**IoT Security Development Framework for Building Trustworthy Smart Car Service notes**

**II. Background**

**CAN**

Car Area Network is a distributed protocol of short messages (signals and measurement values). Major faults with CAN:

* + Node stuck-at-bit fault - faulty node sends constant bit value preventing other nodes from communicating
  + Medium break-up fault - CAN bus split due to damage
  + Babbling idiot fault - node floods CAN bus with high priority messages

**Smart Vehicles Cyber Security**

Smart Vehicle (SV) networks distributed frameworks leave it open to attack. Types of attacks:

* + indirect physical attack
  + short-range wireless access
  + long range wireless access

Autonomous Car (AC) is a special category of SV. An AC has five basic functions:

* + Perception - sense surrounding environment
  + Localization - find position
  + Planning - determine future motion
  + Control - guidance following plan
  + System Management - supervise the overall system

**IoT Cyber Security**

Traditional IT security solutions not applicable to IoT because:

* + IoT extends internet to all devices
  + Smaller devices may not support complex security protocols
  + Multiple entry points and vulnerabilities when all "things" communicate
  + Device IoT services could be shared

**Intrusion Detection System (IDS) and threat model**

Current cyber security solutions are not effective. Two basic intrusion detections techniques:

* Signature based - builds a database of known attack signatures
* Anomaly based – detect new attacks by defining a baseline model of normal behavior.

A threat model is used during design to mitigate potential threats. Steps to create a threat model:

* + Identify attackers
  + Rank threats
  + Choose mitigation strategies
  + Build mitigation solutions

**III. IoT Architecture for Smart Car Services**

IoT SV services use hierarchical architecture:

* + Layer 1 - physical devices and statuses
  + Layer 2 - communication layer between low level devices
  + Layer 3 - services layer provides common middleware and functions
  + Layer 4 - application layer provides custom apps for user needs

**IV. IoT Security Development Framework (ISDF)**

**Secure and Trustworthy Services**

Trustworthy service - one which can self-protect against cyber attack and continue to operate normally despite faults

IoT security is maintained in all layers by using:

* + Authentication - secure identification
  + Authorization - limiting access
  + Integrity - detect whether an object was modified illegally
  + Non-repudiation - prove messages have been sent and received

**IDSF Architecture**

2-D architecture with four layers, each layer has four planes. Descriptions below:

|  |  |  |  |
| --- | --- | --- | --- |
| **Attack Surface** | **Target** | **Impact** | **Mitigation Mechanism** |
| **End-Devices Layer** | | | |
| Controllers | Control, information | Control, human life, safety, time | IDS, behavioral analysis |
| Sensors | Information, access to system | Control, human life, safety, money, energy | Lightweight encryption, IDS, behavior analysis, sensor authentication |
| Actuators | Control | Control, human life, safety, time, money | Lightweight encryption, IDS, ABA, anti-jamming |
| Entertainment | Access to the system | Time, energy, money | Encryption, moving target defense, ABA |
| **Communications Layer** | | | |
| Protocols | Access, information, control | Control, human life, safety, time, money, energy | Authentication, access control, IDS, ABA, anti-jamming |
| Firewalls | Access to system | Time, money, reputation | IDS, behavior analysis, authentication |
| Routers | Access, information | Control, human life, safety, time | IDS, ABA, anti-jamming |
| Comms Bus | Information, control | Privacy, money, human life, safety, time | Encryption, IDS, ABA, moving target defense |
| **Services Layer** | | | |
| Cloud storage | Personal and confidential information | Information, money, time , safety | Encryption, IDS, moving target defense, analysis |
| Web services | Control, monitor | Control, human life, safety, money | Authentication, IDS, behavior analysis |
| **Applications Layer** | | | |
| Mobile devices | Information control | Human life, safety, loss of personal info and money | Authentication, access control, IDS, behavior analysis |
| Programs and apps | Access to the system, control, information | Time, money, safety, reputation | IDS, behavior analysis, authentication |