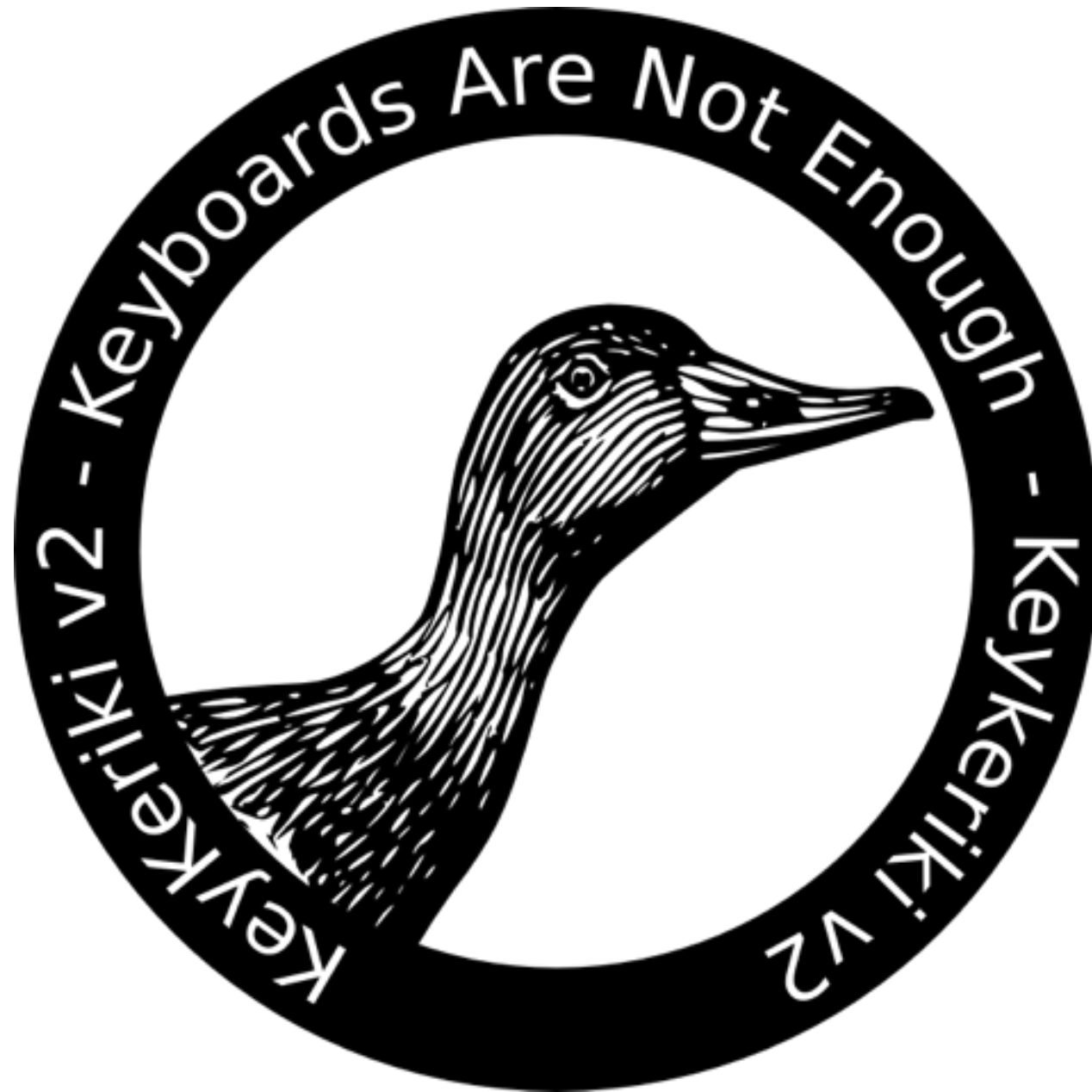


[kɪˌkɛrɪˈkiː]



Practical Exploitation of Modern Wireless Devices



Thorsten Schroeder
ths@dreamlab.net



Max Moser
max.moser@dreamlab.net

Warning!

- Verifying the security of someone else's data transmission or injecting stuff without permission could send you (or the other guy) to jail in most countries :-)



What is this talk all about?

- Brief History
- Nordic Semiconductor Radio
- Practical Exploitation of...
- ... other Mobile Devices
- Demo & Release – Remote Code Execution

History

Evolution

- ❑ Infrared (Not part of this talk)
- ❑ 27 MHz Radio
- ❑ Bluetooth 2.4 GHz Radio
- ❑ Proprietary 2.4 GHz Radio



What is it?

- ❑ 27 MHz frequency band (Citizen Band)
- ❑ Miller encoded radio signal
- ❑ Proprietary protocols
- ❑ Approx. 90 cm guaranteed max. working distance
- ❑ Low cost
- ❑ Battery demanding

What is wrong?

- ❑ Pure one way communication
- ❑ “Encryption” absent or only optionally available
- ❑ No protection against replay attacks
- ❑ No (Message) Authentication

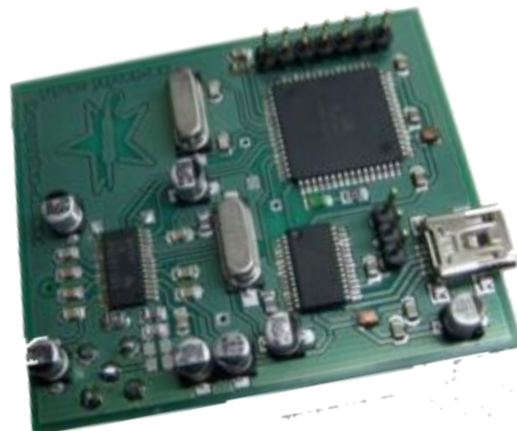
Logitech Packets (27MHz)

a(down) Keyb 1	000000100	10001001001	0000011110	1	00000
a(down) Keyb 2	000000100	100111001111	0000011110	1	0001000
a(up) Keyb 1	000000100	10001001001	0000011110	0	00000
a(up) Keyb 2	000000100	100111001111	0000011110	0	0001000
b(down) Keyb 1	000000100	10001001001	0000000101	1	0101
b(down) Keyb 2	000000100	100111001111	0000000101	1	0100000
b(up) Keyb 1	000000100	10001001001	0000000101	0	0101
b(up) Keyb 2	000000100	100111001111	0000000101	0	0100000

