Protecting your car

Marian Marinov <mm@1h.com>
CEO of 1H Ltd.
CTO of GetClouder Ltd.


Disclamer:
- I'm not a car thief
- All you will see is my own experince
- With my own cars

Who am I?

- System Administrator since 1998
- System Architect since 2004
- CEO of 1H Ltd.
- CTO of GetClouder Ltd.
- Head of DevOps at Siteground.com
- Teaching Linux System Administration and Network Security in Sofia University
- Hardware hacker
- Helping with the organization of OpenFest, BG Perl Workshops and IT Tour

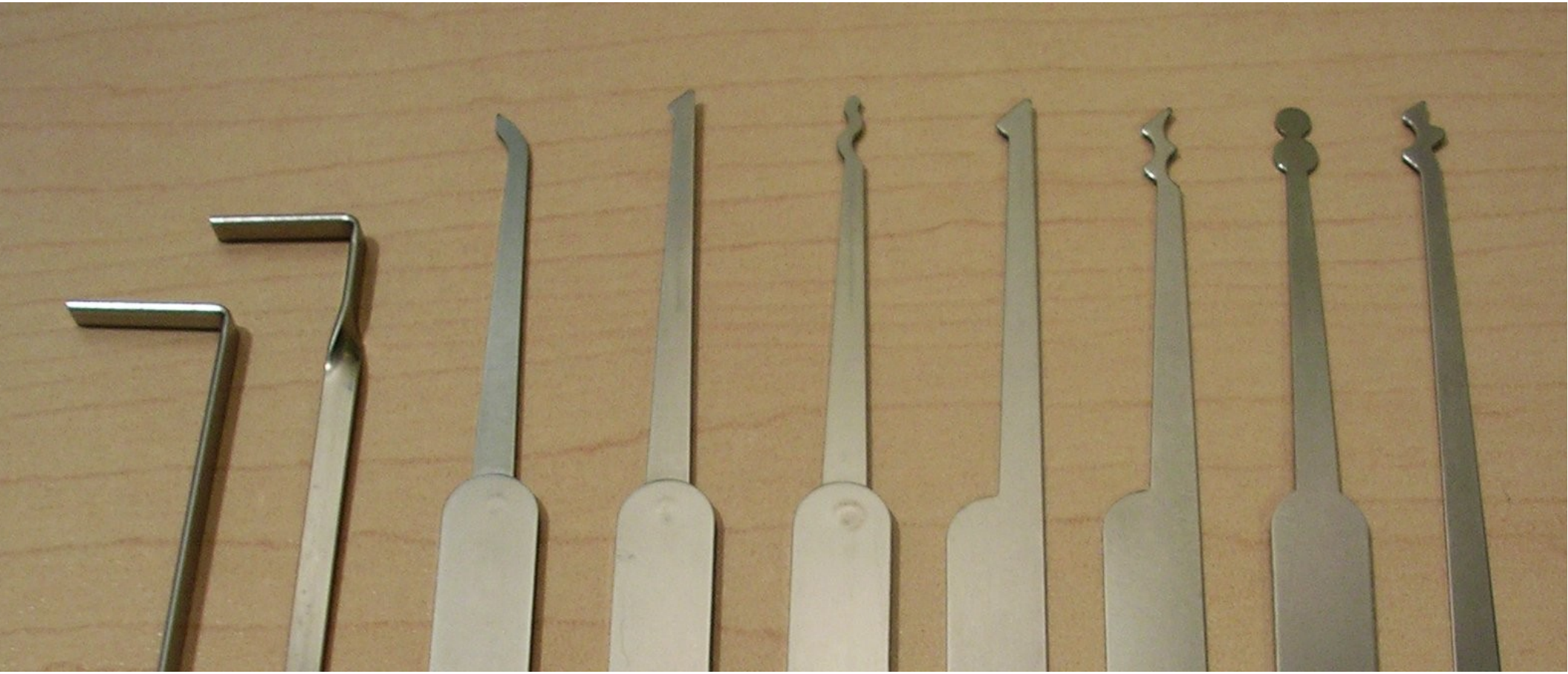
Maznio aka Toadwart aka Toadie

Is there a secure car?

Physical security of your car...

- Door locks can be
  - picked
  - broken
  - completely bypassed trough the window gap
- Your windows can be broken
- Your whole doors my be air jacked or otherwise lifted ♥

Lock picking tools



If you are lucky...


What to do when
your car gets
broken into...


