



R0ket Keyboard Sniffer

30. September 2011

Fabian Kaczmarczyk und Katja Wolff

R0ket Keyboard Sniffer

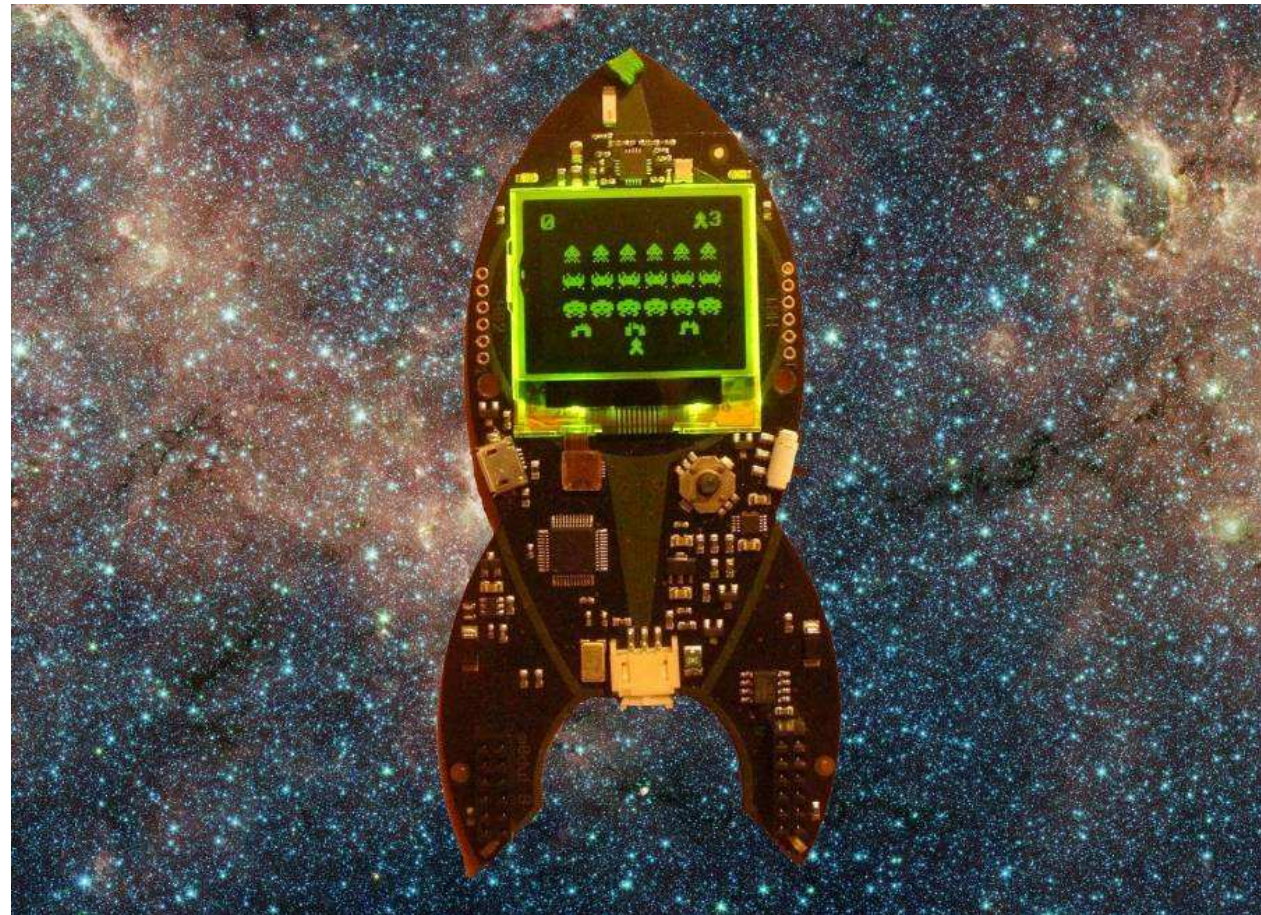
Gliederung

- Projekt
- Theoretisches
 - Aufbau der Datenpakete
 - Ausnutzung der Präambel
 - MAC-Adresse finden
 - Pakete des Keyboards entschlüsseln
- Praktisches
 - Programmierung der R0ket
 - Pakete empfangen
 - Code
- Aktueller Stand und Probleme
- Demonstration

R0ket Keyboard Sniffer

Gliederung

- Projekt
- Theoretisches
 - Aufbau der Datenpakete
 - Ausnutzung der Präambel
 - MAC-Adresse finden
 - Pakete entschlüsseln
- Praktisches
 - Programmierung der R0ket
 - Pakete empfangen
 - Code
- Aktueller Stand und Probleme
- Demonstration