?	Keyboard ID	Keystroke	State	?
---	-------------	-----------	-------	---

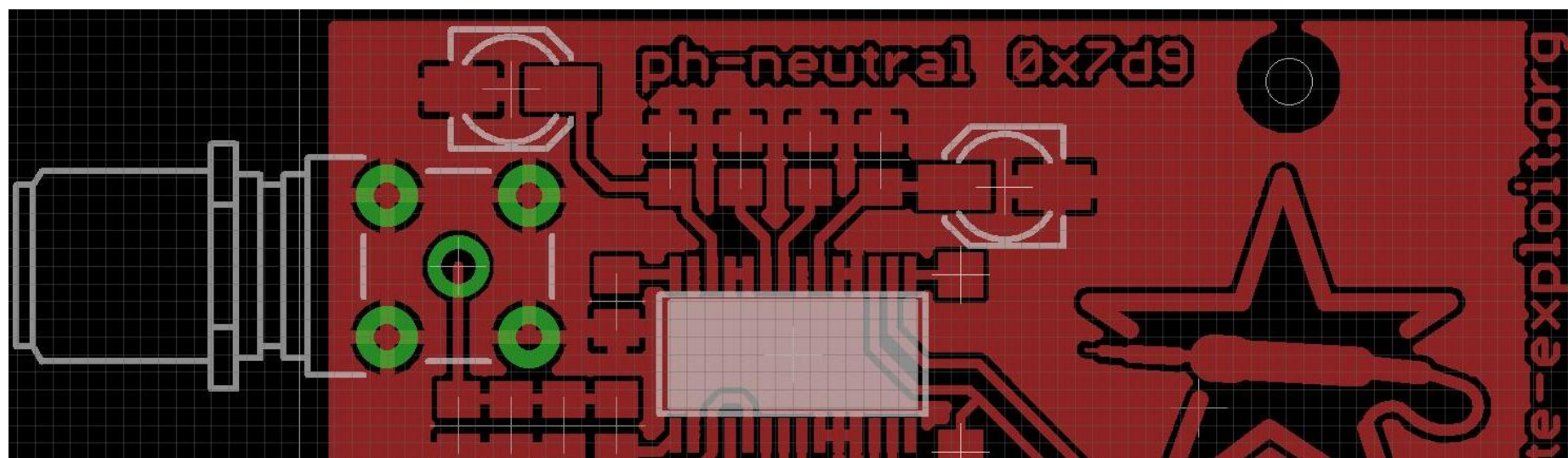
Tools Anyone?

- ❑ Radio transceiver + Taperecorder == replay
- ❑ Two identical receiver + Sync == FAIL
- ❑ Sniffing => Keykeriki V1



Keykeriki V1

- ❑ Released in May 2009 at PH-Neutral
- ❑ Capable of sniffing Microsoft, Siemens-Fujitsu, Logitech, ...
- ❑ SDCard for persistent Storage of data
- ❑ On-the-Fly Crypto Analysis /Cracking



Attack Limitation

- ❑ Full wavelength of 27 MHz is about 11 meters → huge antennas
- ❑ Error correction not part of the design & not implemented. Therefore limited range
- ❑ Injection is limited to replay because some minor bits are still unknown within the packet format

Bluetooth Keyboards

What is it?

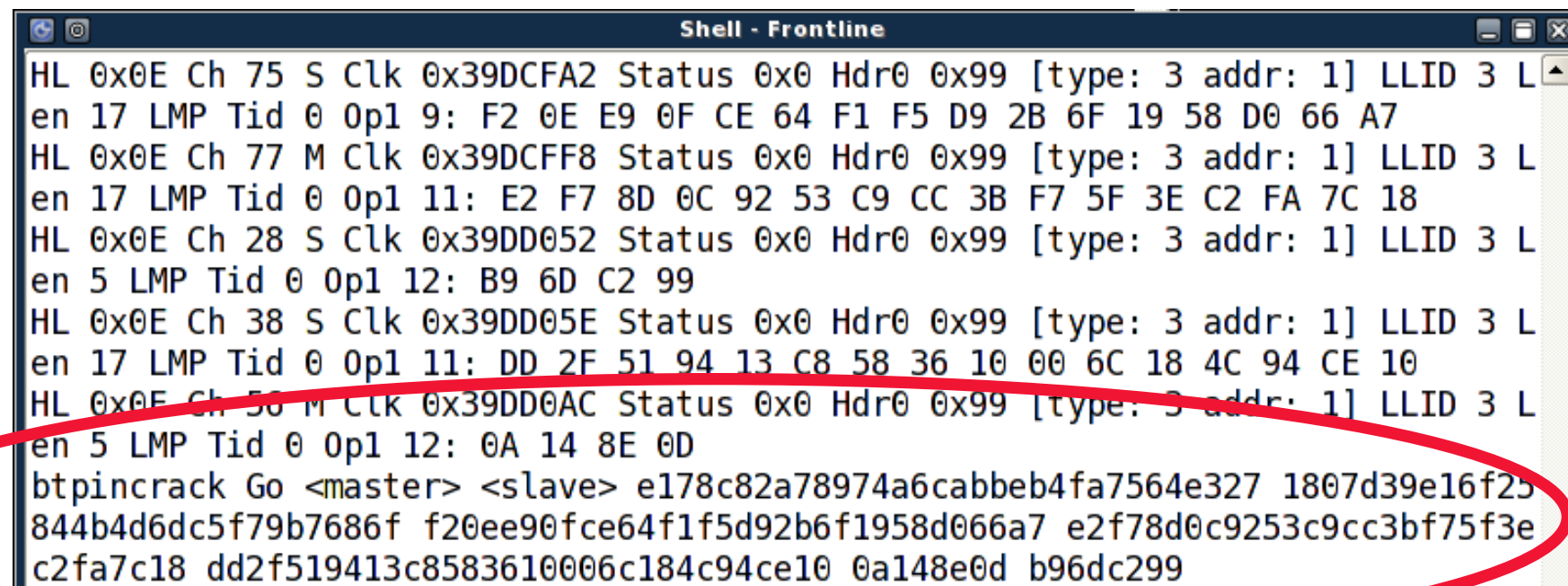
- ❑ Popular transmission technique in mobile area
- ❑ Security features are implemented within firmware and not directly accessible from operating system
- ❑ Pairing process
- ❑ Encryption / Key exchange
- ❑ Fast frequency hopping makes sniffing more difficult

What is wrong?

- ❑ Bluetooth transmission modules are expensive ⇒
Expensive keyboards
- ❑ During pairing process all pre-requirements for a successful PIN-cracking can be sniffed - “Simple Pairing” should fix this
- ❑ Buggy implementations (Complexity)
- ❑ Overdesigned

Tools Anyone?

