IoT DDoS usecases
draft-faibish-iot-ddos-usecases-00

Sorin Faibish <faibish.sorin@dell.com>
IoT DDoS use cases

• The IoT can be used by hackers to start DDoS attacks either by:
  • Generating random traffic
  • Reflecting and or amplifying traffic

• There are 3 ways to connect IoT devices to outside the TA
  • Connected directly to the TAM
  • Connected via a TEEP broker
  • Connected using TEE and multiple TAM’s
IoT DDoS use cases

• Can TEEP address/prevent such attacks? Is this in TEEP charter?

• Types of attacks
  • Generate random traffic packets instead of data sent to operator or cloud
  • Reflect or amplify network traffic
  • Using man-in-the-middle to insert malware generating traffic
  • Use legitimate traffic at much higher volume to flood the network
  • Can be triggered by a signal from operator or during the code upgrade
Use case 1: Upgradable OS less IoT devices

• Assumptions for the use case:
  • Device allows SW upgrades
  • Device is transmitting data back to the service provider or public cloud

• Attack opportunities:
  • Can be externally triggered to transmit random packets or amplified data to SP
  • Can be internally triggered by time
Use case 2: IoT devices connected to gateway

Assumptions for the use case:
- Device receives SW updates secured via the edge server
- Device is transmitting data outside the service provider or public cloud

Attack opportunities:
- Can be internally triggered by time to transmit random packets unfiltered by gateway
- Can be triggered to transmit amplified legitimate traffic

IETF 105 - TEEP WG
Use case 3: Smart IoT devices with rich OS

• Assumptions for the use case:
  • Device allows SW upgrades
  • Device is transmitting data back to the service provider or public cloud

• Attack opportunities:
  • Can be externally triggered to transmit random packets or amplified data to SP
  • Can be internally triggered by time
Specific Examples

• Use cases 1: IoT sensors and meters, health monitors, weather monitors, traffic controllers, public cameras
• Use cases 2: home security and management systems, smart buildings systems, smart cities and smart clouds, hospital servers
• Use cases 3: smart cars, smart air quality sensors, buildings security systems
• Non-use cases: small appliances with no OS, IoT devices not-connected (used for simple functions: garden irrigation, lights, thermostats)
TEEP WG asks

• Should TEEP WG address these use cases in the architecture draft
• Is TEEP the right security protocol against DDoS
• Should this draft be part of TEEP WG
• Does TEEP WG need more detailed protocol implementation
• Ready to adopt as TEEP WG document?