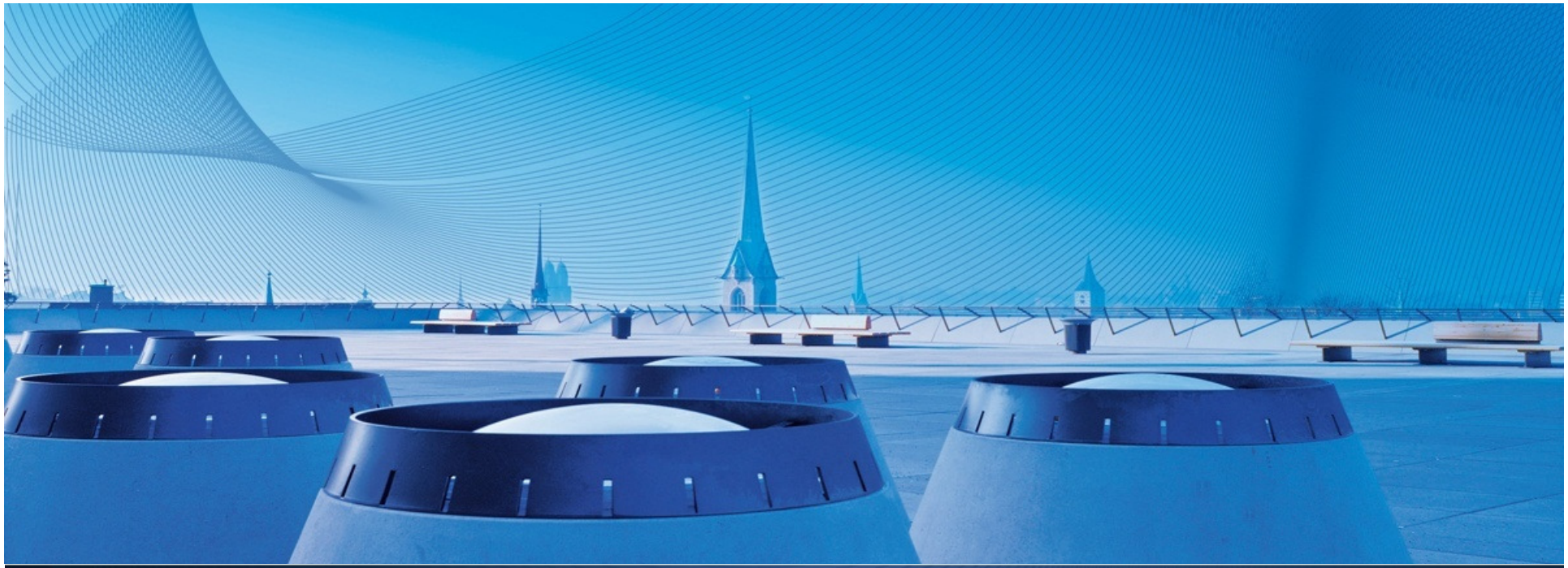
ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

