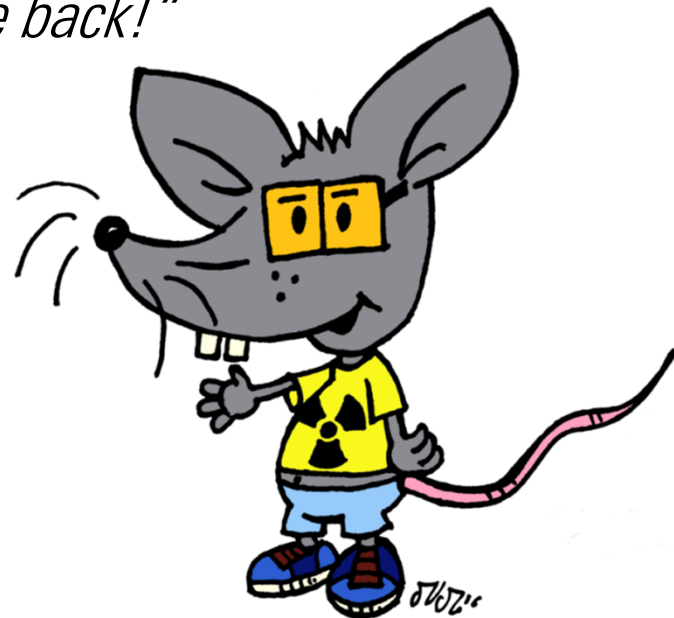


New Tales of Wireless Input Devices

November 28, 2019

„It's good to be back!“

DEEPP SEC



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



Short Introduction to Used Technology



Previous Work of Other Researchers

- KeyKeriki v1.0 and v2.0 by Max Moser and Thorsten Schröder, 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)

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

✓ security issue found

X security issue not found

? security issue may exist (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 | } | Wireless Desktop Set |
| 2. Cherry B.UNLIMITED 3.0 | | |
| 3. Fujitsu Wireless Keyboard Set LX390 | | |
| 4. Logitech Wireless Presenter R400 | } | Wireless Presenter |
| 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 | | |

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

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)

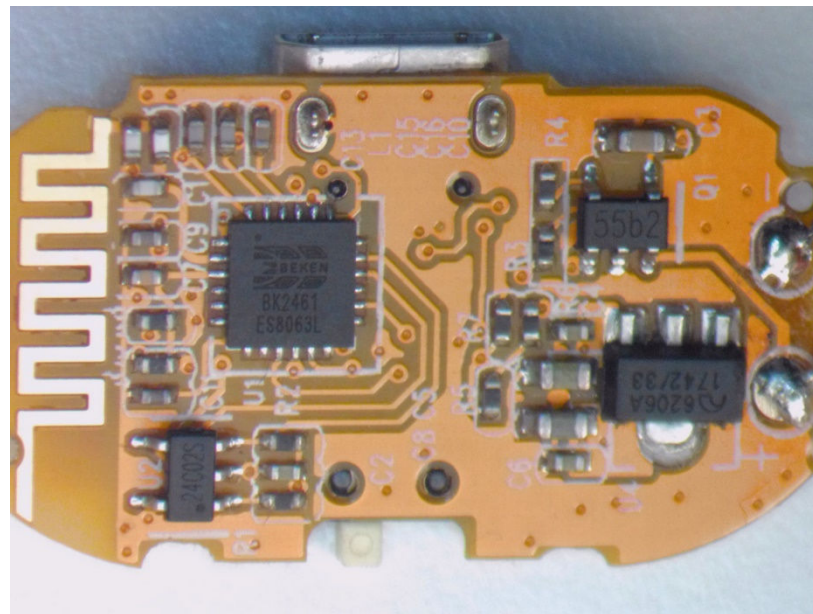


Logitech R700 Laser Presentation Remote

Hardware Analysis

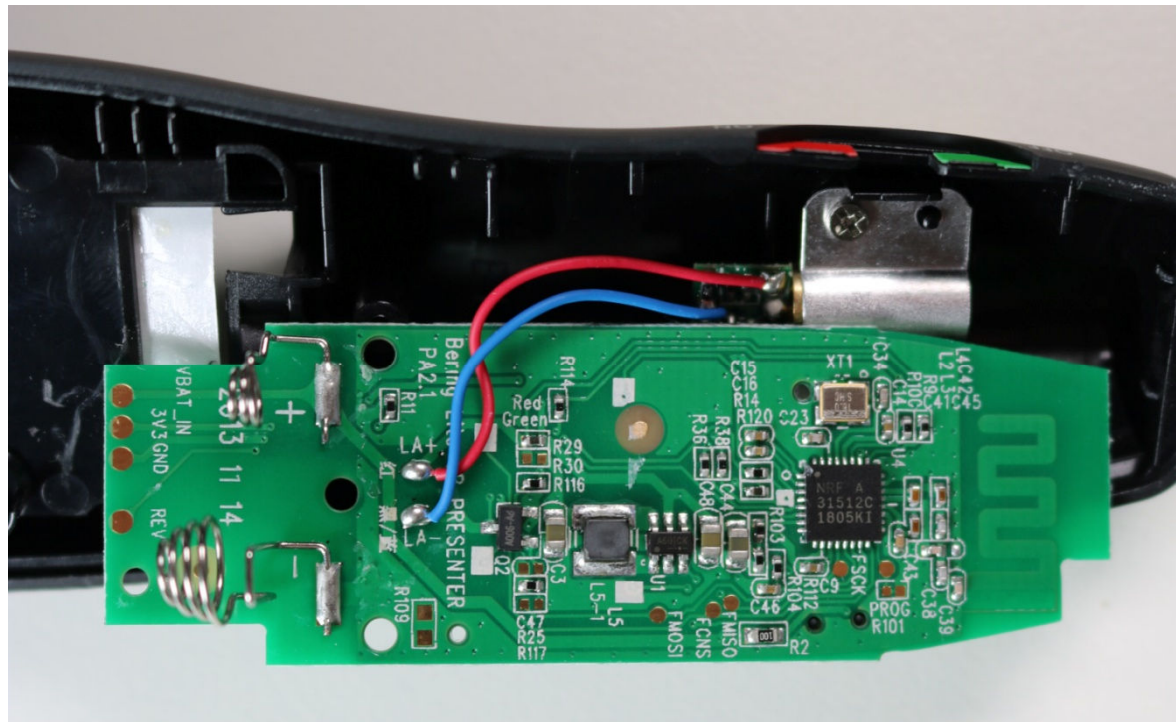


Parts of Inateck WP2002



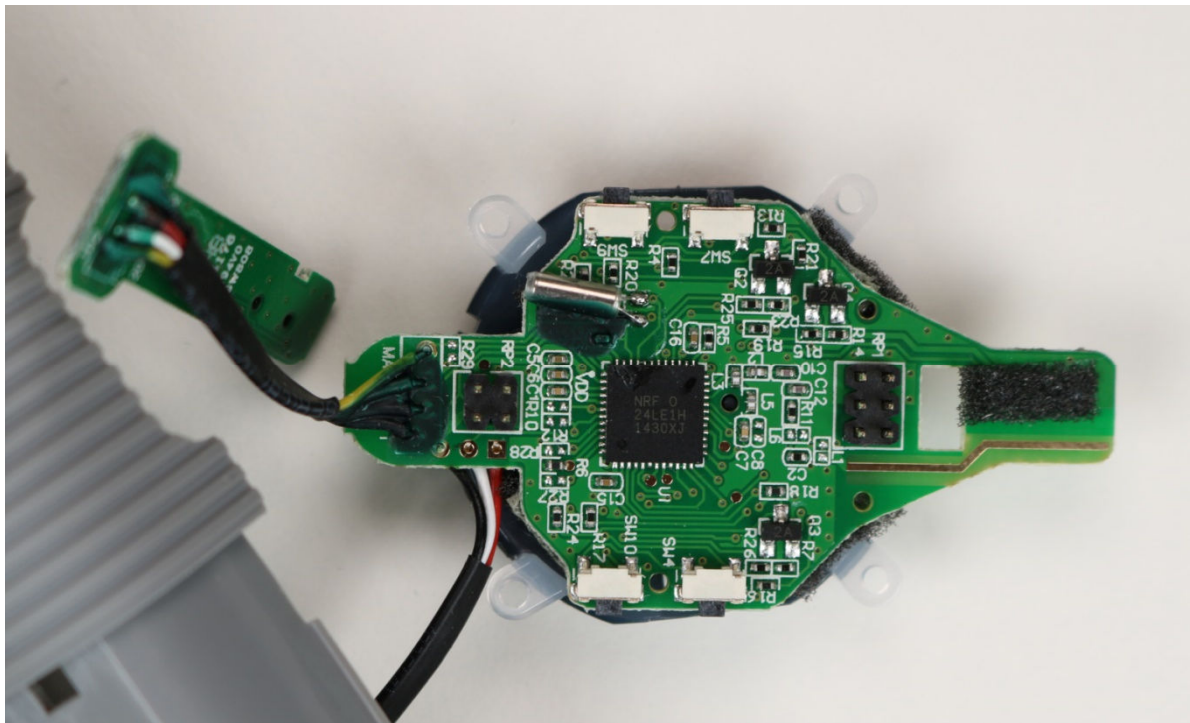
PCB back side of Inateck WP2002

Hardware Analysis



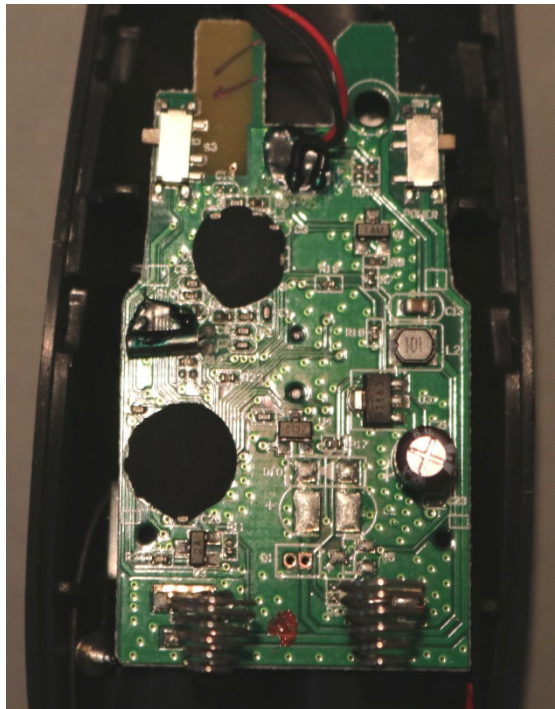
PCB back side of Logitech R400 wireless presenter

