Playing with ICS devices with RF

What can a small device do in modern industrial World

Alexey.Polyakov@kaspersky.com
Konstantin.Sapronov@kaspersky.com
Agenda

- Smart badge
- Sub 1Ghz RF
- Demo with RFCat
- Smart Grids
- Inside Smart Meters
- Threats for smart devices by RF
- Conclusion
ToorCon 14 Badge and DK_Dongle
HardWare – Texas Instrument CC1111 chip

CC1111F32 – Sub 1-Ghz
- Max power 1W, good to transmit to 230Meter!
- With external antenna can transmit even miles away
- 32 kB of in-system programmable flash memory
- 4 kB of RAM, can buffer up to 500 bytes in memory
- full-speed USB 2.0 interface
Sub 1Ghz RF

Sub 1Ghz ISM bands:

900Mhz  Cell phones, Cordless phones, Personal Two-Way Radio;
433MHz  Medical equipment
315 MHz  Car/Garage Remotes
915/868MHz (US/EU)  Smart meters and more … P25 Policy radios
Using Sub 1GHz device: Demo with RFCat

Establishing peer-to-peer session with 2 CC1111 devices

We will show how simple it can be done.

**Advantage:** not able to capture unless you have another one. You can use it without risk of being detected 😊
Discovering RF World: Home Devices

Power Meters (also as for gas, water measuring devices) – 90% in US household, used by all Power Providers

- Use 902-928 MHz to operate, FHSS, Remote reading
Inside Smart Meters

1. Power converts

2. Teridian 71M6531F SOC with a microprocessor core, a real-time clock, flash memory, and an LCD driver.

3. Texas Instruments low-power LM2904 dual operational amplifier.

4. Medium-power RFMD RF2172 amplifier IC.

5. Less-than-1-GHz Texas Instruments CC1110F32 SOC with a microcontroller and 32 kbytes of flash memory.

Elster Rex2
Smart Grid Infrastructure

Power Line equipment

- Transformers, Isolators, Condensers, Switches and line breakers;
- Power meters, field equipment
- 90% still with Leased line (expensive). Moving towards RF grid
- Remote area Readers and Control devices may use RF feature
Impacts of exploitation for RF devices

If you exploit such devices you can:

- remote keys / car fobs: open or close
- 2-ways phones: listen
- power meters: monitor and control
- Smart Grids: power outage
- SCADA: damage
- medical devices: kill
Threats by RF for smart devices

Attacks:
- Reading private data
- Theft of service
- Jamming Tx/Rx signals
- Possible damaging power line equipment:
  - Isolators
  - Condensers
  - Switches
  - Power transformers

Cost of repair can be small (5K) to high (2M for Transformers)
Discovering Smart Meters – troubles

- Before able to read, need to understand next Tx frequency
  - Usually, it is shifted from original basic frequency
    May take days or week of analysis ...

- The transmission is preset with SYNCWORD
  - Usually 2 bytes, but, need to look at thousands of transmission to find correct one.
  - RFCAT is able to help, but, luck and luck needed!

- Another challenge is package length and transmission data ratio
“Security”?

Current prevention solutions:
- FHSS
- SYNCWORDS
- DSSS
- dynamic routing tables

Security:
- encryption. AES 128
- session authentication
Discovering Smart Meters – FHSS

Beginning: transmitting session #1 (approx 913MHz)

