RAPIX SECURITY

22 OCT 2018

COURSE PURPOSE

Introduction to RAPIX Security.

This will help you to understand:

- Why security is important;
- The ways that systems are attacked (and fail);
- How RAPIX solves the security problems.

COURSE PURPOSE

Pre-requisites.

It is recommended that you have already completed:

- DALI Basics;
- RAPIX Introduction.

SECURITY

WHY IS IT NEEDED?

WHY IS SECURITY NEEDED?

sky NEWS

Sponsored By

Hacking Expert 'Took Control Of 200 Hotel Rooms'

A security consultant gains control of the lights, blinds and temperature systems of 200 luxury hotel rooms in China.

08:17, UK
Thursday 07 August 2014

The St Regis hotel in Shenzhen was targeted

The Register®
Biting the hand that feeds IT

DATA CENTRE | SOFTWARE | SECURITY | TRANSFORMATION | DEVOPS | BUSINESS | PERSONAL TECH

Security

81

IoT worm can hack Philips Hue lightbulbs, spread across cities

Easy chain reaction hack would spread across Paris, boffins say

By Darren Pauli 10 Nov 2016 at 06:02

SHARE ▼

Researchers have developed a proof-of-concept worm they say can rip through Philips Hue lightbulbs across entire cities – causing the insecure web-connected globes to flick on and off.

WHY IS SECURITY NEEDED?

WHY DOES SECURITY MATTER FOR LIGHTING?

It isn’t just lighting

- Also HVAC, Curtains & Blinds, Lift Control, Security Systems etc.
- Different systems are interconnected via BMS or LAN.
- Vector to attack other systems (as was done with Philips Hue).

WHY DOES SECURITY MATTER FOR LIGHTING?

Attacker’s Goal: Unauthorised Control of the System

Examples

- Switch off lights, HVAC or other systems to cause embarrassment, financial loss or inconvenience.
- Switch off lights, disarm security or other systems to facilitate physical intrusion.

WHY DOES SECURITY MATTER FOR LIGHTING?

Attacker’s Goal: Prevent legitimate use of system

Examples

- Disrupt use of system to cause embarrassment, financial loss or inconvenience.
- Prevent operation of systems to facilitate physical intrusion.

WHY DOES SECURITY MATTER FOR LIGHTING?

Attacker’s Goal: Unauthorised monitoring of the system

Examples

- Determine occupancy or system status to facilitate physical intrusion.
- Obtain user names, passwords or other useful information.
- Use information obtained for social engineering.
- Selling information obtained.

WHY DOES SECURITY MATTER FOR LIGHTING?

Attacker's Goal: Unauthorised modifications to the system

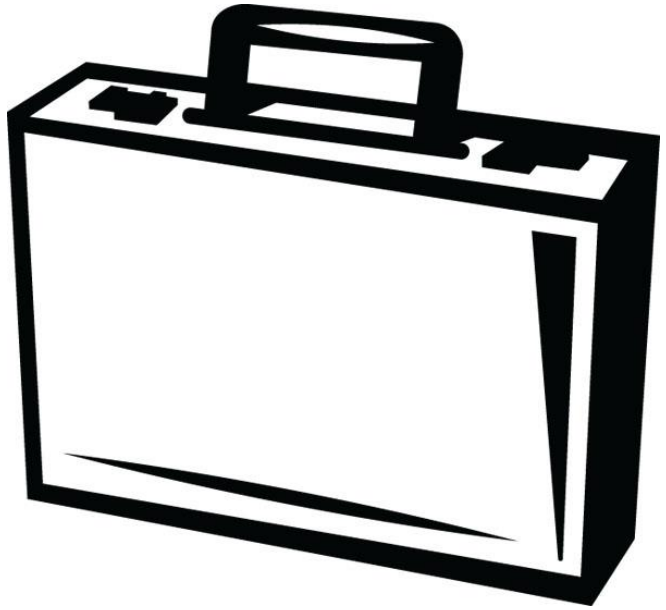
Examples

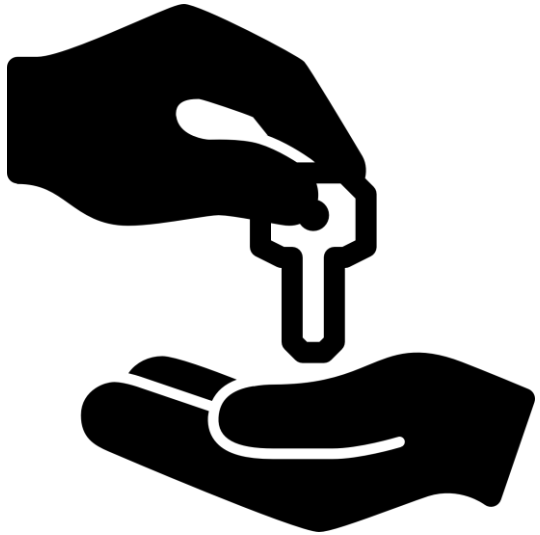
- Change system behaviour (including stopping some or all of it from operating):
  - To cause embarrassment, financial loss or inconvenience;
  - To facilitate physical intrusion;
  - To suit a user's desire (without permission/authority).
- Alter settings to override system settings like temperature, light levels and time-outs.