R0ket Keyboard Sniffer

Gliederung

- Projekt
 - Theoretisches
 - Aufbau der Datenpakete
 - Ausnutzung der Präambel
 - MAC-Adresse finden
 - Pakete entschlüsseln
 - Praktisches
 - Programmierung der R0ket
 - Pakete empfangen
 - Code
 - Aktueller Stand und Probleme
 - Demonstration
- Nordic VLSI nRF24L01+
 - 2,4 GHz Spektrum
 - Funkkeyboards von Microsoft
 - Max Moser und Thorsten Schröder - KeyKeriki V2.0 Projekt
 - Travis Goodspeed
 - Ziel: Code auf die R0ket übertragen

R0ket Keyboard Sniffer

Gliederung

- Projekt
- Theoretisches
 - Aufbau der Datenpakete
 - Ausnutzung der Präambel
 - MAC-Adresse finden
 - Pakete entschlüsseln
- Praktisches
 - Programmierung der R0ket
 - Pakete empfangen
 - Code
- Aktueller Stand und Probleme
- Demonstration

Aufbau der Datenpakete



- Präambel: 0xAA oder 0x55
- SYNC-Field enthält MAC-Adresse bei Microsoft Keyboards

Paket empfangen:

- 8-bit Präambel (0xAA oder 0x55)
- 3-5 Byte Adresse
- CRC muss stimmen

R0ket Keyboard Sniffer

Gliederung

- Projekt

- Theoretisches

- Aufbau der Datenpakete
- Ausnutzung der Präambel
- MAC-Adresse finden
- Pakete entschlüsseln

- Praktisches

- Programmierung der R0ket
- Pakete empfangen
- Code

- Aktueller Stand und Probleme

- Demonstration

Ausnutzung der Präambel

- Trick: Empfange schon, bevor ein Paket beginnt.
- Noise enthält viel 0xAA, 0xEE, 0x00

1. Limitieren der MAC-Adresse auf 2 Byte
2. CRC ausschalten
3. Enhanced ShockBurst deaktivieren
4. MAC Adresse auf den Wert der Präambel setzen
5. Empfangenen Noise auf gültige MAC-Adresse durchsuchen

R0ket Keyboard Sniffer

Gliederung

- Projekt
- Theoretisches
 - Aufbau der Datenpakete
 - Ausnutzung der Präambel
 - MAC-Adresse finden
 - Pakete entschlüsseln
- Praktisches
 - Programmierung der R0ket
 - Pakete empfangen
 - Code
- Aktueller Stand und Probleme
- Demonstration

Ausnutzung der Präambel

	Preamble 1 Byte 0xAA or 0x55	Address 3-5 Byte	Payload 0-32 Byte
Noise Preamble 0xAA or 0x55	new Address 0x00AA or 0x0055	Address 3-5 Byte	Payload 0-32 Byte

1. Limitieren der MAC-Adresse auf 2 Byte
2. CRC ausschalten
3. Enhanced ShockBurst deaktivieren
4. MAC Adresse auf den Wert der Präambel setzen
5. Empfangenen Noise auf gültige MAC-Adresse durchsuchen

R0ket Keyboard Sniffer

Gliederung

- Projekt

- Theoretisches

- Aufbau der Datenpakete
- Ausnutzung der Präambel
- MAC-Adresse finden
- Pakete entschlüsseln

- Praktisches

- Programmierung der R0ket
- Pakete empfangen
- Code

- Aktueller Stand und Probleme

- Demonstration

Ausnutzung der Präambel

- Gesendetes Paket: 0x 55 0102030201 BEEF
 - Empfangen: 0x 55 0055 0102030201BEEF
1. Limitieren der MAC-Adresse auf 2 Byte
 2. CRC ausschalten
 3. Enhanced ShockBurst deaktivieren
 4. MAC Adresse auf den Wert der Präambel setzen
 5. Empfangenen Noise auf gültige MAC-Adresse durchsuchen

R0ket Keyboard Sniffer

Gliederung

- Projekt
- Theoretisches
 - Aufbau der Datenpakete
 - Ausnutzung der Präambel
 - MAC-Adresse finden
 - Pakete entschlüsseln
- Praktisches
 - Programmierung der R0ket
 - Pakete empfangen
 - Code
- Aktueller Stand und Probleme
- Demonstration

MAC-Adresse finden

- Frequenz, Bitrate (2Mbit/s, 1Mbit/s) und Präambel (0xAA/0x55) muss herausgefunden werden.
- Mehrere Pakete pro Konfiguration empfangen
- Die ersten 3 Byte untersuchen
- Häufungen erkennen
- 3-5 Byte lang

