POWER REPLAY ATTACK IN ELECTRONIC DOOR LOCKS

ICS423

RYAN NAKATA

ABSTRACT

What is a Power Replay Attack?

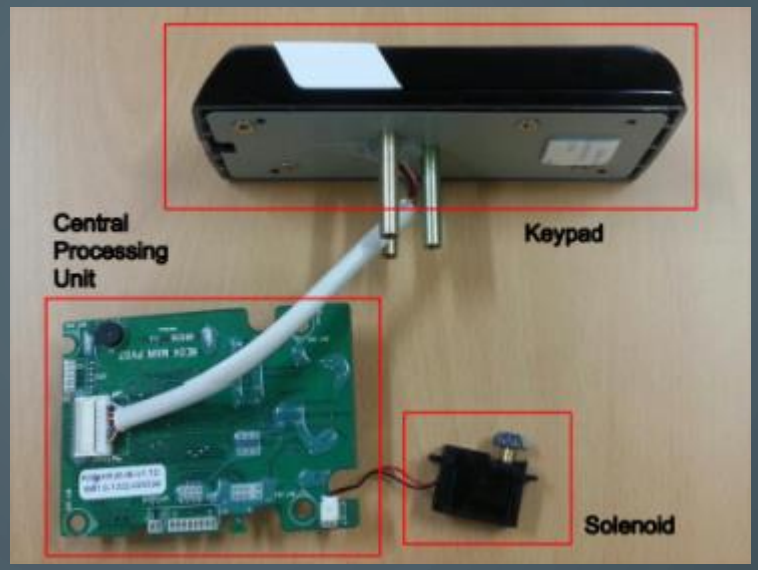
An insider attacker can covertly insert malicious hardware components into an electronic door lock to replay a valid DC voltage pulse to illegally open the door