SECURITY PRINCIPLES

SECURITY PRINCIPLES

Demonstration

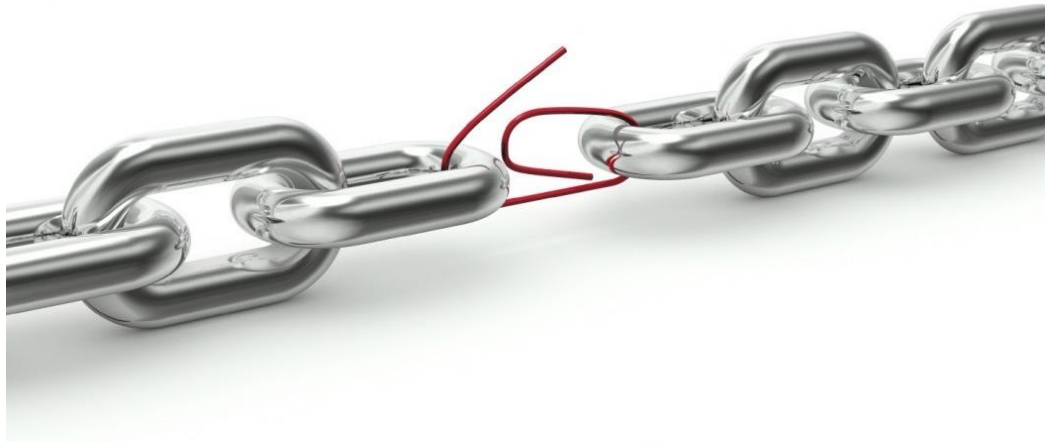




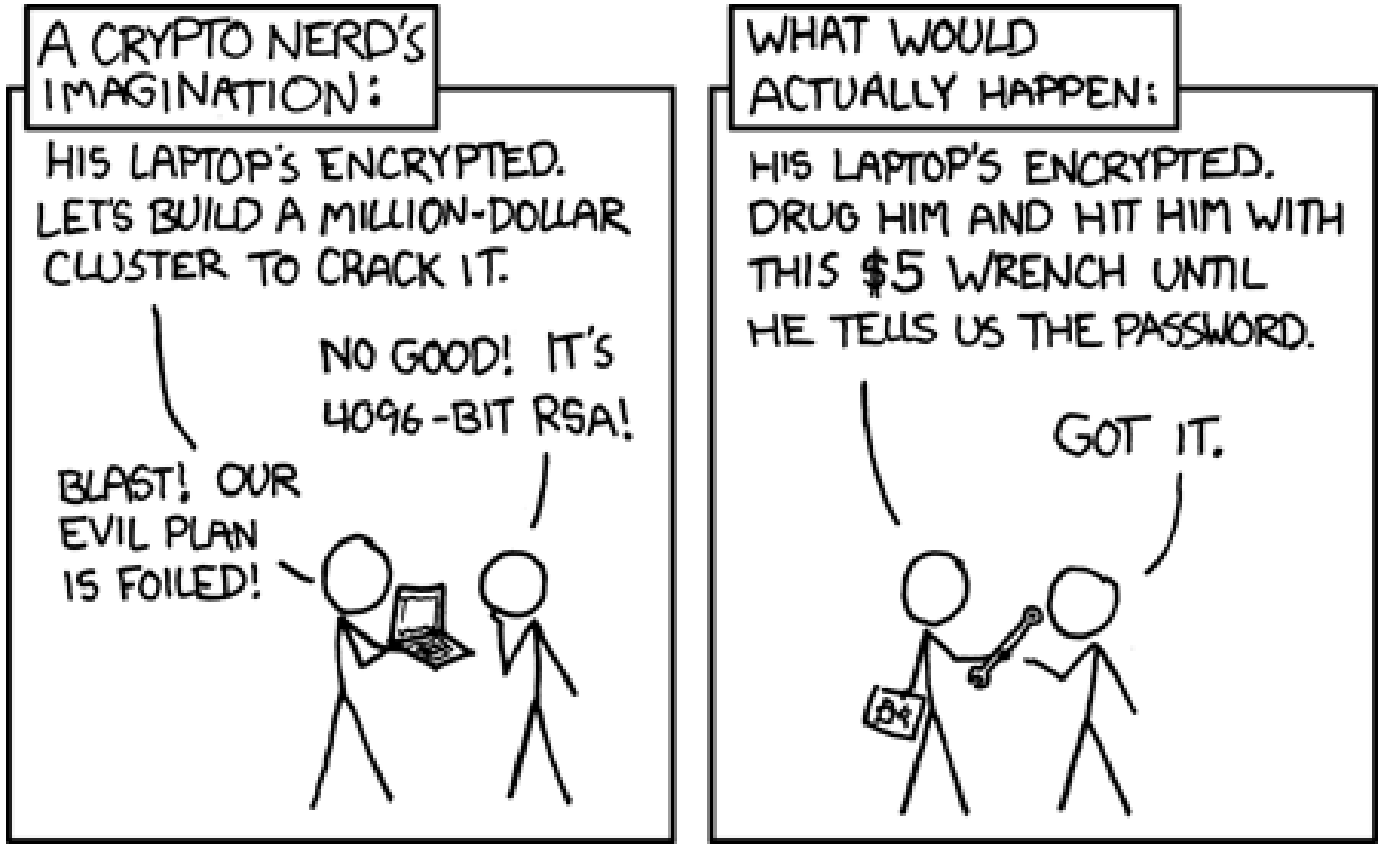
SECURITY PRINCIPLES

“A security system is only as strong as its weakest link”

