Securing Corporate Airspace from the Internet of Radio Threats

-Harshit Agrawal

Overview:

• Corporate airspace is becoming increasingly vulnerable radio-based attacks.

• Visibility over devices capable of producing radio frequency in the premise and monitoring those to prevent possibility of attacks is required.

• Alert triggered on possibility of such attacks can enable corporates to alleviate the risk instantaneously and make corporate airspace more secure.

Abstract:

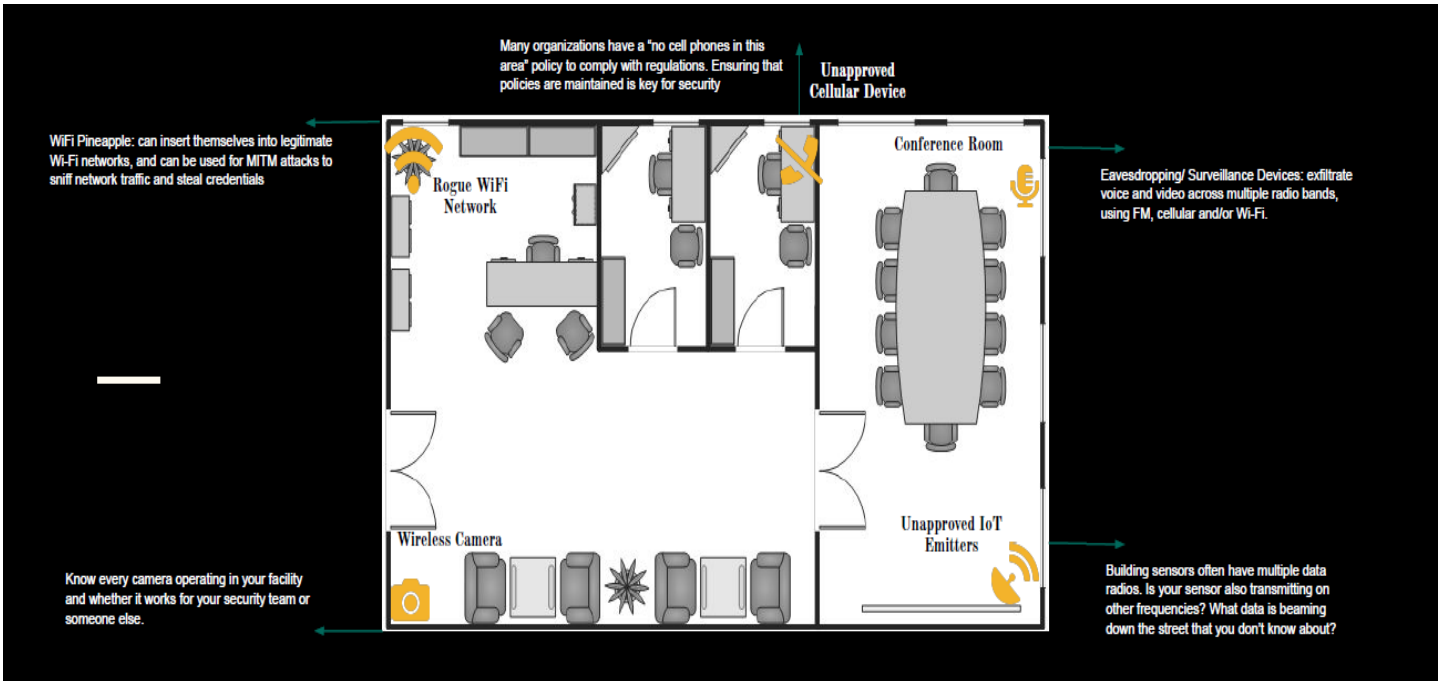
To secure the corporate/business airspace from internet of radio-based threats, Software Defined Radio based solution is a required which would:

• Monitor spectrum, to analyse different aspects of data/ devices in the premise to detect privacy violation

• Trigger alerts on active threats

• Show radio capable devices in the corporate airspace/ environment

It's one thing to have a "no cell phones in this area" policy. It's another thing to detect policy violations!



Background:

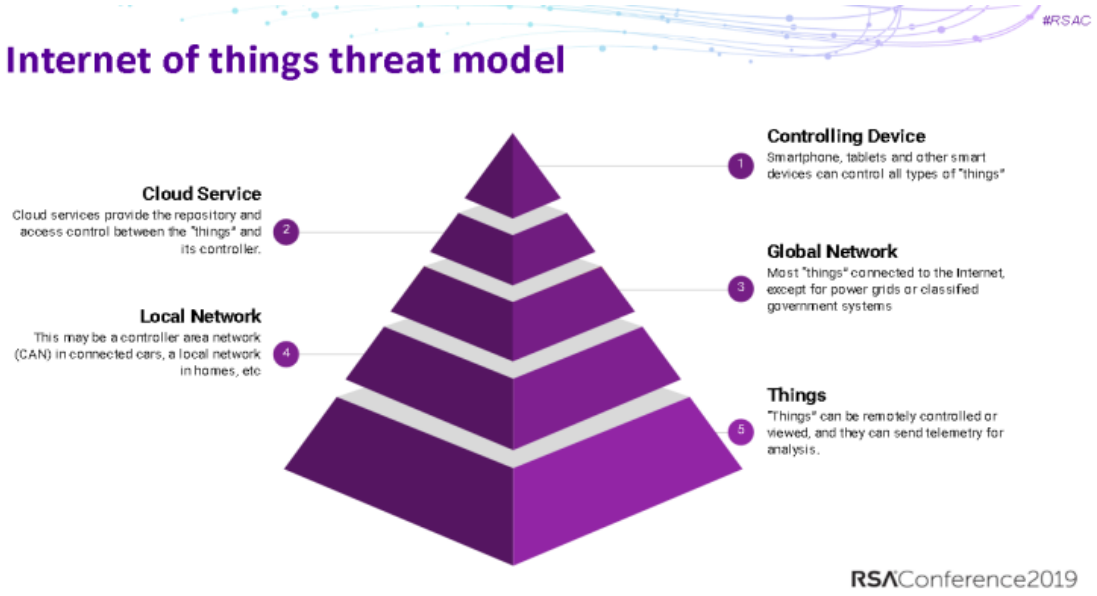
• 600% rise in IoT attacks in 2017-19, out of which 60% of devices are utilizing different wireless frequencies, according to threat report from security firm Symantec