inf | Informatik
Computer Science

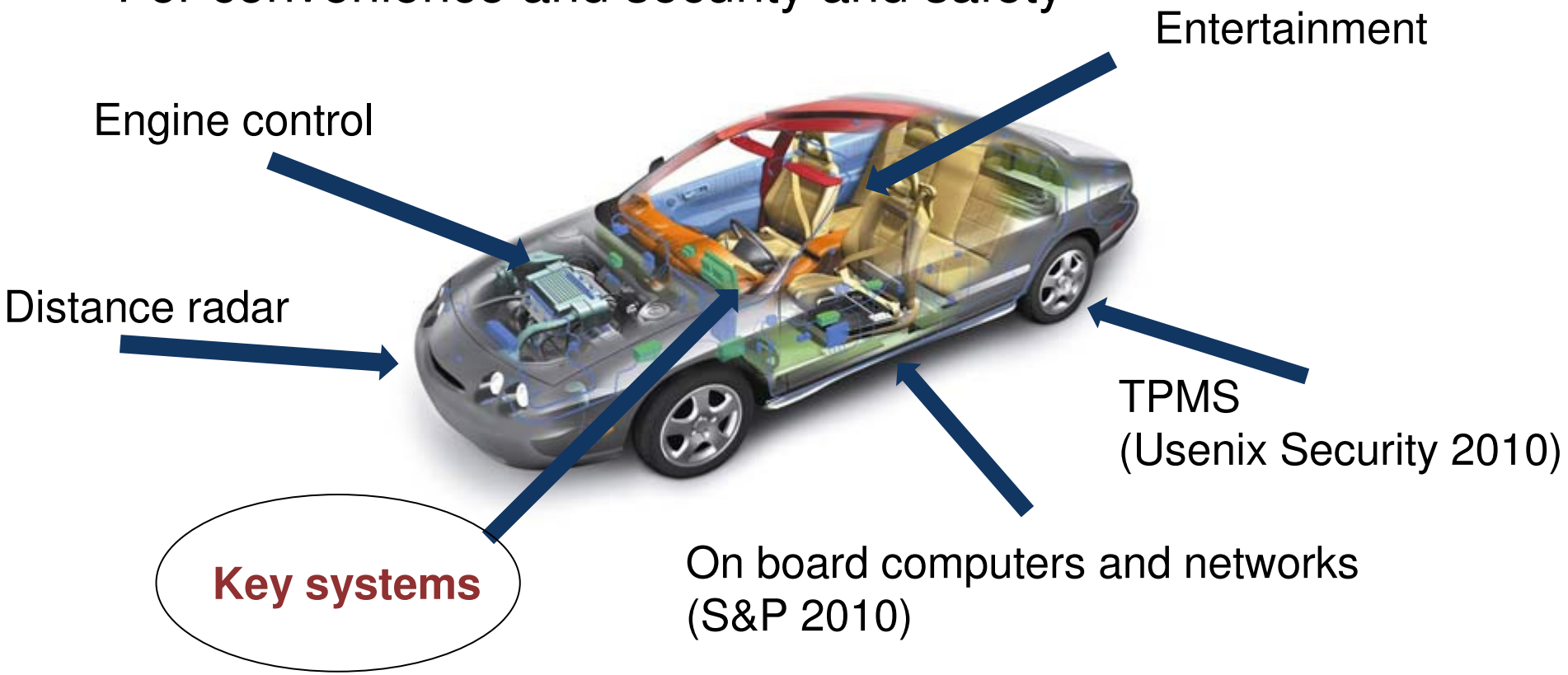
Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars

Aurélien Francillon, Boris Danev, Srdjan Čapkun



Modern Cars Evolution

- Increasing amount of electronics in cars
- For convenience and security and safety



Agenda

1. Overview of Car Key Systems
2. Passive Keyless Entry and Start Systems
3. Relay Attacks
4. Analysis on 10 models
5. Conclusion

4 Categories of Key Systems

- Metallic key
- Remote active open
- Immobilizer chips
- Passive Keyless Entry and Start

Car Keys Active Remote Open

- **Active keys:**
  - Press a button to open the car
  - Physical key to start the car
  - Need to be close (<100m)