Bruce Schneier



SECURITY PRINCIPLES



SECURITY PRINCIPLES

Kerckhoffs's principle

“A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.”

No “security by obscurity” – do it “by the book”

SECURITY PRINCIPLES

Concept	Description
Confidentiality	Information is kept secret from all but authorised parties (e.g. encryption)
Integrity	Messages have not been modified in transit
Authentication	The sender of the message is who they claim to be
Nonrepudiation	The sender of the message cannot deny the creation of the message
Access Control	Restrict access to the resources to privileged entities
Availability	The system needs to be ready to use and responsive when it is needed
Auditing	Provide evidence about security related activities (e.g. by keeping logs about certain events) – needs to be tamper evident
Physical Security	Provide protection against physical tampering and/or responses to physical tampering events
Anonymity	Provide protection against discovery and misuse of identity

SECURITY PRINCIPLES

Symmetric Cipher

- The encryption and decryption process use the same key
- e.g. AES
- Fast

Asymmetric Cipher

- The encryption and decryption process use different keys
- Public / private keys
- e.g. RSA
- Slow

SECURITY PRINCIPLES

Key Size (bits)

- More bits = more secure
- Less bits = faster

Key Size	Combinations
8 bit	256
16 bit	65536
32 bit	4294967296
64 bit	18446744073709551616
128 bit	340282366920938463463374607431768211456
256 bit	115792089237316195423570985008687907853269984665640564039457584007913129639936

SECURITY PLAN

SECURITY PLAN

Goals

- Balance between security and usability.
- Perfect security with perfect usability is impossible.
- We try and strike a balance between security that is robust, and usability that provides appropriate convenience.

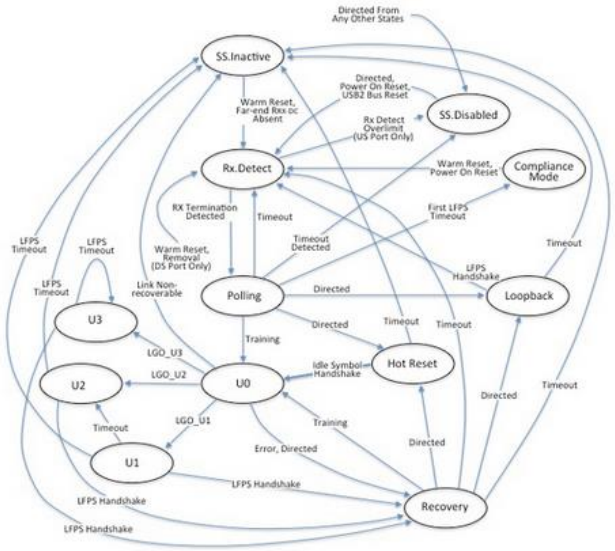
“You can please some of the people all of the time, you can please all of the people some of the time, but you can’t please all of the people all of the time.”

