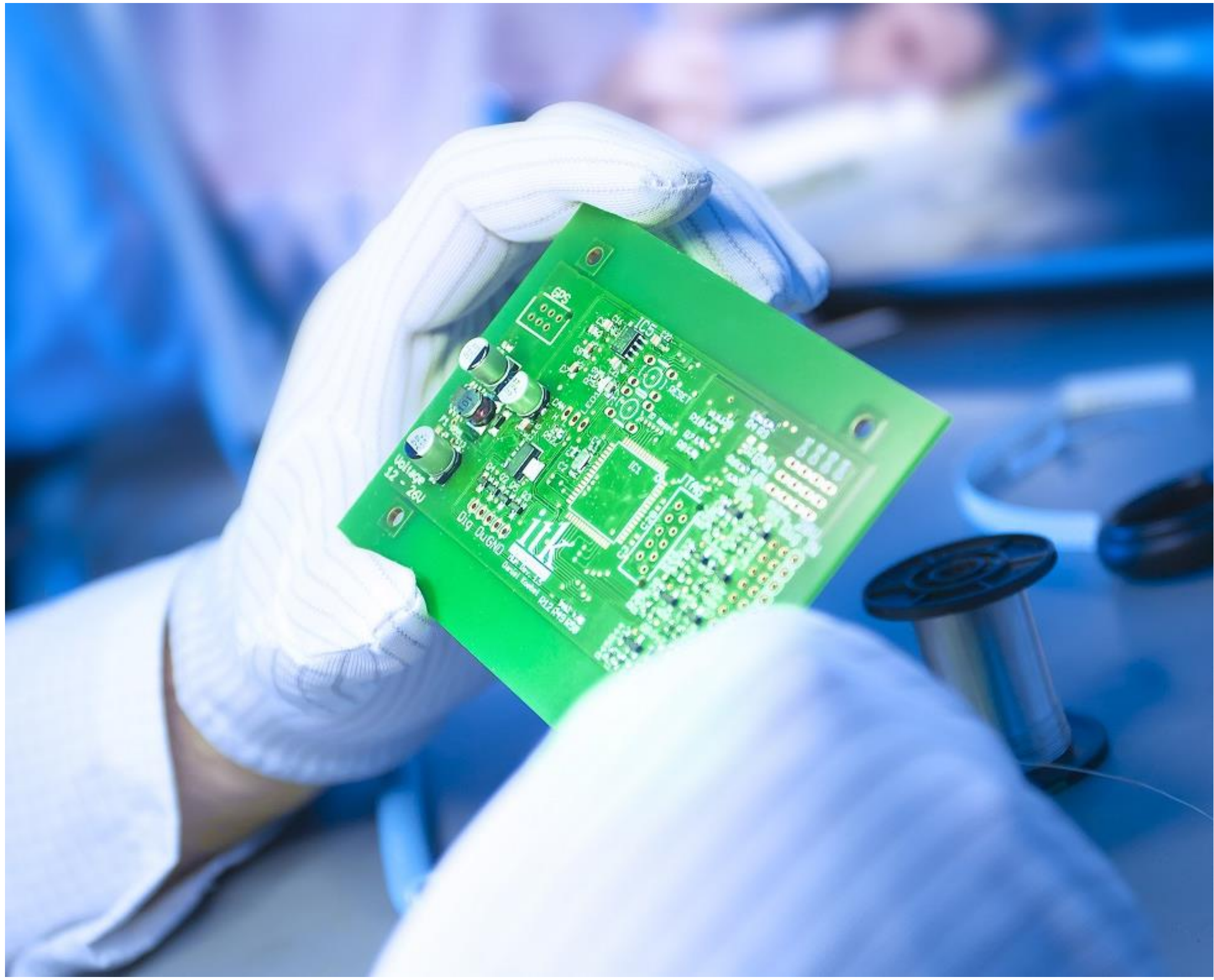
PITFALLS IN EMBEDDED SECURITY

EMBEDDED SECURITY

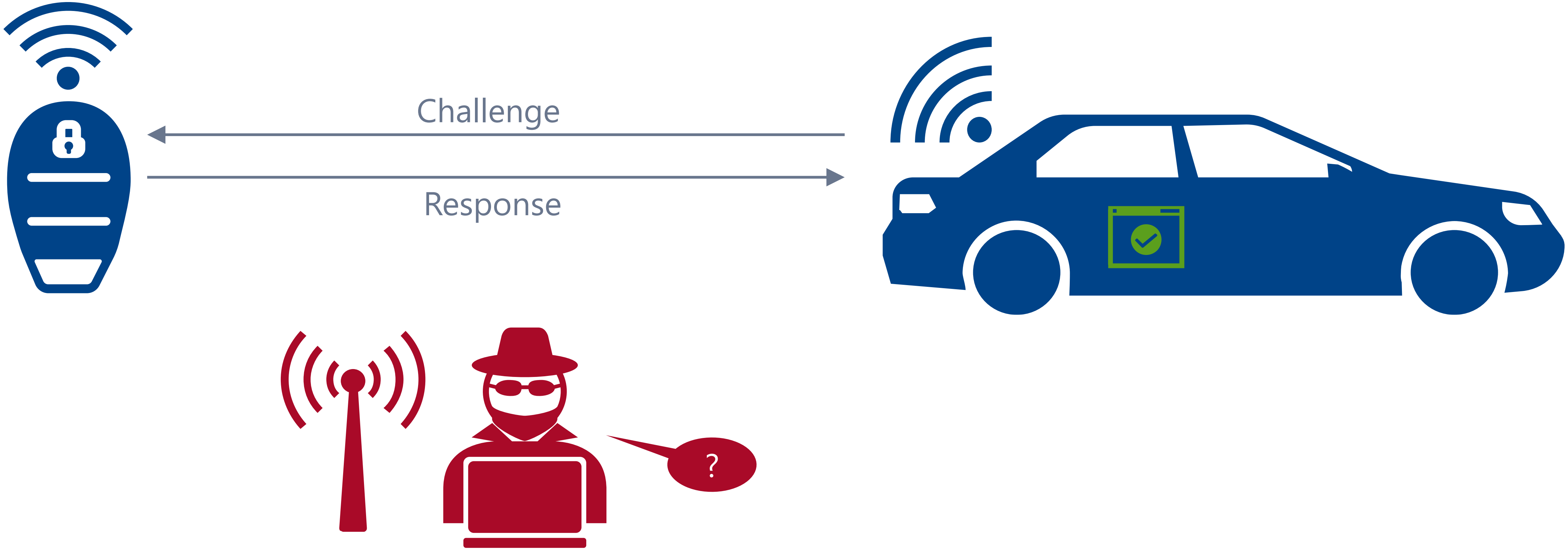
CHALLENGES

- Resource Limitations
  - Computational Power
  - Storage
  - Communication Bandwidth
- Easy Physical Access
- Physical Interaction with Environment
- Remote Controlling