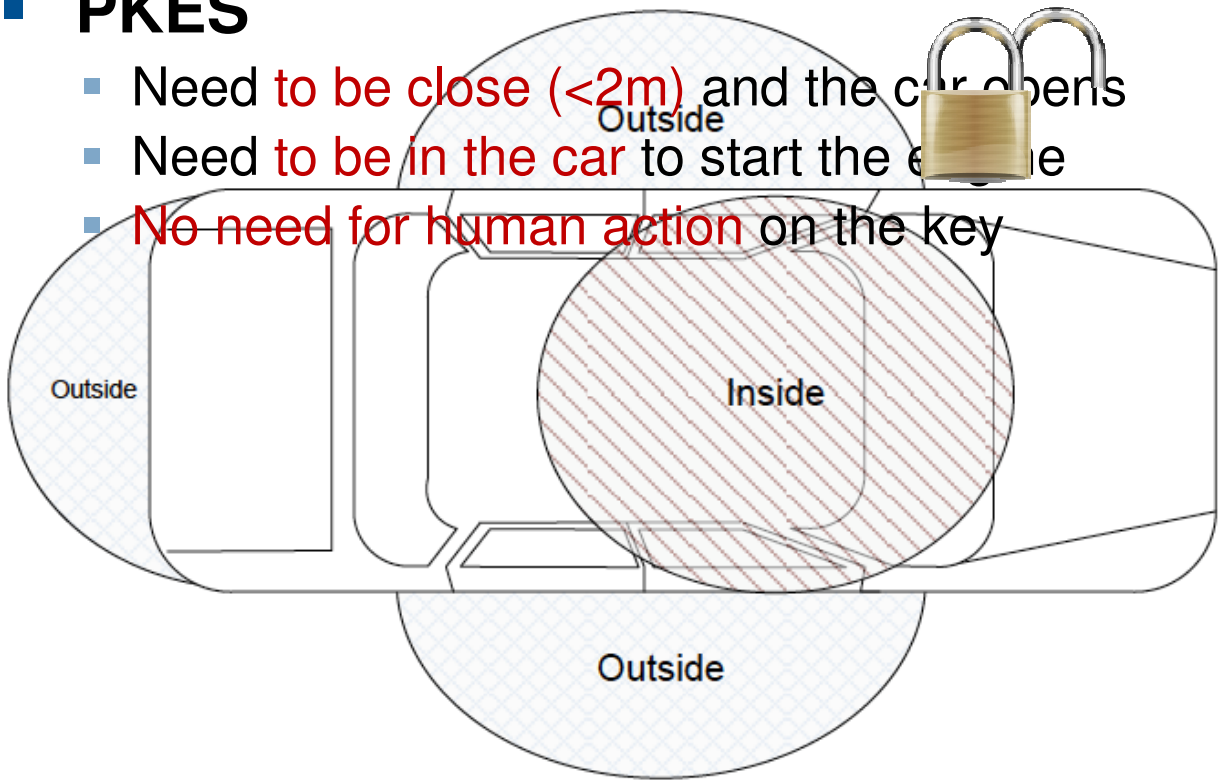
- Shared cryptographic key between the key and the car
- Previous attacks: weak crytpography
  - e.g. Keeloq (Eurocrypt 2008, Crypto 2008, Africacrypt 2009)

Keys With Immobilizer Chips

- **Immobilizer chips**
  - Passive RFID
  - Authorizes to start the engine
  - Close proximity: centimeters
- Are present in most cars today
  - With metallic key
  - With remote open
- Shared cryptographic key between the key and the car
- Previous attacks: weak cryptography
  - e.g. TI DST Usenix Security 2005

Passive Keyless Entry and Start

- **PKES**
  - Need to be close (<2m) and the car opens
  - Need to be in the car to start the engine
  - No need for human action on the key