John Lydgate

SECURITY PLAN

Limits

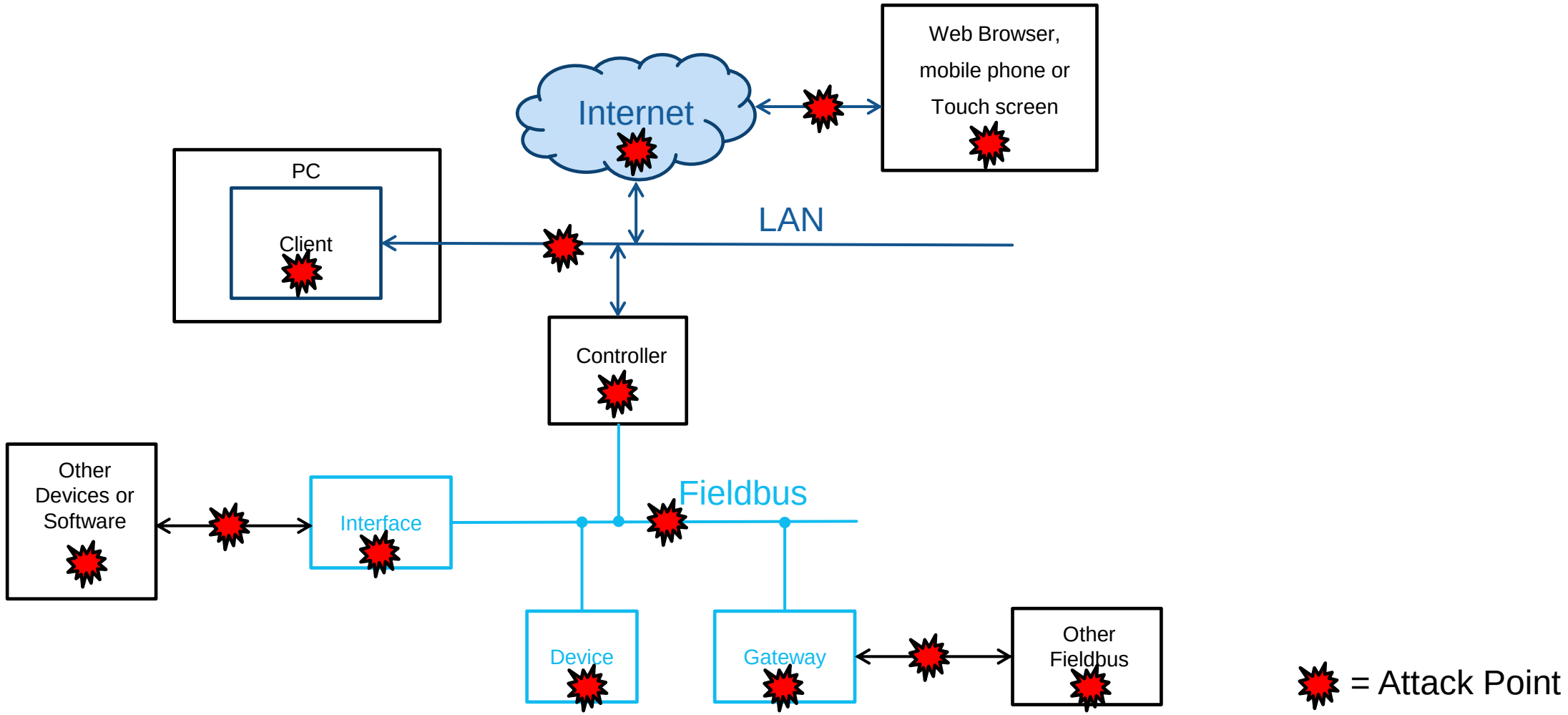
- We are generally less concerned about scenarios where someone requires physical access to the equipment.
- After all, someone could just cut the DALI Line or switch off a circuit breaker to stop it from working…