Hardware Analysis

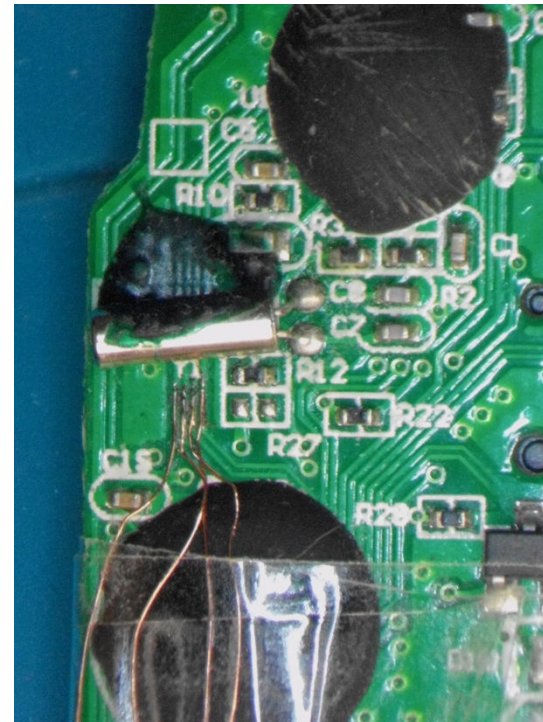


PCB front side of Targus wireless presenter

Hardware Analysis

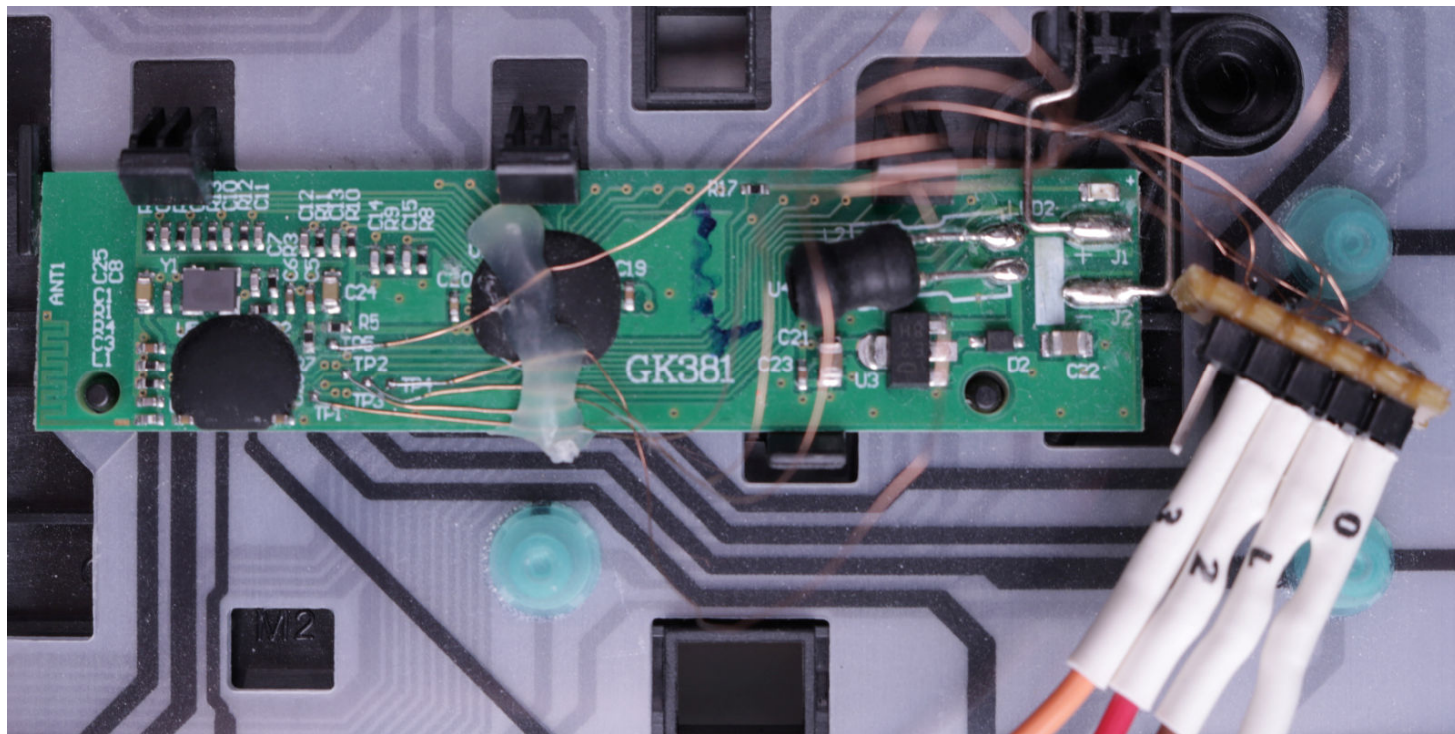


Kensington wireless presenter with some epoxy resin



Wiretapping PCB traces for SPI sniffing

Hardware Analysis



PCB front of Fujitsu Wireless Keyboard LX390

Identified Transceivers/RF ICs (non-Bluetooth)

#	Product Name	Product Type	RF IC	USB IDs (VID:PID)
1	Fujitsu Wireless Keyboard Set LX901	keyboard & mouse	CYRF6936	1a81:1002
2	Cherry B.UNLIMITED 3.0	keyboard & mouse	nRF24	046a:010e
3	Fujitsu Wireless Keyboard Set LX390	keyboard & mouse	LT8900	1a81:1004
4	Logitech Wireless Presenter R400	presenter	nRF24	046d:c538
5	Logitech Wireless Presenter R700	presenter	nRF24	046d:c538
6	Inateck Wireless Presenter WP1001	presenter	BK2423	0c45:6900
7	Inateck Wireless Presenter WP2002	presenter	BK2461	45a8:1701
8	August Wireless Presenter LP205R	presenter	LT8900	1d57:ad03
9	Targus Wireless Presenter AMP09EU	presenter	nRF24	1048:07d2
10	Kensington Wireless Presenter	presenter	PL1167/LT8900	05b8:3226
11	Red Star Tec Wireless Presenter	presenter	HS304	2571:4101
12	BEBONCOOL Wireless Presenter	presenter	HS304	2571:4101

RTFD – Read the Fine Datasheets

- 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

Universal Radio Hacker (URH) interface showing packet analysis results.

File Edit Help

Filter:

Name	Size
generated.noisefuzz	63.42 KiB
hackrf-2_435Ghz-8MHz-complex	221.04 MiB
hackrf-2_435Ghz-10MHz-complex	238.04 MiB
inspectio.fuzz.xml	9.34 KiB
keystroke.fuzz.xml	5.25 KiB
profile.fuzz.xml	5.25 KiB
protocol.packets.xml	2.90 KiB

Protocols:

- New Group
- protocol
- hackrf-2_435Ghz-10MHz-complex

Participants:

View data as:

Configure Decoding:

Decoding errors for message:

Message Types:

Name	Color	Display format	Order (bits/byte)	Value
✓ Default				
✓ preamble	Yellow	Bit	MSB/BE	10101010
✓ receiver address	Green	Bit	MSB/BE	110011110000010100000000000001010101000
✓ packet length	Red	Bit	MSB/BE	000011
✓ packet ID	Blue	Bit	MSB/BE	11
✓ NO_ACK	Brown	Bit	MSB/BE	1
✓ payload	Dark Red	Bit	MSB/BE	010000110100101100000000
✓ crc-16	Dark Blue	Bit	MSB/BE	1001010101010111

Participants:

Participants	Description
not assigned	
Alisa (A)	
Bob (B)	

Enter pattern here:

