New Tales of Wireless Input Devices

October 24, 2019

„It’s good to be back!“
Who am I?

Dipl.-Inf. Matthias Deeg
Senior Expert IT Security Consultant
Head of Research & Development
CISSP, CISA, OSCP, OSCE

- Interested in information technology – especially IT security – since his early days
- Studied computer science at the University of Ulm, Germany
- IT Security Consultant since 2007
Who am I?

B. Sc. Gerhard Klostermeier
Senior IT Security Consultant
Head of Hardware Team
OSCP, OSCE

- Interested in all things concerning IT security – especially when it comes to hardware and radio protocols
- Studied IT security at the University of Aalen, Germany
- IT Security Consultant since 2014
Agenda

1. Introduction to Used Technology of Wireless Input Devices
2. Previous Work of Other Researchers
3. Overview of Our Research
4. Attack Surface and Attack Scenarios
5. Found Security Vulnerabilities
6. (Live) Demos
7. Some Anecdotes
8. Conclusion & Recommendation
9. Q&A
Short Introduction to Used Technology

- Wireless presenter
- USB dongle
- Keyboard
- Mouse

October 24, 2019
M. Deeg & G. Klostermeier | t2'19
Short Introduction to Used Technology

- **HackRF One**
- **Crazyradio PA**
- **Logitech Unifying Receiver**
Previous Work of Other Researchers

- KeyKeriki v1.0 and v2.0 by Dreamlab Technologies, 2010
- Owned Live on Stage: Hacking Wireless Presenters, Niels Teusink, 2010
- Promiscuity is the nRF24L01+'s Duty, Travis Goodspeed, 2011
- KeySweeper, Samy Kamkar, 2015
- MouseJack, Bastille Networks Internet Security, 2016
- KeyJack, Bastille Networks Internet Security, 2016
- KeySniffer, Bastille Networks Internet Security, 2016
- Of Mice and Keyboards, SySS GmbH, 2016
- Presentation Clickers, Marc Newlin, 2019
- LOGItacker, Marcus Mengs, 2019
Overview of Our Research

Follow-up project to our research project *Of Mice and Keyboards*

- Finding answers to open questions
- Focus on another kind of wireless input device with the same or similar used technology: *Wireless presenters*
Recap: Of Mice and Keyboards

Summary of our research results (2016)

<table>
<thead>
<tr>
<th>#</th>
<th>Product Name</th>
<th>Insufficient Code/Data Protection</th>
<th>Mouse Spoofing</th>
<th>Replay</th>
<th>Keystroke Injection</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cherry AES B.UNLIMITED</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>2</td>
<td>Fujitsu Wireless Keyboard Set LX901</td>
<td>?</td>
<td>?</td>
<td>✓</td>
<td>?</td>
</tr>
<tr>
<td>3</td>
<td>Logitech MK520</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓*</td>
</tr>
<tr>
<td>4</td>
<td>Microsoft Wireless Desktop 2000</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>?</td>
</tr>
<tr>
<td>5</td>
<td>Perixx PERIDUO-710W</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

✓ security issue found

X security issue not found

? security issue may exit (more work required)

* first found and reported to Logitech by Bastille Networks
Overview of Our Research

- Tested different **non-Bluetooth** wireless input devices of different manufacturers using 2.4 GHz communication:
  1. Fujitsu Wireless Keyboard Set LX901
  2. Cherry B.UNLIMITED 3.0
  3. Fujitsu Wireless Keyboard Set LX390
  4. Logitech Wireless Presenter R400
  5. Logitech Wireless Presenter R700
  6. Inateck Wireless Presenters WP1001
  7. Inateck Wireless Presenter WP2002
  8. August Wireless Presenter LP205R
  9. Kensington Wireless Presenter
  10. Targus Wireless Presenter AMP09EU
  11. Red Star Tec Wireless Presenter
  12. BEBONCOOL Wireless Presenter
Test Methodology

1. Hardware analysis
   - Opening up keyboards, wireless presenters, and USB dongles
   - Staring at PCBs
   - Identifying chips
   - RTFD (Reading the Fine Documentation™, if available)
   - Finding test points for SPI or wiretap IC pins or PCB traces
   - Soldering some wires
   - Using a logic analyzer to analyze data communication between chips
2. Radio-based analysis

