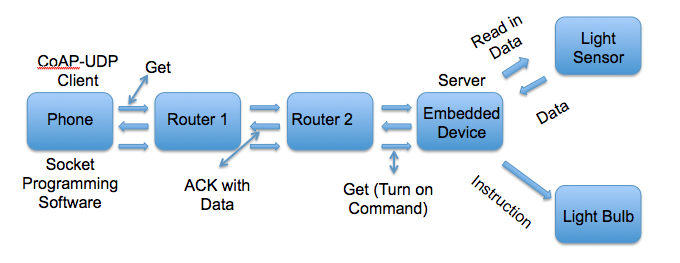
**Application Layer**

1. CoAP (Constrained Application Protocol) is an application layer protocol. It is used in resource-constrained internet devices, such as WSN (wireless sensor network) nodes. One of the benefits for IoT application development is that is designed to easily translate to HTTP for simplified integration in the web, while also meeting specialized requirements such as multicast support, very low overhead, and simplicity. Some IoT applications have constraints due to the devices used, low power or constrained memory. Therefore, having a way to integrate to the web in a simplified way and with specialized requirements can be useful for diverse IoT applications.
2. CoAP is designed to be lightweight and efficient, so it can be used by embedded devices used in IoT with limited processing power and memory. Moreover, UDP is often used in CoAP because it is lightweight as well. Unlike HTTP, it is designed to work on the UDP protocol, instead of TCP. Furthermore, CoAP is a simplified version of HTTP for IoT and WSNs. Since CoAP is simpler than HTTP, it will have lower latency (inactive period) and draw less power.

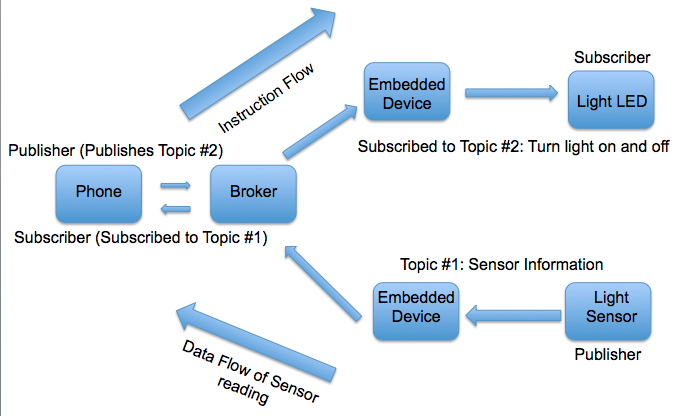
3) Assuming the are two routers in two different rooms to guarantee a connection.

4) MQTT stands for MQ Telemetry Transport. It is a publish/subscribe, extremely simple and lightweight messaging protocol, designed for constrained devices and low-bandwidth, low data rate, high-latency or unreliable networks.

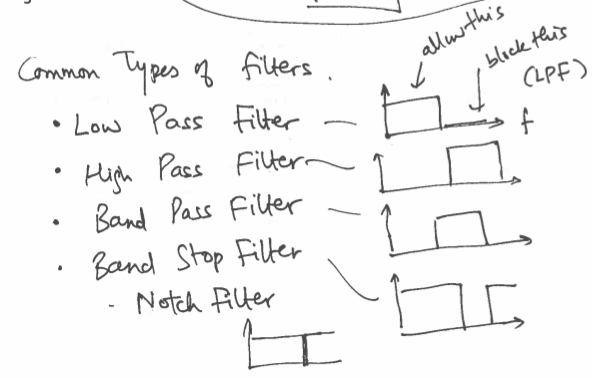
MQTT offers a number of advantages over HTTP. MQTT features faster response and throughput, and lower battery and bandwidth usage. Therefore, MQTT is a good option when connectivity is intermittent, an enterprise application needs to interact with one or more phone apps, and phone or table apps need to send data reliably without requiring code retry logic. Furthermore, MQTT is integrated with enterprise messaging middleware, so it works with enterprise-level applications that push data to mobile apps. Overall, MQTT is designed for low latency, assured messaging, and efficient distribution. In contrast, HTTP is not optimized for low power usage or minimizing the amount of bytes flowing. As a result, MQTT is better for IoT application development due to constrained devices used in this field.

