

# Is my car secure?

April 18th, 2018

---

**Alexander Meisel**

*Dipl. Inf. (FH) (computer scientist), GENIVI Alliance*



# Recent news




# Keyless car theft / relay attack vector

- **2010** – Research:  
<https://eprint.iacr.org/2010/332.pdf>
- **Jan 2011** – Media attention:  
<http://www.zeit.de/auto/2011-01/auto-diebstahl>
- **Oct 2011** – First patent to solve relay attacks:  
<https://patents.google.com/patent/US20140240090A1/en>
- **Jan 2013** – First video of relay attack:  
<https://www.youtube.com/watch?v=I7OadDz3Ums>
- **2014 - 2016** – Theft technology gets adapted to all car brands
- **Since 2017** – This is the favourite way of stealing luxury cars

# Keyless car theft / relay attack vector

- Buy yours here:

<https://codegrabber.ru/specdev/LongDistance>



**Universal Keyless Radio Code Grabber Long Distance Device ver. PRO**  
Product Code: Long Distance  
Availability: In Stock  
**Price: €12 000.00**

Qty:

[Add to Cart](#)

Description [Reviews \(0\)](#)

ALL OF THE CARS EQUIPPED WITH KEYLESS GO!

«WAVE 4» v1.3 is a low distance, low price, fully automatic and compact version of «WAVE 1». It makes a "bridge" between the car and its key.

«Answer» signal to the car comes directly from the key (distance can vary from 15m up to 100m and depends on key type and battery condition inside the key), and allows you to open a doors and start a car.

*Warning!!! Device is not intended for illegal use !!!!*

Tested on:

- Mercedes W222 2015
- Mercedes X164 2014
- Range Rover Evogue 2017
- Range Rover Vogue 2016
- TOYOTA LC200 2016
- LEXUS LX 570 2016 (update required)
- MAZDA CX-5 2015
- KIA Sorento 2014
- BMW 530D 2014
- Porsche Cayenne GTS 2016
- TESLA S

# Attack surface

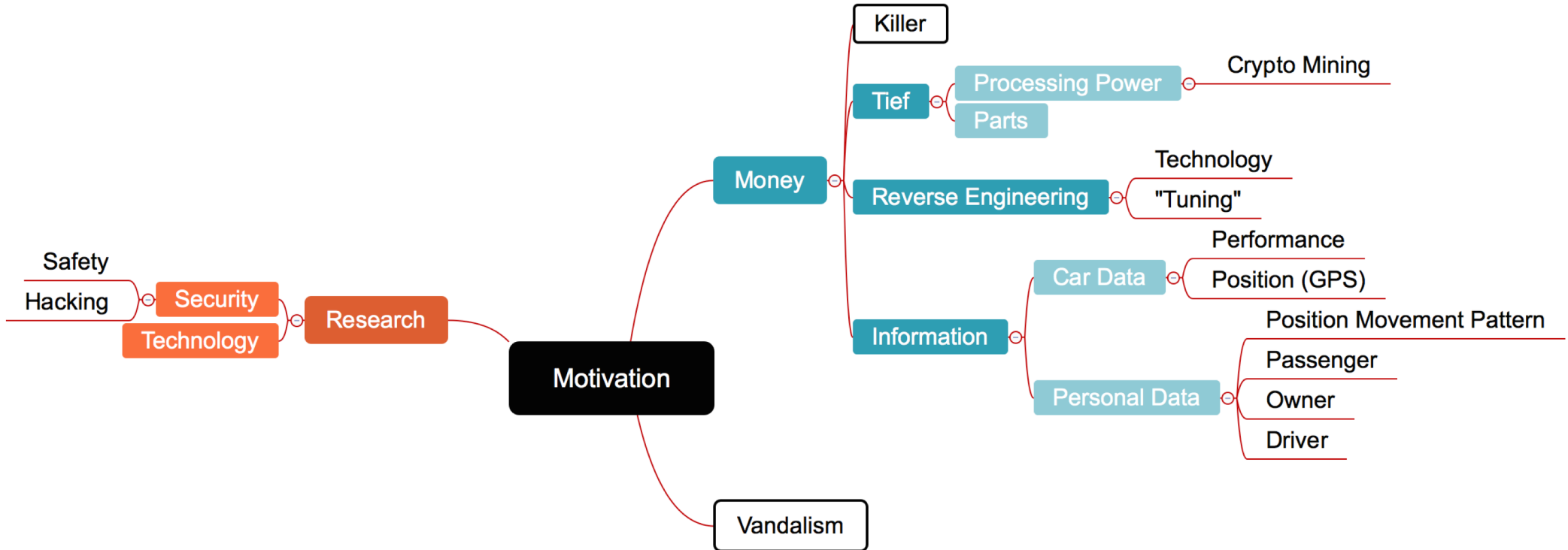
## Over the Air

- Short Range:
  - Wifi / Bluetooth
  - Keyless Entry
  - Tire Pressure Monitoring System (TPMS)
- Long Range:
  - Telematics
  - Backend Connections (Datacenter)