- Using software-defined radio, e.g. HackRF One
- Using CrazyRadio PA with nrf-research-firmware
- Using Universal Radio Hacker, GNU Radio, and inspectrum to record and analyze radio communication
- Trying to identify used transceivers, their configuration, and used communication protocols based on the analyzed radio signals (for unmarked chips)
- Filling knowledge gaps concerning packet formats/framing, payloads, and checksums
Test Methodology

3. Firmware analysis
   - No firmware analysis of tested non-Bluetooth devices, as it was either not necessary for achieving our goals or extracting firmware was not possible
Hardware Analysis

Typical wireless presenter functionality
- Button for a laser
- Buttons for common presentation software hotkeys, e.g.
  - PAGE UP (0x4B)
  - PAGE DOWN (0x4E)
  - ESC (0x29)
  - F5 (0x3E)
  - PERIOD (0x37)
  - B (0x05)
Hardware Analysis

Parts of Inateck WP2002

PCB back side of Inateck WP2002
PCB back side of Logitech R400 wireless presenter
Hardware Analysis

PCB front side of Targus wireless presenter
Hardware Analysis

Kensington wireless presenter with some epoxy resin

Wiretapping PCB traces for SPI sniffing
Hardware Analysis

PCB front of Fujitsu Wireless Keyboard LX390
# Identified Transceivers/RF ICs (non-Bluetooth)

<table>
<thead>
<tr>
<th>#</th>
<th>Product Name</th>
<th>Product Type</th>
<th>RF IC</th>
<th>USB IDs (VID:PID)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Fujitsu Wireless Keyboard Set LX901</td>
<td>keyboard &amp; mouse</td>
<td>CYRF6936</td>
<td>1a81:1002</td>
</tr>
<tr>
<td>2</td>
<td>Cherry B.UNLIMITED 3.0</td>
<td>keyboard &amp; mouse</td>
<td>nRF24</td>
<td>046a:010e</td>
</tr>
<tr>
<td>3</td>
<td>Fujitsu Wireless Keyboard Set LX390</td>
<td>keyboard &amp; mouse</td>
<td>LT8900</td>
<td>1a81:1004</td>
</tr>
<tr>
<td>4</td>
<td>Logitech Wireless Presenter R400</td>
<td>presenter</td>
<td>nRF24</td>
<td>046d:c538</td>
</tr>
<tr>
<td>5</td>
<td>Logitech Wireless Presenter R700</td>
<td>presenter</td>
<td>nRF24</td>
<td>046d:c538</td>
</tr>
<tr>
<td>6</td>
<td>Inateck Wireless Presenter WP1001</td>
<td>presenter</td>
<td>BK2423</td>
<td>0c45:6900</td>
</tr>
<tr>
<td>7</td>
<td>Inateck Wireless Presenter WP2002</td>
<td>presenter</td>
<td>BK2461</td>
<td>45a8:1701</td>
</tr>
<tr>
<td>8</td>
<td>August Wireless Presenter LP205R</td>
<td>presenter</td>
<td>LT8900</td>
<td>1d57:ad03</td>
</tr>
<tr>
<td>9</td>
<td>Targus Wireless Presenter AMP09EU</td>
<td>presenter</td>
<td>nRF24</td>
<td>1048:07d2</td>
</tr>
<tr>
<td>10</td>
<td>Kensington Wireless Presenter</td>
<td>presenter</td>
<td>PL1167/LT8900</td>
<td>05b8:3226</td>
</tr>
<tr>
<td>11</td>
<td>Red Star Tec Wireless Presenter</td>
<td>presenter</td>
<td>HS304</td>
<td>2571:4101</td>
</tr>
<tr>
<td>12</td>
<td>BEBONCOOL Wireless Presenter</td>
<td>presenter</td>
<td>HS304</td>
<td>2571:4101</td>
</tr>
</tbody>
</table>
- Data sheets for most of the identified lost-cost 2.4 GHz transceivers are publicly available
- nRF24 by Nordic Semiconductor and CYRF6936 Cypress Semiconductor have been quite popular for many years and still are
- Beken RF ICs (e.g. BK2423, BK2461) are almost identical to nRF24
- We could not find any publicly available datasheets for HS304 RF ICs, but Marc Newlin reverse engineered and already documented some information about them on GitHub [24]
Radio-based Analysis