5) MQTT is a many-to-many communication protocol for passing messages between multiple clients through a broker. MQTT is really good for communicating live data. In contrast, CoAP is primarily one-to-one protocol for transferring state information between client and server. Moreover, MQTT subscribers make a TCP connection to a broker and CoAP subscribers and servers both send and receive UDP packets.

6) Phone will be used as publisher and subscriber. Also, this diagram is drawn assuming that the light LED and the light sensor use different embedded devices



**Signal Processing**

7)

Low pass filter: it is used to let low frequencies pass, filtering out high frequencies.

High pass filter: it is used to let high frequencies pass, filtering out low frequencies.

Band pass filter: it allows middle frequencies pass, filtering out undesired high and low frequencies.

Notch filter: it is a type of band stop filter. Band stop filters do not allow middle frequencies to pass. Therefore, notch filters allow a narrower range of frequencies to go through.

8) JPEG compression is used for photographs and images. JPEGs eliminatess information that is difficult for the human vision to distinguish. This encoding combines three different methods of image compression: downsampling the chrominance channels, quantization of the discrete cosine transformation, and entropy coding.

Method 1: Downsampling the chrominance channels. JPEG files convert images to the YCbCr system, Green (Y), Blue (Cb), and Red (Cr). Then, it downsamples both blue and red channels by a factor of 2 in both width and height because this has almost no visual effect.

Method 2: Quantization of the discrete cosine transformation. An arbitrary square of 8x8 pixels is chosen and decomposed into a combination of the basis images. Using discrete cosine transform from Fourier transformation theory, a signal (an image) is decomposed into the arbitrary square in O(n logn) time. This is possible because the images are formed by cosine waves of various frequencies in the x and y directions.

Method 3: Entropy coding. Compared to method 1 and method 2, method 3 is lossless. The 8x8 grid of integers is turned into a linear sequence of integers. The sequence starts at the top-left corner and zig-zag in a diagonal pattern across the matrix, going back an forth until we reach the lower-right corner. This sequence is chosen due to distortion from method 2 because distortion in the lower-right corner is not noticeable by human vision. Furthermore, the human eye pays more attention to the upper-right corner of the image. Then the encoding algorithm used for GIF files is applied. Finally, a Huffman compression is applied to the resulting sequence.

9) From class notes, there are two types of errors in binary classification: sleeping or not. False negative: true state is sleeping, but it says not sleeping. False positive: it is not sleeping (it is awake), but it says that it is sleeping. One example of a two-state classification is a sensor used to detect motion. When it detects a person getting close, a light bulb will turn on to light the area where the person is located. The sensor can only detect the motion of a certain range. Therefore, if a person needs the area to be lit, but if it is out of range due to the threshold, then it will end up being a false negative because the sensor will think there is not a person nearby. If the threshold is increased, then the system can end up having more false positives because probably a person whose intentions are not for the light bulb to get lit will trigger the sensor and turn on the light. As a result, energy is wasted. Consequently, as the threshold is increased (more distance is accepted as the threshold) the probability of false positives increases and the probability of false negatives decreases. As the threshold decreases, the false negatives will increases and the false positives will decreases because the person will have to be closer to the sensor.

**Security**

10)

Confidentiality: encrypting data so only relevant parties can use it.

Integrity:

* Verifying the source
* Avoiding getting fraudulent data
* There is no confidentiality. Therefore, anyone can see the data.

Availability:

* Data, services, and network
* Applications are up and running whenever needed as intended.

They are different characteristics of security. Confidentiality is having end-to-end security. It is a system of communication where only relevant parties can decrypt the data, but the received might not be able to verify the validity of data received. If you want to make sure that the information comes from a valid source, then you want to focus in integrity. Availability makes sure that an application is ready to be used when needed.

Confidentiality (end-to-end security) is not Integrity (avoiding getting false data and verifying the source with hash functions). Also, Availability is not the same as Confidentiality and Integrity because they do not require that applications are available all the time.

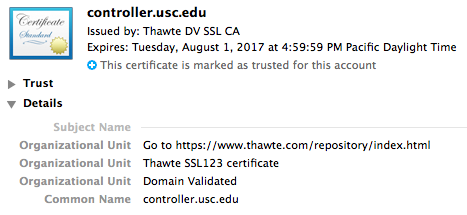
11) Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information. Currently, Intel is implementing native instructions for AES in its hardware.