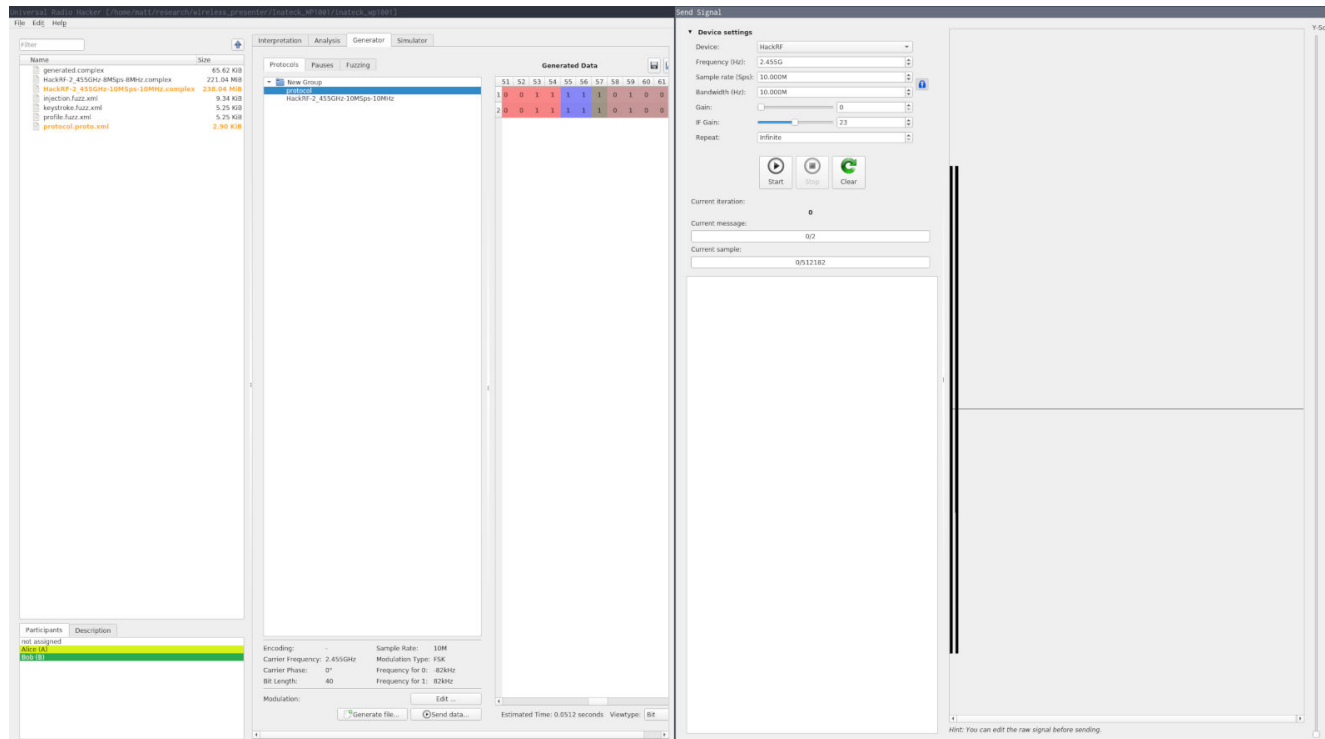
Search:

Time stamp: 01400

Labels for message:

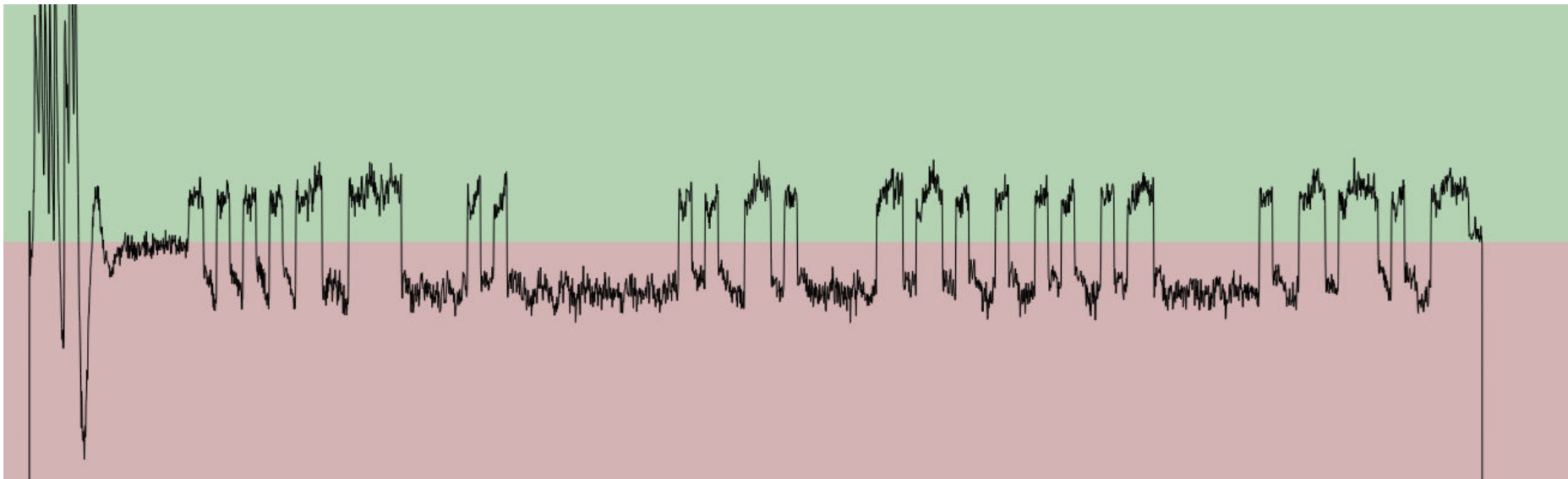
Packet analysis using Universal Radio Hacker (URH)

Radio-based Analysis



Challenges

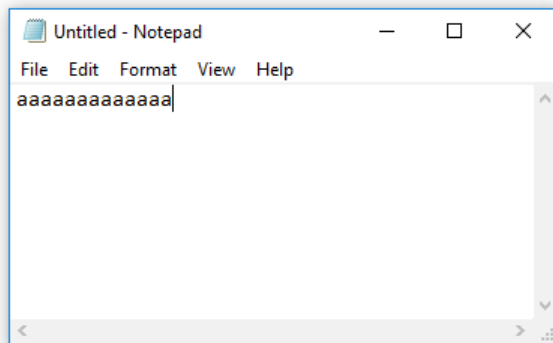
- From RF energy to exploitable security vulnerability



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

Challenges

- Understand this
101010101100111100000101000000000000010100110100000011111
0100101101001110000000001100000011000011
- To eventually achieve this



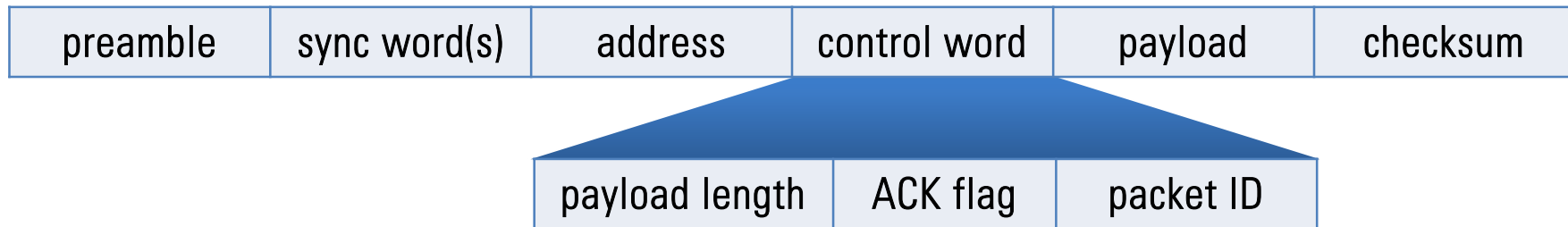
Challenges

- 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

6:0	SCRAMBLE_DATA	R/W	Whitening seed for data <u>scramble</u> . Must be set the same at both ends of radio link (Tx and Rx).	00H
-----	---------------	-----	--	-----

Challenges

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



- Not all fields are used by all 2.4 GHz transceivers

Packet Format

- Example: BK2461 packet format used in Inateck WP2002

1010101011001111000001010000000000000101001101000000111101001011010011100000000110000011000011

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

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

Found Security Vulnerabilities

1. Unencrypted and unauthenticated data communication
2. Missing protection against replay attacks
3. Cryptographic issues

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

C:\Users\Bob\AppData\Local\Temp\cryptLock.html

IMPORTANT - CryptLock L...

ION !!!