## Physical

- On Board Diagnose (ODB2)
- USB / CD / Mobile Phone
- Key

# Attackers' motivation



# Complexity is the greatest enemy of security



# Security Precautions

- Boot Integrity
- Secure Update (over the air)
- Device Identification / Authentication / Authorization
- Communication Proxies
- Message Security
- Secure Storage  
(Data at rest, Credential Management)



# Security Precautions

- Continuous Audit
- Network Enforcement
- Adapting Risk / Threat evaluation
- Secure Coding (Best) Practices
- Privacy
- Legacy & Obsolence Management

# Risk Modeling



# Step 1: Decompose

- What parts are interacting with other systems?
- Which of those entry points can be used by the attacker?
  - What is interesting to the attacker?  
(Trust Levels, Authentication / Authorisation helps)
- Create Data Flow Diagrams and highlight privilege boundaries

## Step 2: Rank threats

- Identify threat targets from attacker points of view
  - Data sources (filesystem, DB, ...)
  - Processes
  - Interaction with users
- Identify threat trees (use mind mapping methodology)
- Assign threat levels
  - Possible / Impossible
  - Cost (Effort) estimation

## Step 3: Countermeasures

1. Prioritize threats indentified in Step 2
2. Determine appropriate counter measures
  - a) Remove risk (fix it)
  - b) Take risk
    - a) Inform users / stakeholders
    - b) Make sure process is in place to deal with ,fallout' (Money!!!)
  - c) Do nothing
    - a) NO NO NO NO NO!!!
3. Assign cost in event of threat / attack is successfully exploited (business impact)

## Step 4: Document and Validate

- Document and validate all steps above
- Document who, when and what about was informed about the a particular threat
- Make sure in case of handing of task to other parties that they have deadline to work with

**Complex systems all go ...**





**BOOM!**



**Keep IT simple ...**



# Communication between ,things‘

Is the car a distributed (software) system?

– YES

When and why did it become so fragmented?

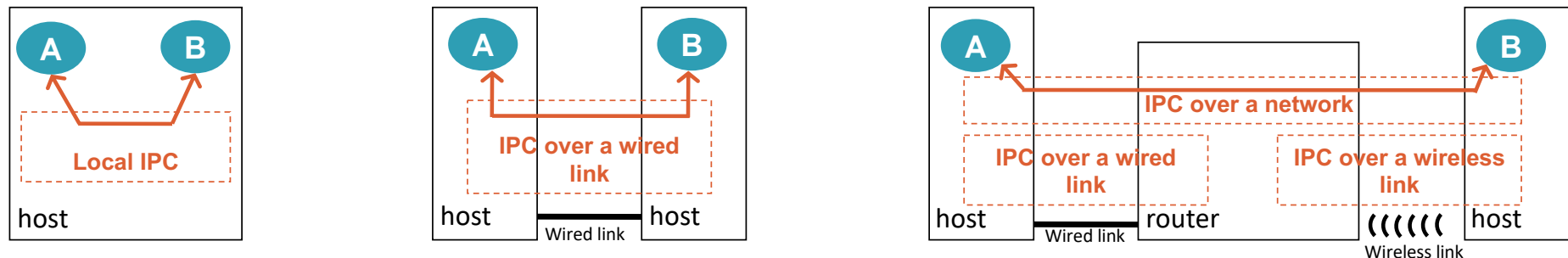
– It all started decades ago and because of new features which seemed easy to do (at the time) but have been piled on top of each other.

What is the common problem we face and what do we do to solve it?

– INTERPROCESS COMMUNICATION

# Back to the basics

- Networking = Inter process communication (IPC)