- ❑ GnuRadio
- ❑ Frontline FTE4BS™
- ❑ Flashing old Frontline FW on CSR Bluecore 3 dongles



```

Shell - Frontline
HL 0x0E Ch 75 S Clk 0x39DCFA2 Status 0x0 Hdr0 0x99 [type: 3 addr: 1] LLID 3 L
en 17 LMP Tid 0 Op1 9: F2 0E E9 0F CE 64 F1 F5 D9 2B 6F 19 58 D0 66 A7
HL 0x0E Ch 77 M Clk 0x39DCFF8 Status 0x0 Hdr0 0x99 [type: 3 addr: 1] LLID 3 L
en 17 LMP Tid 0 Op1 11: E2 F7 8D 0C 92 53 C9 CC 3B F7 5F 3E C2 FA 7C 18
HL 0x0E Ch 28 S Clk 0x39DD052 Status 0x0 Hdr0 0x99 [type: 3 addr: 1] LLID 3 L
en 5 LMP Tid 0 Op1 12: B9 6D C2 99
HL 0x0E Ch 38 S Clk 0x39DD05E Status 0x0 Hdr0 0x99 [type: 3 addr: 1] LLID 3 L
en 17 LMP Tid 0 Op1 11: DD 2F 51 94 13 C8 58 36 10 00 6C 18 4C 94 CE 10
HL 0x0E Ch 50 M Clk 0x39DD0AC Status 0x0 Hdr0 0x99 [type: 3 addr: 1] LLID 3 L
en 5 LMP Tid 0 Op1 12: 0A 14 8E 0D
btpincrack Go <master> <slave> e178c82a78974a6cabbab4fa7564e327 1807d39e16f25
844b4d6dc5f79b7686f f20ee90fce64f1f5d92b6f1958d066a7 e2f78d0c9253c9cc3bf75f3e
c2fa7c18 dd2f519413c8583610006c184c94ce10 0a148e0d b96dc299
  
```


Attack Limitation

- ❑ Sniffing is possible but kind of “unstable”
- ❑ All pre-requirements for a successful PIN-cracking can only be sniffed during pairing
- ❑ Complex documentation
- ❑ GnuRadio or FTE4BS™ are expensive
- ❑ Rarely used

Proprietary 2.4 GHz based Keyboards

What is it?

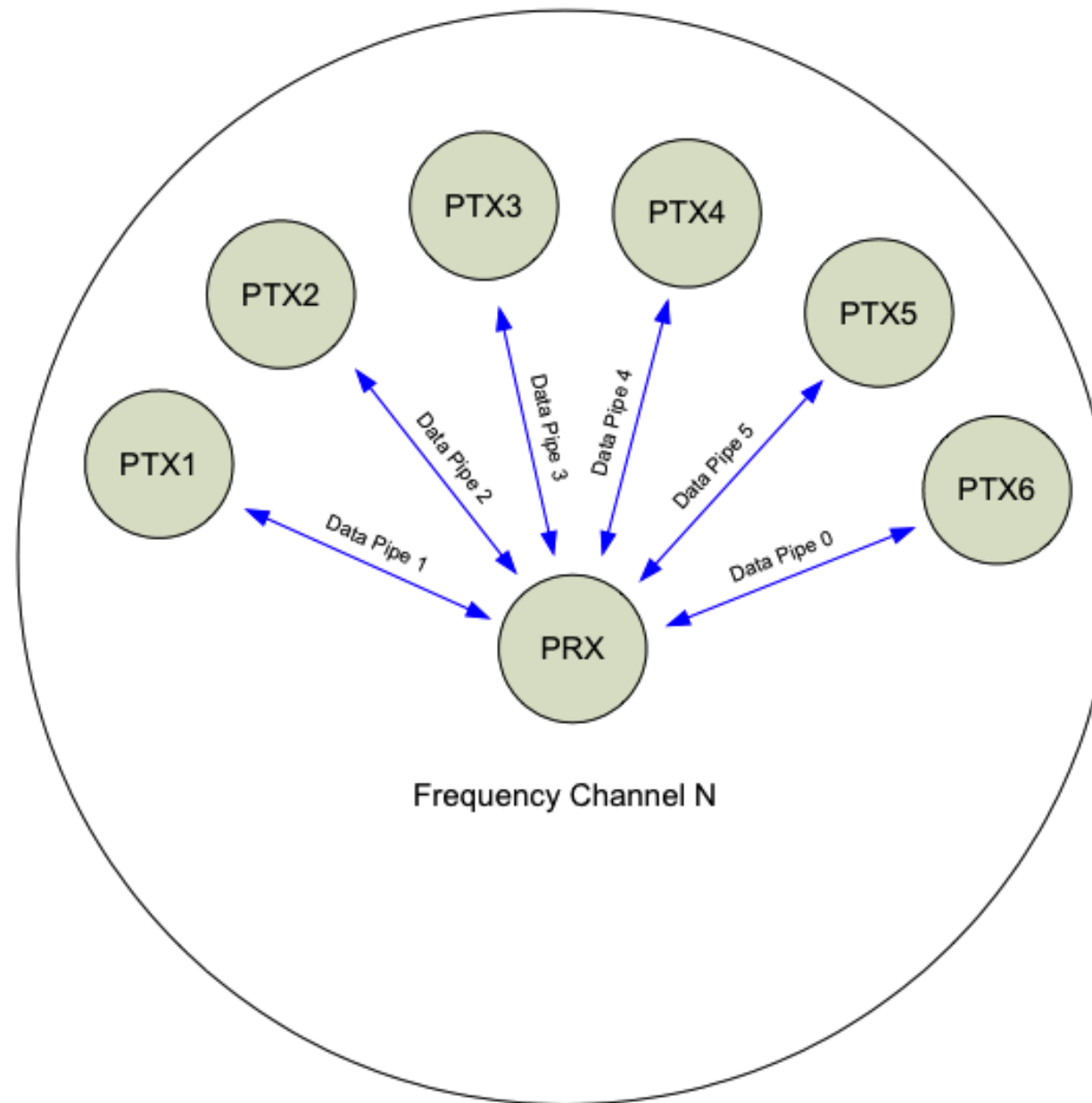
- ❑ Not Bluetooth, not Zigbee, not 802.11xyz
- ❑ Most devices operating with 1 Mbit/sec some at rates up to 2 Mbit/sec
- ❑ Nordic Semiconductor NRF24XXX family widely used
- ❑ Compact form factor (e.g. 2.4 GHz antenna, small IC devices, ...)
- ❑ Faster, less TX time → less power consumption

