Oops, I hacked my PBX
Why auditing proprietary protocols matters

pt

28c3

December 29, 2011
"The enemy knows the system"
Claude Shannon

1. Introduction
2. Reverse engineering the protocol
3. Actual results
4. Conclusion
A few words in beforehand

- Don’t laugh too loud, YOU could have made this mistakes too!
- A real world example is used but slightly obfuscated
Why did I hack the PBX?

- I didn’t want to, seriously!
- Phones with PBX integration can be customized
  - Client has >50 of them
  - 5 Minutes/Phone to read-modify-write, non scriptable!
- They restructured ⇒ Reconfigure all phones
  ⇒ Massive acceptance problems with the admin
Why did I hack the PBX?

- I didn’t want to, seriously!
- Phones with PBX integration can be customized
  - Client has >50 of them
  - 5 Minutes/Phone to read-modify-write, non scriptable!
  - They restructured ⇒ Reconfigure all phones
  - ⇒ Massive acceptance problems with the admin
Why did I hack the PBX?

- I didn’t want to, seriously!
- Phones with PBX integration can be customized
- Client has $>50$ of them
- 5 Minutes/Phone to read-modify-write, non scriptable!
- They restructured $\Rightarrow$ Reconfigure all phones
- $\Rightarrow$ Massive acceptance problems with the admin
Why did I hack the PBX?

- I didn’t want to, seriously!
- Phones with PBX integration can be customized
- Client has >50 of them
- 5 Minutes/Phone to read-modify-write, non scriptable!
- They restructured ⇒ Reconfigure all phones
- ⇒ Massive acceptance problems with the admin
Why did I hack the PBX?

- I didn’t want to, seriously!
- Phones with PBX integration can be customized
- Client has >50 of them
- 5 Minutes/Phone to read-modify-write, non scriptable!
- They restructured ⇒ Reconfigure all phones
  ⇒ Massive acceptance problems with the admin
Why did I hack the PBX?

- I didn’t want to, seriously!
- Phones with PBX integration can be customized
- Client has $>50$ of them
- 5 Minutes/Phone to read-modify-write, non scriptable!
- They restructured $\Rightarrow$ Reconfigure all phones
- $\Rightarrow$ Massive acceptance problems with the admin
Things you will need

- The original software
- Some PBX hardware to tinker with
- Wireshark
- Your brain
- Too much (client) time on your hands
Things you will need

- The original software
- Some PBX hardware to tinker with
  - Wireshark
  - Your brain
  - Too much (client) time on your hands
Things you will need

- The original software
- Some PBX hardware to tinker with
- Wireshark
- Your brain
- Too much (client) time on your hands
Things you will need

- The original software
- Some PBX hardware to tinker with
- Wireshark
- Your brain
- Too much (client) time on your hands
Things you will need

- The original software
- Some PBX hardware to tinker with
- Wireshark
- Your brain
- Too much (client) time on your hands
Understand the original software

- Poke around the interface
- You might find gems ;)
- Try to think behind the GUI
Understand the original software

- Poke around the interface
- You might find gems ;)
- Try to think behind the GUI
Understand the original software

- Poke around the interface
- You might find gems ;)
- Try to think behind the GUI

Oops, I hacked my PBX
Dump the communication

- Define test cases
- Enable debug output
- Repeat test cases while sniffing
- File cleanly

Simple test case

1. Launch Software
2. Click on „Load”
3. Click on „From phone”
4. Select phone
5. Enter password
6. Watch download

Oops, I hacked my PBX
Define test cases
- Enable debug output
- Repeat test cases while sniffing
- File cleanly
Dump the communication

- Define test cases
- Enable debug output
- Repeat test cases while sniffing
- File cleanly

Oops, I hacked my PBX
Dump the communication

- Define test cases
- Enable debug output
- Repeat test cases while sniffing
- File cleanly

Oops, I hacked my PBX
Analyze your dumps

- Correlate debug data and dump with test case
- Make sense of data flow
- Look at hexdumps
- Look for known data
Analyze your dumps