Packet analysis using Universal Radio Hacker (URH)
Radio-based Analysis

Packet generation using Universal Radio Hacker (URH)
Challenges

- From RF energy to exploitable security vulnerability

FSK-demodulated signal of Inateck WP2002 shown in Universal Radio Hacker (URH)
Challenges

- Understand this
  10101010110011110000010100000000000010100110100000011111
  010010110100111000000110000011000011
- To eventually achieve this
Challenges

- Signal modulation
- Packet format/framing
- Field lengths
- Bit and byte order
- Checksums (add, xor, polynomial division [CRC])
- Payload contents
- Use of RF spectrum (e.g. frequency hopping)
- Data whitening/data scrambling/pseudo noise

<table>
<thead>
<tr>
<th>6:0</th>
<th>SCRAMBLE_DATA</th>
<th>R/W</th>
<th>Whitening seed for data scramble. Must be set the same at both ends of radio link (Tx and Rx).</th>
</tr>
</thead>
</table>
Challenges

- Well-documented data structures and educated guesses
- Typical packet format:

<table>
<thead>
<tr>
<th>preamble</th>
<th>sync word(s)</th>
<th>address</th>
<th>control word</th>
<th>payload</th>
<th>checksum</th>
</tr>
</thead>
</table>

- payload length  
- ACK flag  
- packet ID

- Not all fields are used by all 2.4 GHz transceivers
### Example: BK2461 packet format used in Inateck WP2002

```
101010101100111100000010100000000000010100111010000001111010010110100111100000000001100000011000011
```

<table>
<thead>
<tr>
<th>Offset (in bits)</th>
<th>Size (in bits)</th>
<th>Description</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>8</td>
<td>Preamble</td>
<td>10101010</td>
<td>0xAA, typical preamble value</td>
</tr>
<tr>
<td>8</td>
<td>40</td>
<td>Address</td>
<td>11001111 00000101 00000000 00000101 00110100</td>
<td>5 byte address</td>
</tr>
<tr>
<td>48</td>
<td>6</td>
<td>Payload length</td>
<td>000011</td>
<td>3 payload bytes</td>
</tr>
<tr>
<td>54</td>
<td>2</td>
<td>PID</td>
<td>11</td>
<td>packet ID</td>
</tr>
<tr>
<td>56</td>
<td>1</td>
<td>ACK option</td>
<td>1</td>
<td>No auto acknowledgement</td>
</tr>
<tr>
<td>57</td>
<td>variable</td>
<td>Payload</td>
<td>01001011 01001110 00000000</td>
<td>0x4B 0x4E 0x00, 2nd byte is key scan code</td>
</tr>
<tr>
<td>variable</td>
<td>16</td>
<td>Checksum (CRC-16)</td>
<td>11000000 11000011</td>
<td>0xC0 0xC3, CRC-16</td>
</tr>
</tbody>
</table>
Attack Surface and Attack Scenarios

1. Physical access to wireless input device
   - Extract firmware
   - Manipulate firmware
   - Extract cryptographic key material
   - Manipulate cryptographic key material

2. Attacking via radio signals (OTA)
   - Exploiting unencrypted and unauthenticated radio communication
   - Replay attacks
   - Keystroke injection attacks
   - Decrypting encrypted data communication
1. Unencrypted and unauthenticated data communication
2. Missing protection against replay attacks
3. Cryptographic issues – keystroke injection attacks
Mouse Spoofing Attacks

„I exploit the obvious!“

Exploiting unencrypted and unauthenticated data communication
Mouse Spoofing Attacks

- Some tested wireless presenters support mouse features, e.g. Targus wireless presenter
- The data communication is unencrypted and unauthenticated
- By knowing the correct packet format for mouse actions like mouse movements and mouse clicks, mouse spoofing attacks can be performed
Recap: Mouse Spoofing Attacks
Recap: Mouse Spoofing Attacks

All your important files were encrypted with our CryptL0ck malware. The only way to restore your files is to pay us.

CAUTION:
Simply removing CryptL0ck from your computer will not restore your files!

