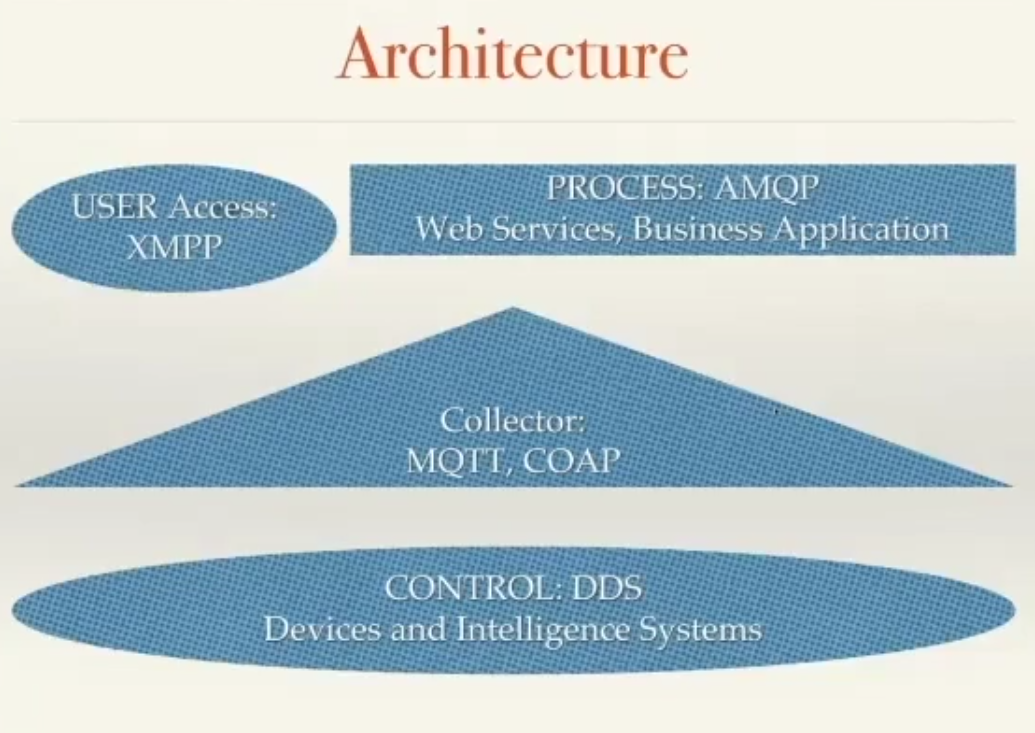
IoT protocols

* IoT data Protocols (presentation/ Application layer)
  + Used to connect to low-power IoT devices
  + Use wired or cellular network for connectivity.
  + Examples
    - MQTT (Message Queuing Telemetry Transport)
      * Lightweight IoT data protocol (so low power consumption)
      * Used the publisher-subscriber messaging model
      * Allows simple data flow between different devices
    - CoAP (Constrained Application Protocol)
      * Application layer protocol
      * Designed to address the needs of HTTP-based IoT systems
      * CoAP can be used instead of HTTP with low overhead, easy to make use of, had the ability to enable multicast support.
    - AMQP (Advanced Message Queuing Protocol)
      * Open standard application layer protocol
      * Since this protocol consider as heavy, it is not recommended to use with IoT sensors with limited memory.
      * Used to perform transactional messages between servers
      * Used in banking industry because of its security level and reliability where the server-based analytical environments are required.
    - DDS (Data Distribution Service)
      * Considered “The First Open International Middleware IoT Standard”
      * Works in publisher-subscriber model
      * Can be deployed in variety of settings such as from Cloud to small devices
      * DDS can exchange and make use of information, which is independent of the software and the hardware platform, unlike MQTT.
    - HTTP (Hyper Text Transfer Protocol)
      * Not that much preferable in IoT industry because of the cost, power consumption and weight issues
      * Used in 3D printing and manufacturing industries. Because it can publish large amount of data.
    - WebSocket
      * Messages can be sent between the server and client using a single TCP connection
      * WebSocket protocol reduces the complexity and difficulties in management of connection and bi-direction communication on the internet.
      * Commonly used in places where the client-server architecture is there.
      * As well as in runtime environments or libraries.
* Network Protocols (Datalink / physical layer)
  + Used to connect devices over a network
  + Typically used over the internet.
    - WiFi
      * Provides the internet connection to devices within the range
      * Uses the radio waves in frequencies 2.4GHz and 5GHz channels.
    - Bluetooth
      * Generally shorter range and tends to frequency hop.
      * Bluetooth 4.0 standard guarantees the maximum data transfer rate up to 3 Mbps.
    - ZigBee
      * Has low power consumption along with high security features, low data range and has a longer communication range.
      * Simple packet data exchange protocol and implemented in devices such as microcontrollers and sensors.
    - Z-Wave
      * Wireless, RF cased communication technology
      * Used in IoT home based applications
      * Operates at 800-900Mhz RF delivers no interference problems with other protocols.
      * The device frequency which Z-Wave operates is based on location (country). So, need to consider that factor before purchasing.
      * Not recommended to use within the business world.
    - LoRaWan
      * MAC (Media Access Control) IoT protocol
      * Long-range wireless connection allows low-powered devices to communicate with internet-connected application directly.
      * Data rate is 50Kbps and sends to the LoRaWAN server.
      * It can be mapped to both Data link and Network Layer of the OSI stack.
      * Communication Range 2-3Kms
    - EnOcean
      * Ultra-low power and **energy harvesting**
      * Communication Range is 30-100 fts
      * Data rate 124 Kbps, data is typically sending to a gateway and gateway routes it to the destination (cloud)

<https://www.nabto.com/guide-iot-protocols-standards/>

<https://www.pressac.com/insights/enocean-or-lorawan-which-iot-protocol-is-right-for-your-smart-building-project/>



Most of the time hackers are trying to use IoT devices as hostiles to launch large-scale DDoS attacks.

Application Types

* Personal of things - interactive, intelligence, wearable
* Home application - gadget, TV, Game console, HVAC
* Home automation - surveillance, remote management, distance operation, logistic supply, healthcare, security
* Industrial control - remote chain manufacturing control
* Large scale public service management
* Defense security

Protocol

* MQTT
* AMQP
  + Used for distributed network
  + Message orientation
  + queuing
  + routing (including p2p and publish-subscribe)
  + Reliability
  + Security
* XMPP Protocol

Privay Challenges

* Personal data and "things" protection
* Managing multiple access across "things"
* Stronger authentication factors (biometrics)
* End to end encrption required at any level
* HSM (Hardware Security Module) based key

Four Primary Connection use cases

* Cloud Connect (Calling Home)
* Self-Connect (Switch and Light)
* Bridge/Server Connect (Reliably there)
* Local User app connect (Unreliability is there)

IDEAL Requirements

* No internet dependencies - local bootstrap
* Root CA Checks
* MITM resistant
* User model
* But no locking
* An authorization models

IOT Comman attack protocol - CoAP, Zigbee, DTLS

IOT comman protocol - MQTT, Zigbee, CoAP, AMQP, XMPP

UDP flooding (CoAP protocol)

Hacking Smart Light Bulb using Bluetooth (Remote Access) [after analizing the bluetooth packet we can get the valubel infomation]

Gateway Exploit (firmware update) - Cloud communication

Identity Spoofing – impersonating as CoAP client [The attacker can then enable remote-access on the device by registering as a legitimate user by sending an appropriate SOAP-formatted POST command]