- Correlate debug data and dump with test case
- Make sense of data flow
  - Look at hexdumps
  - Look for known data

Oops, I hacked my PBX
Analyze your dumps

- Correlate debug data and dump with test case
- Make sense of data flow
- Look at hexdumps
- Look for known data

Oops, I hacked my PBX
Analyze your dumps

- Correlate debug data and dump with test case
- Make sense of data flow
- Look at hexdumps
- Look for known data

Oops, I hacked my PBX
Protocol basics

- Header contains packet length
- Each packet to PBX triggers a response
- Packet type of a positive ACK is the one of the request +1
- Has virtual channels
- Has an idle timeout!

<table>
<thead>
<tr>
<th>Client</th>
<th>PBX</th>
</tr>
</thead>
<tbody>
<tr>
<td>05 21 00 00 00 00</td>
<td>05 22 00 00 12 e0</td>
</tr>
<tr>
<td>09 21 00 00 00 00 00 60 00 16</td>
<td>1f 22 00 00 12 00 00 60 00 16 40 43 90 14 e0 00</td>
</tr>
<tr>
<td>08 81 01 01 00 63 02 00 00</td>
<td>07 82 01 01 02 6b 01 7c</td>
</tr>
</tbody>
</table>

Oops, I hacked my PBX
Protocol basics

- Header contains packet length
- Each packet to PBX triggers a response
- Packet type of a positive ACK is the one of the request +1
- Has virtual channels
- Has an idle timeout!

<table>
<thead>
<tr>
<th>Client</th>
<th>PBX</th>
</tr>
</thead>
<tbody>
<tr>
<td>05 21 00 00 00 00</td>
<td>⇒ 05 22 00 00 12 e0</td>
</tr>
<tr>
<td>09 21 00 00 00 00 00 60 00 16</td>
<td>⇒ 1f 22 00 00 12 00 00 60 00 16 40 43 90 14 e0 00 00 00 00 00 00 90 00 00 00 00 00</td>
</tr>
<tr>
<td>08 81 01 01 00 63 02 00 00</td>
<td>⇒ 07 82 01 01 02 6b 01 7c</td>
</tr>
</tbody>
</table>

Oops, I hacked my PBX
Protocol basics

- Header contains packet length
- Each packet to PBX triggers a response
- Packet type of a positive ACK is the one of the request +1
- Has virtual channels
- Has an idle timeout!

<table>
<thead>
<tr>
<th>Client</th>
<th>PBX</th>
</tr>
</thead>
<tbody>
<tr>
<td>05 21 00 00 00 00</td>
<td>05 22 00 00 12 e0</td>
</tr>
<tr>
<td>09 21 00 00 00 00 00 60 00 16</td>
<td>1f 22 00 00 12 00 00 60 00 16 40 43 90 14 e0 00</td>
</tr>
<tr>
<td>08 81 01 01 00 63 02 00 00</td>
<td>07 82 01 01 02 6b 01 7c</td>
</tr>
</tbody>
</table>

Oops, I hacked my PBX
Protocol basics

- Header contains packet length
- Each packet to PBX triggers a response
- Packet type of a positive ACK is the one of the request +1
- Has virtual channels
- Has an idle timeout!

<table>
<thead>
<tr>
<th>Client</th>
<th>PBX</th>
</tr>
</thead>
<tbody>
<tr>
<td>05 21 00 00 00 00</td>
<td>05 22 00 00 12 e0</td>
</tr>
<tr>
<td>09 21 00 00 00 00 60 00 16</td>
<td>1f 22 00 00 12 00 00 60</td>
</tr>
<tr>
<td>08 81 01 01 00 63 02 00 00</td>
<td>07 82 01 01 02 6b 01 7c</td>
</tr>
</tbody>
</table>

Oops, I hacked my PBX
Protocol basics

- Header contains packet length
- Each packet to PBX triggers a response
- Packet type of a positive ACK is the one of the request +1
- Has virtual channels
- Has an idle timeout!