Vendor Specific Responsibilities

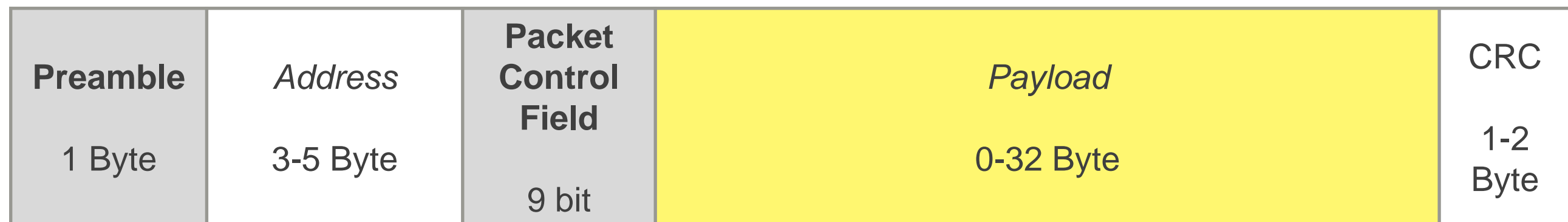
- Any radio based keyboard vendor is responsible for:
 - ▣ Computer System Protection
 - ▣ Authentication
 - ▣ Data Protection & Integrity
- USB receiver is single line of defense (in case of keyboards for example)

Proprietary 2.4 GHz based Devices

Nordic Semi NRF24xxx



Enhanced Shockburst™



- ❑ How does it work?
- ❑ Nordic Multiceiver concept
- ❑ Multiple RX data pipes
- ❑ One channel at a time
- ❑ Dynamic Payload Len

Packet Control Field	
6 bit	Payload Length
2 bit	Sequence / Packet ID
1 bit	Disable Auto ACK

Raw Shockburst Processing

- Difficulties
 - ▣ Speed (2 Mbit/s is fast!)
 - ▣ Auto-Ack and Retransmission Features vs. 1 Mbit solutions
 - ▣ Direct Baseband Signal Access / Interface

How NRF24xxx works

- ❑ Detect valid Enhanced Shockburst Frame:
 - ❑ 8 bit preamble (0xAA or 0x55)
 - ❑ 3-5 byte device address
 - ❑ CRC (if enabled) must match
- ❑ Otherwise it is considered being noise

NRF24L01 + Interface

- ❑ Config and Data Transmission via SPI (Serial Peripheral Interface) using FIFO buffers
- ❑ There is no way to access radio layer directly
- ❑ Target system's device address must be known to read/write data from/to the remote device

Nordic Semi NRF24 Direct Mode

- ❑ Direct Mode allows Software Defined Radio
- ❑ Additional pin on transceiver module which toggles all the time, allowing an MCU doing the raw data processing (SDR)
- ❑ Only available as non-„Enhanced“ Shockburst with speeds $< 1 \text{ mbit/s}$

Radio Layer

□ Raw (valid) Data



Setting up a sniffer

- ❑ Capture raw Enhanced Shockburst Traffic at 2mbit/sec
- ❑ Detect Preamble
- ❑ Get device addresses
- ❑ Decide wether it is a valid device address/Enhanced Shockburst Frame or not
- ❑ Configure NRF24L01 + device via SPI using that address
- ❑ But... how to capture the raw data...?

Alternative 2.4GHz transceiver modules

- We have found a chip vendor in Taiwan who produces a 2.4GHz transceiver with a „Direct Mode“ pin
- Documentation was... Hmm... quite OK

17.1 Direct mode



Direct mode 提供使用者一個 RF 通道，在 TX 端 Base band 系統將資料傳送到 RF IC 的調變，把資料傳送至接收端。RX 端採用數位解調方式，還原資料。Base band 系統需自

Data IO pin 可依使用者需要選擇：

- 1.GPIO1 或 GPIO2 pin 的 TRXD(GPIOx CTRL register 的 GPIOxS3-0=0111, TX / RX 共
- 2.GPIO1 或 GPIO2pin 的 TXD/RXD(GPIOx CTRL register 的 GPIOxS3-0=1000[RXD] or
- 3.SDIO pin(Mode CTRL register 的 DDPC=1, TX / RX 共用雙向 pin)

Challenges

- Remote: NRF Module (TX) with 30ppm crystal
- Local: Amicom A7125 (RX) with 10ppm crystal
- Asynchronous radio transmission at 2mbit/sec →
Clock drift is a real problem when building
hardware tool with SDR
 - ▣ 500 ns (nano seconds) processing time per bit
 - ▣ A 100 MHz CPU has 10 ns per clock cycle

Challenges (cont'd)

- We are looking for an unknown 5 Byte value (device address)
- We know, an 8 bit preamble is located right before the device address, and we know the value (0xAA)
- There is a well defined 9 bit Header right after the device address – the first 6 bit are known to be less than 32
- We need to match $\langle \text{preamble} \rangle \text{unknown} \langle \text{len} \leq 32 \rangle \text{unknown}$.. Within a 2mbit/s noise stream
- Many false positives, still no way to verify a valid address

500 ns

- Using a 100 MHz CPU we have 50 cycles during 500ns
- Having a 2 mbit/s timer interrupt for processing, we have an IRQ handler overhead of approx. 20 cycles.
- 30 CPU cycles left for:
 - ▣ Read current value of A7125's Direct Output pin
 - ▣ Shift new bit in LSb of a 3x32 bit hardware CPU register chain:
trash \leftarrow [reg 3] \leftarrow [reg 2] \leftarrow [reg 1] \leftarrow I/O bit input (new)
 - ▣ Match Preamble in MSB in [reg 3]