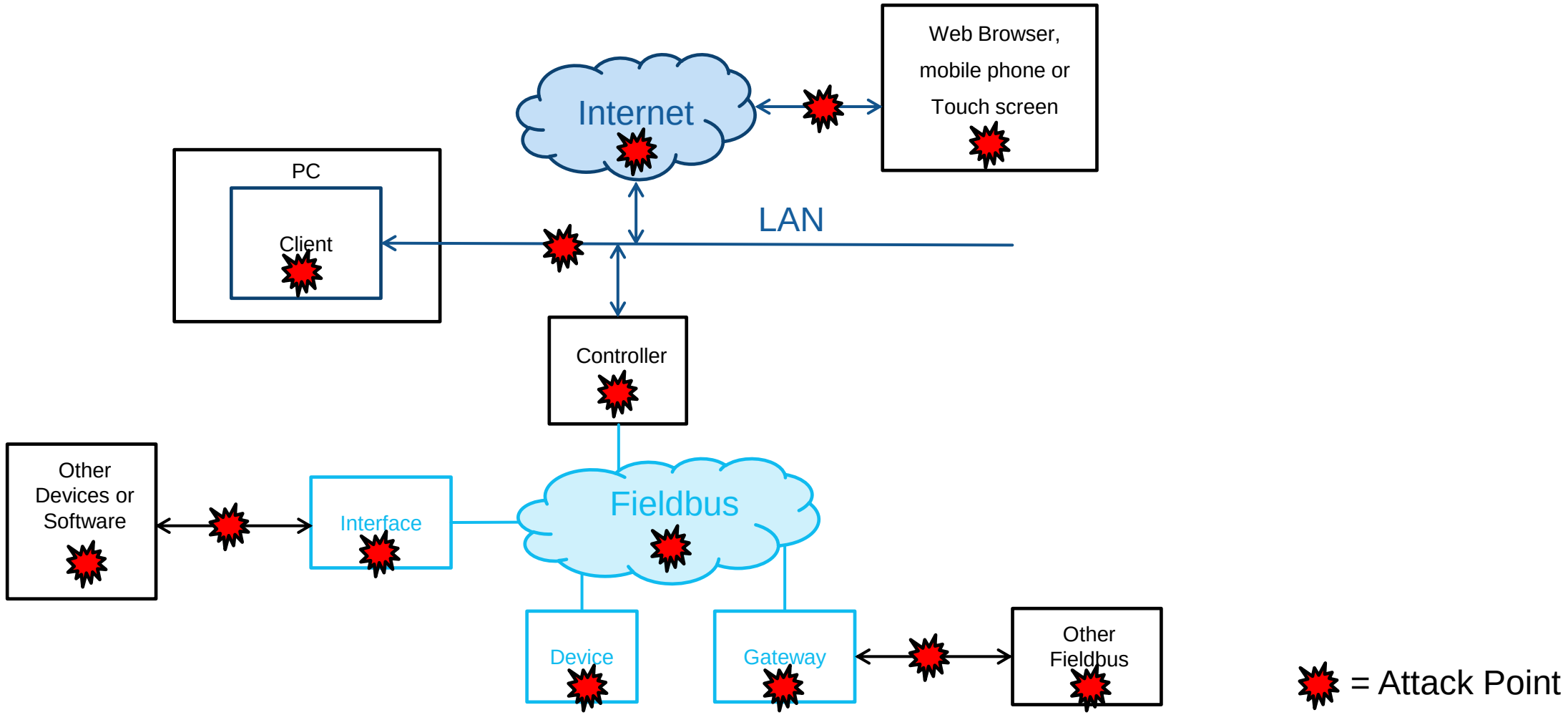
SYSTEM ANALYSIS

HOW DO WE KNOW THE SYSTEM IS SECURE?

ATTACK POINTS

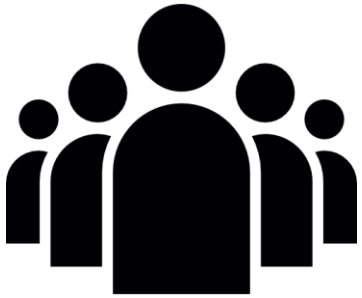


ATTACK POINTS



WHO

People who interact with the system:



- **Guest**: an anonymous user, not known to the system
- **User**: any user of the system
- **Administrator**: a privileged user of the system. Normally an IT person. They have fewer restrictions, granted to them by management.
- **Installer**: The person installing the system.
- **Domain**: a group of people and/or building services. For example, an individual company within a multi-tenant building.
- **Software Client**: software connected to a Zone Controller.
- **Attacker**: anyone trying to do anything malicious with or to the system

WHO

Potential attackers include:

- Hackers (outside of the site)
- Malicious guests (at the site)
- Rival companies (industrial espionage) and governments
- Disgruntled employees (on site) or ex-employees (off-site)
- Criminals (burglars, white collar criminals, extortionists)
- Regular users (who may be wanting to do something they consider quite innocent, but which could have undesirable consequences)
- The installer, or a member of their organisation (particularly if their invoice has not been paid, or there is some sort of dispute)

EXAMPLE

A typical scenario that we provide protection against is where:

- The site network security has not been set up correctly and access to the network is available. This may be via the Internet, WiFi or a guest account.
- The hacker knows that the site uses our system.
- The hacker has our software (can be downloaded).
- The hacker has sufficient skills, familiarity or time to be able to cause problems.

Goals include changing device configuration or switching on/off lights.