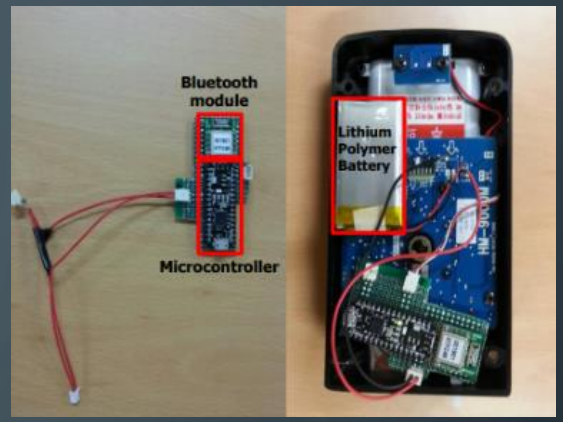
Simplified

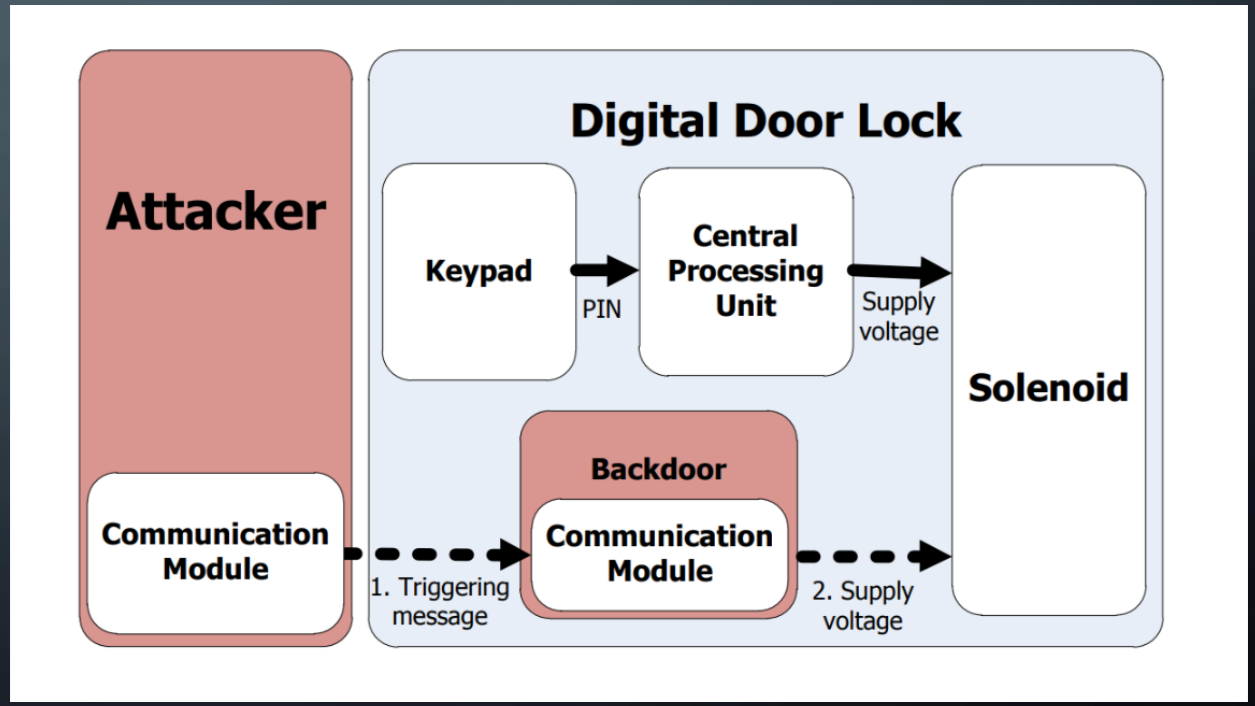
Activating actuator that engages lock.

Circumvent normal unlocking mechanism.

Backdoor using Bluetooth etc.







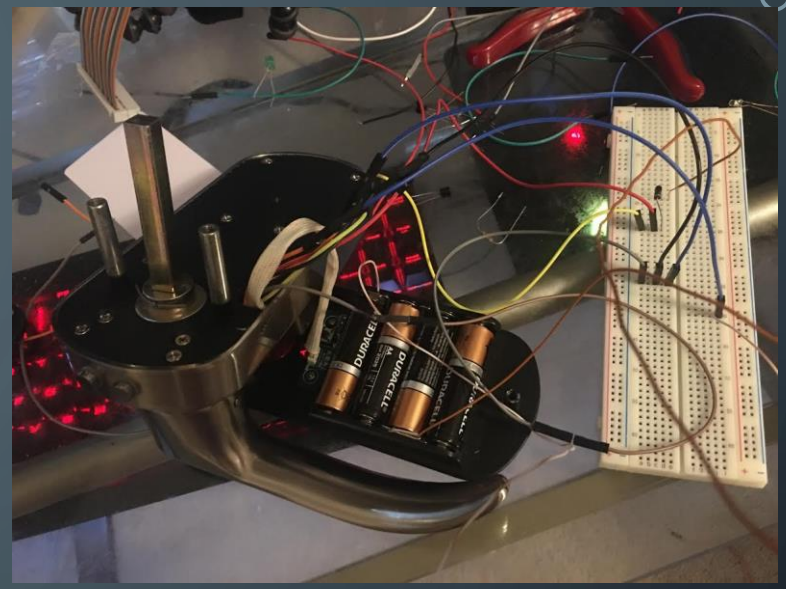
PROBLEMS, MOTIVATIONS AND CHALLENGES

Finding a way to install replay module (Gain temporary access rent)

In real world you don't have the luxury of testing. (scout out victim for model)

Many ways to communicate with communication module. (blue tooth, skimmer)

Finding out how to power module.