30 CPU cycles left (cont'd)

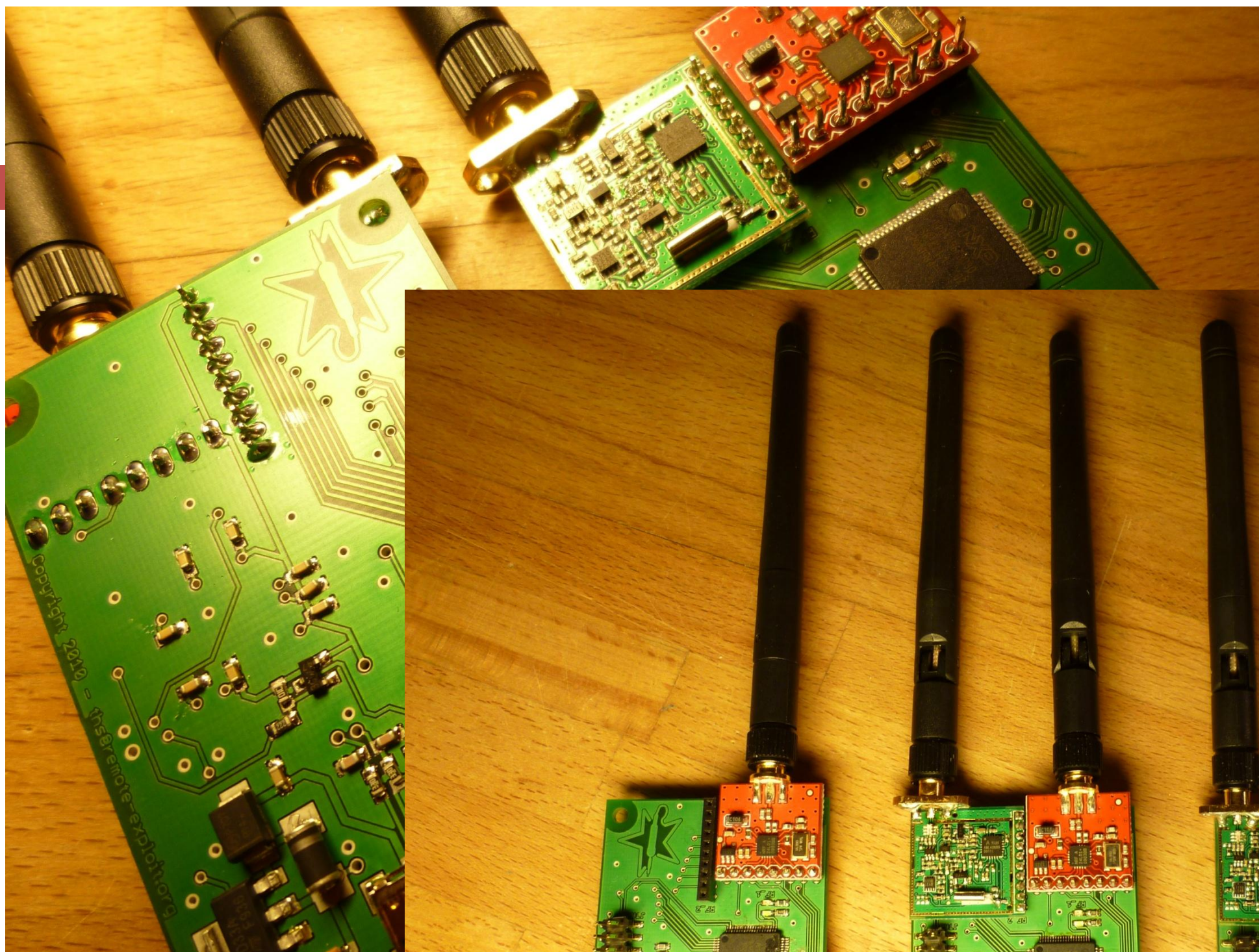
- ▣ Mask Enh. Shockburst Header length value (6-bit)
- ▣ Check wether value is 0, 8, 16 or 32 byte (most likely)
- ▣ If it matches, calculate very basic „hash“ value of address in `reg 3` and `reg 2` – then increment address match counter
- ▣ Check address match counter & decide wether address might be valid or not
- ▣ Disable timer interrupt

30 CPU cycles left (cont'd)

- ▣ Disable A7125 module
- ▣ Enable NRF24L01+ module
- ▣ Set RX/TX address
- ▣ Act like a genuine device, using the valid Enhanced Shockburst device address
- BTW: We might have used an FPGA or CPLD, but this would have been too easy ;-) *
- ▣ * In fact we are currently working on this thing

Keykeriki V2 (beta)

- We built a hardware device, based on an NXP LPC17xx ARM Cortex-M3 Microcontroller at 100 MHz with a Software Defined Radio Firmware
- We are using two different radio transceiver modules
 - ▣ Because we are lazy (SPI + FIFO is easier), less code
→ less errors
 - ▣ Because of probable legal issues
 - ▣ And of course: Using the Nordic Semi chip is consuming less power



Remember the vendor responsibilities?



Payload Analysis

- To be able to successfully TX or RX/parse packets, we need to understand how their protocol works
 - ▣ Find the checksum algorithm (necessary for TX)
 - ▣ Analyze content, find and understand cryptographic algorithms
 - ▣ Sequence IDs
 - ▣ Etc
- Capture/Replay could be helpful

- | | | | | | | | | | | | | | | | | |
|----|----|---|---|----|----|----|----|--|----|----|----|---|----|----|----|----|
| 0a | 78 | 6 | 1 | df | 88 | 4b | 0a | | c0 | C9 | 88 | 8 | 0a | c0 | cd | 57 |
| 0a | 38 | 6 | 1 | df | 88 | 8 | d2 | | | | | | | | | |
| 0a | 38 | 6 | 1 | df | 88 | 8 | d2 | | | | | | | | | |
| 0a | 38 | 6 | 1 | df | 88 | 8 | d2 | | | | | | | | | |
| 0a | 38 | 6 | 1 | df | 88 | 8 | d2 | | | | | | | | | |
| 0a | 38 | 6 | 1 | df | 88 | 8 | d2 | | | | | | | | | |
| 0a | 78 | 6 | 1 | DE | 88 | 4b | 0a | | c0 | CD | 88 | 8 | 0a | c0 | cd | 52 |
| | | | | | | | | | | | | | | | | |
| 0a | 78 | 6 | 1 | D9 | 88 | 4b | 0a | | c0 | C8 | 88 | 8 | 0a | c0 | cd | 50 |
| 0a | 38 | 6 | 1 | d9 | 88 | 8 | d4 | | | | | | | | | |
| 0a | 38 | 6 | 1 | d9 | 88 | 8 | d4 | | | | | | | | | |
| 0a | 38 | 6 | 1 | d9 | 88 | 8 | d4 | | | | | | | | | |
| 0a | 38 | 6 | 1 | d9 | 88 | 8 | d4 | | | | | | | | | |
| 0a | 38 | 6 | 1 | d9 | 88 | 8 | d4 | | | | | | | | | |
| 0a | 78 | 6 | 1 | D8 | 88 | 4b | 0a | | c0 | CD | 88 | 8 | 0a | c0 | cd | 54 |
| | | | | | | | | | | | | | | | | |
| 0a | 78 | 6 | 1 | DB | 88 | 4b | 0a | | c0 | E1 | 88 | 8 | 0a | c0 | cd | 7B |
| 0a | 38 | 6 | 1 | dB | 88 | 8 | d6 | | | | | | | | | |
| | | 6 | 1 | dB | 88 | 8 | d6 | | | | | | | | | |
| | | 6 | 1 | dB | 88 | 8 | d6 | | | | | | | | | |
| | | 6 | 1 | dB | 88 | 8 | d6 | | | | | | | | | |
| | | 6 | 1 | dB | 88 | 8 | d6 | | | | | | | | | |
| | | 6 | 1 | DA | 88 | 4b | 0a | | c0 | CD | 88 | 8 | 0a | c0 | cd | 56 |

Microsoft Payload Encryption

C	0A	78	06	01	C2	98	76	0A	C0	C8	98	35	0A	C0	CD	5B
K					CD	98	35	0A	C0	CD	98	35	0A	C0	CD	
P	0A	78	06	01	0F	00	43	00	00	05	00	00	00	00	00	
	Device type	Packet type	Model	?	Sequence ID	Flags/Meta				HID Code						Checksum

(Key-Down) Packet with device address
CD 98 35 0A C0

Microsoft Encryption & Checksum Algorithm

```
ctx->const_down = ctx->const_up = ~ctx->address[1];  
...  
cksum = ctx->const_down;  
  
for (i=0; i<4; i++) {  
    ctx->c_down[i] = ctx->p_down[i];  
    cksum ^= ctx->p_down[i];  
}  
  
for (i=4; i<15; i++) {  
    cksum ^= ctx->p_down[i];  
    ctx->c_down[i] = ctx->p_down[i] ^ ctx->secret[i % 5];  
}  
ctx->c_down[15] = cksum;
```

Microsoft Mouse

- ❑ Data (x/y) is not encrypted
- ❑ Mouse button press/idle/releases are also simply HID codes
- ❑ Mouse has Device Class ID 0x08

Limited to Keyboards?