SYSTEM DESIGN

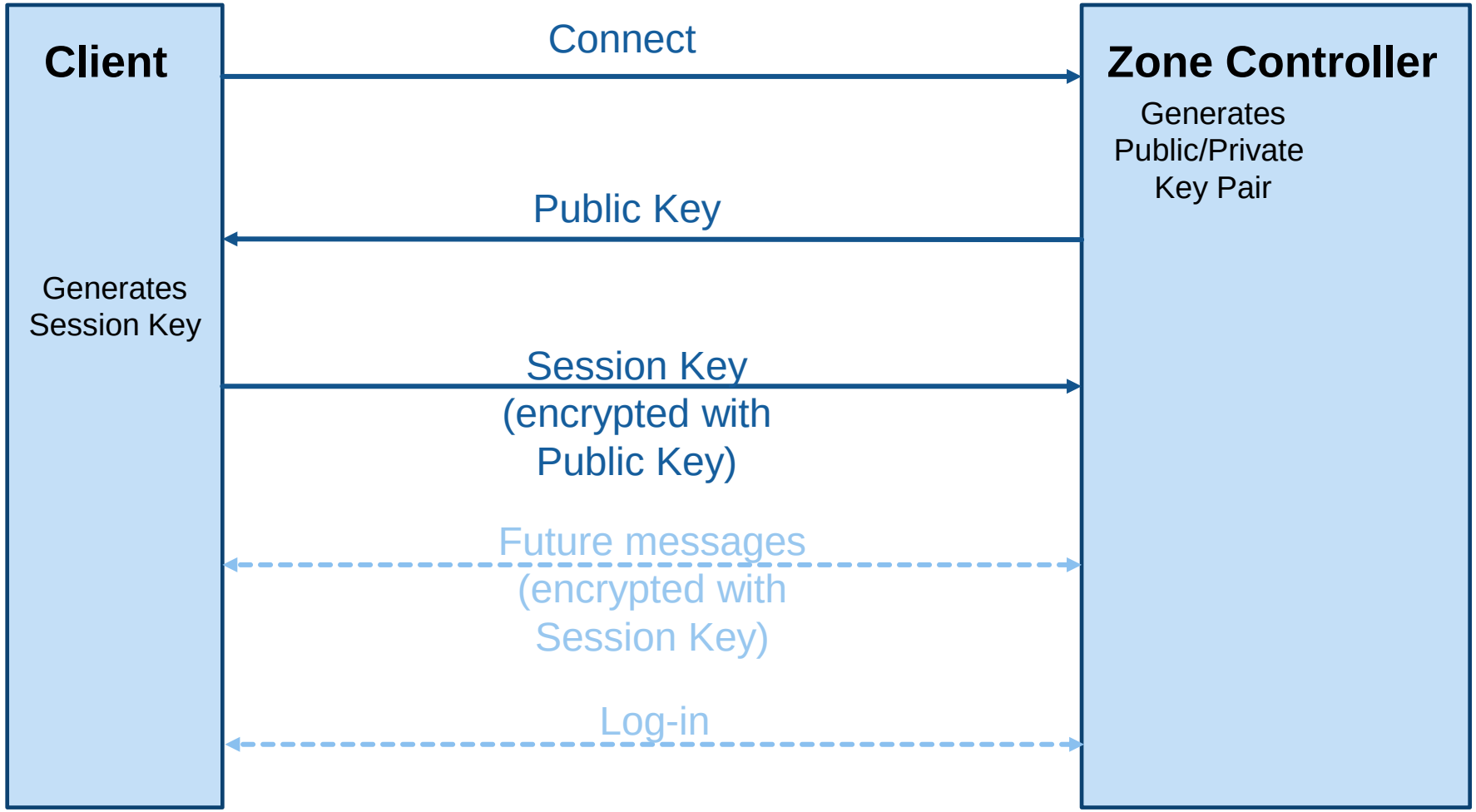
HOW RAPIX IMPLEMENTS SECURITY

COMMUNICATION

Encryption Key Distribution

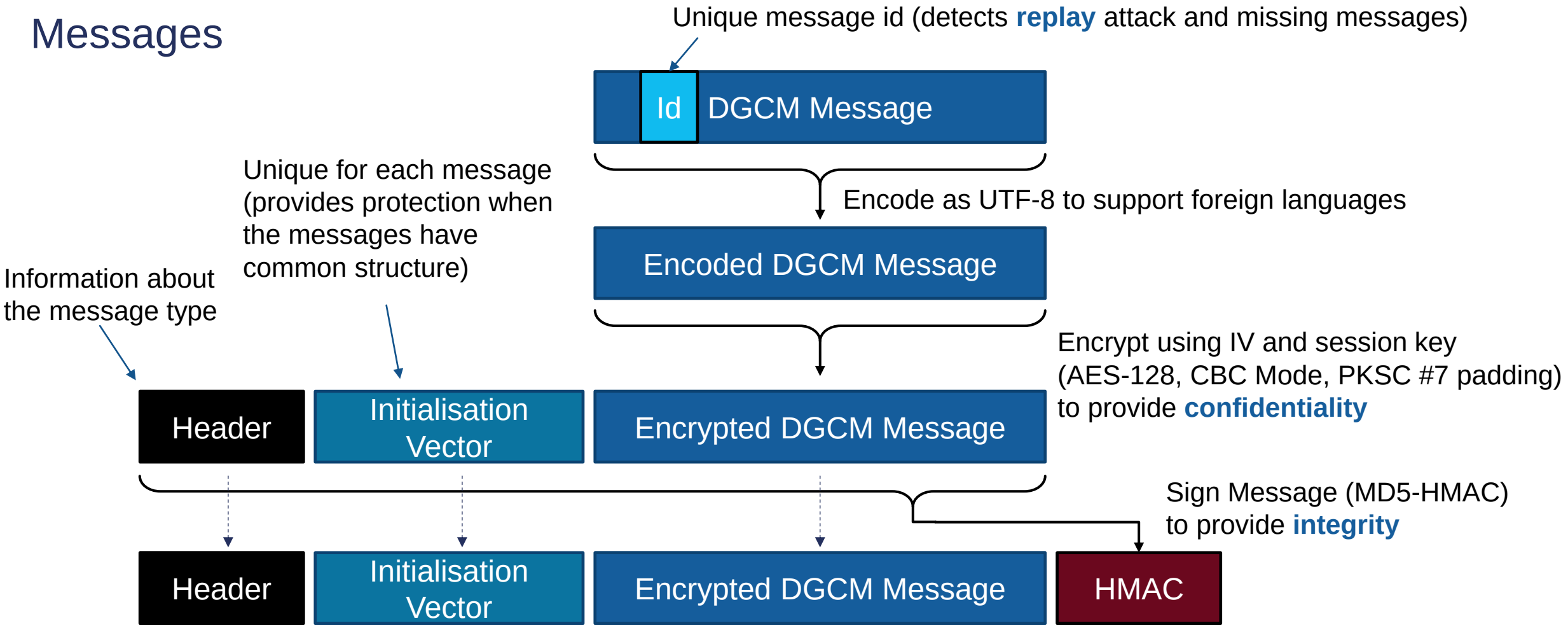
- RSA key exchange for use with RAPIX and 3rd parties
- Zone Controller mesh uses pre-shared key (project key)

COMMUNICATION



COMMUNICATION

Messages



COMMUNICATION

Didn’t we just reveal all our secrets?

