# ATtiny@Keyboard

**Marvin Adomeit**
**Florian Albrecht**

**IT-Security Workshop 2019**

# Idee

- Gefahr von unbekannten USB-Sticks (zumindest) bekannt
  - USB Rubber Ducky
- Welche USB-Geräte erwecken wenig Misstrauen?
  - Mäuse
  - Tastaturen
- **=>** Tastatur für einen Angriff manipulieren

# Angriffe

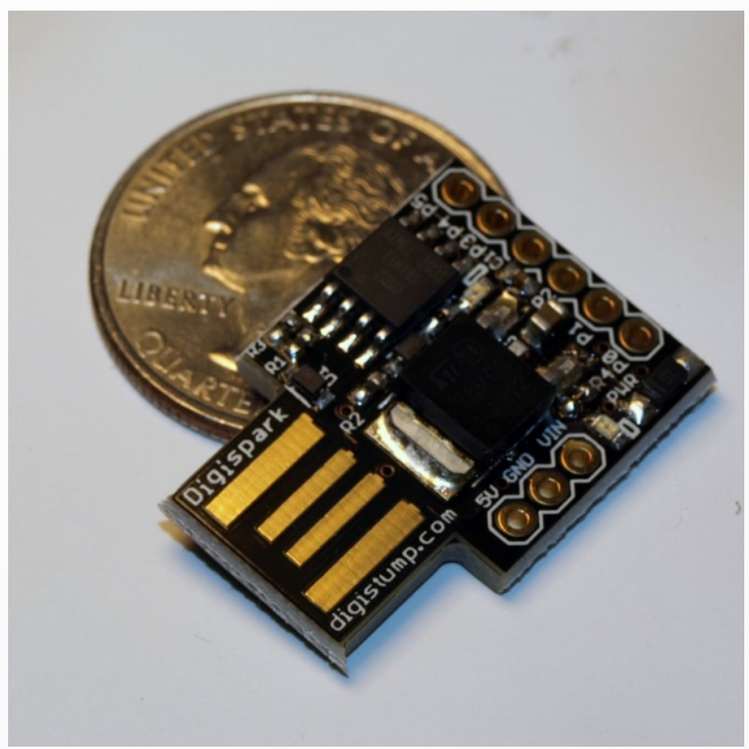
- Keysniffer (Tastatur – [Host] µC [Device] – PC)
  - Übertragung der gesammelten Daten per Funk (Wlan/Bluetooth)
  - SD-Card
- USB-Storage
  - lädt zum geeigneten Zeitpunkt Schadprogramme nach/führt sie aus
- Fake-Tastatur
  - µC gibt sich als Tastatur aus und führt Kommandos aus/lädt Programme aus den Internet nach