Window GAP

Air Jack kit for 60$ ♥

Air jacking ☺

Even easier... just get it with you ☺

I fear... NOT :)

* most alarms don't detect air jacking

* some alarms can be easily disabled from inside

* default alarms use the horns of a car

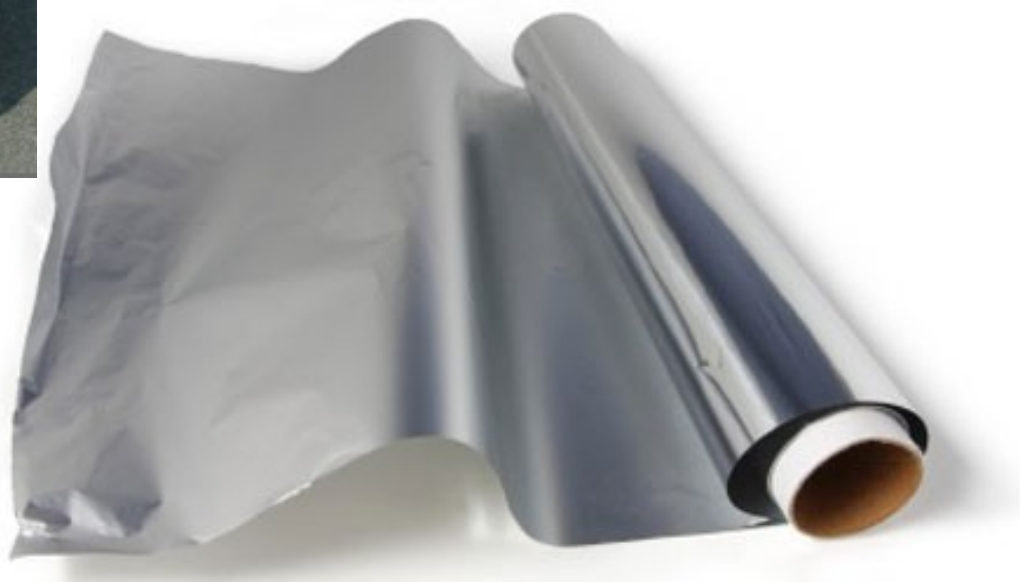
* default alarms have factory procedures for disable

* alarms flash the lights of your car

So what do the immobilizer systems do?

- break the connections between different electical parts in the car
- immobilizers are cutting power in default places
- require "authentication" to "connect" the disconnected parts

Hide all the lights



I fear... NOT :)

* most car security systems use
  - 315Khz and 434Khz

* a scanner for those frequencies will cost you less then 30$

* most of the alarm systems are vulnerable to replay attacks

* those that are not, are easily crackable because the actual remotes lack the power to do hard calculation

Usability always breaks security :)

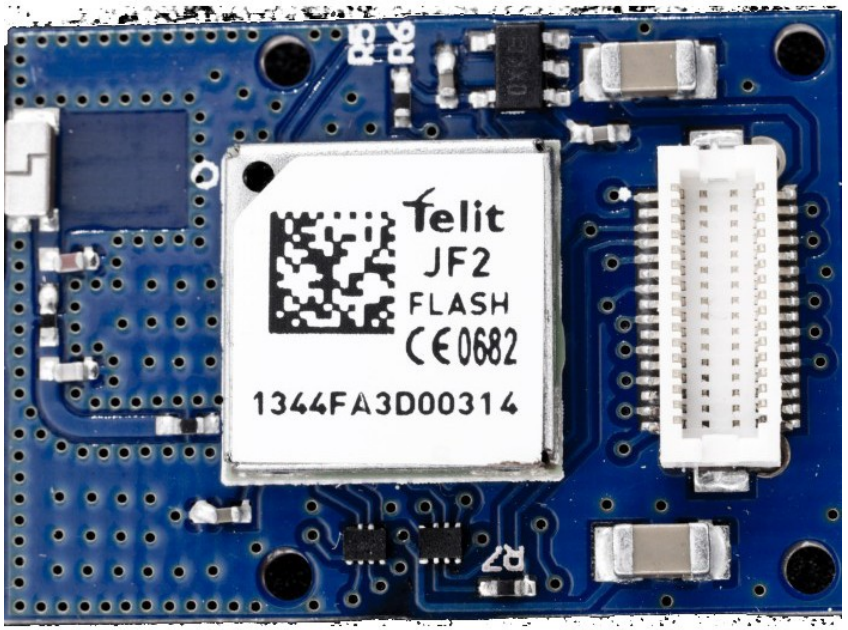
What device am I building?

