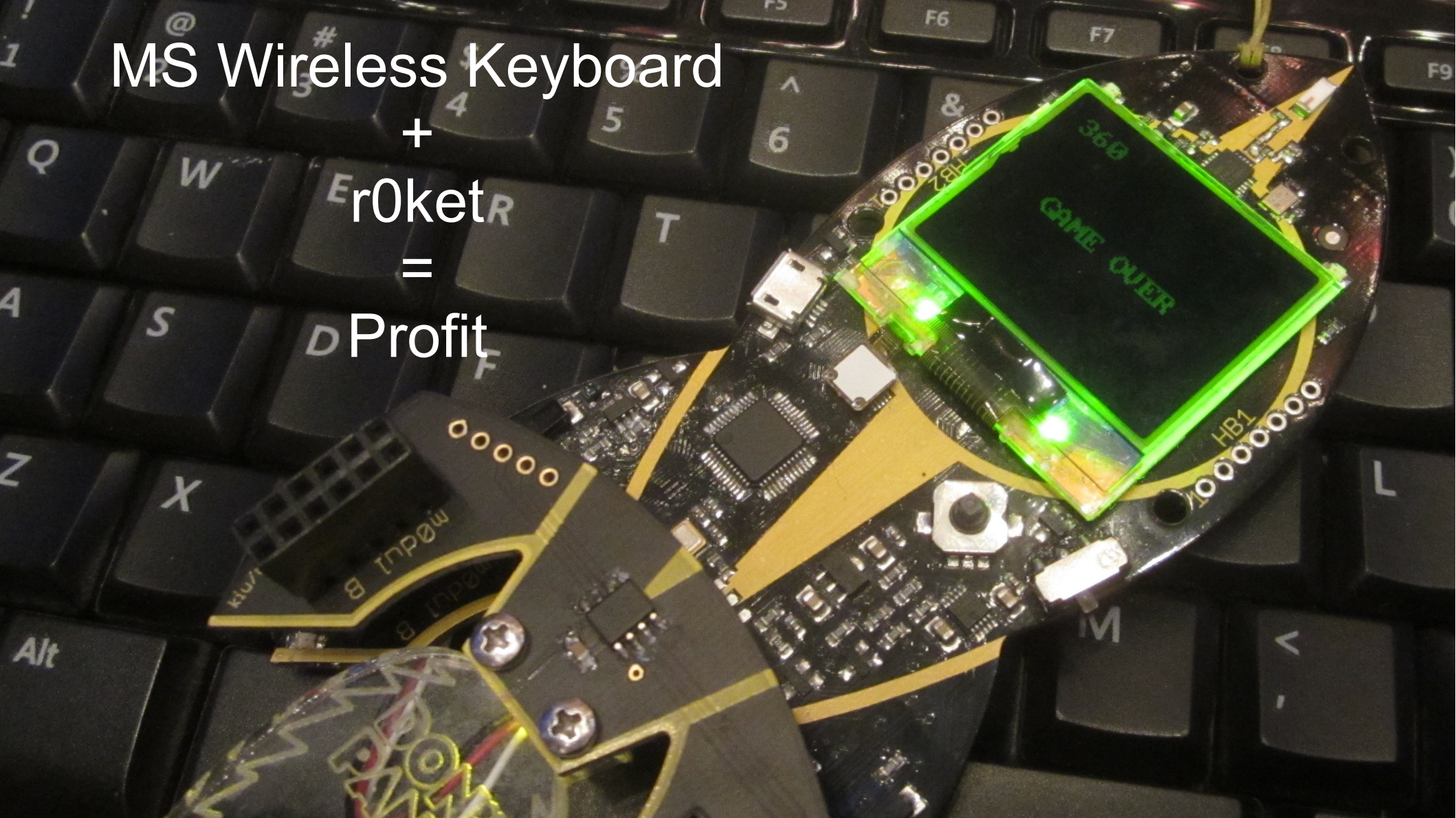

MS Wireless Keyboard
+
r0ket
=
Profit
GAME OVER

NRF24L01+ Enhanced Shockburst Packet Format

Noise	Preamble	MAC	9 Bit Packet Control Field			Payload	CRC
			Payload Length	PID	NO_ACK	0-16 Byte	CCITT
XX	AA	A6 A3 F8 B9 6D	010000	01	0		XX XX

Preamble is 55 if the first bit of the MAC is '0'

MAC is in reversed order than specified in the registers

PID is a 2 bit rolling packet counter to recognize retransmits

Kiss your security goodbye

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

Checksum:

XOR of all payload bytes and 0xFF.