<table>
<thead>
<tr>
<th>Client</th>
<th>PBX</th>
</tr>
</thead>
<tbody>
<tr>
<td>05 21 00 00 00 00</td>
<td>05 22 00 00 12 e0</td>
</tr>
<tr>
<td>09 21 00 00 00 00 00 60 00 16</td>
<td>1f 22 00 00 12 00 00 60 00 16 40 43 90 14 e0 00</td>
</tr>
<tr>
<td>08 81 01 01 00 63 02 00 00</td>
<td>07 82 01 01 02 6b 01 7c</td>
</tr>
</tbody>
</table>
Communication flow

1. Find out packet types
2. Explore the communication sequence
3. Find the authentication sequence.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HELLO</td>
<td>0x21</td>
</tr>
<tr>
<td>READ_NVRAM</td>
<td>0x31</td>
</tr>
<tr>
<td>WRITE_NVRAM</td>
<td>0x33</td>
</tr>
<tr>
<td>CHAN_OPEN</td>
<td>0x81</td>
</tr>
<tr>
<td>CHAN_CLOSE</td>
<td>0x85</td>
</tr>
<tr>
<td>INQUIRE_HARDWARE</td>
<td>0x87</td>
</tr>
<tr>
<td>PING</td>
<td>0x79</td>
</tr>
</tbody>
</table>

Note

These apply to all devices in the system, Phones and PBXe

Oops, I hacked my PBX
Communication flow

1. Find out packet types
2. Explore the communication sequence
3. Find the authentication sequence.

<table>
<thead>
<tr>
<th>Count</th>
<th>Chan</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1x</td>
<td>0</td>
<td>HELLO</td>
</tr>
<tr>
<td>1x</td>
<td>0</td>
<td>READ_NVRAM</td>
</tr>
<tr>
<td>1x</td>
<td>1</td>
<td>CHAN_OPEN</td>
</tr>
<tr>
<td>20x</td>
<td>1</td>
<td>INQUIRE_HW</td>
</tr>
<tr>
<td>1x</td>
<td>1</td>
<td>READ_NVRAM</td>
</tr>
<tr>
<td>1x</td>
<td>1</td>
<td>INQUIRE_HW</td>
</tr>
<tr>
<td>1x</td>
<td>1</td>
<td>PING</td>
</tr>
<tr>
<td>1x</td>
<td>2</td>
<td>CHAN_OPEN</td>
</tr>
<tr>
<td>1x</td>
<td>2</td>
<td>INQUIRE_HW</td>
</tr>
<tr>
<td>nX</td>
<td>2</td>
<td>READ_NVRAM</td>
</tr>
<tr>
<td>1x</td>
<td>2</td>
<td>CHAN_CLOSE</td>
</tr>
<tr>
<td>1x</td>
<td>1</td>
<td>CHAN_CLOSE</td>
</tr>
</tbody>
</table>

Wait: No auth done?!

pt: Oops, I hacked my PBX
Communication flow

1. Find out packet types
2. Explore the communication sequence
3. Find the authentication sequence.

<table>
<thead>
<tr>
<th>Count</th>
<th>Chan</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1×</td>
<td>0</td>
<td>HELLO</td>
</tr>
<tr>
<td>1×</td>
<td>0</td>
<td>READ_NVRAM</td>
</tr>
<tr>
<td>1×</td>
<td>1</td>
<td>CHAN_OPEN</td>
</tr>
<tr>
<td>20×</td>
<td>1</td>
<td>INQUIRE_HW</td>
</tr>
<tr>
<td>1×</td>
<td>1</td>
<td>READ_NVRAM</td>
</tr>
<tr>
<td>1×</td>
<td>1</td>
<td>INQUIRE_HW</td>
</tr>
<tr>
<td>1×</td>
<td>1</td>
<td>PING</td>
</tr>
<tr>
<td>1×</td>
<td>2</td>
<td>CHAN_OPEN</td>
</tr>
<tr>
<td>1×</td>
<td>2</td>
<td>INQUIRE_HW</td>
</tr>
<tr>
<td>nx</td>
<td>2</td>
<td>READ_NVRAM</td>
</tr>
<tr>
<td>1×</td>
<td>2</td>
<td>CHAN_CLOSE</td>
</tr>
<tr>
<td>1×</td>
<td>1</td>
<td>CHAN_CLOSE</td>
</tr>
</tbody>
</table>

Wait: No auth done?!

channel

Oops, I hacked my PBX
Communication flow

1. Find out packet types
2. Explore the communication sequence
3. Find the authentication sequence.
   Wait: No auth done?!