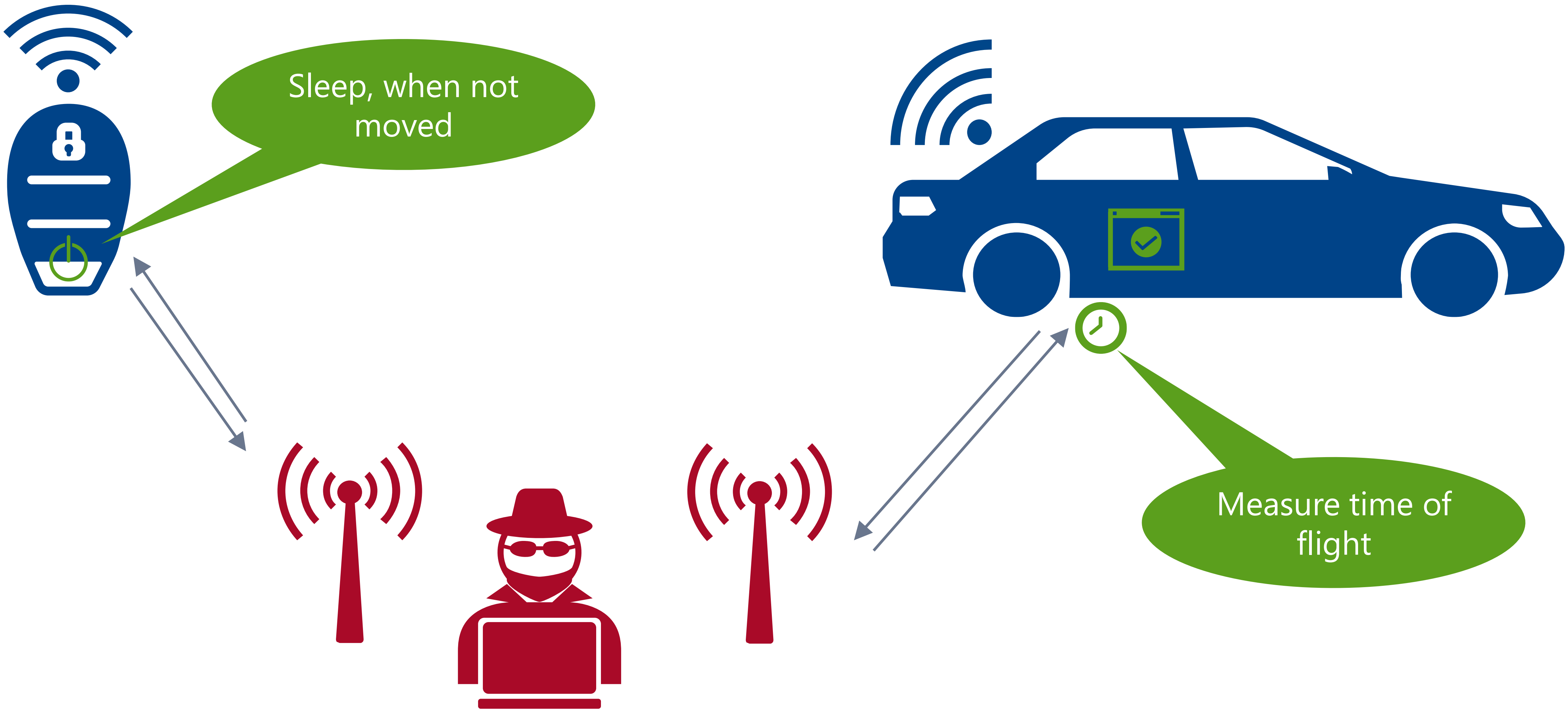


KEYLESS ENTRY

KEYLESS ENTRY

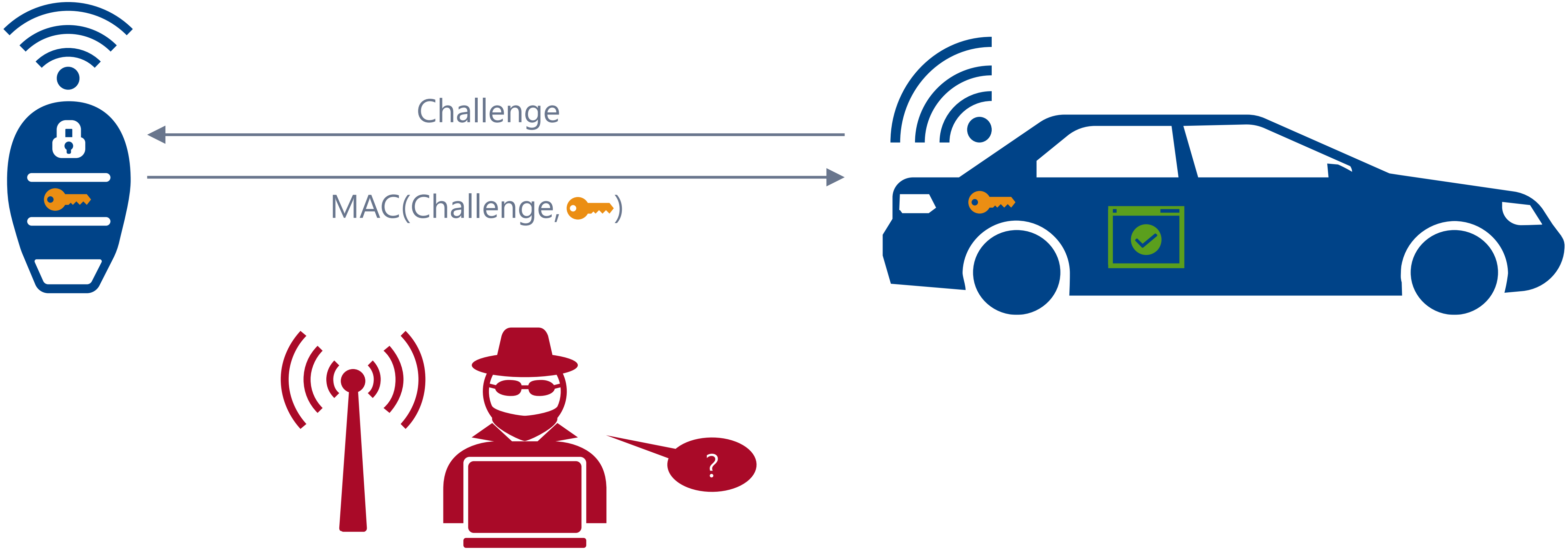


RELAY ATTACK

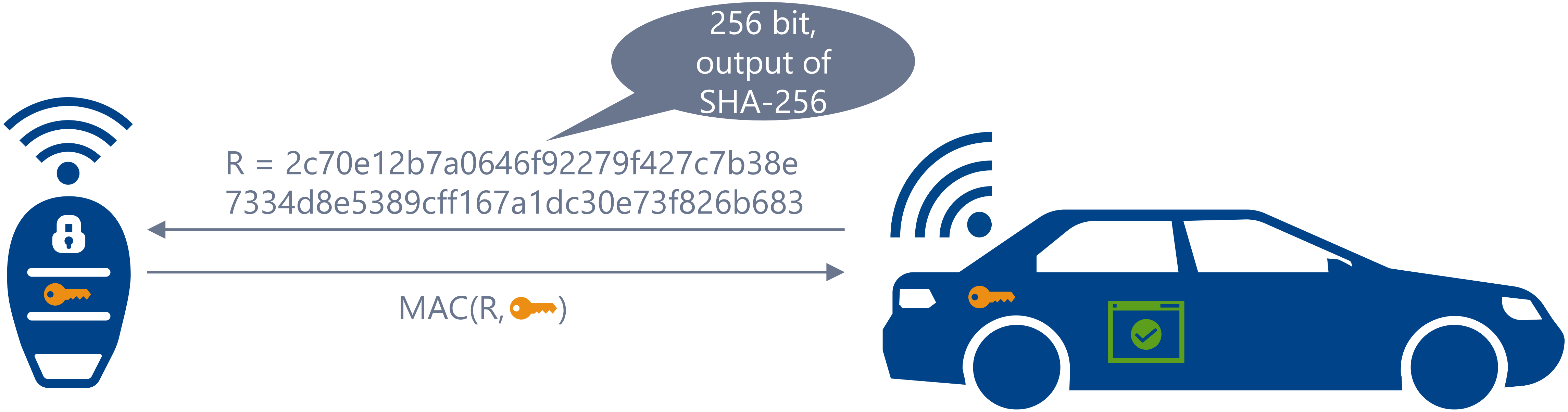

Sleep, when not moved

Measure time of flight

KEYLESS ENTRY



KEYLESS ENTRY



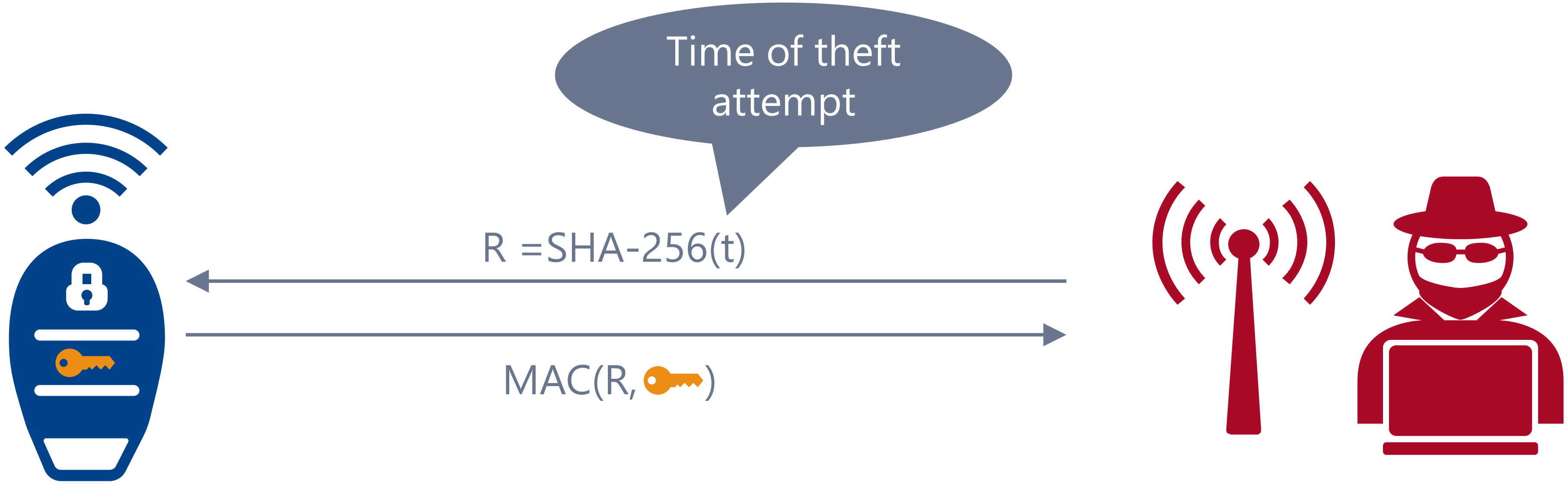
256 bit, output of SHA-256

R = 2c70e12b7a0646f92279f427c7b38e
7334d8e5389cff167a1dc30e73f826b683

MAC(R, 🔑)

```
t = time()
R = SHA-256(t)
```

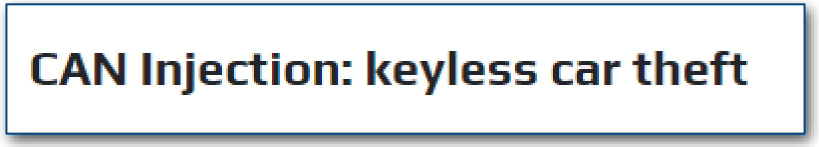
KEYLESS ENTRY



```
t = time()
R = SHA-256(t)
```

PHYSICAL ACCESS

CAN INJECTION



CAN Injection: keyless car theft

[CAN Injection: keyless car theft | Dr. Ken Tindell]

IOT SECURITY

Thieves Use CAN Injection Hack to Steal Cars

An innocent-looking portable speaker can hide a hacking device that launches CAN injection attacks, which have been used to steal cars.

[https://www.securityweek.com/thieves-use-can-injection-hack-to-steal-cars/]