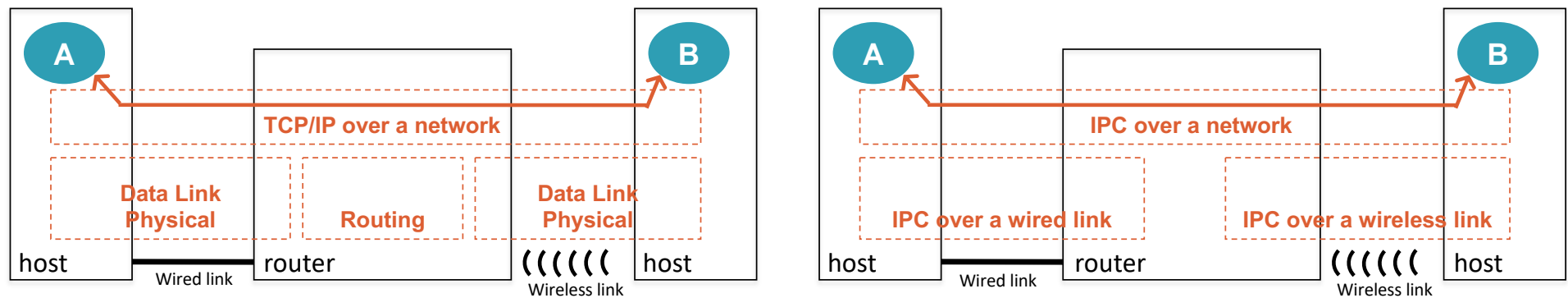


It is a **repeating structure**: distributed applications doing IPC at a bigger scope (network) use the services of distributed IPC at smaller scopes (link)

- **Recursive structure of distributed applications that do IPC!**
- The **mechanisms for doing IPC** in the different cases **are the same**, they just need a **different configuration**.

# So what's the difference then?

- TCP/IP vs RINA (Recursive InterNetwork Architecture)

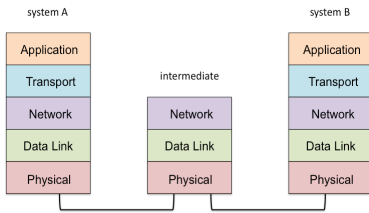


# RINA – What's the difference (extended)

TCP/IP

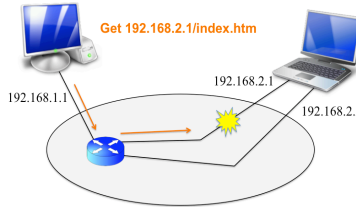
## What's different?

- Functional layering, where each layer has the responsibility of a different function
- Fixed number of layers

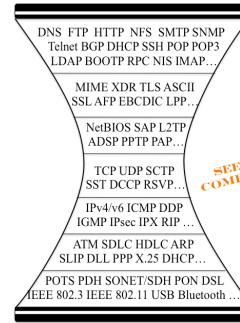


structure

- Routing on the interface (data link layer)
- Exposing addresses to applications
- Use of well-known ports
- Incomplete naming and addressing schema



routing



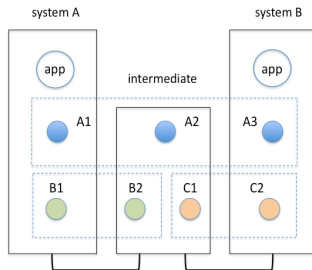
simplicity

- Lack of a security mechanism: A long list of threats and vulnerabilities
- Lack of a built-in mechanism to provide specific QoS: Only best effort service
- Exploding size of router tables
- Lack of a directory that maps applications to nodes

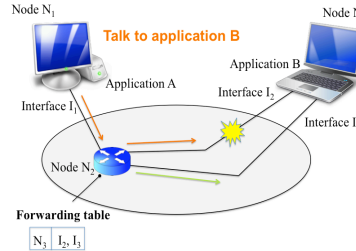
and more

RINA

- A layer (DIF) is a distributed application that provides IPC services over a given scope
- Relative number of layers, each layer manages a range of bandwidth and QoS
- DIFs recurse providing IPC services to each other

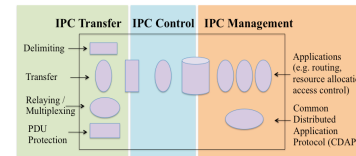


- Routing on the node
- A complete naming and addressing schema
- Applications have an independent namespace
- Mobility and multi-homing inherently



- Fundamental functions to provide communication
- Separation of mechanism and policy
- All layers use the same protocols but are configured differently through policy to achieve the desired service
- A single application protocol
- A single data transfer protocol

### What's inside an IPC layer?



- Joining a DIF requires authentication, addresses are not exposed to the applications, no well-known ports are used, which results to a more secure network
- Each DIF can support a set of QoS cubes and provides an API to allow applications to request service with certain QoS parameters
- Each DIF has its own private internal addresses, which means that a global address space is not required
- Names for applications, nodes and Points of Attachments to the network exist, as well as a directory, mapping applications to nodes

# Partners in digitalisation

 Experience design

 Mobile development

 Software engineering

 HMI & simulation

**intive**



 **intence**  
automotive electronics

 Smart solutions

 Artificial intelligence

 Driver assistance

 Products & tools

**Thank you!** | Alexander Meisel / [a.meisel@intence.de](mailto:a.meisel@intence.de)

# Thank you!

Visit GENIVI at <http://www.genivi.org> or <http://projects.genivi.org>

Contact us: [help@genivi.org](mailto:help@genivi.org)

GENIVI is a registered trademark of the GENIVI Alliance in the USA and other countries.  
Copyright © GENIVI Alliance 2018.