# Fake-Tastatur

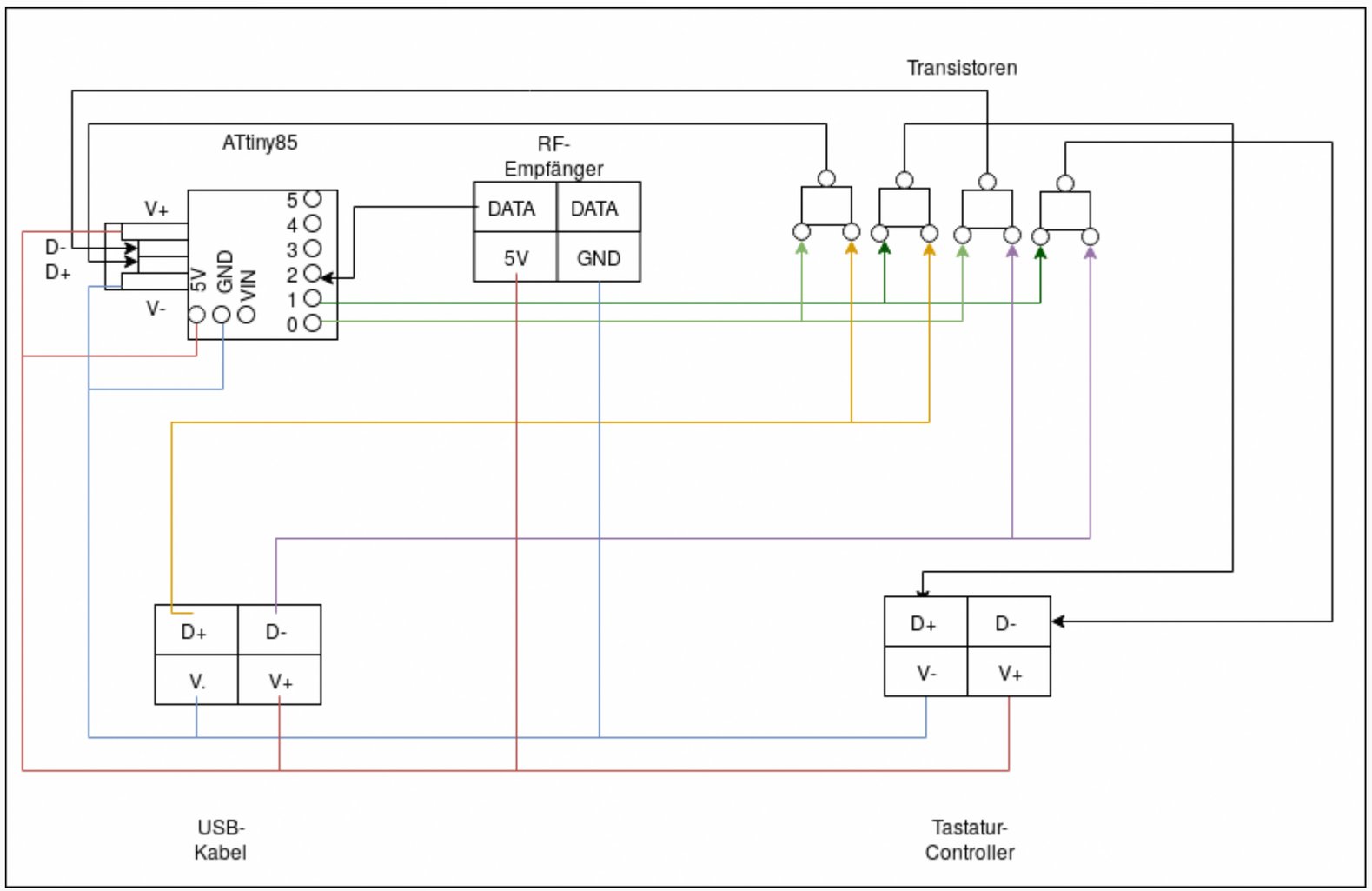
- es findet keine Verifizierung zw. USB-Host und Device statt
  - Device kann beliebigen USB-Header senden
  - theoretisch könnte sich der µC auch als Drucker ausgeben
  - **=>** man kann die originale Tastatur imitieren (Host sieht also keinen Unterschied)
- µC kann beliebige Tastenkombinationen senden
  - z.B. Terminal öffnen und Nutzerverzeichnis löschen

# Aufbau

- Hardware
  - ATtiny85 (8k Flash, 2k RAM, 6 GPIOs) als Digispark USB Dev Board
  - 4 Transistoren
  - 433Mhz-Empfänger
  - Logitech K200
- Software
  - Arduino IDE



# Schaltung


Transistoren
ATtiny85
RF-
Empfänger
V+
D-
D+
V-
5V
GND
VIN
5
4
3
2
1
0
DATA
DATA
5V
GND
D+
D-
V.
V+
D+
D-
V-
V+
USB-
Kabel
Tastatur-
Controller