KICKING THE CAN —

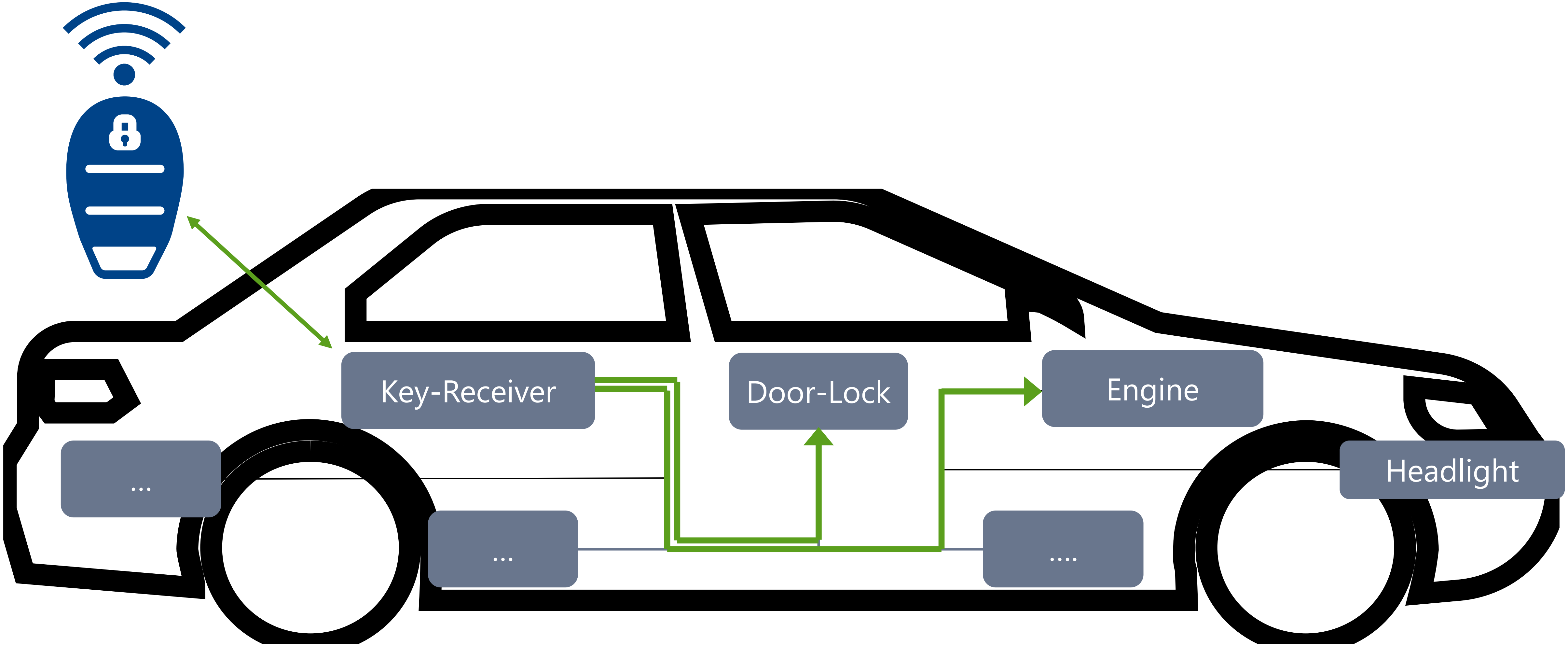
There's a new form of keyless car theft that works in under 2 minutes

As car owners grow hip to one form of theft, crooks are turning to new ones.

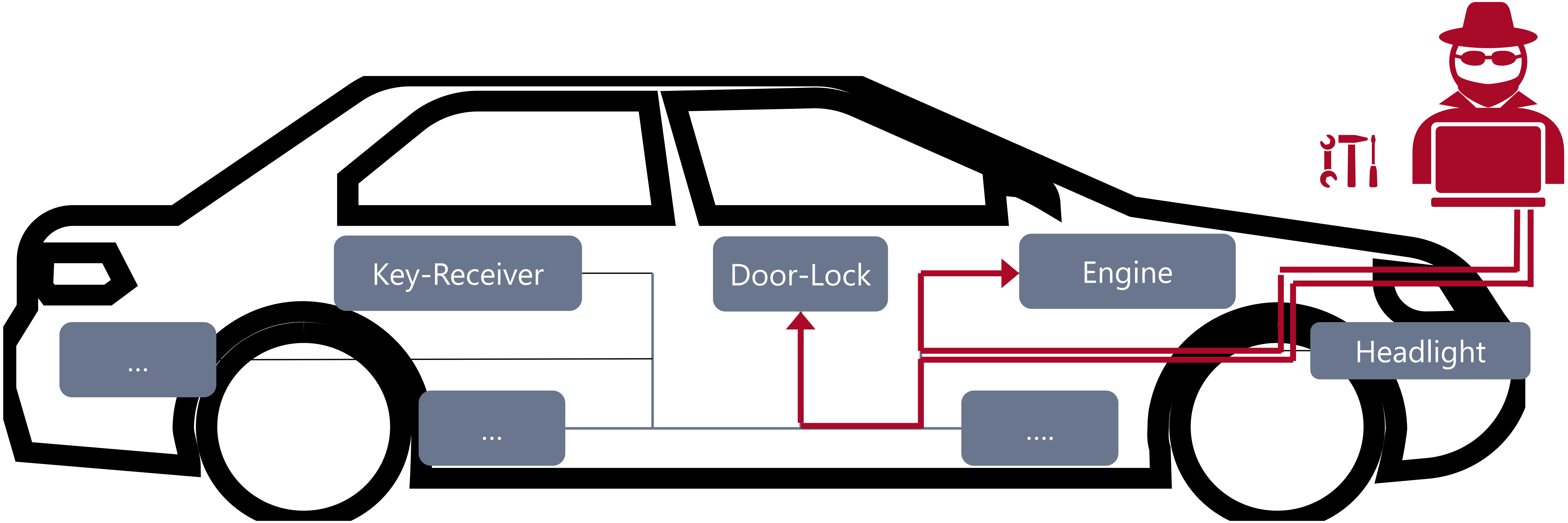
DAN GOODIN - 4/7/2023, 11:24 PM

[https://arstechnica.com/information-technology/2023/04/crooks-are-stealing-cars-using-previously-unknown-keyless-can-injection-attacks/]

