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

BY JESUS MOLINA
@VERIFYTHENTRUST
If I were to tell someone is able to control every appliance in your hotel room, will you move to another hotel tonight?
#WHOAMI

- Security consultant based in SF
- Full name and title
  - Doctor Jesús María Molina Terriza
- Spanish from la Mancha
- www.jesusmolina.com
- @verifythentrust
- Get me a good tequila at the bar
Preliminaries

- Controlled 200+ rooms of a 5 star hotel by abusing an insecure home automation protocol
- While I was a guest of the hotel
- In CHINA
- I did not hack – I abused
- Starwood response was positive

8/6/2014
The ST. REGIS SHENZHEN

HOTEL IS HERE
Could I control the room with my laptop?
1 - IPAD IS OPEN TO INSPECTION AND TAMPERING
2 - IPAD IS CONNECTED TO GUEST NETWORK
3 - THE GUEST NETWORK IS OPEN TO INSPECTION AND TAMPERING
4 - THE AUTOMATION PROTOCOL NEEDS TO BE SECURE
5 - But it is NOT
<table>
<thead>
<tr>
<th>Source IP</th>
<th>Destination IP</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.31.20.160</td>
<td>172.31.14.49</td>
<td>UDP</td>
<td>101</td>
<td>65303</td>
</tr>
<tr>
<td>172.31.20.160</td>
<td>172.31.14.49</td>
<td>UDP</td>
<td>94</td>
<td>efcp</td>
</tr>
<tr>
<td>172.31.20.160</td>
<td>172.31.14.49</td>
<td>UDP</td>
<td>101</td>
<td>efcp</td>
</tr>
<tr>
<td>172.31.20.160</td>
<td>172.31.14.49</td>
<td>UDP</td>
<td>90</td>
<td>65303</td>
</tr>
<tr>
<td>172.31.20.160</td>
<td>172.31.14.49</td>
<td>UDP</td>
<td>90</td>
<td>65303</td>
</tr>
<tr>
<td>172.31.20.160</td>
<td>172.31.14.49</td>
<td>UDP</td>
<td>101</td>
<td>efcp</td>
</tr>
<tr>
<td>172.31.20.160</td>
<td>172.31.14.49</td>
<td>UDP</td>
<td>90</td>
<td>65303</td>
</tr>
<tr>
<td>172.31.20.160</td>
<td>172.31.14.49</td>
<td>UDP</td>
<td>94</td>
<td>65303</td>
</tr>
<tr>
<td>172.31.20.160</td>
<td>172.31.14.49</td>
<td>UDP</td>
<td>101</td>
<td>51440</td>
</tr>
<tr>
<td>172.31.20.160</td>
<td>172.31.14.49</td>
<td>UDP</td>
<td>90</td>
<td>65303</td>
</tr>
<tr>
<td>172.31.20.160</td>
<td>172.31.14.49</td>
<td>UDP</td>
<td>102</td>
<td>efcp</td>
</tr>
<tr>
<td>172.31.20.160</td>
<td>172.31.14.49</td>
<td>UDP</td>
<td>90</td>
<td>65303</td>
</tr>
<tr>
<td>224.0.0.1</td>
<td>172.31.20.160</td>
<td>UDP</td>
<td>118</td>
<td>52000</td>
</tr>
<tr>
<td>224.0.0.1</td>
<td>172.31.20.160</td>
<td>UDP</td>
<td>118</td>
<td>52000</td>
</tr>
</tbody>
</table>
RFC 3671 - IETF Tools
tools.ietf.org/html/rfc3671  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/rfc/rfc3671  Internet Engineering Task Force
Protocol) This document provides schema definitions for collective attributes for use in
LDAP. 1. Introduction. In X.500 [X500], a collective attribute is "a user ...

Documentation - KNXnet/IP Wireshark plugin
knxnetipdissect.sourceforge.net/doc.html
filters all KNXnet/IP 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/products/.../productDetail.jsp?...  Cell Signaling Technology
Gallery. Phospho-Myosin Light Chain 2 (Ser19) Antibody #3671 ... Blotting Membrane
and Paper. (#12369) This protocol has been optimized for nitrocellulose ...

8/6/2014
TRUE FACTS ABOUT KNX/IP

• IP encapsulation of KNX
• KNX is a building automation protocol
• Created in 1990
• Widespread in Europe and China
• Simple to deploy
TRUE FACTS ABOUT KNX/IP

• “Open” meaning “Closed” - 1000€ just to look at it? What is this? 1990s?

• Open source clients – eibd daemon
TRUE FACTS ABOUT KNX/IP

• NO SECURITY

• EIBsec: a security extension to KNX/EIB
  2006!!!!!!!!!!

• New KNX specs (2013) claim security – but I can’t read it – Anyone has 1000 euros?
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 length 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; /* tpu */
treq[20] = 0x81; /* 81: switch on, 80: off */

*According to http://www.eb-systeme.de/
CHECK YOUR EMAIL!!!!

EVALUATIONS
Can I switch TV on in EVERY room?
“Let There Be Light”
COLLECTING INFORMATION

• Program to send tunneling request
  • Code your own
  • Eibd: [http://www.auto.tuwien.ac.at/~mkoegler/index.php/eibd](http://www.auto.tuwien.ac.at/~mkoegler/index.php/eibd)

• KNX Address of each device in the room
  • Press the iPad and automate collecting the result

• IP address and KNX of each room
  • Change rooms and infer the pattern
INFORMATION COLLECTION FAILURE

NO IPAD 😞
How do I know it works?

- DND Lights are outside the room...
- And I control them! DND heartbeat
Where there other things connected?

MAYBE – But I got Scared 😞
WHAT DOES IT MEAN?
For Hotels

- Update security policies according to new technologies
- Open protocols and security for external researchers
- Guest security cannot be an afterthought
- Is this possible in other hotels?
For the IoT

• Guerrilla war when it comes to deployment
• KNX is a standard for home automation!
• Most protocols are closed
• Most protocols rely in external security
• Extra care when deploying automation in shares spaces
So What? What’s the worst thing that could happen?

“One iPad to rule them all”

“The humans have played their hand”
If I were to tell someone is able to control every appliance in your hotel room, will you move to another hotel tonight?

The worst thing that could happen is that we don’t care. Welcome to 2084
Questions?

security@nomeames.com

@verifythentrust
THE STORY
CEMI
/* 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 length 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 */

*According to [http://www.eb-systeme.de/](http://www.eb-systeme.de/)
KNX/IP Sample Network

- Addresses are in the format Area/Line/Device in KNX

- The KNX ShenZhen network works in tunnel mode
The Elephant in the Hotel Room

- I was a guest at the hotel, not a planned security evaluation
- Limited time and resources
- Fear of making a bad mistake
- I **did not** hack anything
- Does not matter if you get caught