<table>
<thead>
<tr>
<th>Count</th>
<th>Chan</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1x</td>
<td>0</td>
<td>HELLO</td>
</tr>
<tr>
<td>1x</td>
<td>0</td>
<td>READ_NVRAM</td>
</tr>
<tr>
<td>1x</td>
<td>1</td>
<td>CHAN_OPEN</td>
</tr>
<tr>
<td>20x</td>
<td>1</td>
<td>INQUIRE_HW</td>
</tr>
<tr>
<td>1x</td>
<td>1</td>
<td>READ_NVRAM</td>
</tr>
<tr>
<td>1x</td>
<td>1</td>
<td>INQUIRE_HW</td>
</tr>
<tr>
<td>1x</td>
<td>1</td>
<td>PING</td>
</tr>
<tr>
<td>1x</td>
<td>2</td>
<td>CHAN_OPEN</td>
</tr>
<tr>
<td>1x</td>
<td>2</td>
<td>INQUIRE_HW</td>
</tr>
<tr>
<td>nX</td>
<td>2</td>
<td>READ_NVRAM</td>
</tr>
<tr>
<td>1x</td>
<td>2</td>
<td>CHAN_CLOSE</td>
</tr>
<tr>
<td>1x</td>
<td>1</td>
<td>CHAN_CLOSE</td>
</tr>
</tbody>
</table>

Oops, I hacked my PBX
Where is the authentication gone?

1. **Launch Software**
2. **Click on ”Load”**
3. **Click on ”From phone”**
4. **Select phone**
5. **Enter password (”012345”)**
6. **Watch download**

---

**Step | Count | Chan | Type**
--- | --- | --- | ---
3 | 1x 0 | HELLO |
3 | 1x 0 | READ_NVROM |
3 | 1x 1 | OPEN |
3 | 20x 1 | INQUIRE_HW |
4 | 1x 1 | READ_NVROM |
4 | 1x 1 | INQUIRE_HW |
5 | 1x 1 | PING |
6 | 1x 2 | OPEN |
6 | 1x 2 | INQUIRE_HW |
6 | nx 2 | READ_NVROM |
6 | 1x 2 | CLOSE |
6 | 1x 1 | CLOSE |

---

Oops, I hacked my PBX
Where is the authentication gone?

1. Launch Software
2. Click on "Load"
3. Click on "From phone"
4. Select phone
5. Enter password ("012345")
6. Watch download

<table>
<thead>
<tr>
<th>Step</th>
<th>Count</th>
<th>Chan</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1x</td>
<td>0</td>
<td>HELLO</td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>0</td>
<td>READ_NVRAM</td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>1</td>
<td>CHAN_OPEN</td>
</tr>
<tr>
<td></td>
<td>20x</td>
<td>1</td>
<td>INQUIRE_HW</td>
</tr>
<tr>
<td>4</td>
<td>1x</td>
<td>1</td>
<td>READ_NVRAM</td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>1</td>
<td>INQUIRE_HW</td>
</tr>
<tr>
<td>5</td>
<td>1x</td>
<td>1</td>
<td>PING</td>
</tr>
<tr>
<td>6</td>
<td>1x</td>
<td>2</td>
<td>CHAN_OPEN</td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>2</td>
<td>INQUIRE_HW</td>
</tr>
<tr>
<td></td>
<td>nx</td>
<td>2</td>
<td>READ_NVRAM</td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>2</td>
<td>CHAN_CLOSE</td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>1</td>
<td>CHAN_CLOSE</td>
</tr>
</tbody>
</table>

Oops, I hacked my PBX
Where is the authentication gone?