Passive Keyless Entry and Start

1. Periodic scan (LF)

2. Acknowledge proximity (UHF)

3. Car ID || Challenge (LF)

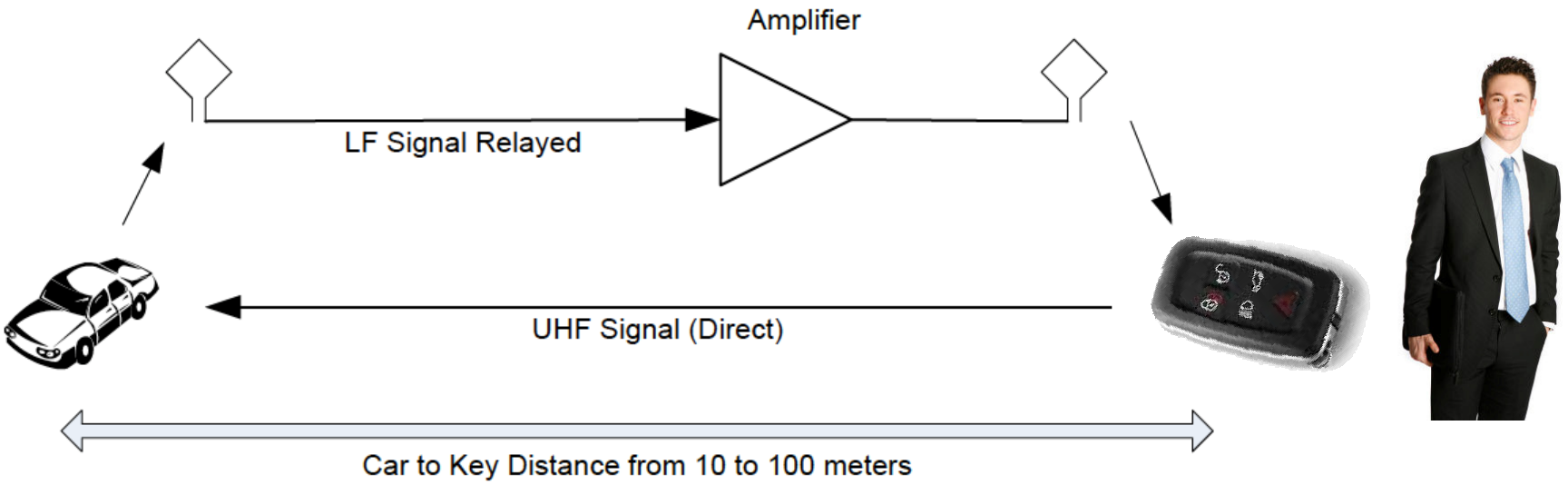
4. Key Response (UHF)

→	LF (120 – 135 KHz),	(1-2 meters)
←	UHF (315 – 433 MHz),	(50-100 meters)

Main Idea of PKES systems

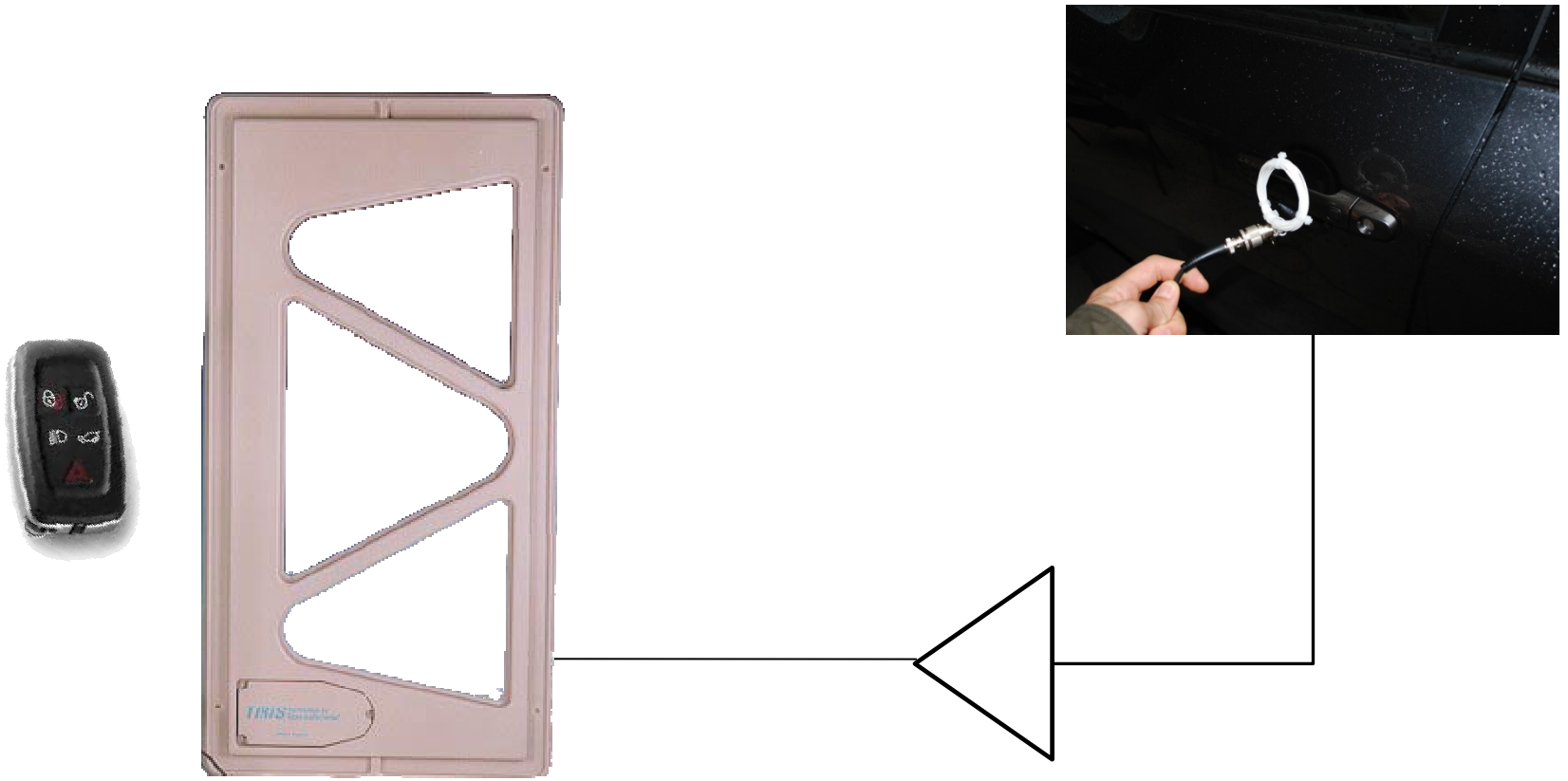
- Cryptographic key authentication with challenge response
  - Replaying old signals impossible
  - Timeouts, freshness
- Car to Key: inductive low frequency signals
  - Signal strength ~ d^{-3}
- Physical proximity
  - Detected by reception of messages
  - Induced in key's antenna
- The system is vulnerable to relay attacks

