New Tales of Wireless Input Devices

June 4, 2019

„Dobrze jest być z powrotem”
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
- USB dongle

June 4, 2019
M. Deeg & G. Klostermeier | CONFidence 2019
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
Overview of Our Research

1. 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*

2. New research project regarding Bluetooth keyboards
   - Having a closer look at wireless keyboards using a more standardized 2.4 GHz communication than the previously tested ones (*Bluetooth Classic & Bluetooth Low Energy*)
# 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. Logitech Wireless Presenter R400
  4. Logitech Wireless Presenter R700
  5. Inateck Wireless Presenters WP1001
  6. Inateck Wireless Presenter WP2002
  7. August Wireless Presenter LP205R
  8. Kensington Wireless Presenter
  9. Targus Wireless Presenter AMP09EU
  10. Red Star Tec Wireless Presenter
  11. BEBONCOOL Wireless Presenter
Overview of Our Research

- Tested three popular Bluetooth keyboards of different manufacturers using:
  1. 1byone keyboard
  2. Logitech K480
  3. Microsoft Designer Bluetooth Desktop (Model 1678, 2017)
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 wireless development platform Ubertooth 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
- Using Bluetooth USB dongles with chipsets CSR8510 and BCM20702A
- Using sniffing capabilities of Linux Bluetooth stack BlueZ
3. Firmware analysis
   - Only had a superficial look at extracted firmware and device configurations of the tested Bluetooth devices due to the limited time available
   - 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 side of 1byone keyboard
PCB front side of Logitech K420 keyboard
Hardware Analysis

PCB back side of Logitech K420 keyboard
Cracked metal casing of Microsoft Designer Bluetooth keyboard
## 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>Logitech Wireless Presenter R400</td>
<td>presenter</td>
<td>nRF24</td>
<td>046d:c538</td>
</tr>
<tr>
<td>4</td>
<td>Logitech Wireless Presenter R700</td>
<td>presenter</td>
<td>nRF24</td>
<td>046d:c538</td>
</tr>
<tr>
<td>5</td>
<td>Inateck Wireless Presenter WP1001</td>
<td>presenter</td>
<td>BK2423</td>
<td>0c45:6900</td>
</tr>
<tr>
<td>6</td>
<td>Inateck Wireless Presenter WP2002</td>
<td>presenter</td>
<td>BK2461</td>
<td>45a8:1701</td>
</tr>
<tr>
<td>7</td>
<td>August Wireless Presenter LP205R</td>
<td>presenter</td>
<td>LT8900</td>
<td>1d57:ad03</td>
</tr>
<tr>
<td>8</td>
<td>Targus Wireless Presenter AMP09EU</td>
<td>presenter</td>
<td>nRF24</td>
<td>1048:07d2</td>
</tr>
<tr>
<td>9</td>
<td>Kensington Wireless Presenter</td>
<td>presenter</td>
<td>PL1167/LT8900</td>
<td>05b8:3226</td>
</tr>
<tr>
<td>10</td>
<td>Red Star Tec Wireless Presenter</td>
<td>presenter</td>
<td>HS304</td>
<td>2571:4101</td>
</tr>
<tr>
<td>11</td>
<td>BEBONCOOL Wireless Presenter</td>
<td>presenter</td>
<td>HS304</td>
<td>2571:4101</td>
</tr>
</tbody>
</table>
# Identified Transceivers/RF ICs (Bluetooth)

<table>
<thead>
<tr>
<th>#</th>
<th>Product Name</th>
<th>Product Type</th>
<th>Bluetooth IC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1byone keyboard</td>
<td>keyboard</td>
<td>BCM20730</td>
</tr>
<tr>
<td>2</td>
<td>Logitech K480</td>
<td>keyboard</td>
<td>CYW20730</td>
</tr>
<tr>
<td>3</td>
<td>Microsoft Designer Bluetooth Desktop</td>
<td>keyboard</td>
<td>nRF51822</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].
SWD (Serial Wire Debug) connection to Microsoft keyboard using Segger J-Link Pro
Firmware Analysis

Device "NRF51822_XXAB" selected.

