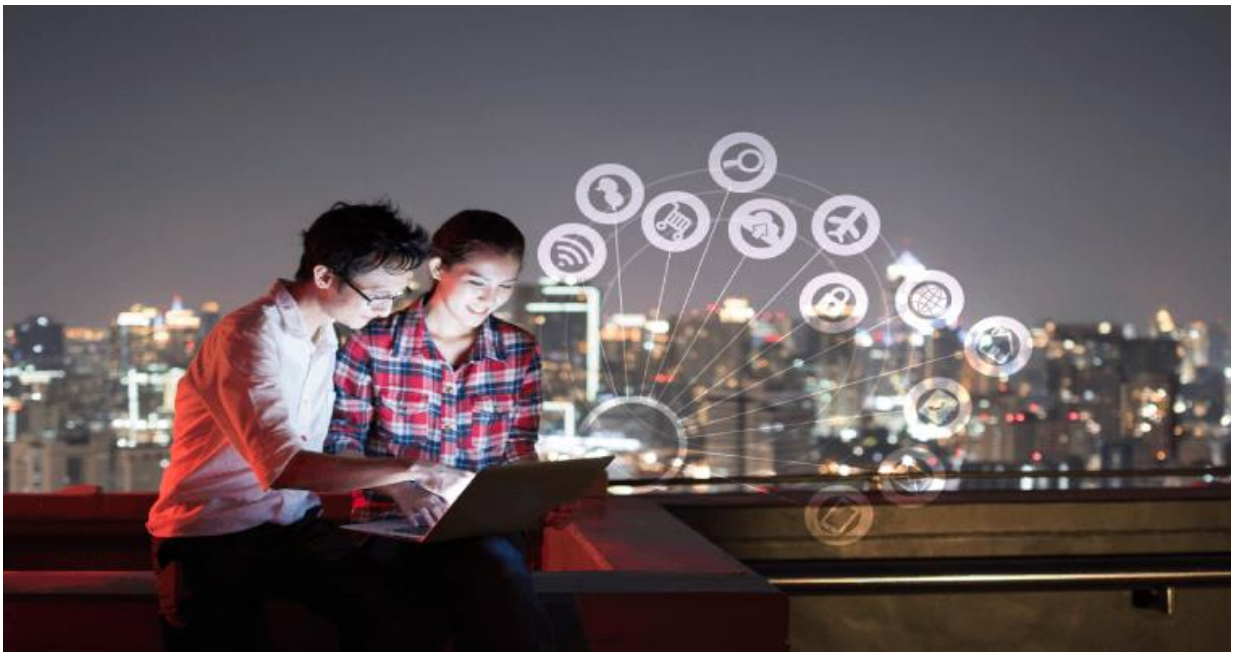
How secure is your IoT Implementation?

by **Satya K Vivek** | June 30, 2017



With real IoT implementation taking place across different industry verticals now, "how secure is your IoT implementation?" is one of the major questions asked by majority of CXOs. The three key threats for IoT implementations are:

- **Service Availability**: The connectivity of an IoT device or service must persist even if there is a link/device failure or DoS attack.
- **Data Confidentiality**: Access to data and information is for authorized users only.
- **Data Integrity**: Accuracy, consistency and trustworthiness of data in transit, or stored on any IoT device, must be maintained and cannot be modified by unauthorized entities.

Addressing Security Concerns

Security must be maintained throughout IoT lifecycle from end device to gateway, to cloud application, and to mobile applications. Security must be addressed at:

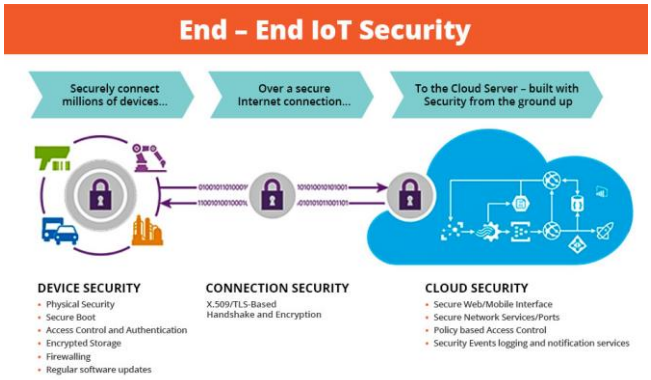
- **Device Level**
- **Transport/ Network Level**
- **Cloud/ Application Level**