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

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

[Click here to learn your individual
follow the instruct](#)

```

root@hacker:~/radioactive# python radioactive.py -h
radioactive Home v0.7 by Matthias Deeg - SySS (c) 2016
shop - radioactive.py (-h) -> ADDRESS -> CHANNEL -> DEVICE -> ATTACK [-1]

optional arguments:
-h, --help            show this help message and exit
-v ADDRESS            address of the device
-c CHANNEL            address of the device
-d DEVICE            device of the device
-a ATTACK            target device (supported: microsoft, cherry, peritel)
-l LIST              list of available attack vectors
-L LIST              list of available attack vectors

root@hacker:~/radioactive# python radioactive.py -a 88:88:88:88:88:88 -c 5 -d microsoft -v win7_german

radioactive Home v0.7 by Matthias Deeg - SySS (c) 2016
[+] Configure RF24 radio
[+] Initialize mouse: Microsoft
[+] Generate mouse actions for selected attack vector 'Windows 7 Default, German keyboard'
[+] Start mouse spoofing attack ...
[+] Done
root@hacker:~/radioactive#

```

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

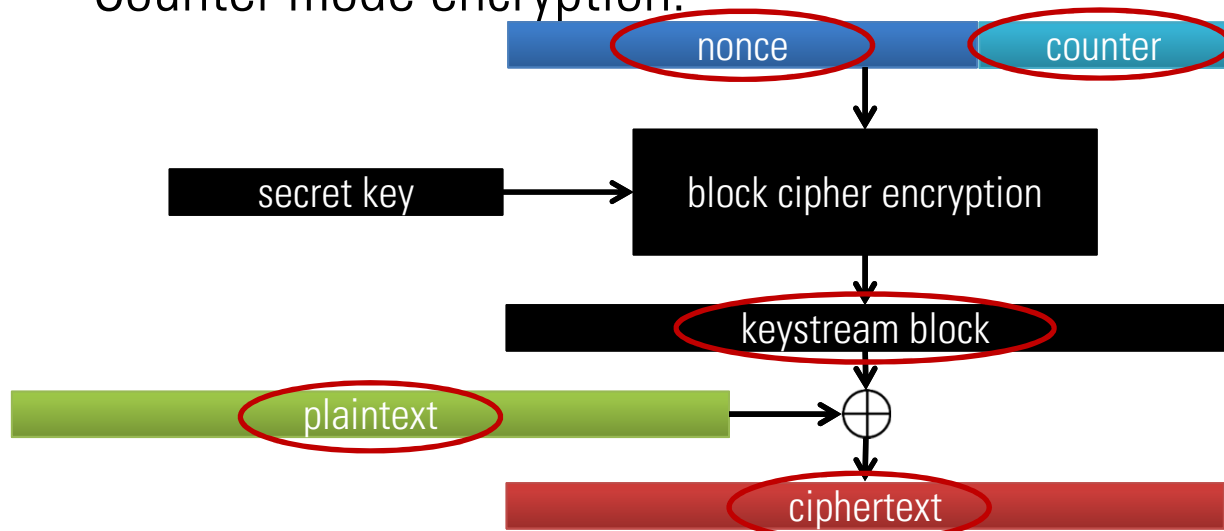
- The Fujitsu Wireless Keyboard Set LX901 uses **AES encryption** for protecting the keyboard communication
- AES-encrypted data packets with payload size of 16 bytes
- **Cryptographic issues** regarding the AES encryption, for instance insecure use of AES CTR mode, could not be found, like in the following 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:



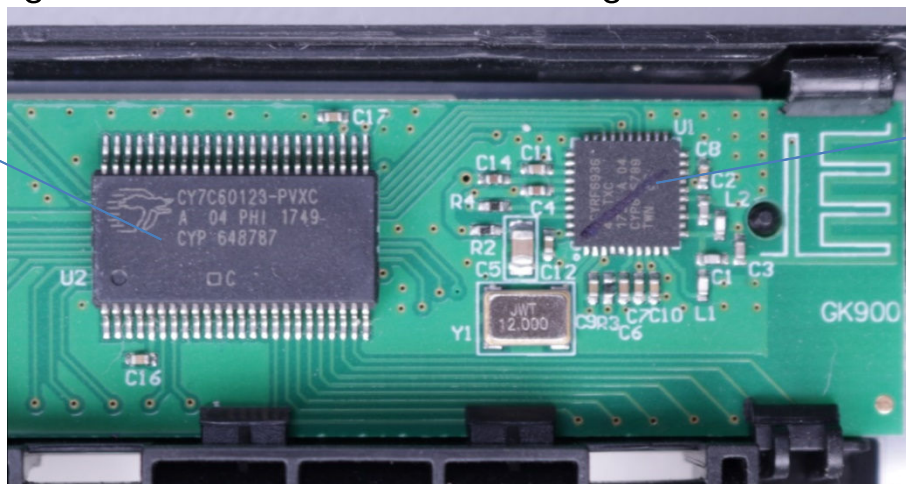
- The data of a key release packet (11 NULL bytes) are the actual keystream block, as $x \oplus 0 = x$ (exclusive or)

⇒ *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

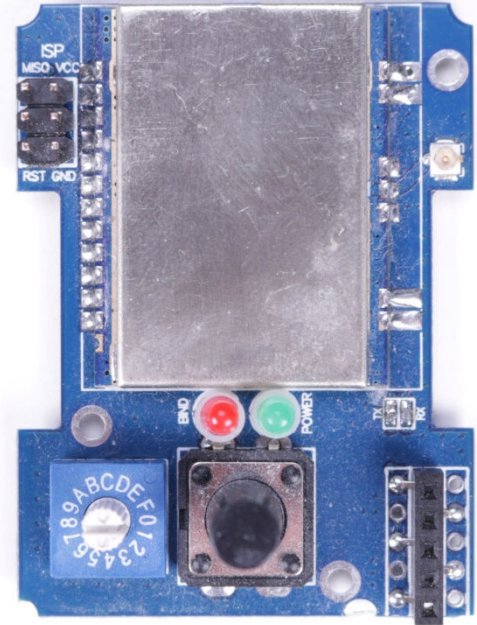
CY7C60123-
PVXC



CYRF6936

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 PRO™ LP/LPstar Technical Reference Manual)
```

```
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\x9E\x82\xDC\x3C",  
    "\xB9\x8E\x19\x74\x6F\x65\x18\x74",  
    "\xDF\xB1\xC0\x49\x62\xDF\xC1\x49",  
    "\x97\xE5\x14\x72\x7F\x1A\x14\x72"  
};
```

```
// key data for Fujitsu wireless keyboard LX901
```

```
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



The Wireless Keyboard Set LX390 is an excellent desktop solution for users with ambition. This durable keyboard set is equipped with 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.

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



The Wireless Keyboard Set LX390 is an excellent desktop solution for users with ambition. This durable keyboard set is equipped with 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.

New data sheet

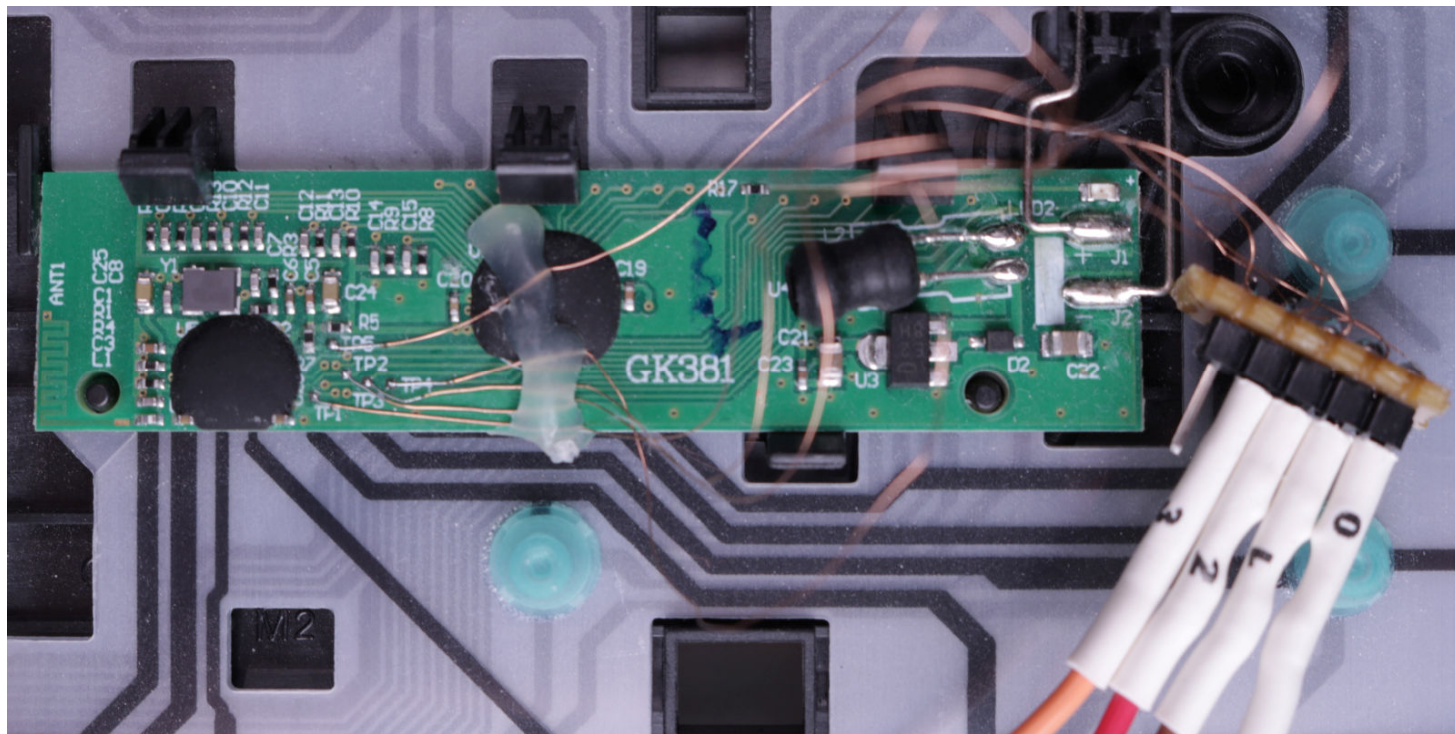
(2019/03/25)

