IOT-Input devices

Part-1

Requirements analysis

**Team:**

Alfred Augustine

Sahil S

Ananya M

Vinutha B

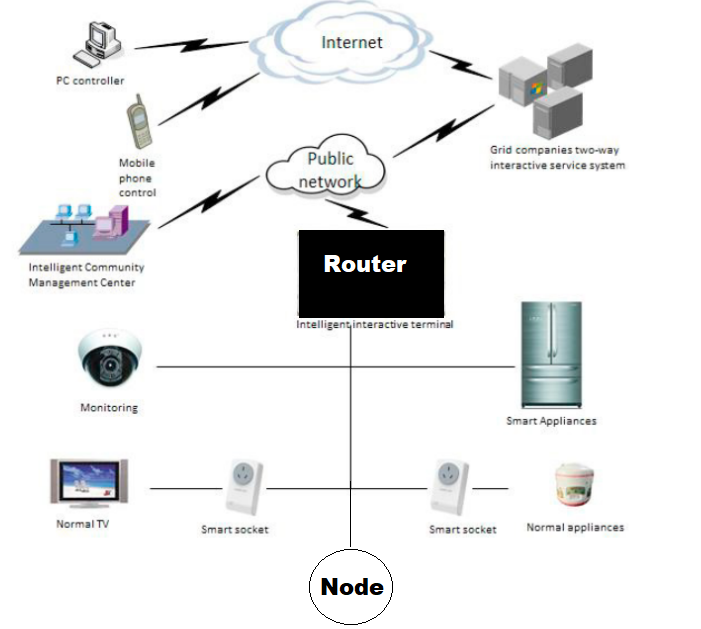
**Devices:**

1. ESP-8266
2. Home IOT devices
3. Attacker devices - laptop with raw socket sniffing enabled
4. Router

**Technology:**

1. Standard home architecture preview(P1)
2. Sniffing, spoofing, IOT attack strategies
3. Cloud computing

**Layout planned:**



Ref:P1

**Implementation:**

Implementation uses Experimental test cases, Control test cases to generate lab results.

The method of execution will involve:

1. Device
2. Communication
3. Logging
4. Attack methodology
5. **Device:**

**Input** to the device will be in the form of recurring commands.

These will be pre-programmed scripts embedded into the devices to emulate the defined architecture.

Psuedo-code:

*Packet=packet(data,headers,flags) #packet construction*

*While (true):*

*Send(packet,protocol,deviceID)# sends packet on protocol to device*

*Sleep(30) #sleeps 30 secs*

1. **Communication:**

The expected problem with this would be interception of logs by the attack methodology implemented, the countermeasure to this would be to either, ensure logging done locally, alternatively, there can be bursts of data sent in intervals. This real-time, batch data has a slight delay in relay of data but ensures continuity in operation.

Device communication is done through the 802.1.1 standard used in in-home devices.

Psuedo-Code:

*Encrypt(packet) #performs required encryption for given device*

*Send(packet,protocol,deviceID, specifier) # Defines packet type, protocol, deviceID, other flags*

1. **Logging:**

The data collected is logged and sent to the Router, and eventually the cloud network.

The data logged will be:

* 1. Communications sent - device
  2. Communications received - device
  3. Interceptions performed – Attacker
  4. Packets stolen – Attacker
  5. Packets decrypted – Attacker

1. **Attack methodology:**

The methodologies implemented will vary depending on the test employed,

Commonly used wi-fi standards can be directly implemented on network stack of the ESP devices, directly implementing control and experimental setups.

Devices working in non-standard wireless standards such as RF/ Infra, can have their network stack implemented on the IOT device, with the physical layer replaced with Wi-Fi standard with adequate virtualization to emulate non-standard stacks.

**Papers:**

1. Li, Min & Gu, Wenbin & Chen, Wei & He, Yeshen & Wu, Yannian & Zhang, Yiying. (2018). Smart Home: Architecture, Technologies and Systems. Procedia Computer Science. 131. 393-400. 10.1016/j.procs.2018.04.219.