3 min later: transmitting session #2 (approx 904 MHz)
5 hours later

Full 902-928MHz spectrum is covered

- FHSS – predefined rules for selecting next transmitting frequency
- Unknown Baud rate unknown packet length
- Same packets sent over and over many times
- Remote receiver
<table>
<thead>
<tr>
<th>Code</th>
<th>Received</th>
<th>Possible Sync Words</th>
</tr>
</thead>
<tbody>
<tr>
<td>1358536379.853</td>
<td>84724811c57cf5c286e830d18a2896d4c0891819f44662568d60be83b36d</td>
<td>'0x1191L', '0x88c8L', '0x4404L', '0x2252L', '0x9191L', '0x488cL'</td>
</tr>
<tr>
<td>1358536380.249</td>
<td>dfef176f6ffdf91f4f2ed297b647185d1d4e8a9e7e85c4e685fed7e6f6f20</td>
<td></td>
</tr>
<tr>
<td>1358536380.327</td>
<td>77f288db9c74d7bbd6cfd8b7f84f6c97c7f28f2e8ef775de9b0bc89ad6fa2c</td>
<td></td>
</tr>
<tr>
<td>1358536381.937</td>
<td>d957330121a27432007414b1b50e93f0a3db491be0f1750479f911bb9</td>
<td></td>
</tr>
<tr>
<td>1358536382.836</td>
<td>359bd2b37bbad2215e8228b79ae0e06d71d66c7c748d0f96c065409b901</td>
<td></td>
</tr>
<tr>
<td>1358536383.293</td>
<td>0419f8021d3f6e0aedd97812f6e3e3b0b776f7062d49f093a8e064c6c</td>
<td></td>
</tr>
<tr>
<td>1358536386.224</td>
<td>c119776822ccf38160a310e30db91d9de9114bf0fa47f20e2d5120d5a40</td>
<td></td>
</tr>
<tr>
<td>1358536387.798</td>
<td>9ace8cc1f96c588f00619fb291458176859baef1674e0f4d2f6b21d16bd</td>
<td></td>
</tr>
<tr>
<td>1358536389.384</td>
<td>1d4a70517de15cc5809e91e6e8156c2085b06ff07fb7b0033f4d44b1e1c</td>
<td></td>
</tr>
<tr>
<td>1358536391.650</td>
<td>1b4d39877f5f0e603d280602a455b4e1a6ae387f201868f930d60635e30</td>
<td></td>
</tr>
<tr>
<td>1358536393.453</td>
<td>5b33a4d0e30835dd4544441c024dd46736379b6818043f0b4f6c8041b4f</td>
<td></td>
</tr>
<tr>
<td>1358536394.657</td>
<td>85950c5e4ee4a9c439b2a97f1e13c221264646963fa09c12bdf080cb8a7</td>
<td></td>
</tr>
<tr>
<td>1358536396.346</td>
<td>21b1fb297ad6e26b6be559ca6449a57a1e7ef8133bfb4cc520007f10009f</td>
<td></td>
</tr>
<tr>
<td>1358536398.084</td>
<td>e59e6f5faccfc9f96294c1425936af0b60029de6e0e6b87d3ce0e1e0001</td>
<td></td>
</tr>
<tr>
<td>1358536401.122</td>
<td>002f6b89ec1518550a0818053c297e81b324e3843528020b268e5237feb</td>
<td></td>
</tr>
<tr>
<td>1358536402.120</td>
<td>30fb638f492be77f7f4b7dd0545063233e216059939610e0b0800059</td>
<td></td>
</tr>
<tr>
<td>1358536404.808</td>
<td>0ef33cc44b3ebf220c8a681cf1285c100157573c3b0b38b4e87f12d04</td>
<td></td>
</tr>
<tr>
<td>1358536408.126</td>
<td>07c43e2c126288b7145e5bfe4071116ef87d1a94a3bb7e534b9030800b47</td>
<td></td>
</tr>
<tr>
<td>1358536410.446</td>
<td>b0e00d5c671e7c79e4531184080db0a97d6e69463333ee093bc6f38af</td>
<td></td>
</tr>
<tr>
<td>1358536415.155</td>
<td>bbed71bcb5cfbe201287924c09274700f6063ab25a5337f60010329323f6o</td>
<td></td>
</tr>
<tr>
<td>1358536416.155</td>
<td>de16874ff018f122ccffdc7f9e021397f34756db252ac327e8ab7dbdf2</td>
<td></td>
</tr>
<tr>
<td>1358536431.310</td>
<td>cfb37621c154a1549c9381f5a0e434366bf9f08e81f1927305fa3b3f5e</td>
<td></td>
</tr>
<tr>
<td>1358536436.367</td>
<td>d7c090b9c3a867f7fca91ff9b9af17c45257e2086ac0b9df94874246010</td>
<td></td>
</tr>
<tr>
<td>1358536436.367</td>
<td>79cf643de0e59599ed9449abfe46c57e9d236f8ab181f98dca83e4d60</td>
<td></td>
</tr>
<tr>
<td>1358536437.160</td>
<td>3b4fcedcd8b060a4d124efbf7915a990d12a5665ecf3d3157bb8e3c42c</td>
<td></td>
</tr>
<tr>
<td>1358536437.160</td>
<td>c5e463e2c33b5ff358adcb9356b185b9bc16ed5f844afa7d8f29293f</td>
<td></td>
</tr>
<tr>
<td>1358536437.740</td>
<td>45a7f3fbb187e583eb84f0f2913bd315e77770e6b47d7af77da2c3b50d01</td>
<td></td>
</tr>
<tr>
<td>1358536438.515</td>
<td>b4e1bf1ca48ee5eeef825092246de98e49413fd5f16c21879daf9b77f6</td>
<td></td>
</tr>
<tr>
<td>1358536438.515</td>
<td>fd2f6421ad6d6c7efa9375b18a6dbcf1e9f1947244aaa443367400a3840</td>
<td></td>
</tr>
</tbody>
</table>

**Discovering Smart Meters - SYNCWORD**
Conclusion

- Power Meters is a good and typical example of Industrial reading devices.
- More recently, they were not easy ways to find equipment for security researches in this area.
- Now, we have a good RF device for testing Smart Meters. However, it takes a lot of time to understand how Smart Meters work.
- “Security” by design (FHSS, frequency hopping, predefined communication list) is widely used but it is not enough. Some advanced ideas (data encryption, session authentication) is less used.

- You can discover what happens around by just using available devices like the one presented earlier. The cost is between $50-$100.
Thanks to

Toorcon team for badge
  Mike Ossman for specan
  Atlas for RFcat

And YOU for attention

Questions ?!