Relay-over-cable Attack on PKES

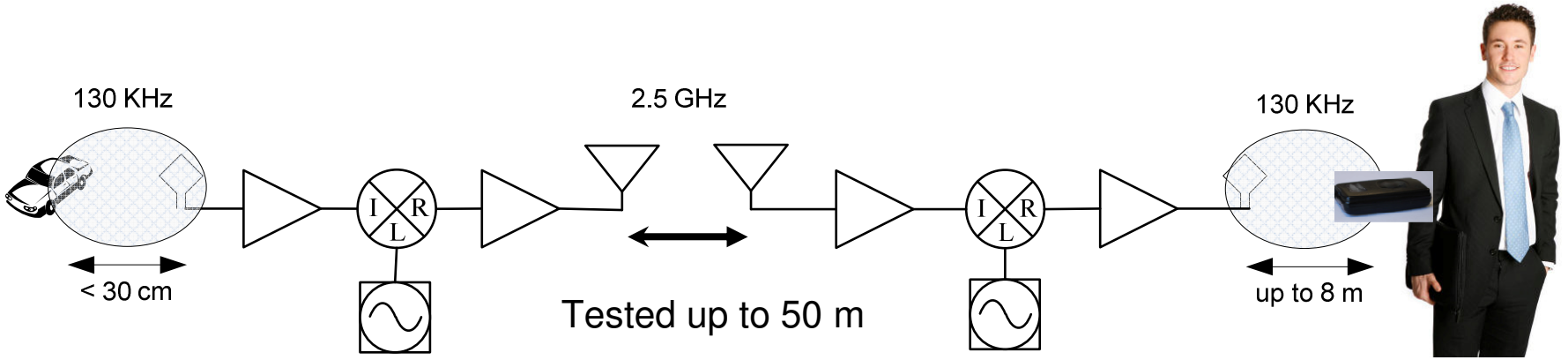


- Very low cost attack (~50€)
- Authentication do not prevent it

Physical Layer Relay With Cable

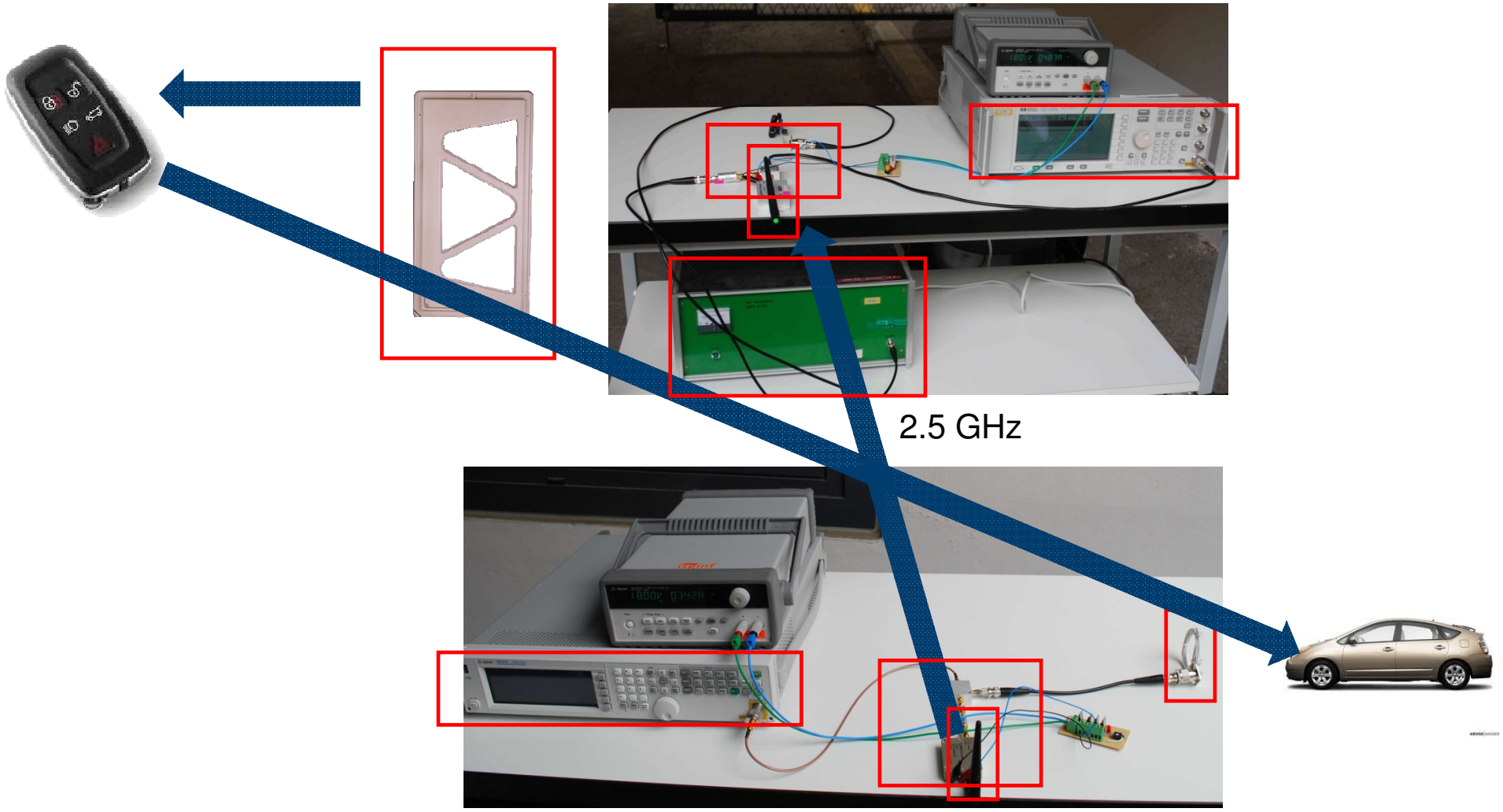


Relay Over the Air Attack



- Higher cost, (~1000 $)
- Fast and difficult to detect
- Authentication do not prevent it