Click here to learn your individual
follow the instructions
Replay Attacks

„Pon de replay!“

Replay attacks against wireless input devices
Replay Attacks

- All tested wireless presenters are vulnerable to replay attacks.
- But replay attacks aren’t that interesting regarding wireless presenters, as there are no security-sensitive inputs like password entries.
Keystroke Injection Attacks

„One small keystroke injection for me, one giant injection attack for mousekind.“

Remotely taking control over a computer system
Keystroke Injection Attacks

- The data communication of all tested wireless presenters is unencrypted and unauthenticated (disregarding data whitening)
- By knowing the correct packet format, keystroke packets can be sent to the corresponding USB receiver dongle
- If there is no input validation performed by the USB receiver dongle (e.g. whitelisting), arbitrary keystrokes (USB HID keyboard events) can be triggered on the target system
- Two of our tested wireless presenters were not vulnerable to keystroke injection attacks
Keystroke Injection Attacks

- The Fujitsu Wireless Keyboard Set LX901 uses AES encryption for protecting the keyboard communication.
- AES-encrypted data packets with payload size of 16 bytes.
- Cryptographic issues regarding the AES encryption, for instance, insecure use of AES CTR mode, could not be found, like in the following previously tested AES-encrypted keyboards:
  - Cherry B.UNLIMITED AES
  - Logitech MK520
  - Perixx PERIDUO-710W
Recap: Keystroke Injection Attacks

- The plaintext of a key release packet is as follows:
  
  `00 00 00 00 00 00 00 00 00 00 00` (11 NULL bytes)

- Counter mode encryption:

  Known values for a key release packet are marked red.
Recap: Keystroke Injection Attacks

- IVs (random counter values) can be reused (see replay attack)
  ⇒ Known plaintext attack
- Encrypted key release packet consists of 16 Bytes:

  ![](image)

  data random value

- The data of a key release packet (11 NULL bytes) are the actual keystream block, as $x \oplus 0 = x$ (exclusive or)
  ⇒ A key release packet can be manipulated arbitrarily
Keystroke Injection Attacks

- However, concerning the Fujitsu LX901 we found out that simply sending unencrypted keystroke packets as described in the Cypress CY4672 PRoC LP Reference Design Kit [21] works just fine.
- The two-chip design also allowed for SPI sniffing.
Keystroke Injection Attacks

- As CYRF6936 uses pseudo noise codes for data whitening, we simply also used a CYRF6936 transceiver with the same configuration.
- Using an ATmega328p-based multiprotocol RF module with some modified code from the project DIY-Multiprotocol-TX-Module worked just fine for our PoC attack.
- This device has the following four transceivers: CYRF6936, CC2500, A7105, nRF24L01.
Keystroke Injection Attacks

// Cypress recommended SOP PN codes (see Table 7-7 of WirelessUSB™ LP/LPstar and PRoC™ LP/LPstar Technical Reference Manual)

```c
uint8_t SOP_PN_CODES[][8] = {
    "\x3c\x37\xCC\x91\xE2\xF8\xCC\x91",
    "\x9b\xC5\xA1\x0F\xAD\x39\xA2\x0F",
    "\xEF\x64\xB0\x2A\xD2\x8F\xB1\x2A",
    "\x66\xCD\x7C\x50\xDD\x26\x7C\x50",
    "\x5C\xE1\xF6\x44\xAD\x16\xF6\x44",
    "\x5A\xCC\xAE\x46\xB6\x31\xAE\x46",
    "\xA1\x78\xDC\x3C\xE8\xDC\x3C",
    "\xB9\x8E\x19\x74\x6F\x65\x18\x74",
    "\xDF\xB1\xC0\x49\x62\xDF\xC1\x49",
    "\x97\xE5\x14\x72\xF7\x1A\x14\x72"
};
```

// key data for Fujitsu wireless keyboard LX901

```c
uint8_t packet_keypress1[] = "\x41\x04"; // a
uint8_t packet_keypress2[] = "\x41\x04\x02"; // A (a + SHIFT)
uint8_t packet_keypress3[] = "\x41\x05\x02"; // B (b + SHIFT)
uint8_t packet_key_release[] = "\x45\x00";
```
Yet Another “Secure” Keyboard

- Was asked about the Fujitsu Wireless Keyboard Set LX390 after the publication of the LX901 security advisories
- The LX390 is also advertised with “secure 2.4 GHz technology” but without AES encryption – thus we had a closer look

The Wireless Keyboard Set LX390 is an excellent desktop solution for users with ambition. This durable keyboard set is equipped with secure 2.4 GHz technology and plug and play technology. The elegant mouse works on most surfaces due to its precise 1000 dpi sensor. It offers fabulous features and ultra slim, portable design.