- Arduino Uno
  - GSM shield
  - GPS shield
  - Bluetooth shield
  - RFID reader
  - Iridium RockBLOCK
  - Relay shields

SparkFun

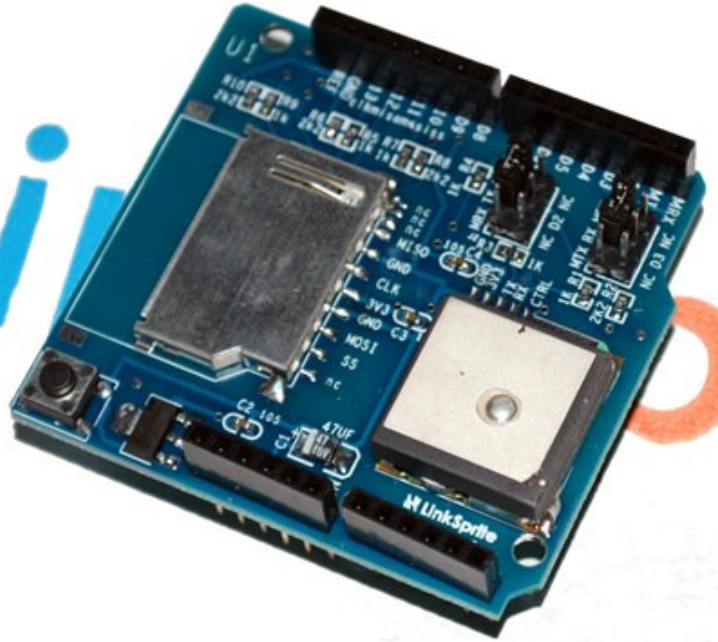
DealExtream

GSM Shields



TinyCircuits GPS

GPS receivers

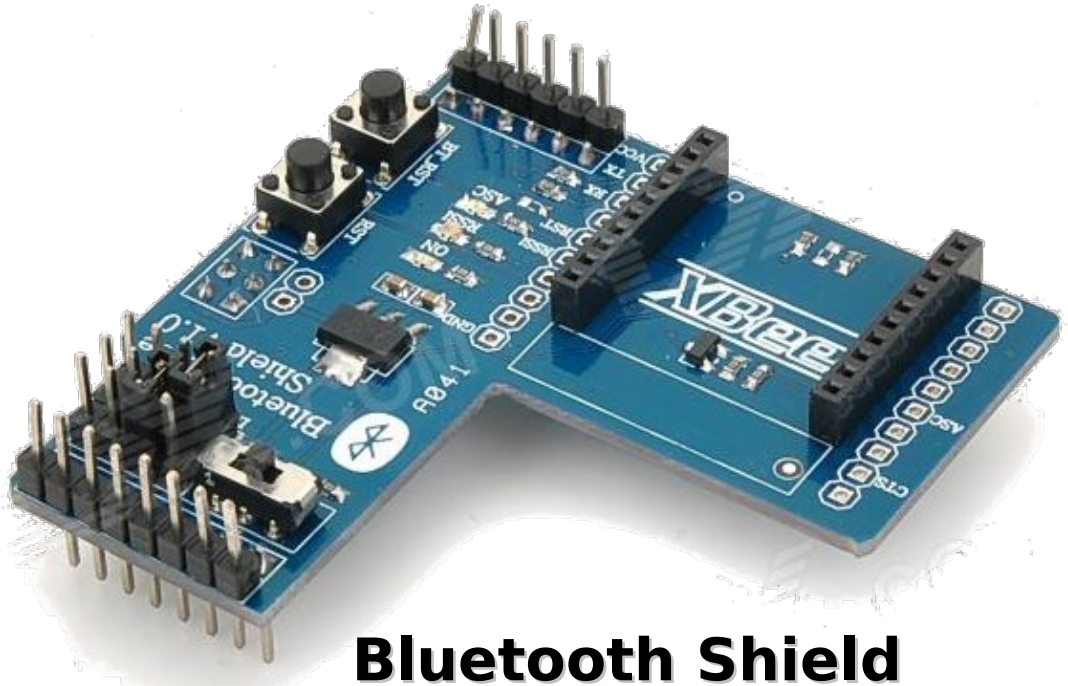


Arduino compatible GPS Shield

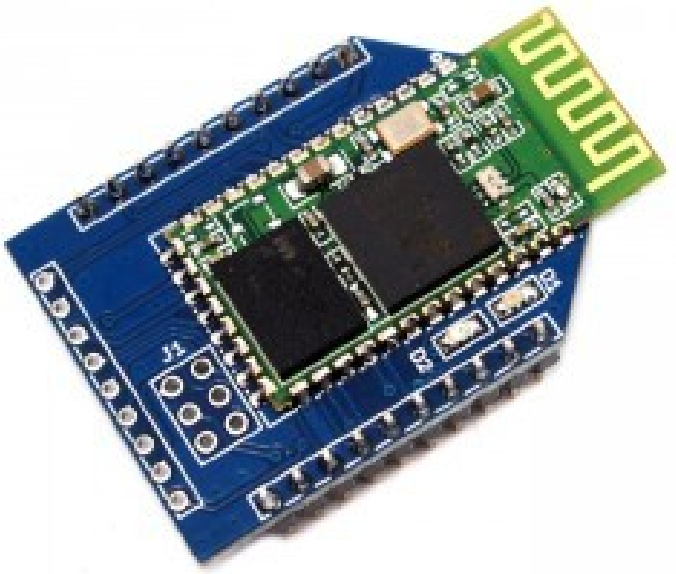
Geogram One

http://dsscircuits.com/index.php/geogram-one

DealExtreme



Bluetooth Shield



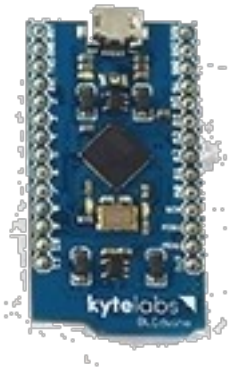
Bluetooth Bee

Leonardo

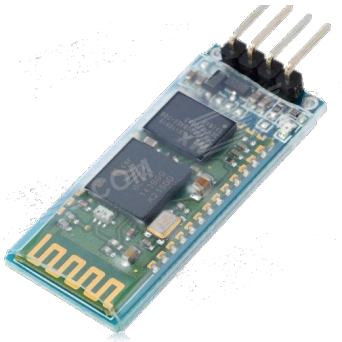
+

BLE

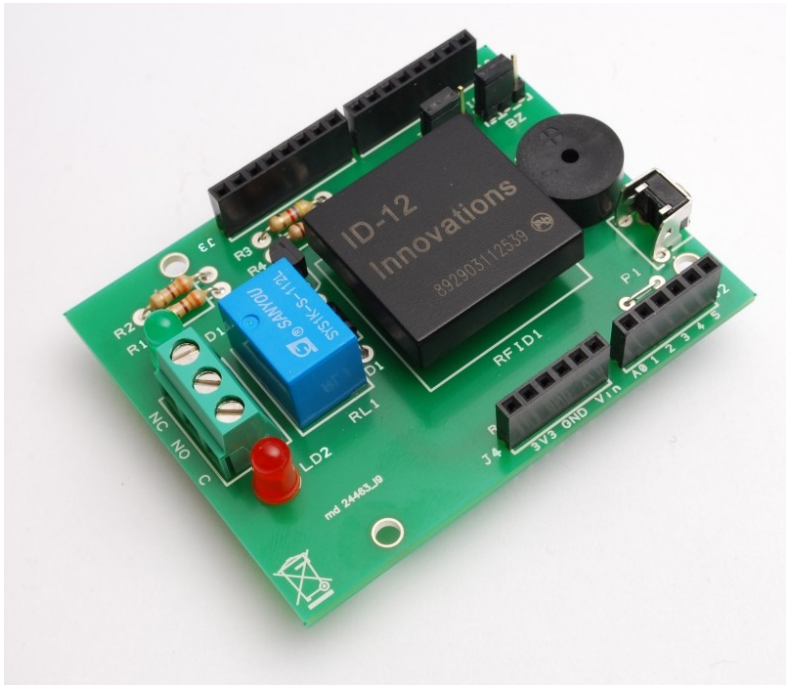
=

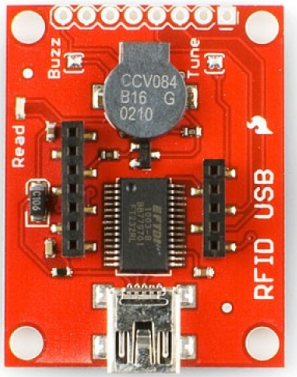


BLEduino



Bluetooth transmitter

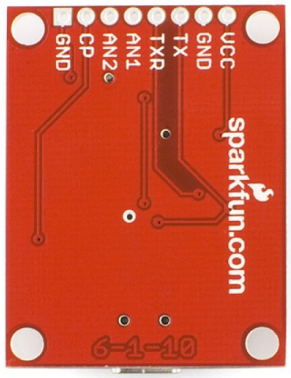

ID-12
Innovations
RFID1
RL1
LD2
NC NO C
3V3 GND VIn


Buzz
Tune
Read
RFID USB


LIBERTY
QUARTER DOLLAR


ID-20LA
Innovations
6A0704130348

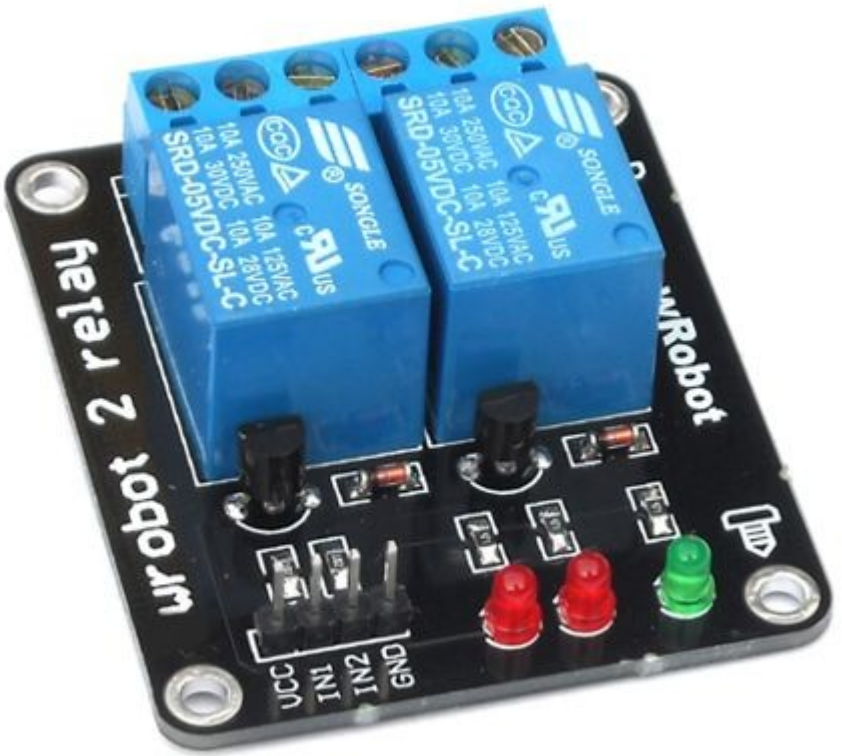

ID-12
Innovations
RFID USB


VCC
GND
TX
TXR
AN1
AN2
CP
GND
sparkfun.com
6-1-10

SparkFun

Iridium RockBLOCK