1. Launch Software
2. Click on "Load"
3. Click on "From phone"
4. Select phone
5. Enter password ("012345")
6. Watch download

<table>
<thead>
<tr>
<th>Step</th>
<th>Count</th>
<th>Chan</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1x</td>
<td>0</td>
<td>HELLO</td>
<td>READ_NVRAM</td>
</tr>
<tr>
<td>1x</td>
<td>0</td>
<td>READ_NVRAM</td>
<td>INQUIRE_HW</td>
</tr>
<tr>
<td>1x</td>
<td>1</td>
<td>CHAN_OPEN</td>
<td>INQUIRE_HW</td>
</tr>
<tr>
<td>20x</td>
<td>1</td>
<td>INQUIRE_HW</td>
<td></td>
</tr>
<tr>
<td>1x</td>
<td>1</td>
<td>INQUIRE_HW</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>PING</td>
<td></td>
</tr>
<tr>
<td>1x</td>
<td>2</td>
<td>CHAN_CLOSE</td>
<td></td>
</tr>
<tr>
<td>1x</td>
<td>2</td>
<td>INQUIRE_HW</td>
<td></td>
</tr>
<tr>
<td>nx</td>
<td>2</td>
<td>READ_NVRAM</td>
<td></td>
</tr>
<tr>
<td>1x</td>
<td>2</td>
<td>CHAN_CLOSE</td>
<td></td>
</tr>
<tr>
<td>1x</td>
<td>1</td>
<td>CHAN_CLOSE</td>
<td></td>
</tr>
</tbody>
</table>
Where is the authentication gone?

<table>
<thead>
<tr>
<th>Step</th>
<th>Count</th>
<th>Chan</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1x</td>
<td>0</td>
<td>HELLO</td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>0</td>
<td>READ_NVRAM</td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>1</td>
<td>CHAN_OPEN</td>
</tr>
<tr>
<td></td>
<td>20x</td>
<td>1</td>
<td>INQUIRE_HW</td>
</tr>
<tr>
<td>4</td>
<td>1x</td>
<td>1</td>
<td>READ_NVRAM</td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>1</td>
<td>INQUIRE_HW</td>
</tr>
<tr>
<td>5</td>
<td>1x</td>
<td>1</td>
<td>PING</td>
</tr>
<tr>
<td>6</td>
<td>1x</td>
<td>2</td>
<td>CHAN_OPEN</td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>2</td>
<td>INQUIRE_HW</td>
</tr>
<tr>
<td></td>
<td>nx</td>
<td>2</td>
<td>READ_NVRAM</td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>2</td>
<td>CHAN_CLOSE</td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>1</td>
<td>CHAN_CLOSE</td>
</tr>
</tbody>
</table>

1. Launch Software
2. Click on ”Load”
3. Click on ”From phone”
4. Select phone
5. Enter password (”012345”)
6. Watch download

Oops, I hacked my PBX
Where is the authentication gone?

1. Launch Software
2. Click on ”Load”
3. Click on ”From phone”
4. Select phone
5. Enter password (”012345”)  
6. Watch download

<table>
<thead>
<tr>
<th>Step</th>
<th>Count</th>
<th>Chan</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1x</td>
<td>0</td>
<td>HELLO</td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>0</td>
<td>READ_NVRAM</td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>1</td>
<td>CHAN_OPEN</td>
</tr>
<tr>
<td></td>
<td>20x</td>
<td>1</td>
<td>INQUIRE_HW</td>
</tr>
<tr>
<td>4</td>
<td>1x</td>
<td>1</td>
<td>READ_NVRAM</td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>1</td>
<td>INQUIRE_HW</td>
</tr>
<tr>
<td>5</td>
<td>1x</td>
<td>1</td>
<td>PING</td>
</tr>
<tr>
<td>6</td>
<td>1x</td>
<td>2</td>
<td>CHAN_OPEN</td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>2</td>
<td>INQUIRE_HW</td>
</tr>
<tr>
<td></td>
<td>nx</td>
<td>2</td>
<td>READ_NVRAM</td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>2</td>
<td>CHAN_CLOSE</td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>1</td>
<td>CHAN_CLOSE</td>
</tr>
</tbody>
</table>

pt
Oops, I hacked my PBX
Where is the authentication gone?