Usability
- Reliable wireless 2.4 GHz technology for home and office use
- Slim and sleek design for space saving
- USB Plug&Play with 1-click fast connection
- Mouse with precise 1000 dpi
- USB nano receiver

(Source: Data Sheet FUJITSU Accessory Wireless Keyboard Set LX390, 2019/02/21)
Yet Another “Secure” Keyboard

The Wireless Keyboard Set LX390 is an excellent desktop solution for users with ambition. This durable keyboard set is equipped with secure 2.4 GHz technology and plug and play technology. The elegant mouse works on most surfaces due to its precise 1000 dpi sensor. It offers fabulous features and ultra slim, portable design.

Old data sheet
(2019/02/21)

Usability
- Reliable wireless 2.4 GHz technology for home and office use
- Slim and sleek design for space saving
- USB Plug&Play with 1-click fast connection
- Mouse with precise 1000 dpi
- USB nano receiver

New data sheet
(2019/03/25)

Usability
- Reliable wireless 2.4 GHz technology for home and office use
- Slim and sleek design for space saving
- USB Plug&Play with 1-click fast connection
- Mouse with precise 1000 dpi
- USB nano receiver
Yet Another “Secure” Keyboard

The Wireless Keyboard Set LX390 is an excellent desktop solution for users with ambition. This durable keyboard set is equipped with secure 2.4 GHz technology and plug and play technology. The elegant mouse works on most surfaces due to its precise 1000 dpi sensor. It offers fabulous features and ultra slim, portable design.

Old data sheet
(2019/02/21)

Usability
- Reliable wireless 2.4 GHz technology for home and office use
- Slim and sleek design for space saving
- USB Plug&Play with 1-click fast connection
- Mouse with precise 1000 dpi
- USB nano receiver

New data sheet
(2019/03/25)

Usability
- Reliable wireless 2.4 GHz technology for home and office use
- Slim and sleek design for space saving
- USB Plug&Play with 1-click fast connection
- Mouse with precise 1000 dpi
- USB nano receiver
Yet Another “Secure” Keyboard

PCB front of Fujitsu Wireless Keyboard LX390
Yet Another “Secure” Keyboard

PCB front of Fujitsu Wireless Keyboard LX390
Yet Another “Secure” Keyboard

- By analyzing the SPI communication between the microcontroller and the transceiver, the use of an LT8900-based RF IC could be deduced.
- With knowing the transceiver and its configuration, the captured radio signals could be properly decoded.
### Example: LT8900 packet format used by Fujitsu LX390 (keypress “a”)

<table>
<thead>
<tr>
<th>Offset (in bits)</th>
<th>Size (in bits)</th>
<th>Description</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>8</td>
<td>Preamble</td>
<td>01010101 (0x55)</td>
<td>10101010 (0xAA) or 01010101 (0x55)</td>
</tr>
<tr>
<td>8</td>
<td>48</td>
<td>Sync word</td>
<td>001110110110110110101001111011111111111010001011110111100011111011110111011000001011</td>
<td>6 byte sync word for addressing</td>
</tr>
<tr>
<td>56</td>
<td>4</td>
<td>Trailer</td>
<td>1010</td>
<td>4 bit trailer, 1010 (0xA) or 0101 (0x5)</td>
</tr>
<tr>
<td>60</td>
<td>variable</td>
<td>Payload</td>
<td>0100001011101111000111101</td>
<td>payload bytes, 1st byte is payload length, scrambled (data whitening)</td>
</tr>
<tr>
<td>variable</td>
<td>16</td>
<td>Checksum (CRC-16)</td>
<td>01111011000001011</td>
<td>CRC-16 with device-specific 1-byte init value, scrambled (data whitening)</td>
</tr>
</tbody>
</table>
Yet Another “Secure” Keyboard

