IoT

The new and dangerous internet world!

November 16, 2016

Tony and Tim

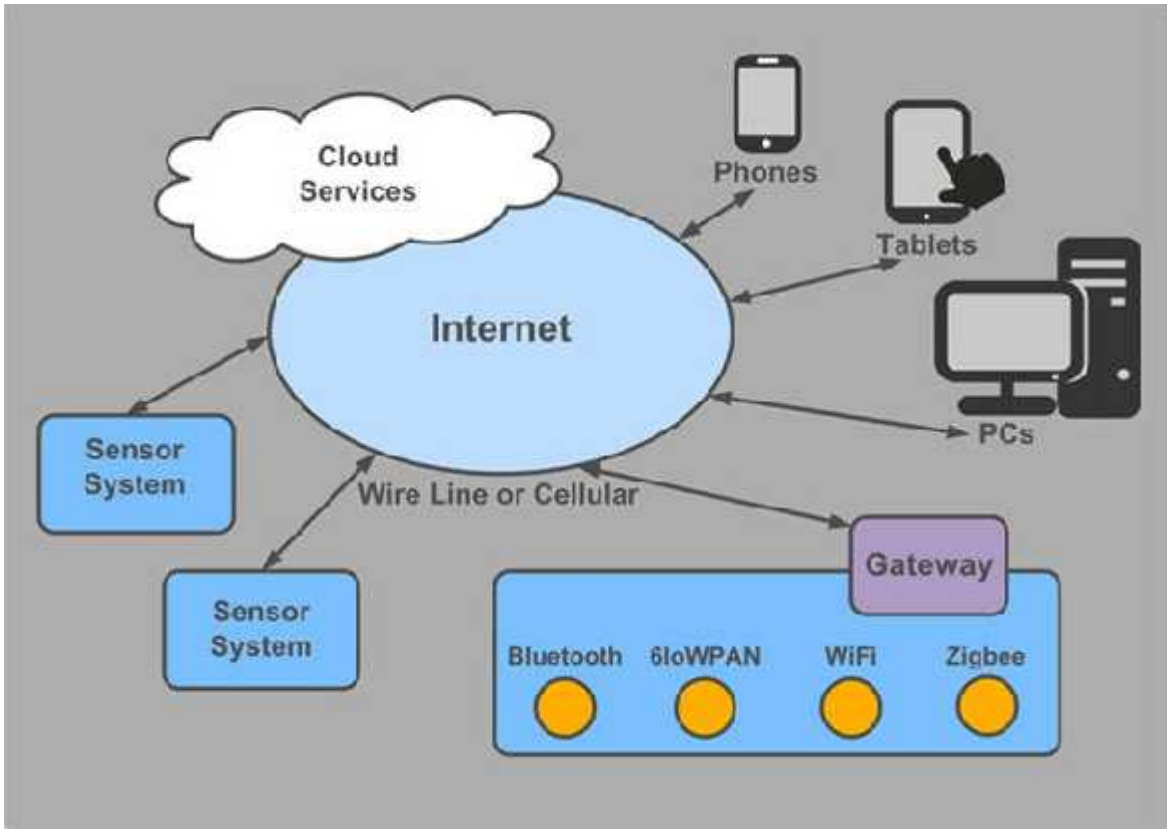
WWW.LoveMyTool.com

By – Tim O'Neill
The Oldcommguy®

What is IoT

- The acronym for The Internet of Things
  - Many things
  - Easy access and visibility – maybe private things
- Currently totally unregulated!
- Can control our homes, cars, industry, medical devices (like my leg), utilities, transportation, etc
- Personal information
  - Invasion into privacy!

IoT connectivity



IoT devices automatically try to force connection to their hosts!
They will even try to connect through your car to send their sensor information!
<u>Without users permission!</u>

IoT Layers

- **Infrastructure** (6LowPAN, IPv4/IPv6, RPL, NanoIP)
- **Identification** (EPC, uCode, IPv6, URIs)
- **Comms / Transport** (Wifi, Bluetooth, LPWAN, IEEE 802.15 – Zigbee, ISA100.11a, EnOcean, GPRS/2G/3G/4G cellular, 40+ methods)
- **Discovery** (Physical Web, mDNS, DNS-SD)
- **Data Protocols** (MQTT, CoAP, AMQP, Websocket, Node, Mosquito)
- **Device Management** (TR-069, OMA-DM)
- **Semantic** (JSON-LD, Web Thing Model)
- **Multi-layer Frameworks** (Alljoyn, IoTivity, Weave, Homekit)

These are about 10% of the known layers methods!

