Keyless Gone

Stealing Your Car, the Easy Way

mrq, bibor

29.12.2016

Chaos Computer Club Aachen

Keyless Entry / Keyless Go Systems

- **Goal:** Open the car and start the engine without taking your key out of the pocket
- Independed from classical rf key functionality
- Deployed in most mid-range to high-end cars today

Keyless Entry / Keyless Go Systems

Procedure

1. Car probes for the key on LF ($\sim$125 kHz)
    - Short range
2. Key answers on HF ($\sim$430 MHz)
    - Long range
3. Car opens/starts

Keyless Entry / Keyless Go Systems

Procedure

1. Car probes for the key on LF ($\sim$125 kHz)
    - Short range $\Leftarrow$ this is the security feature
2. Key answers on HF ($\sim$430 MHz)
    - Long range
3. Car opens/starts

Keyless Entry / Keyless Go Systems

Procedure

1. Car probes for the key on LF (∼125 kHz)
    - Short range ⇐ this is the security feature
2. Key answers on HF (∼430 MHz)
    - Long range
3. Car opens/starts

Relay Attack !

Relay Attack

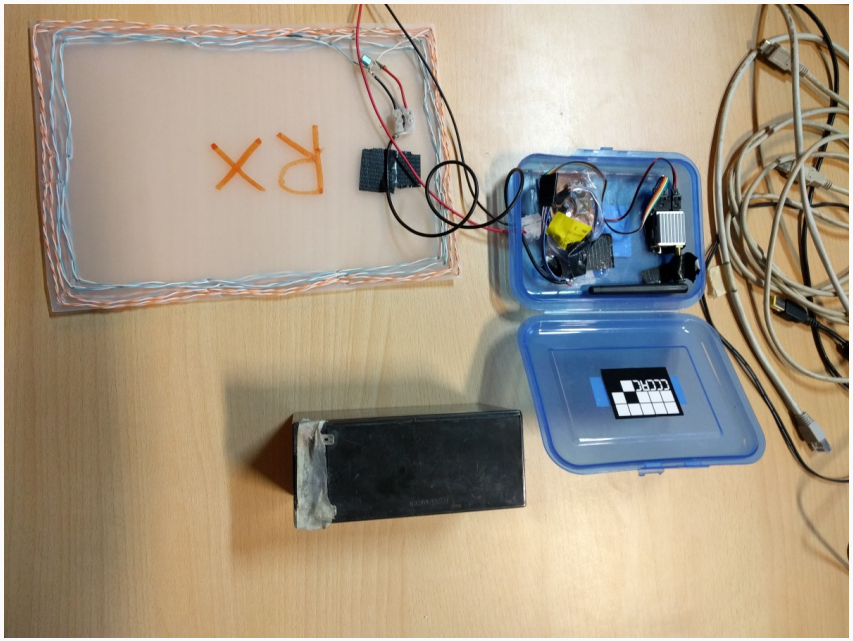


Figure 1: Key side

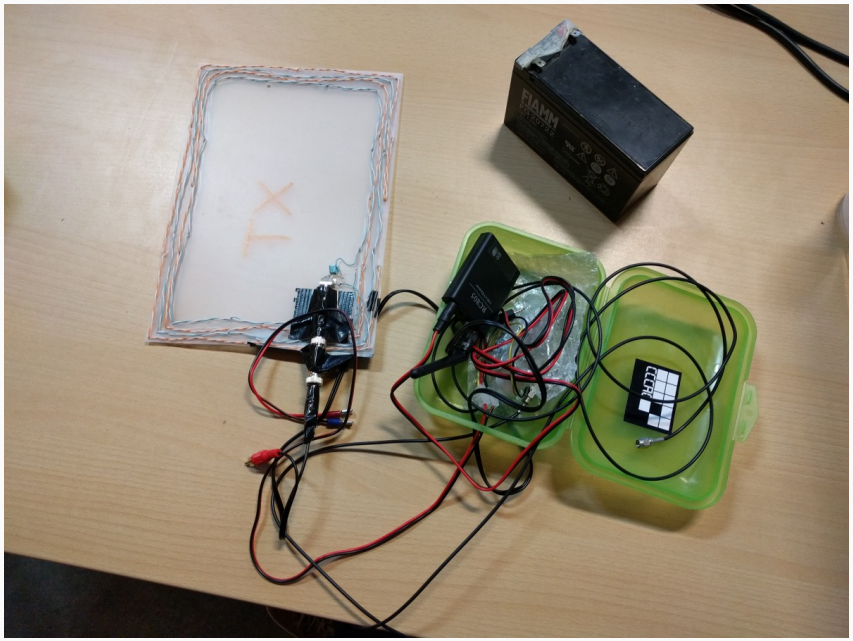
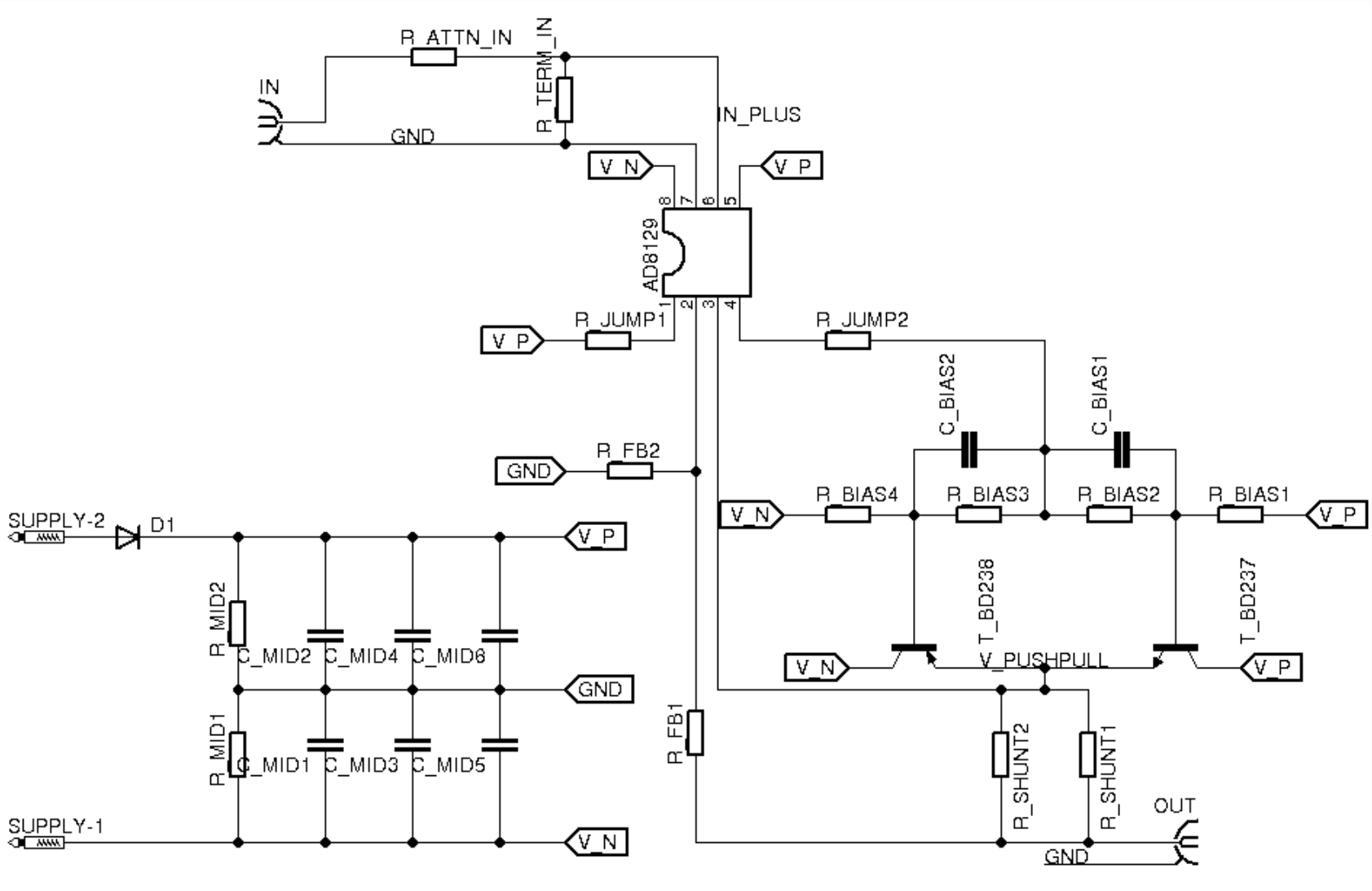


Figure 2: Car side

Relay Attack



Relay Attack

Conclusio

- Shit's broken, yo
  - Almost all tested vehicles affected
  - Hard to fix
  - Easy to exploit
- **Web:** https://ccc.ac/keyless-klau/ (English version is wip)
- **Contact:** pwnmyride (at) aachen.ccc.de