- Data scrambling (data whitening) of the LT8900 is used
- The same plain text payload (044504) resulted in the same cipher text payload for two different sample devices
  - Keyboard #1: 553B5B53BD43DB542EF1D760B
  - Keyboard #2: AA49E9ECA5A42CA42EF1DA7B1
- Note: The CRC-16 checksums are different due to different init values

⇒ The same data scrambling is used by different devices
⇒ The used “keystream” can be extracted by analyzing one device
⇒ There is no message authentication code (MAC)
Yet Another “Secure” Keyboard

- Performed a **known plaintext attack** to get the “keystream”

<table>
<thead>
<tr>
<th>Byte (OTA)</th>
<th>Bits (OTA)</th>
<th>Reversed Bits</th>
<th>Reversed Byte</th>
<th>Plain Text Byte</th>
<th>Key Byte</th>
<th>The Math</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x42</td>
<td>01000010</td>
<td>01000010</td>
<td>0x42</td>
<td>0x02</td>
<td>0x40</td>
<td>0x42 ^ 0x40 = 0x02</td>
</tr>
<tr>
<td>0xEF</td>
<td>11101111</td>
<td>11101111</td>
<td>0xF7</td>
<td>0x45</td>
<td>0xB2</td>
<td>0xF7 ^ 0xB2 = 0x45</td>
</tr>
<tr>
<td>0x1D</td>
<td>00011101</td>
<td>10111000</td>
<td>0xB8</td>
<td>0x04</td>
<td>0xBC</td>
<td>0xB8 ^ 0xBC = 0x04</td>
</tr>
<tr>
<td>0x76</td>
<td>01101110</td>
<td>01101110</td>
<td>0x6E</td>
<td>0xAD</td>
<td>0xC3</td>
<td>0x6E ^ 0xC3 = 0xAD</td>
</tr>
<tr>
<td>0x0B</td>
<td>00001011</td>
<td>11010000</td>
<td>0xD0</td>
<td>0xCF</td>
<td>0x1F</td>
<td>0xD0 ^ 0x1F = 0xCF</td>
</tr>
</tbody>
</table>

… … … … … … … … … …
The CRC-16 calculation uses the following configuration:

- Polynomial: \( x^{16} + x^{12} + x^5 + 1 = 0x11021 \)
- Reflection of input data (reversed bit order)
- Device specific one-byte init value, e.g. 0x9A
- CRC-16 is transmitted in big endian byte order
- 256 possibilities for CRC init value
Yet Another “Secure” Keyboard

The Fujitsu Wireless Keyboard Set LX390 with “secure 2.4 GHz technology” is affected by the following security vulnerabilities:

1. Missing Protection against Replay Attacks
2. Missing Encryption of Sensitive Data
3. Insufficient Verification of Data Authenticity

⇒ Replay Attacks
⇒ Keystroke Sniffing Attacks
⇒ Keystroke Injection Attacks
(Live) Demo Time

1. Old news are so exciting: Attacking wireless presenters
2. Attacking yet another AES-encrypted wireless desktop set, but this time differently
3. From wiretapping to keystroke sniffing attack
(Live) Demo: Wireless Presenter
(Live) Demo: AES-encrypted Keyboard
# python3 fujitsu_lx390_sniffer.py -l -p "3b:5b:53:bd:43" -c 28

SySS Fujitsu LX390 Keystroke Sniffer - PoC Tool v0.1 by Matthias Deeg - SySS GmbH
Based on different tools by Marc Newlin

---

3B:5B:53:BD:43:DB  42:CF:1D:70:ED  02:41:04:CD:A8  KEY_A
3B:5B:53:BD:43:DB  42:EF:1D:76:0B  02:45:04:AD:CF  KEY_A
3B:5B:53:BD:43:DB  42:CF:1D:70:ED  02:41:04:CD:A8  KEY_A

(...)