CAN INJECTION

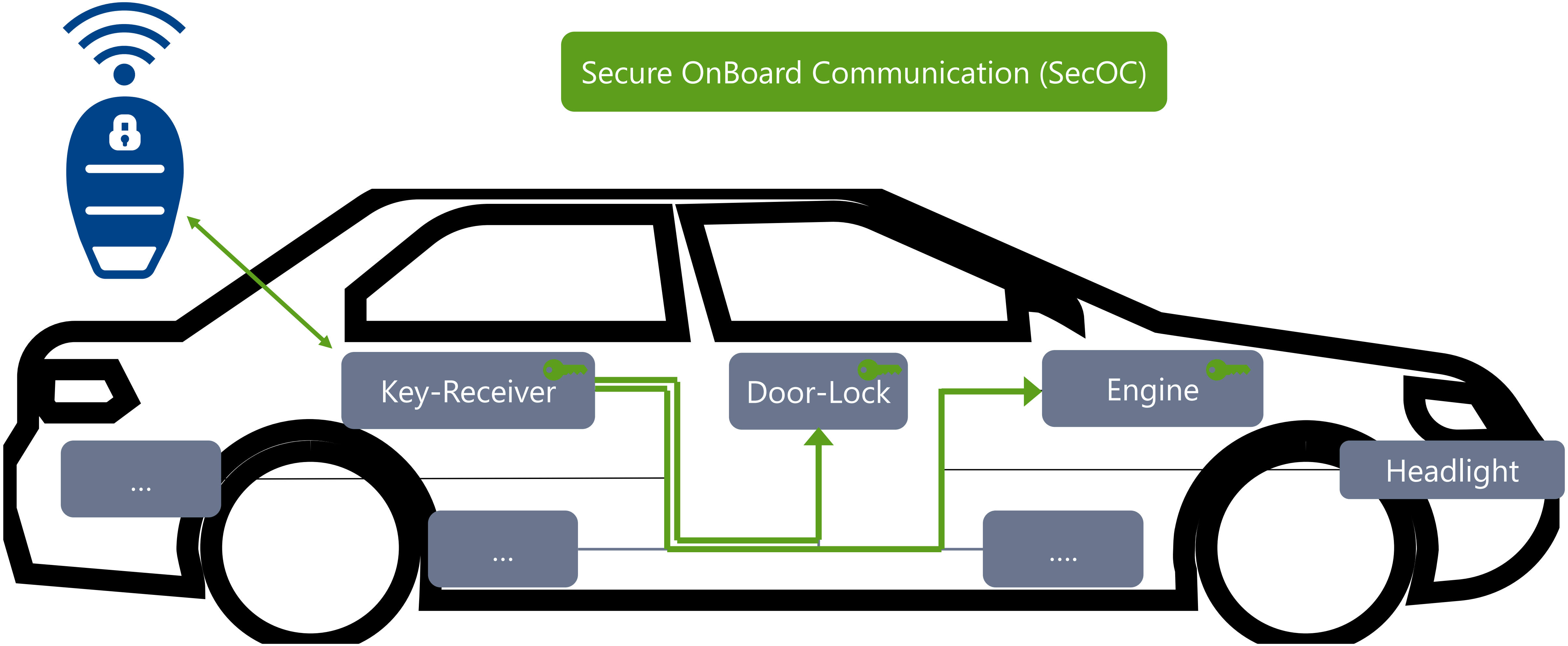


CAN INJECTION

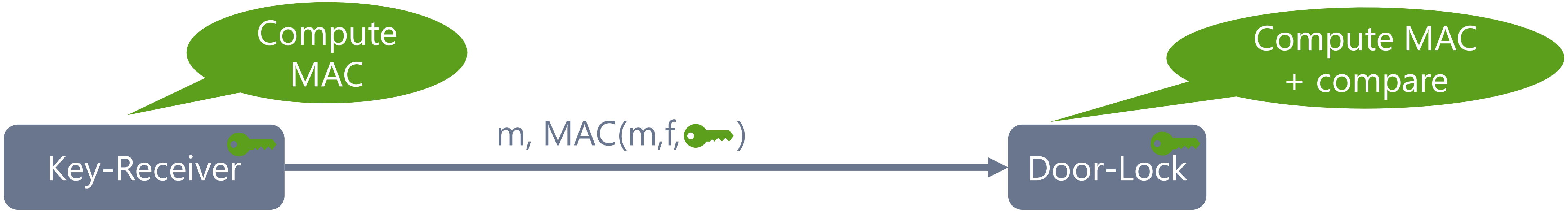


CAN INJECTION

Secure OnBoard Communication (SecOC)