It works by taking the data and loading it to a 4x4 square. Then, it XORs each input byte with the corresponding byte of the first round key. Then, it derives more keys from the initial key for later rounds. Then, it shifts the orther of the bytes in the last column. Afterwards, it is run through a substitution box. Later, that column is XOR with a “round constant” that changes every round. Finally, the first columnd is XOR of the previous round key. The other columns are XOR with the same column of the previous round key. Next, a series of steps are repeated several times. The number of repetitions depends on the size of the key.

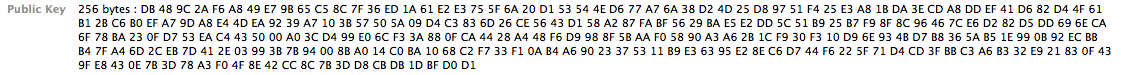
Later, confusion is applied (substitution of bytes). Then, diffusion is applied (rows are shifted and columns are mixed). Finally, key secrecy is applied (a round key is added). The more rounds the merrier. AES should be used as a building block to a decent “mode.”

12) To encrypt the message, I will need the public key of the person I want to receive the message. To ensure integrity of the message, I will use a hash function and the public key of the person I want to receive the message.

13) A replay attack is a form of network attack in where data transmission is fraudulently repeated or delayed. In the case for a keyless entry in cars, it can work even if an encrypted channel is used if a hacker records the message that the owner of the car sends to the car to open it. Then, the hacker can open the car at all times. In order to prevent it, a nonce needs to be used regardless if asymmetric or symmetric key cryptography is used. With a nonce, if the owner of the car wants to open it, it sends a message to the car that requests the car to open. Then, the car sends a nonce, an arbitrary number that may only be used once. Then, the owner sends back the encrypted message that requests the car to open with the encrypted nonce. If a hacker records the message and tries to use it, that person would not be able to break into the car. This is due to the fact that the hacker does not have the private key or shared key (depending if asymmetric or symmetric key cryptography is used) of the car and cannot decrypt the message. Therefore, the hacker would not be able to know there is a nonce in the encrypted message. After sending the message to the car, the nonce from the hacker’s message would not match with the one generated by the car. As a result, the replay attack will fail.

14) 

1. Thawte DV SSL CA
2. The certificate expires on Tuesday, August 1, 2017
3. 256 bytes



1. Certification path: thawte Primary Root CA -> Thawte DV SSL CA -> controller.usc.edu

Root certification authority: thawte Primary Root CA

15)

1. AAA Certificate Services
2. AffirmTrust Commercial
3. CA Disig
4. Certigna
5. Federal Common Policy CA
6. thawte Primary Root CA

16) I will have to set up SSL (Secure Socket Layer) on my website. I will have to have my own dedicated IP address. Then, I will have to buy a certificate. Later, I will have to active my certificate. I will install the certificate. Finally, I will update my site to use https.

17) Denial of Service (DoS) is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intender users by disruption the services of a host connected to the Internet.

* Sha1 (Secure Hash Algorithm 1) is a cryptographic hash function designed by the NSA. It produces a 160-bit (20-byte) hash value known as a message digest.
* RSA (Rivest, Shamir, and Adleman) is one of the first practical public-key systems of cryptography. This system is widely used for secure data transmission.
* DDoS (Distributed Denial of Service) is a type of DoS attack where multiple compromised systems are infected with a Trojan. They are used to target a single system causing a DoS attack.
* Botnet is a network of private computers infected with malicious software and controlled as a group without the owners’ knowledge.
* UDP flood is a DoS attack using User Datagram Protocol (UDP). A UDP flood attack can be initiated by sending a large number of UDP packets to random ports on a remote host.
* SYN flood is a form of DoS attack in which an attacker sends a succession of SYN requests to a target’s system. This is because it is attempted to consume enough server resources to make the system unresponsive to legitimate traffic. SYN is a TCP packet sent to another computer requesting that a connection be established between them.
* Slowloris is a type of DoS attack. It allows a single machine to take down another machine’s web server with minimal bandwidth and side effects on unrelated services and ports. It tries to keep many connections to the target web server open and hold them open as long as possible.
* Homomorphic Encryption is a form of encryption that allows computations to be carried out on ciphertext. Therefore, it generates an encrypted result. When the encrypted result is decrypted, it matches the result of operations performed on the plaintext.
* SGX (Software Guard Extensions) is a set of new instructions from Intel that allows user-level code to allocate private regions of memory, called enclaves. Unlike normal process memory, it is also protected from processes running at a higher privilege levels.