SySS Fujitsu LX390 Keystroke Sniffer - PoC Tool v0.1 by Matthias Deeg - SySS GmbH
Based on different tools by Marc Newlin
Some Anecdotes

1. Product rebranding
2. What’s my CVSS Base Score again?
3. Fake or real?
Some Anecdotes: Product Rebranding

- Cherry released the B.UNLIMITED AES as B.UNLIMITED 3.0
- It uses the same 128-bit AES encryption with the same security issues
- Not all people buying this Cherry wireless desktop set know this, e.g. one of our customers who was made aware of it during a security awareness event
Some Anecdotes: Product Rebranding

- When having a closer look at the Cherry B.UNLIMITED 3.0 USB dongle, realized that there is something wrong with the FCC ID.
Some Anecdotes: CVSS Base Scores

- Was asked for CVSSv3 base scores for the two reported Fujitsu LX901 vulnerabilities
  - SYSS-2016-068: Cryptographic Issues (CWE-310) – Missing Protection against Replay Attack
  - SYSS-2018-033: Cryptographic Issues (CWE-310) – Keystroke Injection Vulnerability
- Had good arguments for different CVSSv3 base scores

<table>
<thead>
<tr>
<th>Exploitation Metrics</th>
<th>Impact Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Exploitability Metrics</strong></td>
<td><strong>Scope (S)</strong></td>
</tr>
<tr>
<td>Attack Vector (AV)*</td>
<td>Unchanged (SU)</td>
</tr>
<tr>
<td>Network (AV:N)</td>
<td>Local (AV:L)</td>
</tr>
<tr>
<td>Adjacent Network (AV:A)</td>
<td></td>
</tr>
<tr>
<td>Attack Complexity (AC)*</td>
<td></td>
</tr>
<tr>
<td>Low (AC:L)</td>
<td>High (AC:H)</td>
</tr>
<tr>
<td>Privileges Required (PR)*</td>
<td></td>
</tr>
<tr>
<td>None (PR:N)</td>
<td>Low (PR:L)</td>
</tr>
<tr>
<td>User Interaction (UI)*</td>
<td></td>
</tr>
<tr>
<td>None (UI:N)</td>
<td>Required (UI:R)</td>
</tr>
<tr>
<td>Confidentiality Impact (C)*</td>
<td></td>
</tr>
<tr>
<td>None (C:N)</td>
<td>Low (C:L)</td>
</tr>
<tr>
<td>Integrity Impact (I)*</td>
<td></td>
</tr>
<tr>
<td>None (I:N)</td>
<td>Low (I:L)</td>
</tr>
<tr>
<td>Availability Impact (A)*</td>
<td></td>
</tr>
<tr>
<td>None (A:N)</td>
<td>Low (A:L)</td>
</tr>
</tbody>
</table>
SYSS-2016-068: Cryptographic Issues (CWE-310) – Missing Protection against Replay Attack

CVSSv3 Base Score: 3.5 (Low)

CVSSv3 Base Score: 4.3 (Medium)

CVSSv3 Base Score: 6.1 (Medium)

CVSSv3 Base Score: 8.2 (High)

CVSSv3 Base Score: 9.6 (Critical)

CVSSv3 Base Score: 7.6 (High)
SYSS-2018-033: Cryptographic Issues (CWE-310) – Keystroke Injection Vulnerability

CVSSv3 Base Score: 9.6 (Critical)

CVSSv3 Base Score: 8.2 (High)
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:C/N/I:H/A:L

CVSSv3 Base Score: 4.8 (Medium)
Some Anecdotes: Real or fake?

- Bought three Logitech R400 via Amazon and got three different devices
- Logitech could/would not help us find out which are real and which are fake
Some Anecdotes: Real or fake?

Response from Logitech Support:

“(…) Alle internen Informationen zu den Teilen usw. sind urheberrechtlich geschützte Informationen von Logitech und können nicht bereitgestellt werden. (…)”

“(…) All internal information regarding parts and so forth are copyright protected information of Logitech and cannot be provided. (…)” (translation of quote)
Conclusion

1. Unencrypted and unauthenticated data communication
   ⇒ Mouse spoofing attacks
   ⇒ Keystroke injection attacks
   ⇒ Keystroke sniffing attacks