SECURE ONBOARD COMMUNICATION (SECOC)

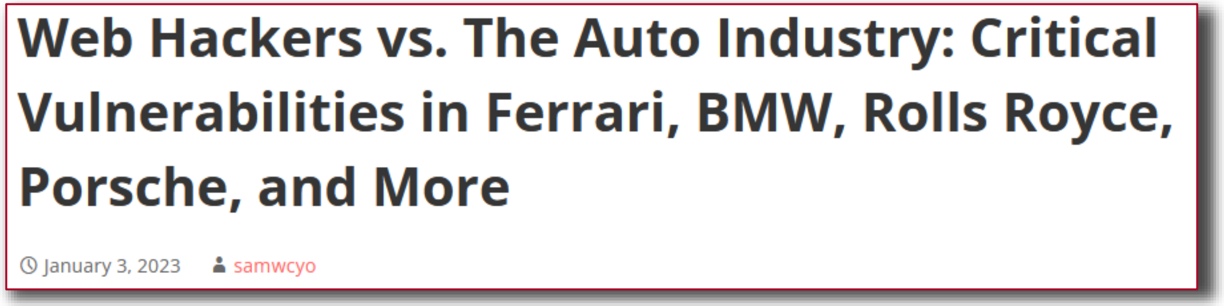


- Pre-shared **symmetric** cryptographic keys
  - Asymmetric cryptography to slow!
- Computation of MAC for every message
- Freshness value
  - Prevent replay attacks

- Practical Issues:
  - How many different keys does an ECU need?
  - How are keys managed if an ECU is replaced?
  - How are the freshness values synchronized?
  - The messages with MAC are too long!

REMOTE COMMUNICATION

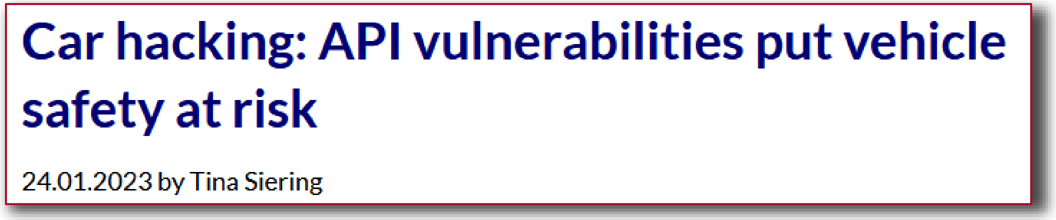
BACKEND HACK



Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More

January 3, 2023 samwcyo

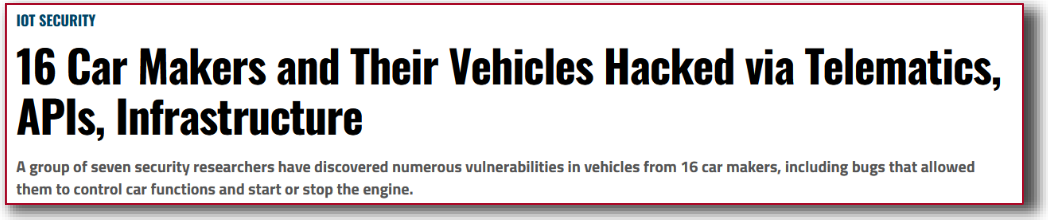
[https://samcurry.net/web-hackers-vs-the-auto-industry]



Car hacking: API vulnerabilities put vehicle safety at risk

24.01.2023 by Tina Siering

[https://www.secion.de/en/blog/blog-details/car-hacking-api-vulnerabilities-put-vehicle-safety-at-risk]



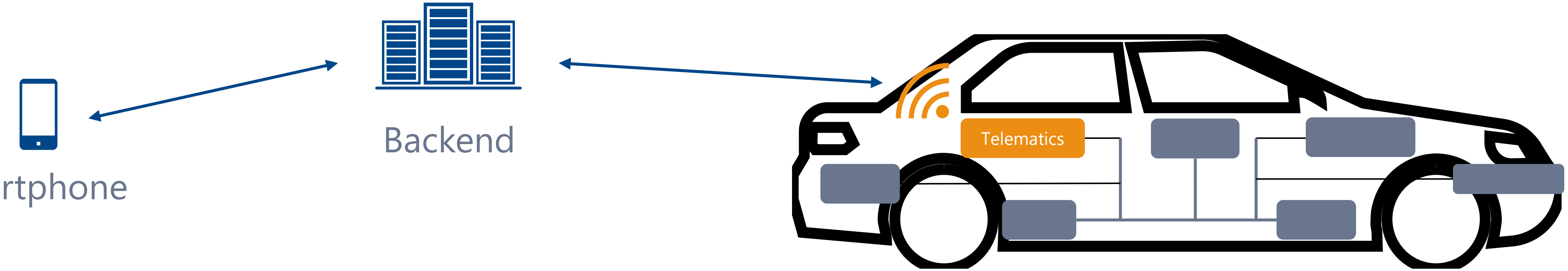
IOT SECURITY

16 Car Makers and Their Vehicles Hacked via Telematics, APIs, Infrastructure

A group of seven security researchers have discovered numerous vulnerabilities in vehicles from 16 car makers, including bugs that allowed them to control car functions and start or stop the engine.