DEMO

Very discrete

Simple

Materials:

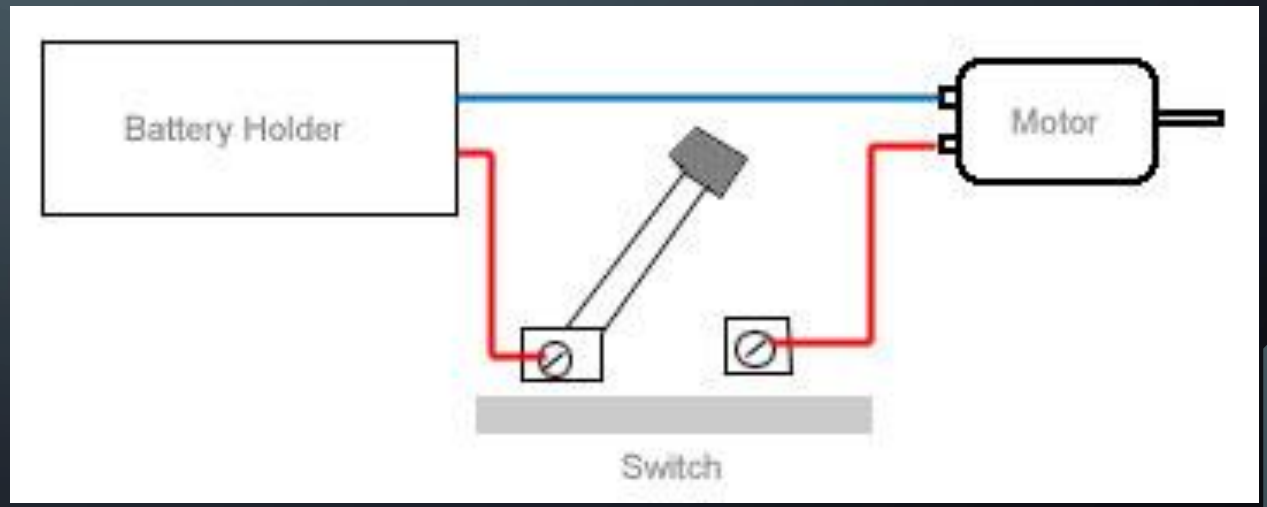
Electronic Door Lock

Wires

Can (Battery leads to steal power)

Diodes (preserves functionality of lock)

No Microcontroller



RELATED WORKS

Replay attacks:

Similar to card skimmers

A discrete backdoor circuit can be installed into any device to replay signals (thermostat(Mr robot))

SOLUTIONS

Posters solution

1.providing an alarm to warn users when the door lock was tampered

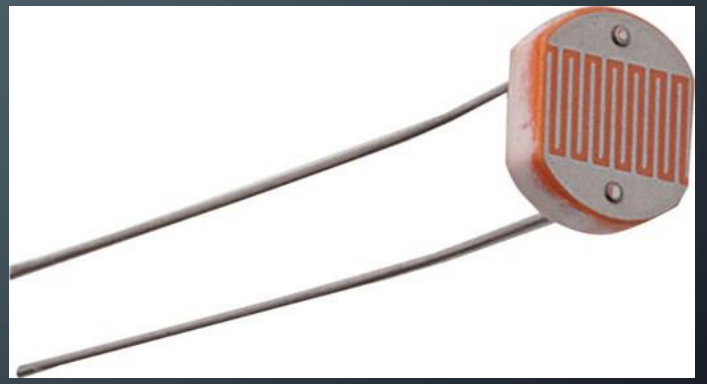
2.detecting additional hardware installation by sensing variations in the capacitances of inner circuit.

My solution

1.Light sensor

2.Destory the circuit board if cover is removed (Similar to security ink tags on clothes)

3.Remove attack vectors(Don't have a physical key, numpad and a Bluetooth module)



CONCLUSIONS

As analogue devices switch to digital we need to consider the security risks. (Door locks switched from keys to NFC/RFID)

European style locks are more secure than electronic door locks due to their lock picking counter measures.(good locks take hours to pick) (Physical locks cannot be tampered without destroying functionality)

Electronic locks are probably inevitable due to their convenience and this poster brings to light issues that are not normally thought about.

THANK YOU

Poster: Power Replay Attack in Electronic Door Locks
Seongyeol Oh, Joon-sung Yang, Andrea Bianchi, Hyoungshick Kim
College of Information and Communication Engineering Sungkyunkwan University Suwon, Republic of Korea
Email: {seongyeol, js.yang, abianchi, hyoung}@skku.edu