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

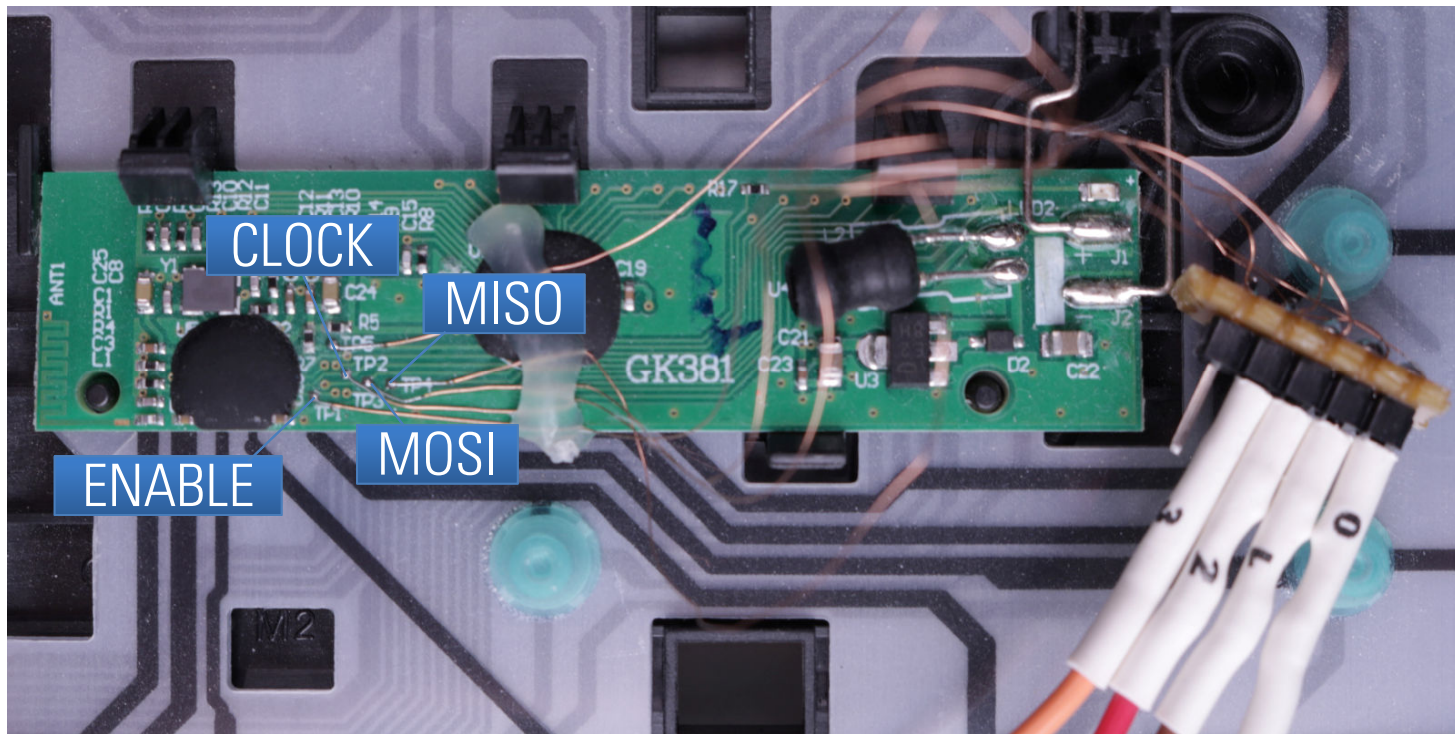


Yet Another “Secure” Keyboard



PCB front of Fujitsu Wireless Keyboard LX390

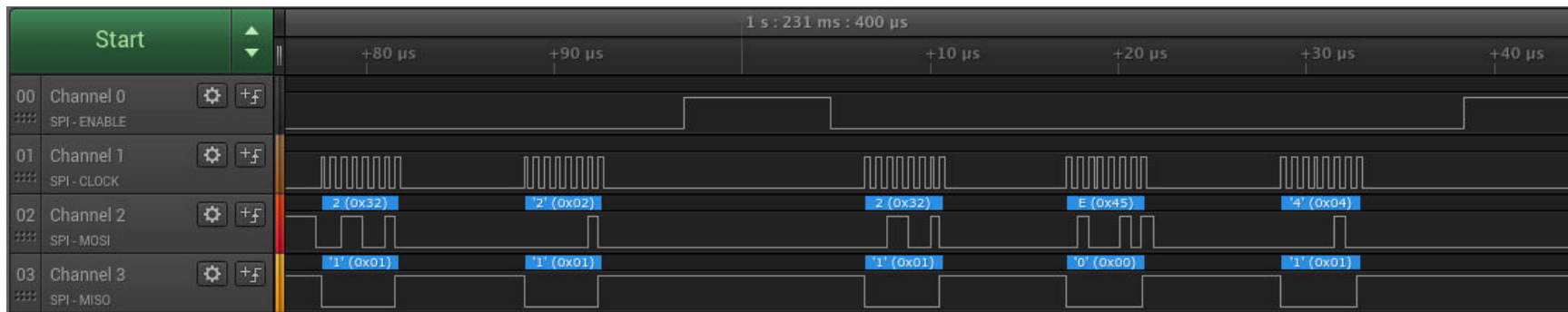
Yet Another “Secure” Keyboard



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



Yet Another “Secure” Keyboard

- Example: LT8900 packet format used by Fujitsu LX390 (keypress “a”)

010101010011101101011011010100111011110101000011110110111010010000101110111100011101011101100001011

Offset (in bits)	Size (in bits)	Description	Value	Comment
0	8	Preamble	01010101 (0x55)	10101010 (0xAA) or 01010101 (0x55)
8	48	Sync word	001110110101101101010011101111010100001111011011	6 byte sync word for addressing
56	4	Trailer	1010	4 bit trailer, 1010 (0xA) or 0101 (0x5)
60	variable	Payload	010000101110111100011101	payload bytes, 1 st byte is payload length, scrambled (data whitening)
variable	16	Checksum (CRC-16)	0111011000001011	CRC-16 with device-specific 1-byte init value, scrambled (data whitening)

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”

Byte (OTA)	Bits (OTA)	Reversed Bits	Reversed Byte	Plain Text Byte	Key Byte	The Math
0x42	01000010	01000010	0x42	0x02	0x40	$0x42 \wedge 0x40 = 0x02$
0xEF	11101111	11110111	0xF7	0x45	0xB2	$0xF7 \wedge 0xB2 = 0x45$
0x1D	00011101	10111000	0xB8	0x04	0xBC	$0xB8 \wedge 0xBC = 0x04$
0x76	01110110	01101110	0x6E	0xAD	0xC3	$0x6E \wedge 0xC3 = 0xAD$
0x0B	00001011	11010000	0xD0	0xCF	0x1F	$0xD0 \wedge 0x1F = 0xCF$
...

Yet Another “Secure” Keyboard

- 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

7:0	CRC_INITIAL_DATA	R/W	Initialization constant for CRC calculation.	00H
-----	------------------	-----	--	-----

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*

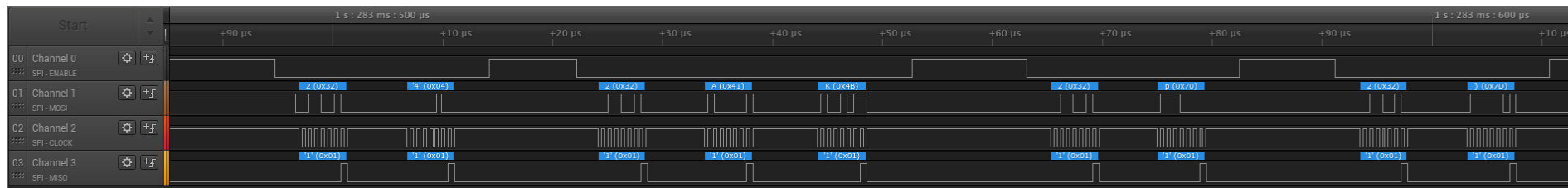
⇒ *Replay Attacks*

⇒ *Keystroke Sniffing Attacks*

⇒ *Keystroke Injection Attacks*

Open Challenge: Kensington Presenter

- SPI communication between microcontroller and transceiver indicates that an **LT8900**-based RF IC is used
- However, the used **data scrambling algorithm** is still unknown
- Using the same method as with the Fujitsu LX390 did not work
- Experiments with PL1167 RF ICs (claimed to be compatible with LT8900) using the extracted RF IC configuration did not work, either