Relays



What have I done differently?

- New cars require so much computational power that they can't even start without computers.
- I decided to cut more wires and each at 3-5 places, in order to make their repair take hours or days if you don't know where to look.
- With that in mind I sabotaged the Car Area Network (CAN) by isolating the start computer.

TODO: detect the serial number of the installed start computer and engine control unit and if they are not the ones that should be connected to this car, fry the hell out of them by sending 12V on each pair.

What functionality I have working?

- RFID protection
- SMS location tracking
- SMS lock/unlock
- Sabotaged a few important parts of the car with relays
- The relays are connected to a second Arduino mini
- Temperature control in the second arduino

How is that working?

- If the RFID reader does not detect an RFID card within 30sec from start of the car it stops power to the fuel pump and to the engine electronics
- If the car is started
  - Using the GPS shield, constantly take GPS readings
  - Check for SMS messages on the GSM/GPRS shield
  - If a message from authenticated phone number with a proper code and command is received
  - send a predefined message with our current coordinates
  - lock or unlock the car
  - start or stop the car
- If the car is offline, every 30min get its position. If it has changed and the RFID card is not detected, send an SMS.

What will I have in the future?

- Single button start/stop system
- SMS start/stop
- Bluetooth lock/unlock
- Iridium RockBLOCK for location reporting and lock/unlock

Resources

- https://github.com/hackman/GPS_Lock
- http://arduiniana.org/libraries/iridiumsbd/
- http://dsscircuits.com/index.php/geogram-one
- http://arduino.cc/en/Guide/ArduinoGSMShield
- https://learn.adafruit.com/adafruit-ultimate-gps-logger-shield
- http://bildr.org/2011/02/rfid-arduino/
- https://tiny-circuits.com/

Marian Marinov <mm@1h.com>
CEO of 1H Ltd.
CTO of GetClouder Ltd.