1. Launch Software
2. Click on "Load"
3. Click on "From phone"
4. Select phone
5. Enter password ("012345")
6. Watch download

<table>
<thead>
<tr>
<th>Step</th>
<th>Count</th>
<th>Chan</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1x</td>
<td>0</td>
<td>HELLO</td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>0</td>
<td>READ_NVRAM</td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>1</td>
<td>CHAN_OPEN</td>
</tr>
<tr>
<td></td>
<td>20x</td>
<td>1</td>
<td>INQUIRE_HW</td>
</tr>
<tr>
<td>4</td>
<td>1x</td>
<td>1</td>
<td>READ_NVRAM</td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>1</td>
<td>INQUIRE_HW</td>
</tr>
<tr>
<td>5</td>
<td>1x</td>
<td>1</td>
<td>PING</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>2</td>
<td>CHAN_OPEN</td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>2</td>
<td>INQUIRE_HW</td>
</tr>
<tr>
<td></td>
<td>nx</td>
<td>2</td>
<td>READ_NVRAM</td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>2</td>
<td>CHAN_CLOSE</td>
</tr>
<tr>
<td></td>
<td>1x</td>
<td>1</td>
<td>CHAN_CLOSE</td>
</tr>
</tbody>
</table>
Where is the authentication gone?

- A short READ_NVRAM
- Reads some binary gibberish
- Original software shows an auth-window
- Or was it...
Where is the authentication gone?

- A short READ_NVRAM
- Reads some binary gibberish
- Original software shows an auth-window
- Or was it...

**Client**: 09 31 01 02 00 00 00 A0 24 06
  - Len
  - Type
  - Chan
  - Addr

**PBX**: 10 32 01 02 02 00 00 A0 24 06 86 87 84 85 82 83
  - Len
  - Type
  - Chan
  - Addr
  - Len
  - Surprise

Oops, I hacked my PBX
Where is the authentication gone?

- A short READ_NVRAM
- Reads some binary gibberish
- Original software shows an auth-window
- Or was it...

Client:

```
09 31 01 02 00 00 00 A0 24 06
```

PBX:

```
10 32 01 02 02 00 00 A0 24 06
```

86 87 84 85 82 83

```
Surprise
```

Oops, I hacked my PBX
Where is the authentication gone?

- A short READ_NVRAM
- Reads some binary gibberish
- Original software shows an auth-window
- Or was it...

**Client**:  09 31 01 02 00 00 00 A0 24 06

<table>
<thead>
<tr>
<th>Len</th>
<th>Type</th>
<th>Chan</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Addr</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Len</td>
</tr>
</tbody>
</table>

**PBX**:  10 32 01 02 02 00 00 A0 24 06 86 87 84 85 82 83

<table>
<thead>
<tr>
<th>Len</th>
<th>Type</th>
<th>Chan</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Addr</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Len</td>
</tr>
</tbody>
</table>

XOR B

\[ \text{Surprise} \]

⇒ "012345"

Oops, I hacked my PBX
Where is the authentication gone?

- A short READ_NVRAM
- Reads some binary gibberish
- Original software shows an auth-window
- Or was it...

**Client**: 09 31 01 02 00 00 00 A0 24 06

**PBX**: 10 32 01 02 02 00 00 A0 24 06 86 87 84 85 82 83

**XOR**: B6 B6 B6 B6 B6 B6

\[ \begin{align*}
86 & \oplus B6 = 30 \\
87 & \oplus B6 = 31 \\
84 & \oplus B6 = 32 \\
85 & \oplus B6 = 33 \\
82 & \oplus B6 = 34 \\
83 & \oplus B6 = 35 
\end{align*} \]

⇒ "012345"

Oops, I hacked my PBX
### Where is the authentication gone?