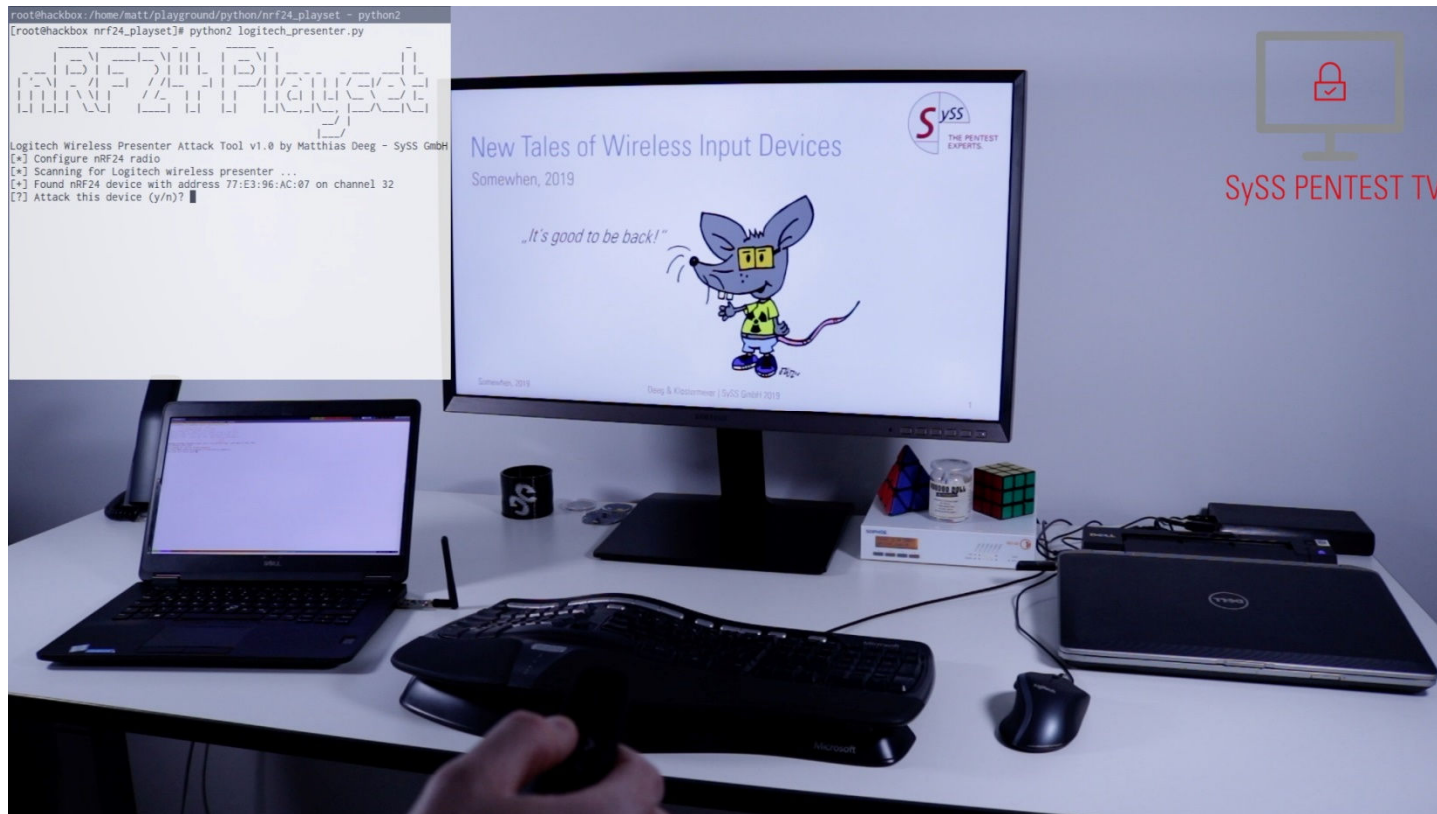


(Live) Demo Time

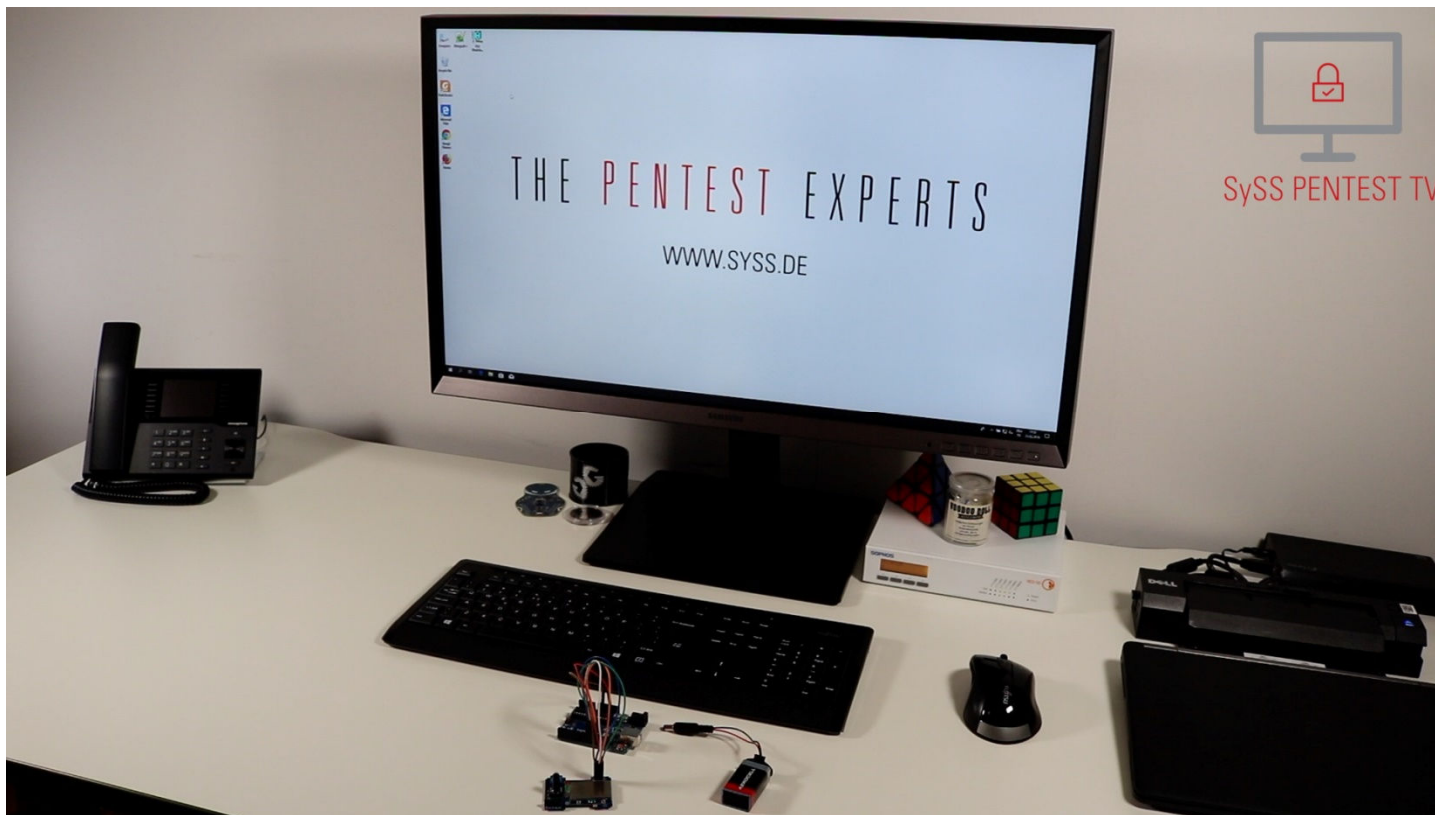
1. Old news are so exciting: Attacking wireless presenters
2. Attacking yet another AES-encrypted wireless desktop set, but this time differently
3. From wiretapping to keystroke sniffing attack
4. Exploiting Bluetooth Trust Relationships



(Live) Demo: Wireless Presenter



(Live) Demo: AES-encrypted Keyboard



$\frac{1}{\sqrt{2}} \left(\begin{array}{c} |0\rangle \\ |1\rangle \end{array} \right) = \frac{1}{\sqrt{2}} \left(\begin{array}{c} 1 \\ 1 \end{array} \right)$