Connecting to target via SWD
Found SW-DP with ID 0x0BB11477
Scanning AP map to find all available APs
AP[1]: Stopped AP scan as end of AP map has been reached
AP[0]: AHB-AP (IDR: 0x04770021)
Iterating through AP map to find AHB-AP to use
AP[0]: Core found
AP[0]: AHB-AP ROM base: 0xF0000000
CPUID register: 0x410CC200. Implementer code: 0x41 (ARM)
Found Cortex-M0 r0p0, Little endian.
FPUnit: 4 code (BP) slots and 0 literal slots
CoreSight components:
ROMTbl[0] @ F0000000
ROMTbl[0][0]: E00FF000, CID: B105100D, PID: 000BB471 ROM Table
ROMTbl[1] @ E00FF000
ROMTbl[1][0]: E000E000, CID: B105E00D, PID: 000BB008 SCS
ROMTbl[1][1]: E0001000, CID: B105E00D, PID: 000BB00A DWT
ROMTbl[1][2]: E0002000, CID: B105E00D, PID: 000BB00B FPB
ROMTbl[0][1]: F0002000, CID: 00000000, PID: 00000000 ??
Cortex-M0 identified.
J-Link>savebin C:\Users\syss\Documents\nrf51_code.dump 0x20000
Opening binary file for writing... [C:\Users\syss\Documents\nrf51_code.dump]
Reading 131072 bytes from addr 0x00000000 into file...O.K.
J-Link>
Radio-based Analysis

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

Packet generation using Universal Radio Hacker (URH)
Challenges

- Understand this
  1010101011001111000001010000000000000101001101000000111101001011010011100000001100000011000011
  010010110100111100000000011000000110000011000011
- To eventually achieve this
Challenges

- Signal modulation
- Packet format/framing
- Field lengths
- Bit and byte order
- Checksums (add, xor, polynomial division [CRC])
- Payload contents
- 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>
<th>00H</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

```
1010101011001111000000101000000000000101001101000000011110100101101001110000000001100000011000011
```

<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>0xA, 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>
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
Found Security Vulnerabilities

1. Insufficient protection of code (firmware) and data (cryptographic key)
2. Unencrypted and unauthenticated data communication
3. Missing protection against replay attacks
4. Cryptographic issues – keystroke injection attacks
Insufficient Protection of Code and Data

„All your sensitive data are belong to me!“

Unauthorized access to sensitive data (firmware & cryptographic key)
Insufficient Protection of Code and Data

- Embedded flash memory of all tested Bluetooth keyboards can be read and written
- 1byone and Logitech K420 keyboards store the link key in an external SPI serial flash memory chip (e.g. 24C256A)
- The flash memory contents of the Microsoft Designer Bluetooth Desktop (nRF51822) could be extracted via SWD
- Did not analyze any wireless presenter firmware as it was not necessary
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
- The tested Bluetooth keyboards are not vulnerable to replay attacks
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 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:

```
8C 49 A1 35 2D 9F 67 C0 1E 0D B8 5F 42 A7 23 9E
```

- 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
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\xA3\xA2\x0F",
    "\xEF\x64\xB0\xA2\xD2\x8F\xB1\xA2",
    "\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\x9E\x82\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";
```
Bluetooth Trust Relationships

In the course of our research project, we made the following two interesting observations that combined result in an interesting attack vector:

1. Cryptographic key material of bonded Bluetooth devices can be extracted by an attacker with physical access without much difficulties

2. Most of the Bluetooth stacks of modern operating systems do not strictly bind specific properties of a bonded Bluetooth device with its pairing information (Bluetooth address and link key)
Connected Bluetooth Headphones

- Bluetooth headphones are connected to a Google Pixel 2 smartphone with Android 9
- By default, the headphones have different privileges
Android Smart Lock

- Optionally, Bluetooth devices can be used to automatically unlock Android devices using the Smart Lock feature.
Physical Access
Extracting Cryptographic Key Material

Serial Flash memory chip

Qualcomm CSR8635 Bluetooth Audio Platform
Extracting Cryptographic Keys (Chip-Off)
Extracting Cryptographic Keys (In-Circuit)
Extracting Cryptographic Key Material

- Among other things, the memory dump contains Bluetooth pairing information
  - Bluetooth address (funny data format)
  - Shared secret (link key)
Exploiting the Trust Relationship

- During the Bluetooth pairing process, by default, specific Bluetooth devices are granted access to specific functionalities.
- If the trust relationship of the attacked Bluetooth device already allows for using more functionality, an attacker can directly exploit this.
- For example, Bluetooth headphones with a built-in microphone often get phone book access (PBAP) and can answer calls (HSP).
- With the link key and the Bluetooth device addresses, an attacker is able to emulate a different device (e.g., keyboard) and exploit the existing Bluetooth trust relationship.
Exploiting the Trust Relationship