Only about 20% are defined as a standard!

IoT Security issues

- Open access easy to hack and Bot
- Recently several IoT devices were used as Bots in the DDOS internet attacks
  - No easy way to track
  - No easy way to stop
  - New strain of IoT attack - Mirai scours the Web for IoT devices protected by little more than factory-default usernames and passwords, and then enlists the devices in attacks that hurl junk traffic at an online target until it can no longer accommodate legitimate visitors or users.
  - The recent attack cyber criminals began training their attack cannons on **Dyn**, an Internet infrastructure company that provides critical technology services to some of the Internet's top destinations.
  - The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix…etc

DDOS/DNS amplification using IoT devices

- DNS amplification attack (aka DNS reflection attack)
  - Advanced (DDos) attack using Botted IoT devices
  - Using the advantage that a small DNS query can generate a much larger response.
- When combined with source address spoofing, an attacker can direct a large volume of network traffic to a target system/address /URL by initiating relatively small DNS queries.
- The amplification factor in this type of attack depends on the type of DNS query and whether or not a DNS server (used as a middleman in the attack) supports sending large UDP packets in a response.
  - If the DNS server does not support large (>512 bytes) UDP packets in a response, it can revert to TCP. This reduces the effectiveness of an amplification attack because TCP is much less vulnerable to source address spoofing.

IoT DDOS attack needs

- An attacker who is planning a DNS amplification attack can take advantage of the following:
  - **Factory settings and passwords:** in about 90+% of IoT devices
  - **Open recursion**: Name servers on the Internet that have recursion enabled and provide recursive DNS responses to anyone are referred to as “open resolvers.” The number of DNS servers providing open recursion have been estimated to be several hundred thousand to several million. In a DNS amplification attack, the open resolver functions as the source of amplification, receiving a small DNS query and returning a much larger DNS response.
  - **Source address spoofing**: Source address spoofing alters a packet's return address so that the packet appears to have come from a source other than the sender. In a DNS amplification attack, the source address for the DNS query is spoofed with the target of the attack, similar to a “Smurf” attack. The response is redirected.
  - **Botnets**: Botnets are groups of online computers that have been compromised by an attacker. Botnets are used in a DNS amp attacks to send DNS queries to open resolvers in a gang attack form
  - **Malware**: Malware like Mirai, can be used to gain access to or create botnet devices, like IoT devices and provide a means to trigger DNS amplification attacks/DDOS.
  - **EDNS0**: Extension Mechanisms for DNS (RFC 2671) allow DNS requestors to advertise the size of their UDP packets and facilitate the transfer of packets larger than 512 bytes, up to 8 times larger!
  - **DNSSEC**: DNSSEC adds security to DNS responses by providing for DNS servers to validate DNS responses. DNSSEC prevents cache-poisoning attacks, but adds cryptographic signatures resulting in larger DNS message sizes to be used in attacks.

IoT Technical Future

- IPv4 has a limited address field
- IoT will thrive in the IPv6 environment
- Soon IoT devices can be attacked through their open IPv6 advertisements, ICMP v3
- High end RF access technologies
  - Many different types of access in one device
- Low end security and protection
- Amount of Data collected and shared
- Technical demand for knowledge of IoT invasion

IoT Summary

- Not controlled
- Not secure
- Power struggle for bandwidth
- Many access methods
- Loss of privacy
- Loss of control
- Hidden access and unknown information
- Easy to Bot
- Vulnerable by IPv4 and or IPv6 attacks

IoT future

- Manufacturers pushing for inclusion
  - Refrigerators, freezers, TV's, even computers and even toilets (some 100K$), security applications, Medical monitoring and much more!
- Users need to have the ability to turn off
  - Control access
  - Control information being shared
    - Audio
    - Video and other imaging info
    - Usage parameters
    - Medical info
- Needs built in and updated security
- Scary invasion into our lives

Questions?

Thinking is never driven
by answers
but driven
by Questions