Encryption:

XOR with MAC address

Sniffing and CRC

Travis showed sniffing without known MAC

MAC		Payload													
Noise	Preamble	MAC					9 Bit Packet Control Field			Payload	CRC				
							Payload Length		PID	NO_ACK	0-16 Byte	CCITT			
XX	AA	A6	A3	F8	B9	6D	010000		01	0		XX	XX		

Uses an undocumented 2 byte MAC length
(SETUP_AW = 0)

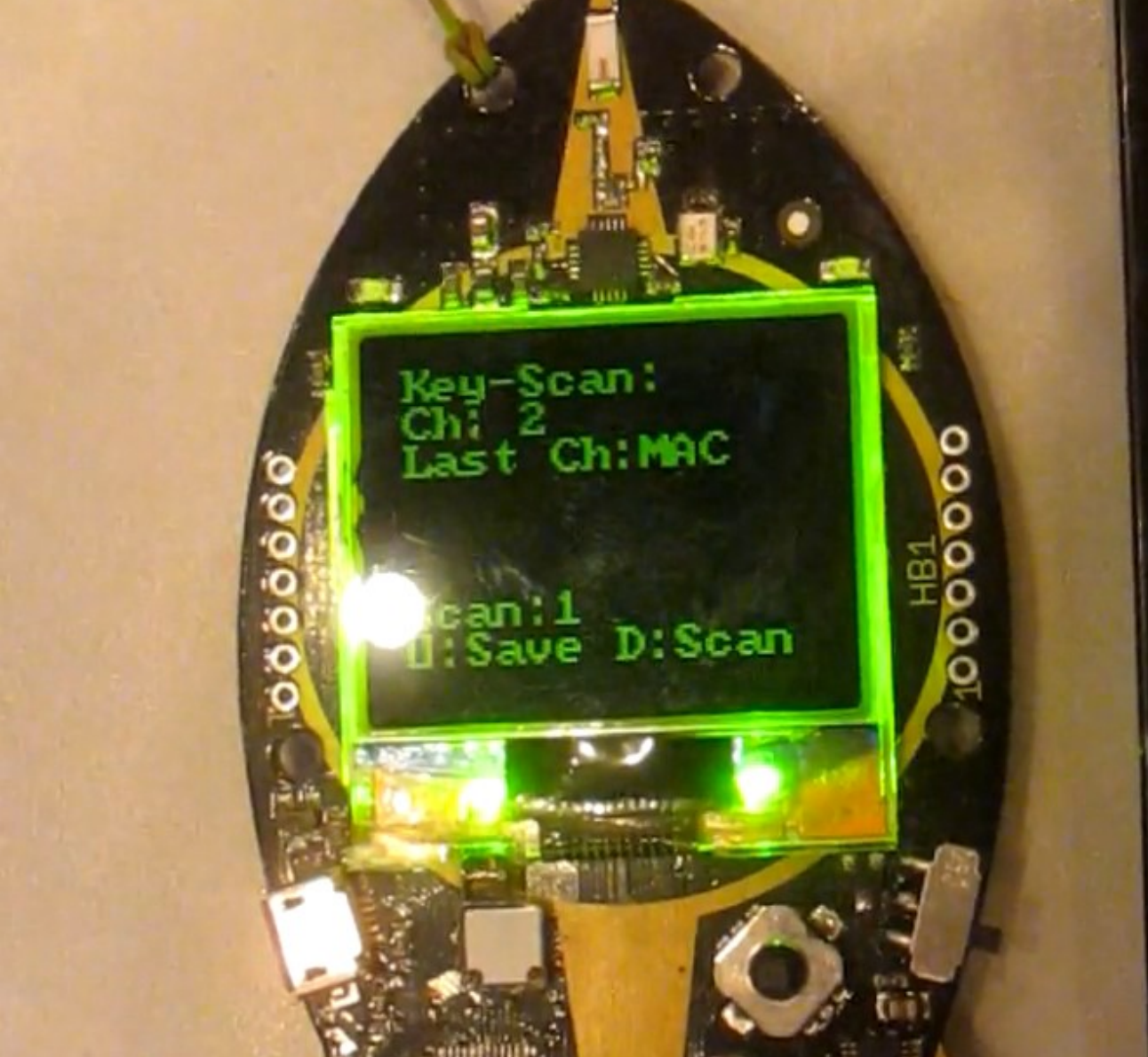
Current State

Three l0dables available:

* key-scan: Scan for keyboards and save channel + MAC

* key-sniff: Sniff key presses and log to file

* key-send: Send key presses


Key-Scan:
Ch: 2
Last Ch:MAC
can:1
:Save D:Scan
HB1


Ch:MAC
50:6DB9F8A3A6
q
Caps Lock
A
S
Shift
Ctrl

TODO

- Better key injection
- Better packet detection while scanning (think mouse)
- Analyze possible connection setup packets
- Analyze frequency hopping mechanism

- Code & slides available at https://github.com/r0ket/r0ket
- Reach us at

  @r0ket on twitter

  sec@42.org

  schneider@xtort.eu
- Thanks to

  Travis Goodspeed

  Thorsten Schroeder, Max Moser