```
[syss@Livehack-VM pypbap]$ python2 pbapclient.py
Welcome to the PhoneBook Access Profile!
2018-10-02 16:03:57,287 __main__ INFO     Finding PBAP service ...
2018-10-02 16:03:58,492 __main__ INFO     PBAP service found!
2018-10-02 16:03:58,751 __main__ INFO     Connect success
pbap> pull_vcard_listing telecom/pb
2018-10-02 16:04:12,145 __main__ INFO     Requesting pull_vcard_listing with parameters
   {'name': 'telecom/pb', 'self': <__main__.PBAPClient instance at 0x7f8b0cd58ab8>,
    'list_startoffset': 0, 'search_value': None, 'search_attribute': 0, 'order': 0,
    'max_list_count': 65535}
2018-10-02 16:04:13,145 __main__ INFO     Result of pull_vcard_listing:
   <?xml version="1.0"?><!DOCTYPE vcard-listing SYSTEM "vcard-listing.dtd"><vCard-listing
   version="1.0"><card handle="0.vcf" name="Live Hack"/></card>
   <card handle="1.vcf" name="Micky Maus"/></card>
   <card handle="2.vcf" name="Donald Duck"/></card>
   <card handle="3.vcf" name="Daisy Duck"/></card>
   <card handle="4.vcf" name="Dagobert Duck"/></card>
   <card handle="5.vcf" name="Daisy Duck"/></card>
   <card handle="6.vcf" name="Daisy Duck"/></card>
   <card handle="7.vcf" name="Daisy Duck"/></card>
   <card handle="8.vcf" name="Klarabella Kuh"/></card>
   <card handle="9.vcf" name="Goofy"/></card>
   <card handle="10.vcf" name="Gundel Gaukeley"/></vCard-listing>
```
# Tested Operating Systems

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Version</th>
<th>Attack successful?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>7.1.2</td>
<td>yes</td>
</tr>
<tr>
<td>Android</td>
<td>8.1.0</td>
<td>Yes</td>
</tr>
<tr>
<td>Android</td>
<td>9</td>
<td>yes</td>
</tr>
<tr>
<td>Arch Linux</td>
<td>4.16.13-2-ARCH #1</td>
<td>no</td>
</tr>
<tr>
<td>Apple iOS</td>
<td>11.2.6</td>
<td>yes</td>
</tr>
<tr>
<td>Apple iOS</td>
<td>11.3</td>
<td>yes</td>
</tr>
<tr>
<td>Apple iOS</td>
<td>11.4</td>
<td>yes</td>
</tr>
<tr>
<td>Apple Mac OS X</td>
<td>10.13.4</td>
<td>yes</td>
</tr>
<tr>
<td>Apple Mac OS X</td>
<td>10.13.5</td>
<td>yes</td>
</tr>
<tr>
<td>Microsoft Windows 10</td>
<td>1709 (OS Build 16299.125)</td>
<td>no</td>
</tr>
</tbody>
</table>
(Live) Demo Time

1. Exploiting the obvious: Bluetooth trust relationships
2. Old news are so exciting: Attacking wireless presenters
3. Attacking yet another AES-encrypted wireless desktop set, but this time differently
(Live) Demo: Bluetooth Trust Relationship
(Live) Demo: Wireless Presenter
(Live) Demo: AES-encrypted Keyboard
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

![USB dongle image](image-url)
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
Some Anecdotes: CVSS Base Scores

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)
Some Anecdotes: CVSS Base Scores

SYSS-2018-033: Cryptographic Issues (CWE-310) – Keystroke Injection Vulnerability

CVSSv3 Base Score: 9.6 (Critical)

CVSSv3 Base Score: 8.2 (High)

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
Conclusion

1. Insufficient protection of code (firmware) and data (cryptographic key) ⇒ Access to sensitive data
2. Unencrypted and unauthenticated data communication ⇒ Mouse spoofing attacks ⇒ Keystroke injection attacks
3. Missing protection against replay attacks ⇒ Replay attacks
4. Cryptographic issues ⇒ Keystroke injection attacks
Conclusion

- Every Bluetooth device deserves protection
- Bluetooth stacks of different operating systems behave differently
Conclusion

Research results concerning Bluetooth keyboards

<table>
<thead>
<tr>
<th>#</th>
<th>Product Name</th>
<th>Insufficient Code/Data Protection</th>
<th>Insecure Pairing</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1byone keyboard</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>2</td>
<td>Logitech K480</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>3</td>
<td>Microsoft Designer Bluetooth Desktop</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

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

? security issue may exit (more work required)

* first found and reported to Logitech by Bastille Networks
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 presenter wisely
- Do not use wireless desktop sets with known security vulnerabilities in security-related environments
- Regularly check trust relationships of used IT systems (e.g., Bluetooth devices)
- Consider all Bluetooth-capable devices in your IT security concept (complete life cycle)
- Consider Bluetooth wireless input devices more secure than non-Bluetooth keyboards using proprietary 2.4 GHz radio communication until proven otherwise
- If in doubt, use wired input devices
Current & Future Work

- Marc Newlin (@marcnewlin) is also researching wireless presentation clickers and has publicly released new tools and many keystroke injection vulnerabilities in such devices a couple of weeks ago [24]

- Marcus Mengs (@mame82) is doing awesome research, for instance concerning current Logitech Unifying receivers, that will hopefully be publicly disclosed soon

- 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

28. SySS Security Advisory SYSS-2019-015, Matthias Deeg,

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: @iiijikarus