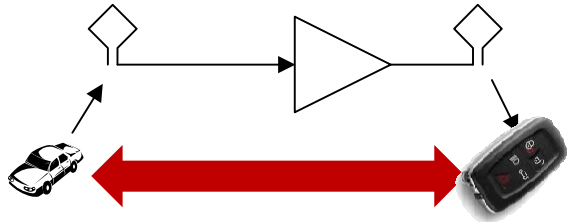
Physical Layer Wireless Relay



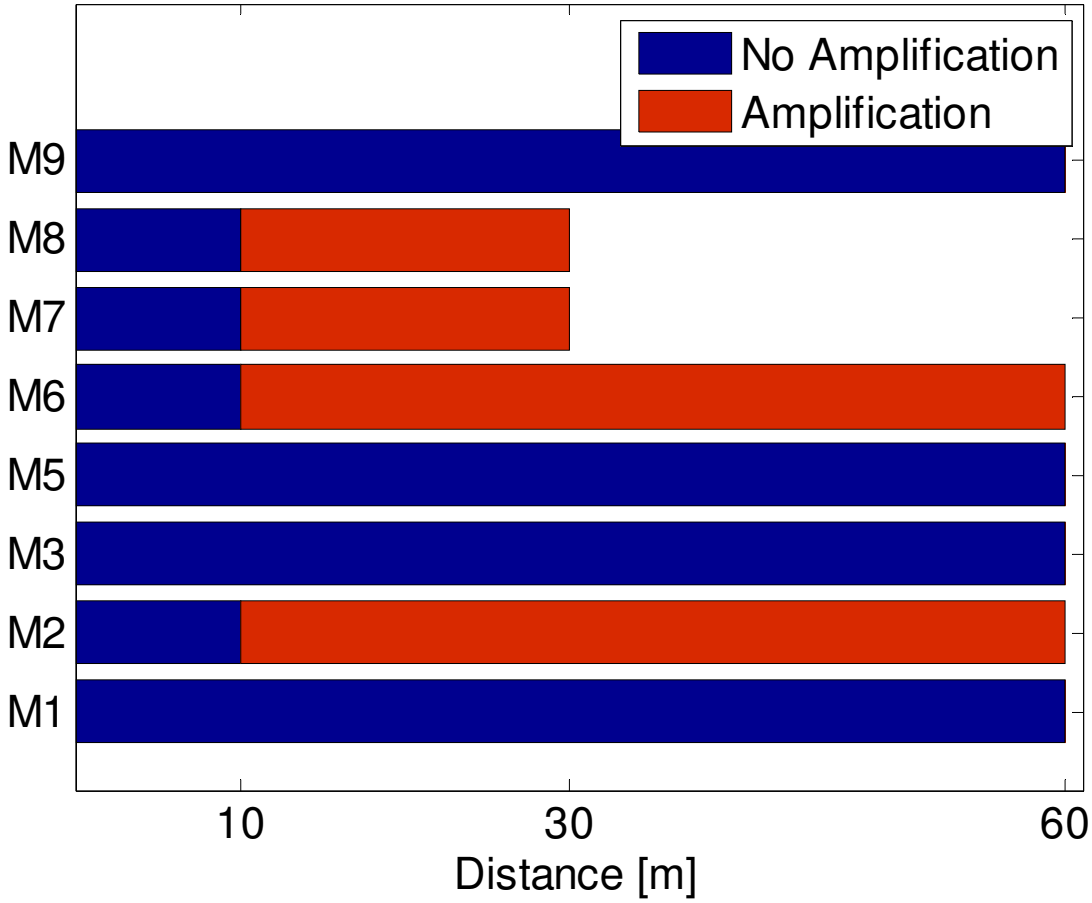
Analysis on 10 Models

- Car models with PKES
  - 10 models from 8 manufacturers
  - All use LF/UHF technology
- None uses the exact same protocol
  - Form recorded traces
- Some use longer messages
  - Strong crypto?