Obviously



Logitech® Unifying receiver
Plug it. Forget it. Add to it.



Apartment Whispering?



Logitech®
Z-5450 Digital/Numériques

er Manual
ide
l'utilisateur



Election / Voting?



Tuesday 23, March 2010

NEWS

12.11.09

Nordic 2.4GHz transceivers provide wireless link for up to 15,500 audience voting touchscreen keypads in latest Ativa® platform from Fleetwood Group



Subscribe to eNews

Get info, offers, and news via email.

NEWS

22.03.10 Digifit Ecosystem for iPhone® and iPod touch® makes final three shortlist in Andrew Seybold MobileApp Challenge award at International CTIA Wireless 2010

09.03.10 Nordic nRF24AP2 8-channel ANT chip named as finalist in top US industry Awards



DREAMLAB
TECHNOLOGIES

D&R Headline News

[D&R Headline News](#) | [Most Popular](#) | [SoC News Alerts](#) | [RSS](#) | [twitter](#)

Suunto Chooses Nordic Semiconductor's 2.4GHz RF devices for the Suunto t6 Sports Instrument, the first sports instrument able to measure the effect of training

July 23, 2004 - Nordic Semiconductor ASA (OSE:NOD) today announced that Suunto uses Nordics 2.4GHz RF-devices for their new Suunto t6 wristop computer and the Peripheral Observation Devices (PODs).

Suunto t6 is an innovative personal training tool to optimize training effects and the first sports instrument ever able to measure the effect of every training session on one's physical condition. The recently launched three PODs expand Suunto t6 to a wireless network area with even more training possibilities for an athlete and fitness enthusiast.



Dragos, see the issue?



What is going through your mind, when you see terms like...

- ❑ Identification Keypad Module
- ❑ In/Out Module
- ❑ GSM Module
- ❑ Driver Identification Module
- ❑ Engine Blocking Module
- ❑ ... all interconnected within **cars**, using proprietary 2.4GHz techniques..

Security / Safety

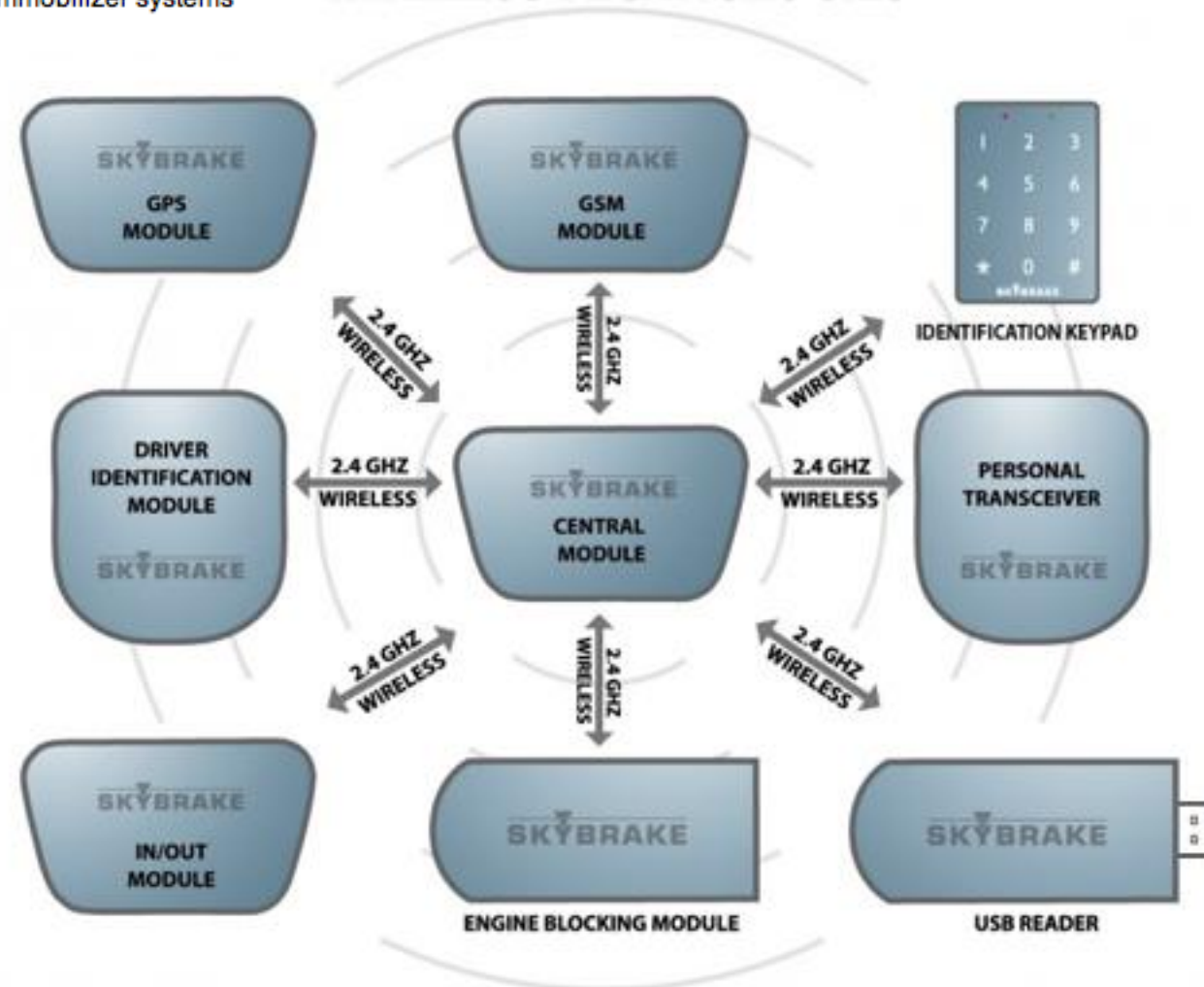
D&R Headline News

[D&R Headline News](#) | [Most Popular](#) | [SoC News Alerts](#) | [RSS](#) | [twitter](#)

Autonams LLC Chooses Nordic Semiconductor's 2.4GHz Transceiver nRF2401A for Car Immobiliser Systems "SKYBRAKE DD"

Oslo, Norway - June 30th, 2005 - Nordic Semiconductor ASA (OSE: NOD) today announced that Autonams has selected Nordic's 2.4 GHz transceiver nRF2401A for its new line of car immobilizer systems "SKYBRAKE DD".