Device Level Security

The main device level security considerations include:

- ***Physical Security:*** Physical security weaknesses are present when an attacker can disassemble a device to easily access the storage medium and any data stored on that medium. Weaknesses are also present when external ports can be used to access the device. These issues can be mitigated by ensuring:

  - ✓ Device cannot be easily disassembled
  - ✓ Stored data is encrypted
  - ✓ Only required external ports (Port Protection)
  - ✓ Product can limit administrative capabilities
  - ✓ Secure Console access



- ***Secure booting:*** When power is introduced to device the authenticity and integrity of software is verified using cryptographically generated digital signatures. A digital signature is attached to software image and verified by device ensuring only authorized software can run on that device.
- ***Access control:*** Mandatory or role-based access controls built into the operating system limit the privileges of device components. If any component is compromised, access control ensures the intruder has minimal access.
- ***Device authentication:*** When plugged into a network, the device should authenticate itself prior to receiving or transmitting data. Machine authentication allows a device to access a network based on credentials stored in a secure storage area.
- ***Encrypted Storage:*** Embedded devices store user data. This data can be protected by encrypting or signing. The challenge lies in securely storing cryptographic keys.
- ***Firewalling and IPS (Intruder Prevention System):*** The device also needs a firewall or deep packet inspection capability to control traffic destined to terminate at the device. A "host-based" firewall or IPS is required in this case, as deeply embedded devices have unique protocols distinct from enterprise IT protocols.
- ***Security Monitoring or IDS (Intruder Detection System):*** Existing embedded devices can be attacked without detection. A hacker could execute millions of invalid logins attempts without the attack being reported, so Embedded devices must be able to detect and report invalid login attempts and other potentially malicious activities.
- ***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 the devices need to authenticate them in a way that does not consume bandwidth, impair functional safety of the device or compromise functional safety.
- ***Device Tampering Detection:*** This enables the detection of any unauthorized attempt to access the system at the hardware or software level. Example: the detection of tamper events through IO pins. Once detected it can respond to this attack with custom actions, such as: erasing critical data partition or other secure keys in the flash.

Transport / Network Level Security

The main Transport / Network level security considerations include:

- ***Secured Communication:*** In typical embedded system architectures, devices and systems are connected across heterogeneous networks employing various standard and proprietary protocols. To protect communication against eavesdropping and message falsification it must be secured between systems.
- ***Decentralized or Distributed Intelligence:*** The capability of embedded and distributed intelligence in the network is a core architectural component of any Industrial IoT solutions. This distributed intelligence capability (also known as Fog Computing) helps to avoid the issue of a single point of failure.

Cloud / Application Level Security

The main security vulnerabilities pointed out by the OWASP (*Open Web Application Security Project*) for any Web / Mobile Application products include;

- ***Insecure Web Interface:*** An insecure web interface can be present when issues such as account enumeration, lack of account lockout or weak credentials are present. So, a secure web interface requires:
  - ✓ Default usernames / passwords should be changed during initial setup
  - ✓ Ensuring web interfaces are not susceptible to XSS, SQLi or CSRF
  - ✓ Ensuring credentials are not exposed to network traffic
  - ✓ Ensuring weak passwords are not allowed
  - ✓ Ensuring account lockout mechanism
  - ✓ Ensuring password recovery mechanisms are secure
  - ✓ Ensure credentials are properly protected.
- ***Insecure Network Services:*** Services may be susceptible to buffer overflow attacks creating a denial of service condition leaving the device inaccessible. Denial of service attacks against other users may also be facilitated when insecure network services are available. Insecure services can often be detected by automated tools such as port scanners.
- ***Lack of Transport Encryption:*** Lack of transport encryption allows data to be viewed as it travels over local networks or the internet. Lack of transport encryption is prevalent on local networks as it is easy to assume that local network traffic will not be widely visible, however in the case of a local wireless network, misconfiguration of that wireless network can make traffic visible to anyone within the range of that wireless network. So, in a data transport:
  - ✓ The channel should be encrypted using protocols such as SSL/TLS
  - ✓ Ensure accepted encryption standards are used and avoid using proprietary encryption protocols
- ***Privacy Concerns:*** Privacy concerns over the collection of personal data is prevalent. Minimizing privacy concerns requires:
  - ✓ Ensuring only data critical to the functionality of the device is collected
  - ✓ Ensuring any data collected is properly protected and stored with encryption
  - ✓ Ensuring only authorized individuals have access to the collected personal information.
- ***Insufficient Security Configurability:*** Insufficient security configurability is present when users of the device have limited or no ability to alter its security controls. Sufficient security configurability requires:
  - ✓ Ensuring the ability to separate normal users from administrative users