- A short READ_NVRAM
- Reads some binary gibberish
- Original software shows an auth-window
- Or was it... D’ough

**Client**:

<table>
<thead>
<tr>
<th>Len</th>
<th>Type</th>
<th>Chan</th>
<th>Addr</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>09</td>
<td>31</td>
<td>01</td>
<td>02 00 00 00</td>
<td>A0 24</td>
</tr>
</tbody>
</table>

**PBX**:

<table>
<thead>
<tr>
<th>Len</th>
<th>Type</th>
<th>Chan</th>
<th>Addr</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>32</td>
<td>01</td>
<td>02 02 00 00</td>
<td>A0 24</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>86 87 84 85 82 83</td>
<td></td>
</tr>
</tbody>
</table>

**XOR**

| B6 | B6 | B6 | B6 | B6 | B6 | B6 |

$$\begin{align*}
86 & \quad 87 & \quad 84 & \quad 85 & \quad 82 & \quad 83 \\
\text{XOR} & \quad B6 & \quad B6 & \quad B6 & \quad B6 & \quad B6 & \quad B6
\end{align*}$$

$$\begin{align*}
= & \quad 30 & \quad 31 & \quad 32 & \quad 33 & \quad 34 & \quad 35 \quad \Rightarrow \quad "012345"
\end{align*}$$

Oops, I hacked my PBX
The story so far – But how could it happen?

- Authentication neither necessary nor useful
- No privilege system implemented
- Many commands useful for debugging
- ⇒ Maybe a developers interface?
The story so far – But how could it happen?

- Authentication neither necessary nor useful
- No privilege system implemented
- Many commands useful for debugging
- ⇒ Maybe a developers interface?
The story so far – But how could it happen?

- Authentication neither necessary nor useful
- No privilege system implemented
- Many commands useful for debugging
  ⇒ Maybe a developers interface?
The story so far – But how could it happen?

- Authentication neither necessary nor useful
- No privilege system implemented
- Many commands useful for debugging
- ⇒ Maybe a developers interface?
What could happen...

- Read/Write any phone
- Reset PBX password
- Really bad stuff: Read/Write firmware

Oops, I hacked my PBX
What could happen..

- Read/Write any phone
- Reset PBX password
- Really bad stuff: Read/Write firmware
What could happen..

- Read/Write any phone
- Reset PBX password
- Really bad stuff: Read/Write firmware
And now?

- Contact the vendor
- Be nice, they will be too!
- Help them improve!
- Carry on and find more bugs!
And now?

- Contact the vendor
- Be nice, they will be too!
- Help them improve!
- Carry on and find more bugs!
And now?

- Contact the vendor
- Be nice, they will be too!
- Help them improve!
- Carry on and find more bugs!
And now?

- Contact the vendor
- Be nice, they will be too!
- Help them improve!
- Carry on and find more bugs!
Lessons learned

- Anchor authentication/encryption in protocol
- Do not use debugging interfaces in production
- Audit your codebase once in a while
- Shannon was right..
- Vendors are happy to be informed (at least good ones)
Lessons learned

- Anchor authentication/encryption in protocol
- Do not use debugging interfaces in production
- Audit your codebase once in a while
- Shannon was right..
- Vendors are happy to be informed (at least good ones)
Lessons learned

- Anchor authentication/encryption in protocol
- Do not use debugging interfaces in production
- Audit your codebase once in a while
- Shannon was right..
- Vendors are happy to be informed (at least good ones)
Lessons learned

- Anchor authentication/encryption in protocol
- Do not use debugging interfaces in production
- Audit your codebase once in a while
- Shannon was right..
- Vendors are happy to be informed (at least good ones)
Lessons learned

- Anchor authentication/encryption in protocol
- Do not use debugging interfaces in production
- Audit your codebase once in a while
- Shannon was right..
- Vendors are happy to be informed (at least good ones)
Thank you for your attention

Any Questions?