DOUBLE DIALOGUE WIRELESS TECHNOLOGIES

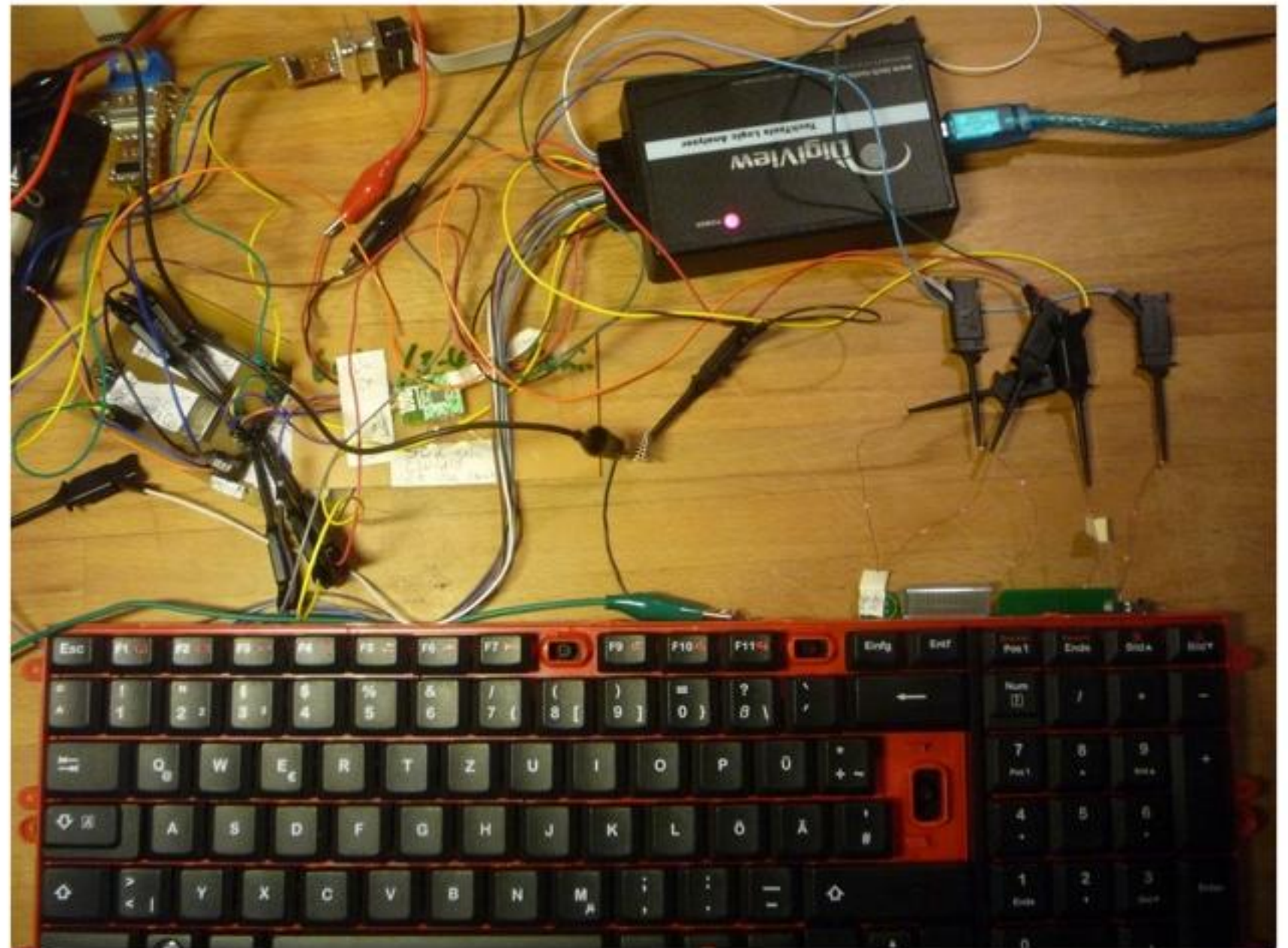


More targets...

- ❑ Just have a look at the Nordic Semiconductor „Press Releases“ Webpage
- ❑ How many of the vendors, using the NRF24xxx based transceivers in their devices, might implement crypto in a proper way? Message authentication?
- ❑ How many of the vendors might use the NRF24xxx crypto hardware in a proper way?

Back to the keyboard topic

Logitech Hardware



Logitech Payload Patterns

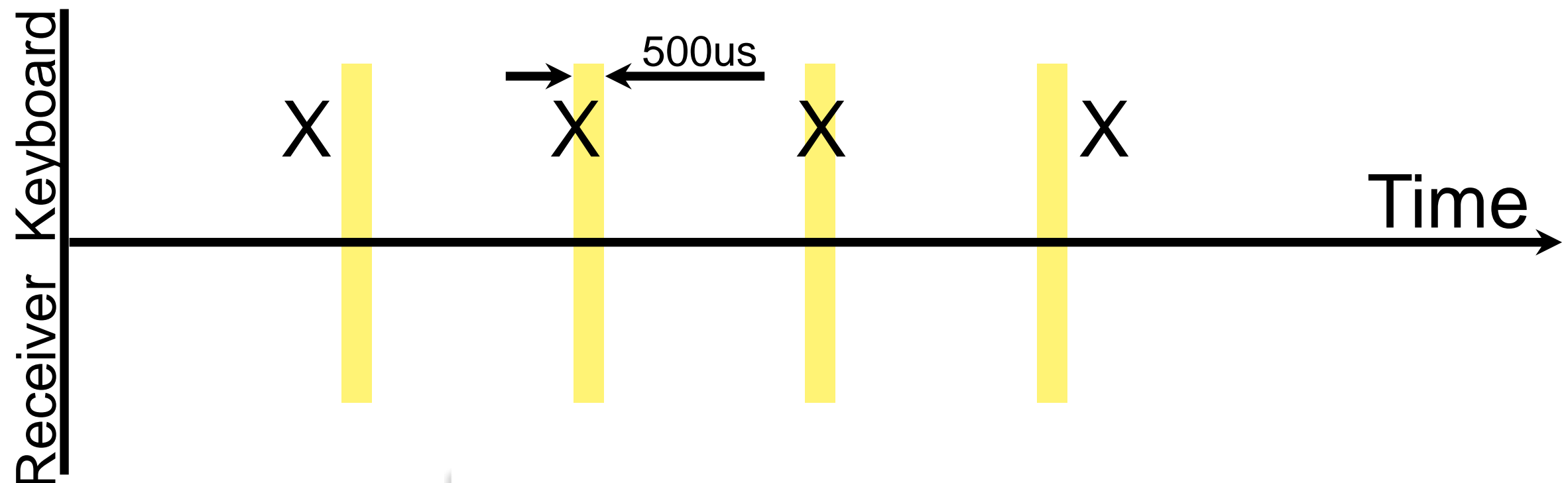
0	d3	ef	9c	84	0a	e1	17	1d	b2	b2	fd	76	11	0	0	0	0	0	0	0	17
0	d3	e1	4a	35	4f	74	7b	4	15	b2	fd	76	12	0	0	0	0	0	0	0	3f
0	d3	77	70	5b	d5	1d	a8	f5	5f	b2	fd	76	13	0	0	0	0	0	0	0	c5
0	d3	af	46	f0	c2	4a	b0	f8	65	b2	fd	76	14	0	0	0	0	0	0	0	f6