Yes we did!

We can disclose everything about our system, but it is still secure

- Remember Kerckhoffs's principle

ZONE CONTROLLER DESIGN

Operating System

- Only a few ports are open (but protected)
- Firewall
- User cannot deploy their own apps
- Operating system only has bare minimum services running (e.g. no Telnet or FTP)
- No useful (to a hacker) tools installed
- Can be in-system upgraded if problems are found in the future

SPECIFIC ATTACKS

HOW RAPIX DEALS WITH THEM

CONNECTING TO A ZONE CONTROLLER

Problem

- Attacker tries to connect to Zone Controller.
- Goal is to make changes to system or control loads.

Mitigation

- Connection requires project key, which is 120 bits long (i.e. 10^{36} possible keys)
- Keys are randomly generated (you can't use "12345" or "password" even if you want to)
- Handshake uses salt to prevent replay of log-in
- RAPIX also has secret key to prevent spoofing
- Channel uses randomly generated key to prevent replay of other messages

REPLAY ATTACK

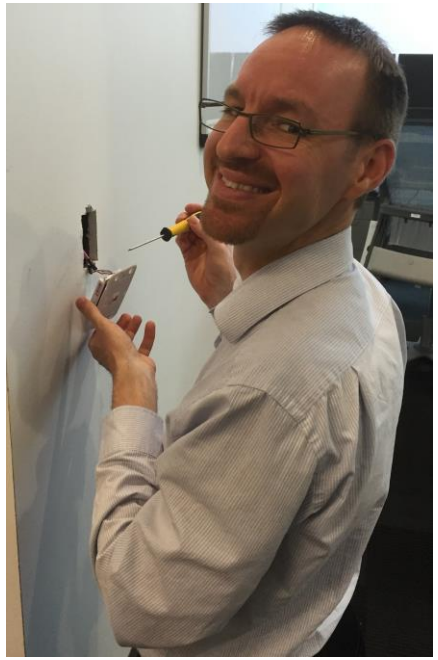
Problem

- Attacker tries to control the system by
- recording messages and replaying them.
- Goal is to make changes to system or control loads.
- *Note that the attacker does not need to be able to actually decrypt the message*.

Mitigation

- External connections have unique session keys
  - Prevents replay of individual message or whole session
- RAPIX login uses a “salt” to prevent replay
  - Prevents replay of individual message or whole session
- All message have ids to allow detection of replayed messages

HOTEL ROOM HACKER



Problem

- Attacker tries to control the system from a publicly accessible location that has physical access to the network (e.g. by removing a wall switch or a TV Ethernet cable).
- Goal is to make changes to the system or control loads.

Mitigation

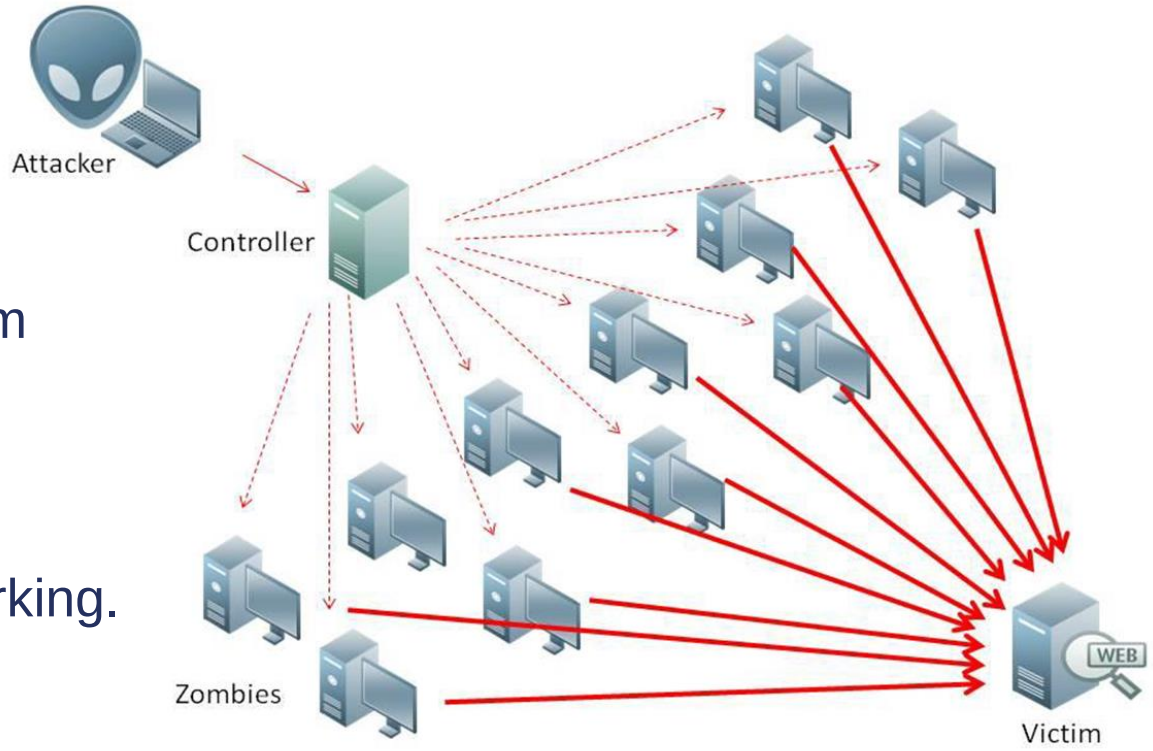
- External connections have unique session keys
  - Prevents replay of individual message or whole session
- RAPIX login uses a “salt” to prevent replay
  - Prevents replay of individual message or whole session
- All message have ids to allow detection of replayed messages