2. Missing protection against replay attacks
   ⇒ Replay attacks

3. Cryptographic issues
   ⇒ Keystroke injection attacks
   ⇒ Keystroke sniffing attacks
## Conclusion

### Our research results concerning wireless presenters

<table>
<thead>
<tr>
<th>#</th>
<th>Product Name</th>
<th>Keystroke Injection</th>
<th>Mouse Spoofing</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Logitech Wireless Presenter R400</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>2</td>
<td>Logitech Wireless Presenter R700</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>3</td>
<td>Inateck Wireless Presenter WP1001</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>4</td>
<td>Inateck Wireless Presenter WP2002</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>5</td>
<td>August Wireless Presenter LP205R</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>6</td>
<td>Targus Wireless Presenter AMP09EU</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>7</td>
<td>Kensington Wireless Presenter</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>8</td>
<td>Red Star Tec Wireless Presenter</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>9</td>
<td>BEBONCOOL Wireless Presenter</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

✓ security issue found  
X security issue not found  
? security issue may exist (more work required)
## Conclusion

Marc Newlin’s research results concerning wireless presenters [24]

<table>
<thead>
<tr>
<th>#</th>
<th>Product Name</th>
<th>Keystroke Injection</th>
<th>Mouse Spoofing</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Amazon Basics P-001</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>2</td>
<td>Canon PR100-R</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>3</td>
<td>Funpick Wireless Presenter</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>4</td>
<td>BEBONCOOL D100</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>5</td>
<td>ESYWEN Wireless Presenter</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>6</td>
<td>Red Star Tech PR-819</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>7</td>
<td>DinoFire D06-DF-US</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>8</td>
<td>TBBSC DSIT-60</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>9</td>
<td>Rii Wireless Presenter</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>10</td>
<td>Logitech R400</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>11</td>
<td>Logitech R500</td>
<td>✓ (limited)</td>
<td>X</td>
</tr>
<tr>
<td>12</td>
<td>Logitech R800</td>
<td>✓</td>
<td>X</td>
</tr>
</tbody>
</table>
# Conclusion

## Updated research results concerning wireless desktop sets (2019)

<table>
<thead>
<tr>
<th>#</th>
<th>Product Name</th>
<th>Insufficient Code/Data Protection</th>
<th>Mouse Spoofing</th>
<th>Replay</th>
<th>Keystroke Injection</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cherry AES B.UNLIMITED</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>2</td>
<td>Fujitsu Wireless Keyboard Set LX901</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>3</td>
<td>Logitech MK520</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>* first found and reported to Logitech by Bastille Networks</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Microsoft Wireless Desktop 2000</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>5</td>
<td>Perixx PERIDUO-710W</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

- ✓ security issue found
- X security issue not found
- ? security issue may exit (more work required)
Conclusion

- Security vulnerabilities may be reimplemented in new product versions
- Logitech R400 is a good example
  - 2010: Reported issue in CYRF69103-based version
  - 2016: Reported issue in nRF24-based version
  - 2019: Vulnerable versions still available
Recommendation

- Choose your wireless input devices wisely, e.g. wireless presenter
- Do not use wireless desktop sets with known security vulnerabilities in environments with higher security demands
- Consider Bluetooth wireless input devices more secure than non-Bluetooth keyboards using proprietary 2.4 GHz radio communication until proven otherwise
- Replace or update vulnerable devices (e.g. Logitech [30])
- If in doubt, use wired input devices
Interesting New Software Tools

- Marc Newlin (@marcnewlin) is also researching wireless presentation clickers and has publicly released new tools and many keystroke injection vulnerabilities in such devices in April 2019 [24]
- Marcus Mengs (@mame82) published his research results concerning new security vulnerabilities in different Logitech wireless input devices using Logitech Unifying Receiver (LOGITacker [31], munifying [32])
- We have forked Marc Newlin’s presentation-clickers GitHub repository and are going to create a somewhat unified nRF24-based keystroke injection toolbox for different kinds of non-Bluetooth 2.4 GHz wireless input devices named KeyJector [29]
One More Thing

- Barcode scanners are just keyboards with a special form factor
References

2. KeyKeriki v2.0 – 2.4 GHz, Dreamlab Technologies, http://www.remote-exploit.org/articles/keykeriki_v2_0_8211_2_4ghz/, 2010
References


References


References


32. munifying, Marcus Mengs, https://github.com/mame82/munifying, 2019


Thank you very much ...  

... for your attention.

Do you have any questions?

E-mail: matthias.deeg@syss.de  
Twitter: @matthiasdeeg

E-mail: gerhard.klostermeier@syss.de  
Twitter: @iiikarus