Twelve IoT Controls

For Auditing Security on Connected Devices

http://twelveiotcontrols.com

Why Twelve Controls for IoT Devices?

In the future, IoT devices will have a white goods equivalent rating scale, measuring not energy, but controls.

- Similar to washing machines and refrigerators
- Manufacturers will be measured on the number and type of controls
- The implementation of the controls will vary based on
  - The environment of use of the IoT devices
  - The investment consumers will be willing to make, in purchasing these
- IoT devices will be certified against specific controls

This work will hopefully assist in the journey towards having a white goods equivalent rating scale for IoT devices

Objective & Rationale

- This presentation describes the three (3) step process used to derive a list of 12 controls for IoT devices.
- The method applied to derive these controls is *technology-agnostic* and focuses on the environment of operation of the IoT device.
  - Step 1 – Transforms the known set of the NIST 800-53 controls to IoT controls
  - Step 2 – Groups these controls based on two common (for all IoT) characteristics
  - Step 3 – Shortlists 12 re-occurring controls, based on the patterns for controls

Step 1 – From NIST Controls to IoT Controls

- Starting from a standard set of controls, take the NIST SP 800-53 controls:
  - Replace "Information System" with "IoT Device"
  - Replace "Organization" with either
    - "Environment of Use" or
    - "Manufacturer“
- Examine the environment of use for the IoT device,
  - Replace wordy clauses
  - Remove not applicable statements
  - Check for bad grammar and any tautology

Step 2 – A Simple Way to Group Controls for IoT Devices

- Almost all IoT devices have two things in common:
  - A TCP/IP stack with a wireless interface
  - A specific business purpose that the IoT device fulfils
- Looking at the environment of use of different IoT devices, patterns emerge that allow us to layer the controls as:
  - Specific to the TCP/IP stack
  - Specific to the Organization, Mission and Information System View
- We can thus examine the control objective for each control, specific to the purpose and environment of use of the IoT device.

Step 3 – Shortlisting 12 Controls

- Customise the control objective for each control, based on the purpose and environment of use of each IoT device. Re-occurring control themes are:

Physical Access Control	Transmission Confidentiality and Integrity	Boundary Protection	Device Identification and Authentication
Collaborative Computing Devices	Identification and Authentication IoT Users	Account Management	Least Functionality
Protection of Information at Rest	System Security Plan	Mission/Business Process Definition	Information Security Program Plan

- Based on these re-occurring themes, a dozen critical security controls that apply almost to all IoT devices are explained in the following slides

IoT-1 Physical Access Control

- The manufacturer enforces access authorisations to the IoT device, verifying individual access authorisations before granting access to the IoT device, also controlling ingress/egress to it. The manufacturer maintains physical access audit logs and controls access to areas within the IoT device. The manufacturer inventories the environment of use and changes combinations and keys on the IoT device when combinations are compromised.
- **NIST Control Reference:** PE-3
  - https://nvd.nist.gov/800-53/Rev4/control/PE-3

IoT-2 Transmission Confidentiality and Integrity

- The IoT device protects the confidentiality and integrity of transmitted information
- **NIST Control Reference:** SC-8
  - https://nvd.nist.gov/800-53/Rev4/control/SC-8

IoT-3 Boundary Protection

- The IoT device monitors and controls communications at the external boundary of the system and at key internal boundaries within the system. Implements subnetworks for publicly accessible system components separated from the internal environment of use. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with the manufacturer's security architecture.
- **NIST Control Reference:** SC-7
  - https://nvd.nist.gov/800-53/Rev4/control/SC-7

IoT-4 Device Identification and Authentication

- The IoT device uniquely identifies other devices before establishing a local, remote, or network connection.
- **NIST Control Reference:** IA-3
  - https://nvd.nist.gov/800-53/Rev4/control/IA-3

IoT-5 Collaborative Computing Devices

- The IoT device prohibits remote activation of collaborative computing devices, except where the manufacturer explicitly allows it. Provides an explicit indication of use to users physically present at the devices.
- **NIST Control Reference:** SC-15
  - https://nvd.nist.gov/800-53/Rev4/control/SC-15

IoT-6 Identification and Authentication IoT Users

- The IoT device uniquely identifies and authenticates manufacturer users (or processes acting on behalf of manufacturer users).
- **NIST Control Reference:** IA-2
  - https://nvd.nist.gov/800-53/Rev4/control/IA-2

IoT-7 Account Management

- The manufacturer identifies nd selects the system accounts to support the missions/business functions. Assigns account managers and establishes conditions for group and role membership. The manufacturer, or the owner creates, enables, modifies, disables and removes IoT device accounts in accordance with manufacturer-defined procedures or conditions. Notifies account managers, authorizes access and reviews accounts for compliance with account management requirements. Manages group credentials.
- **Reference**
- AC-2
- https://nvd.nist.gov/800-53/Rev4/control/AC-2

IoT-8 Least Functionality

- The manufacturer configures the IoT device to provide only essential capabilities. The manufacturer also prohibits or restricts the use of the a set of defined functions, ports, protocols and/or services.
- **Reference**
- CM-7
- https://nvd.nist.gov/800-53/Rev4/control/CM-7

IoT-9 Protection of Information at Rest

- The IoT device protects the confidentiality and integrity of information at rest.
- **NIST Control Reference:** SC-28
  - https://nvd.nist.gov/800-53/Rev4/control/SC-28

IoT-10 System Security Plan

- The manufacturer develops a security plan consistent with their enterprise architecture and explicitly defines the authorisation boundaries. Describes the operational context and operational environment of the IoT device in terms of missions and business processes. Provides an overview of the security requirements for the system. Describes security controls in place to meet these requirements, including reasons. Reviews, updates and protects the plan from authorised disclosure and modification.
- **NIST Control Reference:** PL-2
  - https://nvd.nist.gov/800-53/Rev4/control/PL-2

IoT-11 Mission/Business Process Definition

- The manufacturer defines mission/business processes with consideration for information security and the resulting risk to environment of use operations, manufacturer assets, individuals, other manufacturers and the nation. Determines information protection needs arising from the de ned mission/business processes and revises the processes as necessary until achievable protection needs are obtained.
- **NIST Control Reference:** PM-11
  - https://nvd.nist.gov/800-53/Rev4/control/PM-11/

IoT-12 Information Security Program Plan

- The manufacturer develops and disseminates an information security program plan. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements. Coordinates among organizational entities responsible for the different aspects of information security Ensures approval of the plan by a senior official with responsibility and accountability for the risk.
- **NIST Control Reference:** PM-1
  - https://nvd.nist.gov/800-53/Rev4/control/PM-1

Conclusion

- A short list of 12 NIST controls, customised for IoT was presented.
- With this list you can conduct a technology-agnostic audit
  - Based on the purpose and
  - Environment of use of the IoT device
- Hopefully, this will serve as motivation towards *IoT devices one day having a white goods equivalent rating scale, measuring not energy, but the amount of security in the presence of security controls.*

http://twelveiotcontrols.com