R0ket Keyboard Sniffer

Gliederung

Pakete entschlüsseln

- Projekt
- Theoretisches
 - Aufbau der Datenpakete
 - Ausnutzung der Präambel
 - MAC-Adresse finden
 - Pakete entschlüsseln
- Praktisches
 - Programmierung der R0ket
 - Pakete empfangen
 - Code
- Aktueller Stand und Probleme
- Demonstration

R0ket Keyboard Sniffer

Tasten:

a b

Beispiel für
Tastatur mit
Adresse:
CD 98 35 0A C0

Packet Header	0a	78	6	1	df	88	4b	0a		c0	C9	88	8	0a	c0	cd	57
Sequence ID / Counter	0a	38	6	1	df	88	8	d2									
Metakey Flags / Bitfield	0a	38	6	1	df	88	8	d2									
HID code	0a	38	6	1	df	88	8	d2									
Checksum	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	78	6	1	D8	88	4b	0a		c0	CD	88	8	0a	c0	cd	54

R0ket Keyboard Sniffer

Gliederung

- Projekt
- Theoretisches
 - Aufbau der Datenpakete
 - Ausnutzung der Präambel
 - MAC-Adresse finden
 - Pakete entschlüsseln
- Praktisches
 - Programmierung der R0ket
 - Pakete empfangen
 - Code
- Aktueller Stand und Probleme
- Demonstration

Pakete entschlüsseln

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

R0ket Keyboard Sniffer

Gliederung

- Projekt
- Theoretisches
 - Aufbau der Datenpakete
 - Ausnutzung der Präambel
 - MAC-Adresse finden
 - Pakete entschlüsseln
- Praktisches
 - Programmierung der R0ket
 - Pakete empfangen
 - Code
- Aktueller Stand und Probleme
- Demonstration

Programmierung der R0ket

Quellcode in C

Firmware bringt Ausgabeprozeduren

Cross-Compiler für Laptop zu ARM

CodeSourcery und GNU-Compiler

Flashen über USB

Autoflasher-Skript mitgeliefert

R0ket Keyboard Sniffer

Gliederung

- Projekt
- Theoretisches
 - Aufbau der Datenpakete
 - Ausnutzung der Präambel
 - MAC-Adresse finden
 - Pakete entschlüsseln
- Praktisches
 - Programmierung der R0ket
 - Pakete empfangen
 - Code
- Aktueller Stand und Probleme
- Demonstration

Pakete empfangen:

Chips konfiguriert um Pakete zu empfangen.
(CRC, Adresslänge, Adresse, etc.)

Funktionen der R0ket Firmware zum Auslesen von Paketen nutzen und anpassen

MAC-Adresse des Keyboards finden.

Mit der MAC-Adresse gezielt das Keyboard aushorchen

Pakete entschlüsselt

R0ket Keyboard Sniffer

Gliederung

- Projekt
- Theoretisches
 - Aufbau der Datenpakete
 - Ausnutzung der Präambel
 - MAC-Adresse finden
 - Pakete entschlüsseln
- Praktisches
 - Programmierung der R0ket
 - Pakete empfangen
 - Code
- Aktueller Stand und Probleme
- Demonstration

Code

Hauptprogramm setzt Register und scannt Frequenzen

Scan setzt Register für Vor- und Nachbereitung des Empfangs von Paketen

Vorgegebene Funktionen zum Empfang wurden manipuliert, um Datenempfang zu ermöglichen

Viele falsche Treffer müssen gefiltert werden

R0ket Keyboard Sniffer

Gliederung

- Projekt
- Theoretisches
 - Aufbau der Datenpakete
 - Ausnutzung der Präambel
 - MAC-Adresse finden
 - Pakete entschlüsseln
- Praktisches
 - Programmierung der R0ket
 - Pakete empfangen
 - Code
- Aktueller Stand und Probleme
- Demonstration

Aktueller Stand

- Pakete werden empfangen.
- Frequenz und Bitrate der Tastatur konnten noch nicht bestimmt werden.

Probleme

- Kein Debugger
- Firmware musste verändert werden (CRC)
- Viele Unsicherheiten:
 - Keyboard
 - Verhalten des Programms

R0ket Keyboard Sniffer

Gliederung

- Projekt
- Theoretisches
 - Aufbau der Datenpakete
 - Ausnutzung der Präambel
 - MAC-Adresse finden
 - Pakete entschlüsseln
- Praktisches
 - Programmierung der R0ket
 - Pakete empfangen
 - Code
- Aktueller Stand und Probleme
- Demonstration

Demonstration