- ✓ Ensuring the ability to encrypt data at rest or in transit
- ✓ Ensuring the ability to force strong password policies
- ✓ Ensuring the ability to enable logging of security events
- ✓ Ensuring the ability to notify end users of security events

A Checklist to ensure the security of your IoT Devices:

Security Considerations	Device	Transport	Cloud
Physical Security	✓ Make sure that the device cannot be easily disassembled ✓ Make sure that only minimal external ports are needed for the product to function. ✓ Make sure that the Console access is secured	NA	NA
Secure Booting	✓ Make sure that only the Software that has been authorized to run on the device is loaded	NA	NA

Authentication	✓ Make sure that whenever a device is plugged into the network, it should authenticate itself prior to receiving or transmitting data	NA	✓ Ensure that the Web or Mobile App is authenticated using a multi-factor authentication mechanism before use. ✓ Ensure that the default usernames/passwords are changed during initial setup ✓ Ensure that the web interfaces are not susceptible to XSS (Cross-site scripting), SQLi (SQL Injection) or CSRF (Cross-Site Request Forgery) ✓ Ensure that the credentials are not exposed to network traffic ✓ Ensure that a check for weak passwords is in place. ✓ Ensure that an account lockout mechanism is in place ✓ Ensure that the password recovery mechanisms are secure ✓ Ensure that the credentials are properly protected.
Access control	✓ Make sure that a role-based access control is built into the operating system to limit the privileges of device components and applications, so that they access only the resources they need to do their jobs.	NA	✓ Ensure that the application has the ability to separate normal users from administrative users ✓ Ensure that only authorized individuals have access to the collected personal information.
Privacy Concerns	✓ Ensure that the data stored in the device is protected and stored with encryption.	NA	✓ Ensure that any data collected is properly protected and stored with encryption
Security Monitoring or IDS	✓ Make sure that the Embedded devices can detect/limit and report invalid login attempts and other potentially malicious activities.	NA	✓ Ensure that the application has the ability to enable logging of security events ✓ Ensure that the application has the ability to notify end users of security events ✓ Ensure that only data critical to the functionality of the device is collected

Firewalling or IPS	✓ Make sure that a host based firewall is implemented at the edge devices (gateways) to control the data traffic.	NA	✓ Ensure that only necessary secure ports are exposed ✓ Ensure that the services are not vulnerable to buffer overflow and fuzzing attacks ✓ Ensure that the services are not vulnerable to DoS (Denial of Service).
Updates and patches	✓ Make sure that the operators roll out patches/updates regularly. ✓ Make sure that the devices authenticate these updates, in a way that does not consume bandwidth or impair the functional safety of the device.	NA	✓ Ensure that a regular update of Mobile/Web Applications is rolled out.
Device Tampering Detection	✓ Make sure that a tampering detection mechanism is in place that enables the detection of any unauthorized attempt to access the system at the hardware or software level	NA	NA
Secured Communication	NA	✓ Ensure that the data is encrypted when in transit, to protect your data communication against eavesdropping and message falsification.	NA
Distributed Intelligence	✓ In Industrial IoT solutions, it will be always better to have a decentralized architecture such as Fog computing to avoid any single point of failures as well as better utilization of resources.	NA	NA

Gadgeon Systems, Inc. (www.gadgeon.com) is not just a Design House that specializes in IoT Design. We are IoT Consultants, helping our customers navigate though the myriad decisions facing the typical customer implementing their own IoT product. As we engage with customers in an End-to-End IoT design implementation, our unique approach ensures an optimum result; combining the ideal architecture, cloud, mobile app, and connectivity choices, resulting in optimal user-experience.