DoS / DDoS

Problem

- Attacker either:
- Rapidly makes connection attempts
- Sends large numbers of messages to the system
- Sends misconfigured packets to the system

Goal is to overload the system and stop it from working.



DoS / DDoS

Mitigation

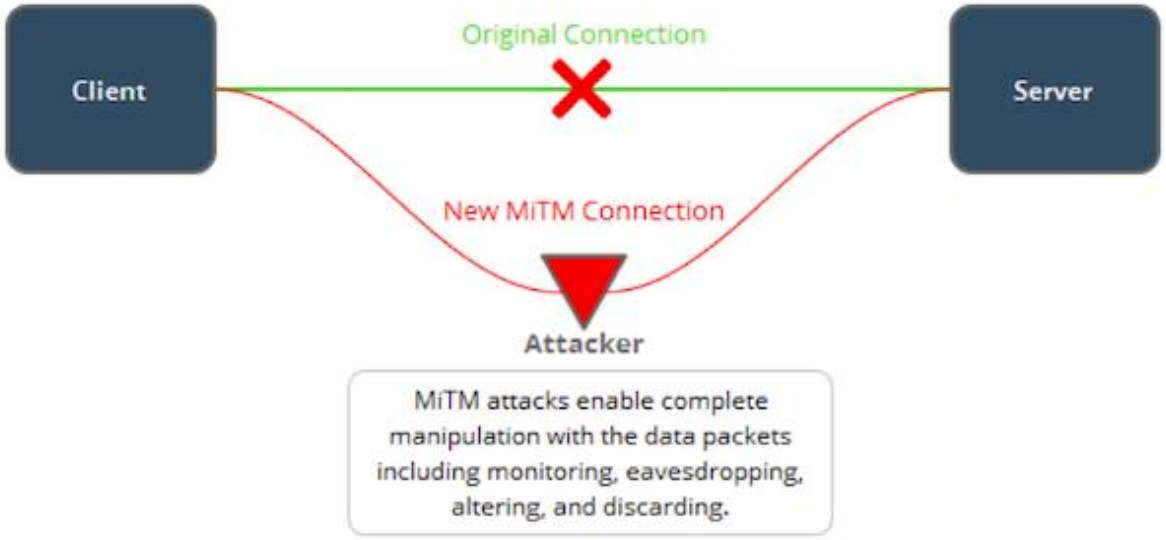
- External Access (Internet)
  - Web server will run on separate device – doesn't matter as much if it overloads or crashes.
  - Zone Controller network should not be accessible externally if the system is configured correctly
- Internal Access (LAN)
  - Zone Controllers should be on a VLAN
  - Well configured Ethernet switches can (should) limit rogue traffic

MAN-IN-THE-MIDDLE ATTACK

Problem

- Attacker tries to intercept communications between a client (e.g. RAPIX Integrator) and a server (Zone Controller).

Goal is to read the encrypted messages and either obtain passwords or control the system.



MAN-IN-THE-MIDDLE ATTACK

Mitigation

The usual way to prevent this is though the use of public certificates. This makes the system too complex and has been avoided.

External Access (Internet)

- The ports used to connect to the Zone Controllers should be blocked by the firewall

Internal Access (LAN)

- Man-in-the-middle attacks are not possible with the Zone Controller mesh (PGM) since there is no handshake process to get in the middle of (it uses a pre-shared key)

This attack requires access to the LAN and is very complex to implement; generally beyond the capability of a casual hacker.

VERIFICATION

HOW DO WE KNOW THE SYSTEM IS SECURE?

VERIFICATION

- Nessus – vulnerability scanner
- Shodan – searches for vulnerable iOT devices
- Independent review
- There are no “back-doors” than can be exploited by ex-employees or others

SUMMARY

SUMMARY

Design Priorities

- Prevent any unauthorised access to the system from the Internet
- Minimise the damage someone can do if they have physical access to the Local Area Network or Fieldbus (DALI)
- Don’t worry so much what someone can do if they have access to the switchboard

The RAPIX system has been designed from the start with security in mind

- Designed in accordance with industry best practice
- Security “out-of-the-box”
  - You don’t need to configure anything

THE END