Based on different tools by Marc Newlin

November 28, 2019

Demo: Exploiting Bluetooth Trust Relationships

```
sudo tmux attach -t kbdemu

bluetoothd[6554]: src/adaptec.c:settings_changed() Changed settings: 0x00000002
bluetoothd[6554]: src/agent.c:agent_ref() 0x5621d119c0: ref=1
bluetoothd[6554]: src/agent.c:register_agent() agent :1.123
bluetoothd[6554]: src/agent.c:add_default_agent() Default agent set to :1.123 /test/agent
bluetoothd[6554]: src/adaptec.c:set_mode() sending set mode command for index 0
bluetoothd[6554]: src/adaptec.c:property_set_mode() sending Set Discoverable command for index 0
bluetoothd[6554]: src/adaptec.c:property_set_mode_complete() Success (0x00)
bluetoothd[6554]: src/adaptec.c:new_settings_callback() Settings: 0x000000a0
bluetoothd[6554]: src/adaptec.c:settings_changed() Changed settings: 0x00000008
bluetoothd[6554]: src/profile.c:register_profile() sender :1.122
bluetoothd[6554]: src/profile.c:create_ext() Created ":1.122/bluez/syssh/btkbd_profile/00001124-0000-1000-8000-00005f9b34fb"
bluetoothd[6554]: src/profile.c:ext_adapter_probe() ":1.122/bluez/syssh/btkbd_profile/00001124-0000-1000-8000-00005f9b34fb" probed
bluetoothd[6554]: src/adaptec.c:adapter_service_add() /org/bluez/hci0
bluetoothd[6554]: src/sdp-service.c:add_record_to_server() Adding record with handle 0x10001
bluetoothd[6554]: src/sdp-service.c:add_record_to_server() Record pattern UUID 00000011-0000-1000-8000-00005f9b34fb
bluetoothd[6554]: src/sdp-service.c:add_record_to_server() Record pattern UUID 00000100-0000-1000-8000-00005f9b34fb
bluetoothd[6554]: src/sdp-service.c:add_record_to_server() Record pattern UUID 000001002-0000-1000-8000-00005f9b34fb
bluetoothd[6554]: src/sdp-service.c:add_record_to_server() Record pattern UUID 00001124-0000-1000-8000-00005f9b34fb
bluetoothd[6554]: src/adaptec.c:adapter_service_insert() /org/bluez/hci0
bluetoothd[6554]: src/adaptec.c:add_uuid() sending add uuid command for index 0
bluetoothd[6554]: src/adaptec.c:connected_callback() hci0 device AC:22:0B:E4:D6:F5 connected eir_len 9

[root@hackbox bluetooth-keyboard-emulator]# cd $C_PATH/keyboard/ && sleep 5 && sudo python3 keyboard_client.py
[*] Initialize keyboard
[*] Initialize D-Bus keyboard client
[*] Start event loop ...
[161, 1, 4, 0, 0, 0, 0, 0, 0, 0, 0]
[161, 1, 4, 0, 41, 0, 0, 0, 0, 0, 0]
[161, 1, 4, 0, 0, 0, 0, 0, 0, 0, 0]
[161, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0]
^C[161, 1, 0, 0, 70, 0, 0, 0, 0, 0, 0]
[161, 1, 0, 0, 70, 0, 0, 0, 0, 0, 0]
[161, 1, 0, 0, 70, 0, 0, 0, 0, 0, 0]

[root@hackbox bluetooth-keyboard-emulator]# cd $C_PATH/server && sudo python3 keyboard_server.py
[*] Initialize D-Bus Bluetooth keyboard service
[*] Read configuration file
[*] Initialize Bluetooth device
[*] Configuring emulated Bluetooth keyboard
[*] Spoof device hci0 address F4:0E:11:76:71:AD via btmgmt
[*] Set Bluetooth address: F4:0E:11:76:71:AD
[*] Set device class
[*] Set device name: SE-MJ553BT
[*] Turn on discoverable mode
[*] Configuring BlueZ Profile
[*] Reading service record
[*] Profile registered
[*] Connecting to ac:22:0b:e4:d6:f5

[root@hackbox bluetooth-keyboard-emulator]# cd $C_PATH && sudo /usr/bin/bluetoothctl
Agent registered
[CHG] Controller F4:0E:11:76:71:AD Powered: yes
[CHG] Controller F4:0E:11:76:71:AD Class: 0x000000540
[CHG] Controller F4:0E:11:76:71:AD Alias: SE-MJ553BT
[CHG] Controller F4:0E:11:76:71:AD Discoverable: yes
[CHG] Controller F4:0E:11:76:71:AD UUIDs: 00001801-0000-1000-8000-00005f9b34fb
[CHG] Controller F4:0E:11:76:71:AD UUIDs: 00001124-0000-1000-8000-00005f9b34fb
[CHG] Controller F4:0E:11:76:71:AD UUIDs: 00001200-0000-1000-8000-00005f9b34fb
[CHG] Controller F4:0E:11:76:71:AD UUIDs: 00001800-0000-1000-8000-00005f9b34fb
[CHG] Device AC:22:0B:E4:D6:F5 Connected: yes
[Nexus 7]#

[kbdemu] 0:os+
"root@hackbox: /home/ma" 15:38 15-Jun-18
```

Some Anecdotes

1. Product rebranding
2. Fake or real?

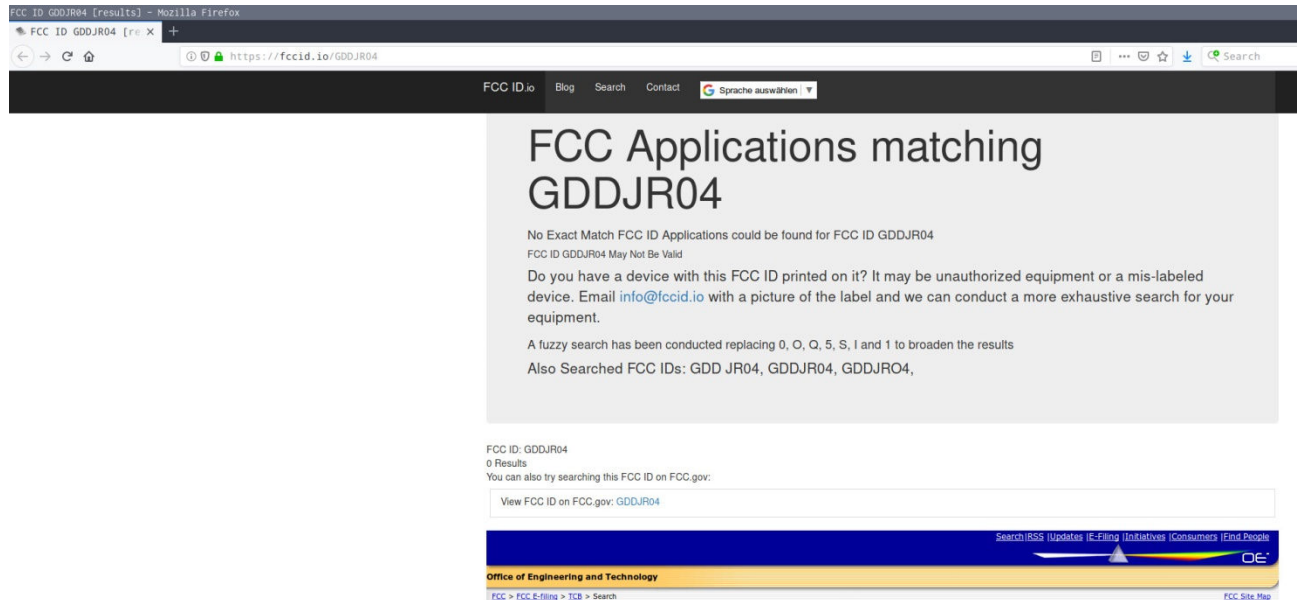
Some Anecdotes: Product Rebranding

- 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



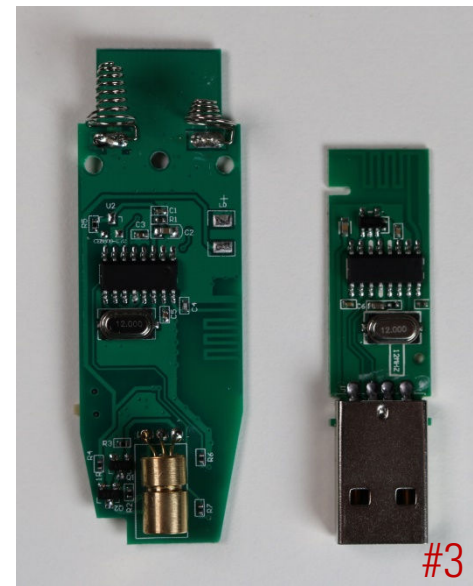
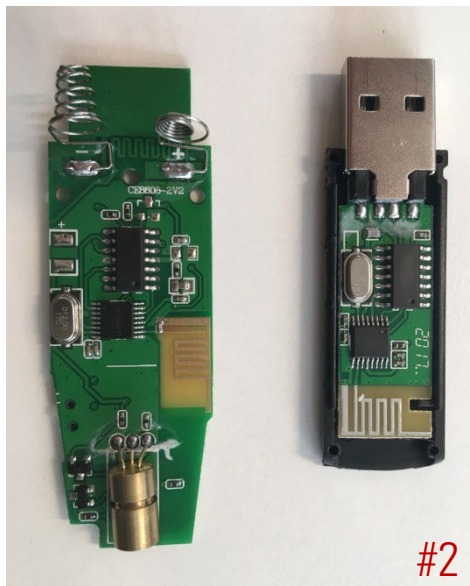
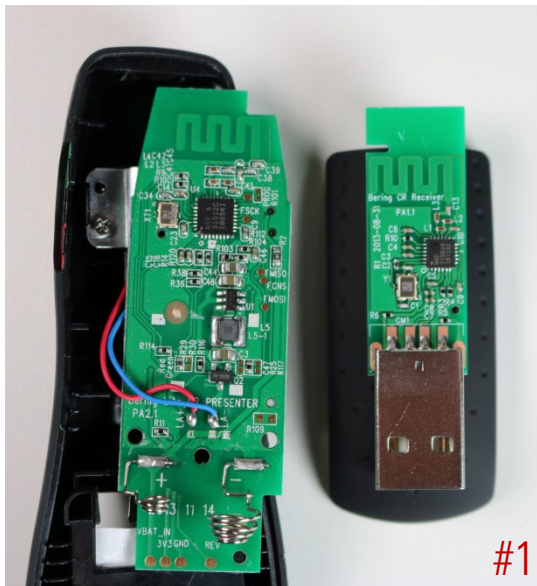
Some Anecdotes: Product Rebranding

- 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: 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

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

- ✓ 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]

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

Conclusion

Updated research results concerning wireless desktop sets (2019)