• BYOD policies, sniffing through Logic-Tracker or strategic discussions monitoring, DDoS by high noise transmission in sensors, can give hacker entry to premise.

• Only 10 percent of device manufacturers reported feeling fully confident their devices had adequate security protocols in place.

• Security evaluations should be carried out against the following attack methods:

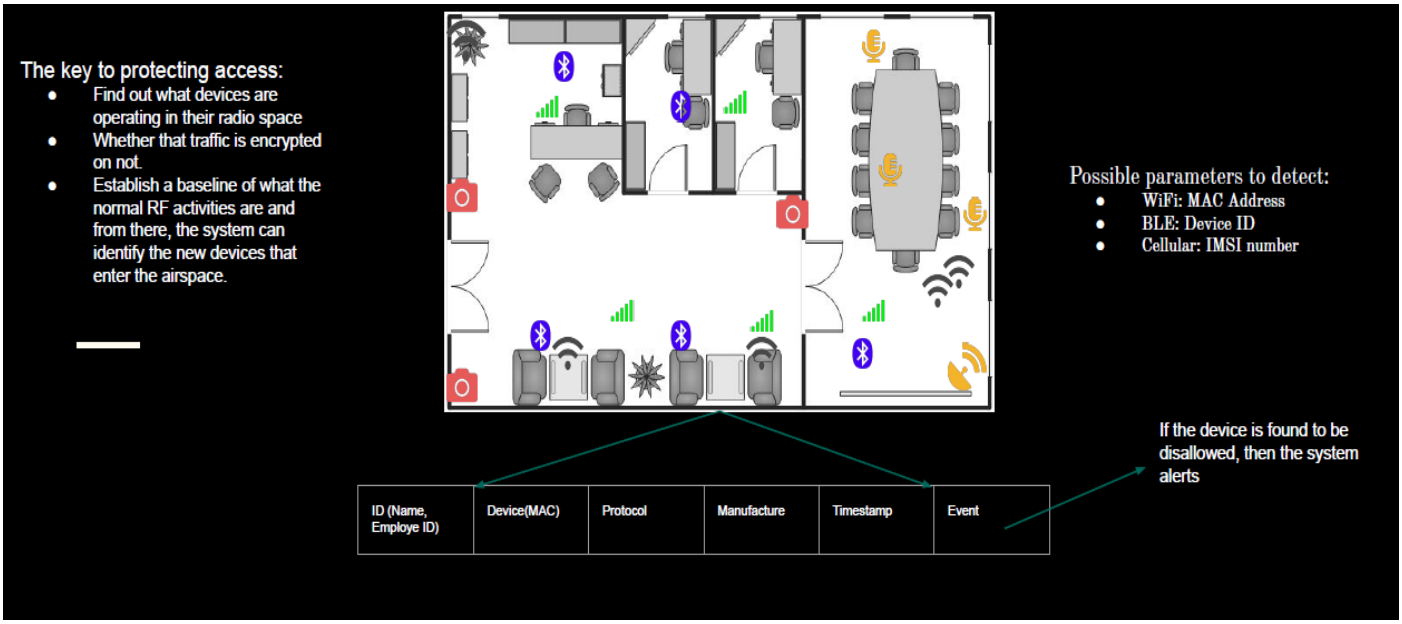
- Wireless packet sniffing
- Wireless signal replay
- wireless signal deception
- Wireless signal hi-jacking



End State:

- Monitoring/ visibility of devices (including shadow IT), detection and alerts of imminent radio-based attacks
- Inventory of radio capable devices in the premise
- Ease of functioning without concerns of BYOD policies, privacy violations
- Improved business performance

Possible Solution:



Technology innovation associated with solution:

As enterprises continue to grow and we're getting new smart devices, the boundaries are essentially eroding on a traditional perimeter. A firewall's not going to protect you from an RF based attack. Enterprise will need to be able to react to these new threats entering their environments through the Internet of Radios. The wireless defence must be designed based on attack surfaces. A reliable communication protocol, strong authentication method, strong communication encryption, and resistance to signal interference are the core of wireless security. Analysis needs to be carried out case by case. The solution will do analysis on the Physical layer of the OSI Model.