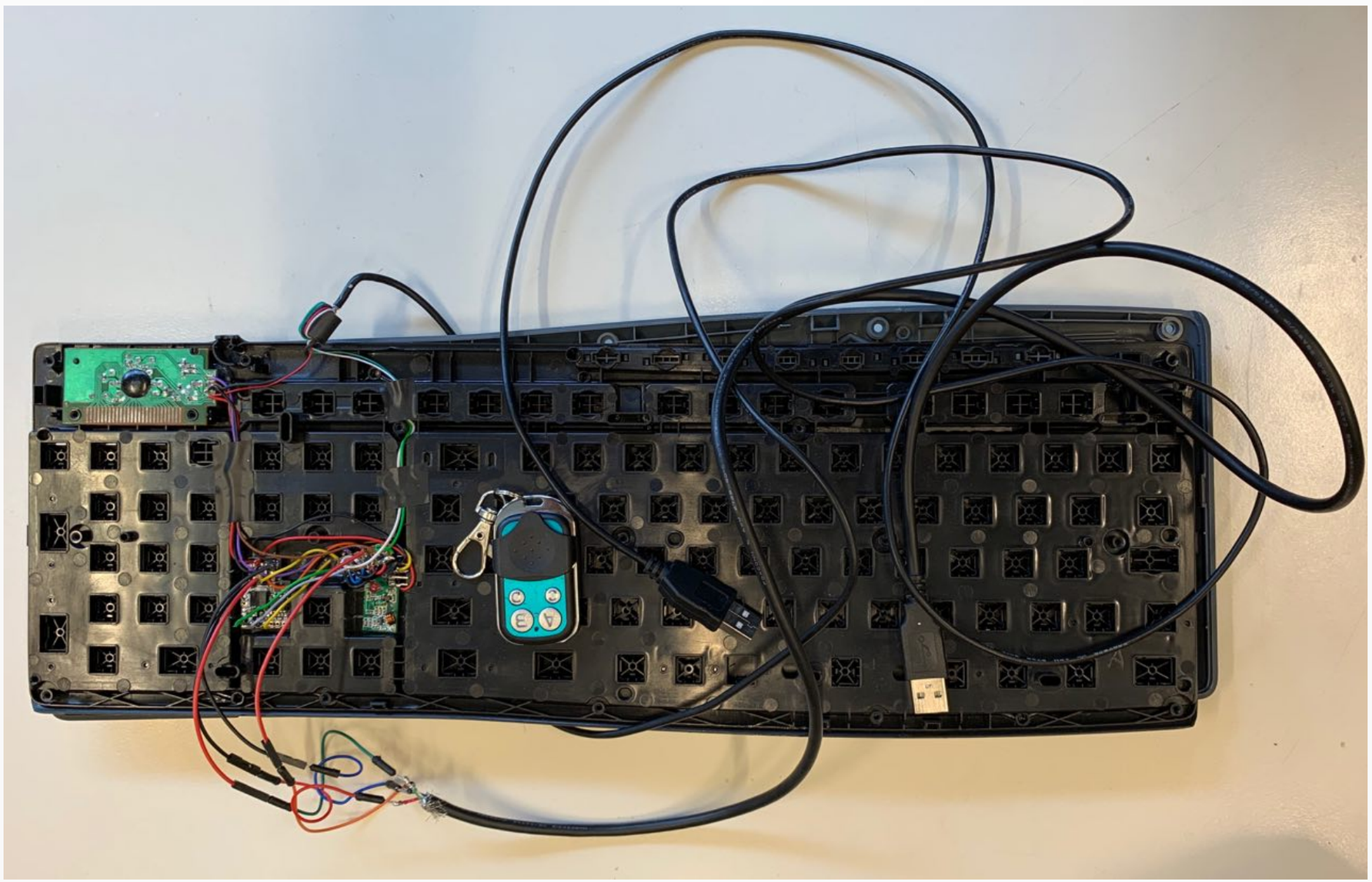
# (eigene) Angriffe

- DOS-Attacke
  - ständiges Öffnen des Terminal
- Schadsoftware nachladen und ausführen
  - Terminal öffnen → Software von Dropbox nachladen → ausführen
- Listen and Repeat
  - über den 433Mhz-Empfänger werden Zeichen empfangen und dann ausgegeben

# Schutzmaßnahmen

- ohne Verifizierung (Zertifikate, …) keine Möglichkeit
  - eventuell durch prüfen der Stromversorgung oder ähnlicher Indikatoren
- sperren jedes neuen USB-Gerätes und manuelle Bestätigung des Geräts
  - sehr nervig
  - wird für die Bestätigung allerdings die Tastatur benötigt, wäre kein Angriff möglich (außer es ist eine simple Abfrage (j/n))
  - bei Bestätigung per Maus, würde der Nutzer zwar den Angriff sehen, aber ohne Tastatur wird ein Eingriff in das Geschehen schwierig

# Demonstration



# Probleme

- Programmiermodus funktioniert nur über externen Anschluss
  - umschalten von Attiny/Logitech nur per Software-Reset, Bootloader wird aber nur bei Hardware-Reset aktiv
- Erkennung des Betriebssystems schwierig
- Platzprobleme
- PC müsste entsperrt sein und Kontakt zum Opfer müsste gegeben sein

# Fazit

- kostengünstig, Reproduktionszeit gering, kein wirksamer Schutz in gängigen Betriebssystemen
- für Angriffe auf viele Personen zu aufwändig
- für gezielte Angriffe auf Personen perfekt (Geheimdienste, ...)