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

✓ security issue found

X security issue not found

? security issue may exist (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

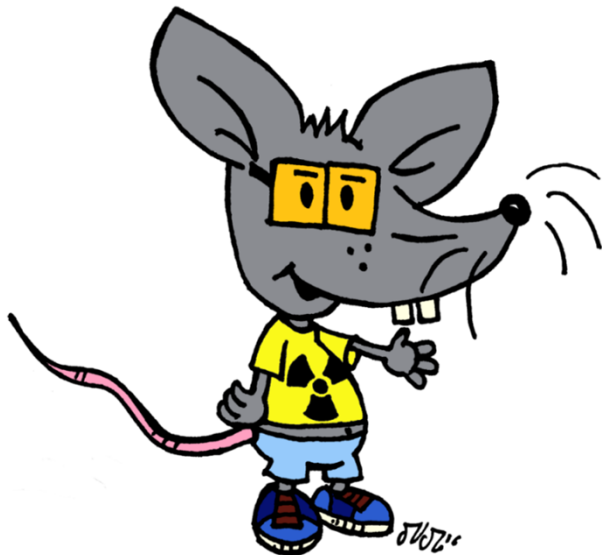
- Choose your wireless input devices wisely, e.g. wireless presenter
- Do not use wireless desktop sets with known security vulnerabilities in environments with higher security demands
- Consider Bluetooth wireless input devices more secure than non-Bluetooth keyboards using proprietary 2.4 GHz radio 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



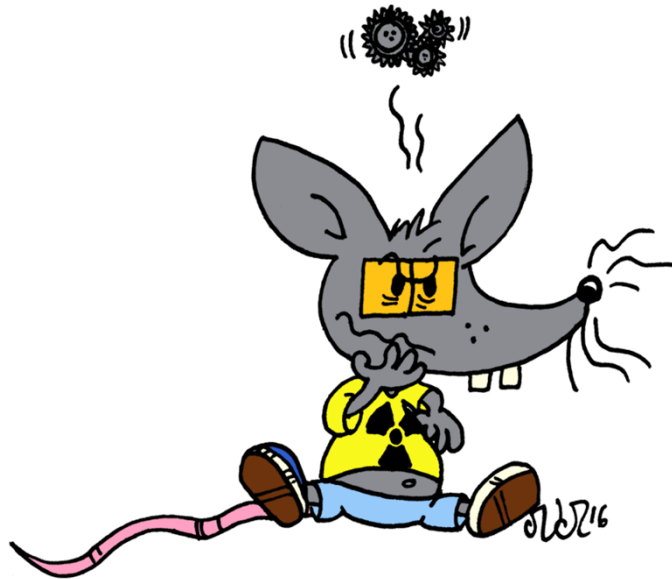
Example: Inateck BCST-60

- 2.4 GHz communication using BK2535 transceiver
- More complicated communication protocol
- Unencrypted and unauthenticated data communication
⇒ *Keystroke injection attacks*
- See security advisory SYSS-2019-027 [37]

Thank you very much ...

... for your attention.

Do you have any questions?



E-mail: matthias.deeg@syss.de

Twitter: [@matthiasdeeg](https://twitter.com/matthiasdeeg)

E-mail: gerhard.klostermeier@syss.de

Twitter: [@iiiiikarus](https://twitter.com/iiiiikarus)

References

1. Crazyradio PA, <https://www.bitcraze.io/crazyradio-pa/>
2. KeyKeriki v2.0 – 2.4 GHz, Max Moser and Thorsten Schröder, http://www.remote-exploit.org/articles/keykeriki_v2_0_8211_2_4ghz/, 2010
3. Owned Live on Stage – Hacking Wireless Presenters, Niels Teusink, Fox-IT, <http://conference.hitb.org/hitbsecconf2010ams/materials/D1T1%20-%20Niels%20Teusink%20-%20Owned%20Live%20on%20Stage.pdf>, 2010
4. Promiscuity is the nRF24L01+'s Duty, Travis Goodspeed, <http://travisgoodspeed.blogspot.de/2011/02/promiscuity-is-nrf24l01s-duty.html>, 2011
5. KeySweeper, Samy Kamkar, <http://samy.pl/key sweeper>, 2015
6. MouseJack, Bastille Networks Internet Security, <https://www.mousejack.com/>, 2016
7. nrf-research-firmware, Bastille Networks Internet Security, <https://github.com/BastilleResearch/nrf-research-firmware>, 2016
8. KeyJack, Bastille Networks Internet Security, <https://www.bastille.net/research/vulnerabilities/keyjack/keyjack-intro/>, 2016
9. KeySniffer, Bastille Networks Internet Security, <https://www.bastille.net/research/vulnerabilities/keysniffer-intro>, 2016
10. Teils kritische Schwachstellen in AES-verschlüsselten, funkbasierten Maus-Tastatur-Kombinationen, SySS GmbH, <https://www.syss.de/pentest-blog/2016/teils-kritische-schwachstellen-in-aes-verschluesselten-funkbasierten-maus-tastatur-kombinationen/>, 2016

References

11. *Of Mice and Keyboards: On the Security of Modern Wireless Desktop Sets*, Matthias Deeg and Gerhard Klostermeier, *Hack.lu*, https://www.youtube.com/watch?v=Ja_VgUMz43Q, 2016
12. *Radioactive Mouse States the Obvious – Proof-of-Concept Video*, SySS GmbH, <https://www.youtube.com/watch?v=PkR8EODee44>, 2016
13. *SySS Security Advisory SYSS-2016-074*, Matthias Deeg, <https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2016-074.txt>, 2016
14. *SySS Security Advisory SYSS-2016-075*, Matthias Deeg, <https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2016-075.txt>, 2016
15. *Of Mice and Keyboards: On the Security of Modern Wireless Desktop Sets*, Matthias Deeg and Gerhard Klostermeier, https://www.syss.de/fileadmin/dokumente/Publikationen/2017/2017_06_01_of-mice-and-keyboards_paper.pdf, 2017
16. *nrf24-playset*, SySS GmbH, <https://github.com/SySS-Research/nrf24-playset>, 2017
17. *Case Study: Security of Modern Bluetooth Keyboards*, Gerhard Klostermeier and Matthias Deeg, https://www.syss.de/fileadmin/dokumente/Publikationen/2018/Security_of_Modern_Bluetooth_Keyboards.pdf, 2018
18. *Rikki Don't Lose that Bluetooth Device*, Matthias Deeg and Gerhard Klostermeier, https://www.syss.de/fileadmin/dokumente/Publikationen/2018/Rikki_Dont_Lose_That_Bluetooth_Device.pdf, 2018

References

19. *Bluetooth Keyboard Emulator*, SySS GmbH, <https://github.com/SySS-Research/bluetooth-keyboard-emulator>, 2018
20. *SySS Security Advisory SYSS-2018-033*, Matthias Deeg, <https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2018-033.txt>, 2018
21. *CY4672 PRoC LP Reference Design Kit*, Cypress Semiconductor, <http://www.cypress.com/documentation/reference-designs/cy4672-proc-lp-reference-design-kit>
22. *Fujitsu LX901 Keystroke Injection Attack – Proof-of-Concept Video*, SySS GmbH, <https://www.youtube.com/watch?v=87jZKTTBdtc>, 2019
23. *Multiprotocol TX Module*, Pascal Langer, <https://github.com/pascallanger/DIY-Multiprotocol-TX-Module>, 2019
24. *Presentation Clickers*, Marc Newlin, <https://github.com/marcnewlin/presentation-clickers>, 2019
25. *Logitech R400 Keystroke Injection Attack – Proof-of-Concept Video*, SySS GmbH, https://www.youtube.com/watch?v=p32o_jRRL2w, 2019
26. *SySS Security Advisory SYSS-2019-007*, Matthias Deeg, <https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2019-007.txt>, 2019
27. *SySS Security Advisory SYSS-2019-008*, Matthias Deeg, <https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2019-008.txt>, 2019

References

- 28. SySS Security Advisory SYSS-2019-015, Matthias Deeg,
<https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2019-015.txt>, 2019
- 29. KeyJector, SySS GmbH, <https://github.com/SySS-Research/keyjector>, 2019
- 30. Logitech Update zu den Presentern R400, R700 und R800, <https://support.logi.com/hc/en-001/community/posts/360033353213-Logitech-Update-zu-den-Presentern-R400-R700-und-R800>, 2019
- 31. LOGITacker, Marcus Mengs, <https://github.com/mame82/LOGITacker>, 2019
- 32. munifying, Marcus Mengs, <https://github.com/mame82/munifying>, 2019
- 33. SySS Security Advisory SYSS-2019-009, Matthias Deeg,
<https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2019-009.txt>, 2019
- 34. SySS Security Advisory SYSS-2019-010, Matthias Deeg,
<https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2019-010.txt>, 2019
- 35. SySS Security Advisory SYSS-2019-011, Matthias Deeg,
<https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2019-011.txt>, 2019

References

- 36. *Exploiting Bluetooth Trust Relationships – Proof-of-Concept Video*, SySS GmbH,
<https://www.youtube.com/watch?v=Haaw3iWmzPM>, 2019
- 37. *SySS Security Advisory SYSS-2019-027*, Matthias Deeg,
<https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2019-027.txt>, 2019

THE PENTEST EXPERTS

WWW.SYSS.DE