[https://www.securityweek.com/16-car-makers-and-their-vehicles-hacked-telematics-apis-infrastructure]

REMOTE COMMUNICATION



Smartphone

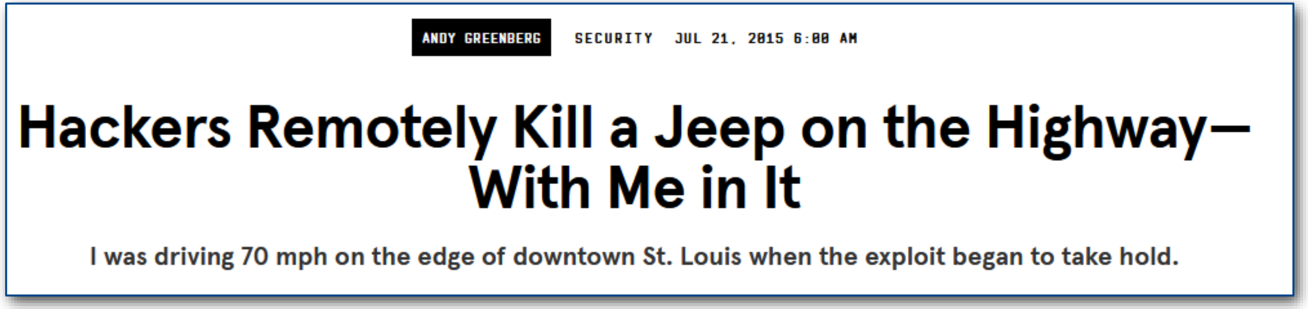
Backend

Telematics

- Remote control vehicle functions available via API
  - Lock/unlock door
  - Start/stop engine
  - Honk/flash lights

- Locate vehicle (GPS)
- Obtain driving statistics
- Lock out owner of remote control
- Flash/Update Firmware

Taking it one step further



ANDY GREENBERG SECURITY JUL 21, 2015 6:00 AM

Hackers Remotely Kill a Jeep on the Highway—With Me in It

I was driving 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

TAKE AWAY MESSAGES

TAKE-AWAY MESSAGES

- Consider cryptographic needs when selecting hardware
- If applicable, consider attacks with direct physical access
- Secure backends and mobile applications (and carefully select the features available through APIs)

OUR CYBERSECURITY SERVICES

From requirement elicitation to testing

Ignition-phase security services:

Cybersecurity Check Up

How secure is my product / company?

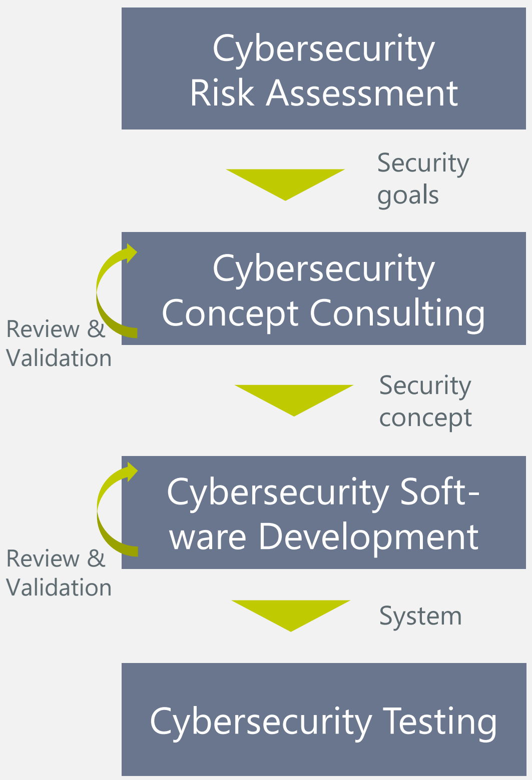
(e.g., assessment of current product / concept / process security state)

Baseline Cybersecurity Concept

How to make my architecture "security-ready?"

(e.g., identification of hardware requirements, crypto benchmarking, security-by-design)

Product security services:



Cybersecurity Risk Assessment

Security goals

Cybersecurity Concept Consulting

Review & Validation

Security concept

Cybersecurity Software Development

Review & Validation

System

Cybersecurity Testing

What does "secure" mean in my system?

(e.g., damage-scenario identification, attack-tree modeling, risk analysis)

Which security mechanisms have to be put in place?

(e.g., secure onboard communication, secure boot)

How to implement security mechanisms securely?

(e.g., cryptographic library integration, HSM integration, secure code hardening)

Are there attack vectors that were missing?

(e.g., penetration testing, fuzz testing)

Enabler Services:

Cybersecurity Trainings

How to enable my company to deal with security?

Training: Basics of Security Engineering
Training: Secure Coding in C

Cybersecurity Process Consulting

How to establish a security process in my company?

(e.g., ISO/SAE 21434, safety-security interaction)

THANK YOU

Dr. techn. Niklas Grimm

niklas.grimm@itk-engineering.com