- ❑ 8 Byte encrypted data
- ❑ 4 Byte Sequence ID incremented
- ❑ 1 Byte checksum
- ❑ The following checksum algorithm can be applied to the payload:

```
cksum = 0xFF
for n in len(data):
    cksum -= data[n]
    cksum += 1
```


Logitech AES 128 Secret Key

Exchange



$$MATCH_{CH} := \{m_{CHn}, \dots, m_{CHm}\}$$

$$AESKEY_{128}(MATCH_{CH})$$

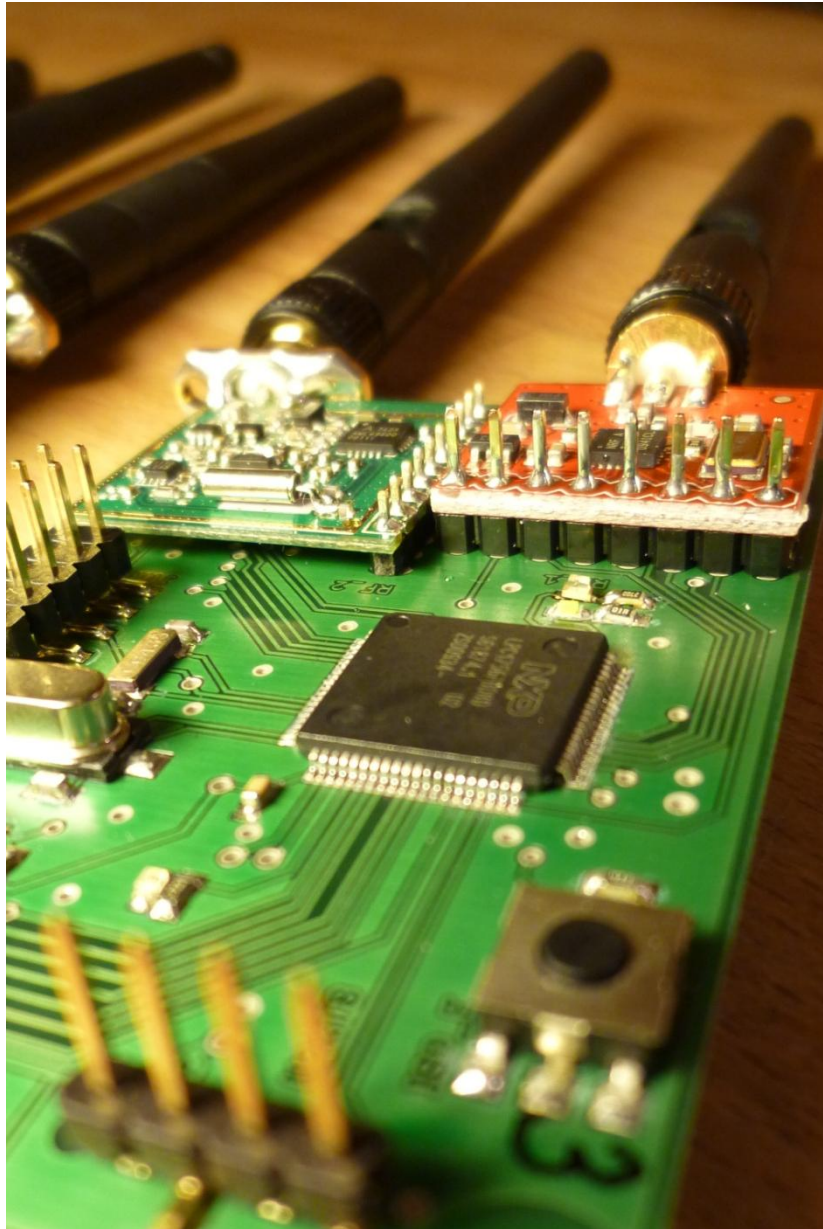
Logitech AES Key Derivation

- ❑ 128 bit AES cipher needs block sizes of 16 Byte
- ❑ Only 8 Bytes are seemingly random or encrypted
- ❑ We assume, that AES128 is used in a mode, to generate random data for an arbitrary stream-cipher initialization.
- ❑ Even when pressing the same key again and again, the 8 Byte ciphertext block differs completely

More Logitech...

- ❑ Keyboard Multimedia Keys are not encrypted
- ❑ Mouse data is not encrypted

Keykeriki V2 - DEMO



1. Scanning channels for valid Enhanced Shockburst frames
2. Setup sniffer & NRF module
3. Perform Remote Command Execution:
 - ▣ `<WINMETA-R>`
 - ▣ `cmd.exe<return>`
 - ▣ `calc.exe<return>`
 - ▣ `46/2=`

Risk & Impact

- ❑ Malware infection
- ❑ Remote key- and command injection (Drive-by shooting)
- ❑ About 75 meters with default antenna
- ❑ Interception / Identity theft
- ❑ Where lies the burden of proof....?

Whats Next?

- ❑ Fall 2010 2.4 GHz software defined radio
 - ❑ Can support different protocols
 - ❑ Can support different channels
 - ❑ Can support different encodings
- ❑ Free & commercial version
- ❑ New hardware, using more powerful programmable logic devices
- ❑ Analysis software, Wireshark, ...

Questions?

Write us:

ths@dreamlab.net

max.moser@dreamlab.net

Infos, Software & Hardware Release:

<http://www.remote-exploit.org/>

Greetings & thx to:

n1ck, greg, eric, phil