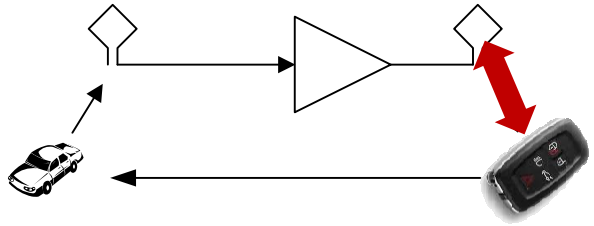
Relay Over Cable vs. Model

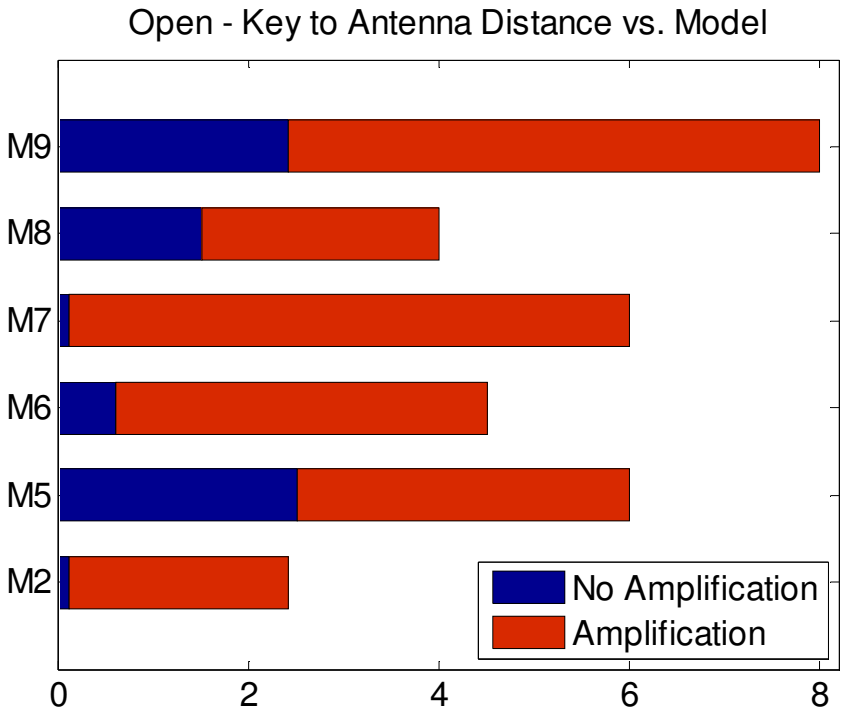


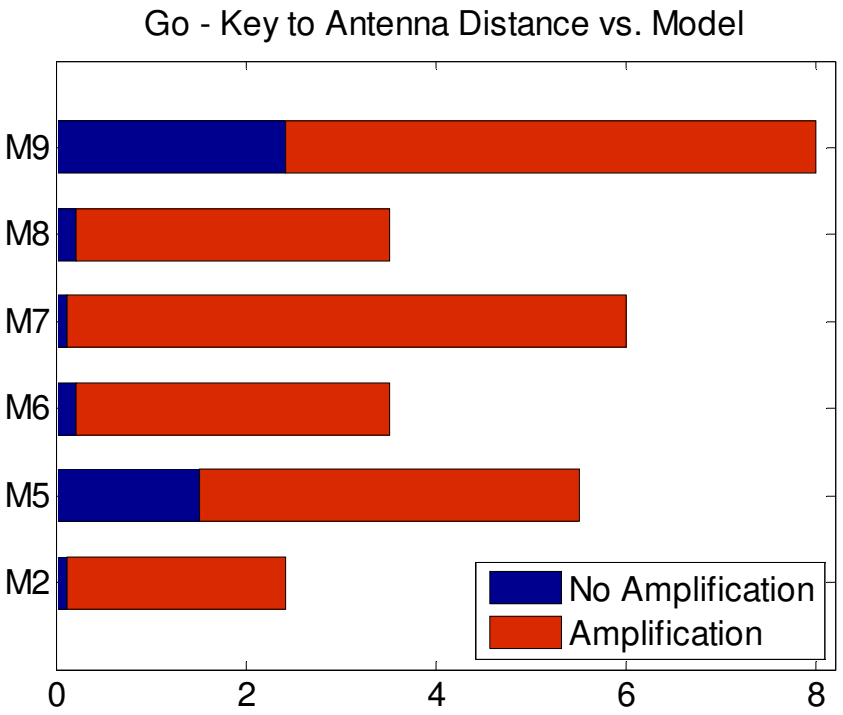
- Cables
  - 10, 30 and 60m
- Longer distances
  - Depend on the setup



Key to Antenna Distance







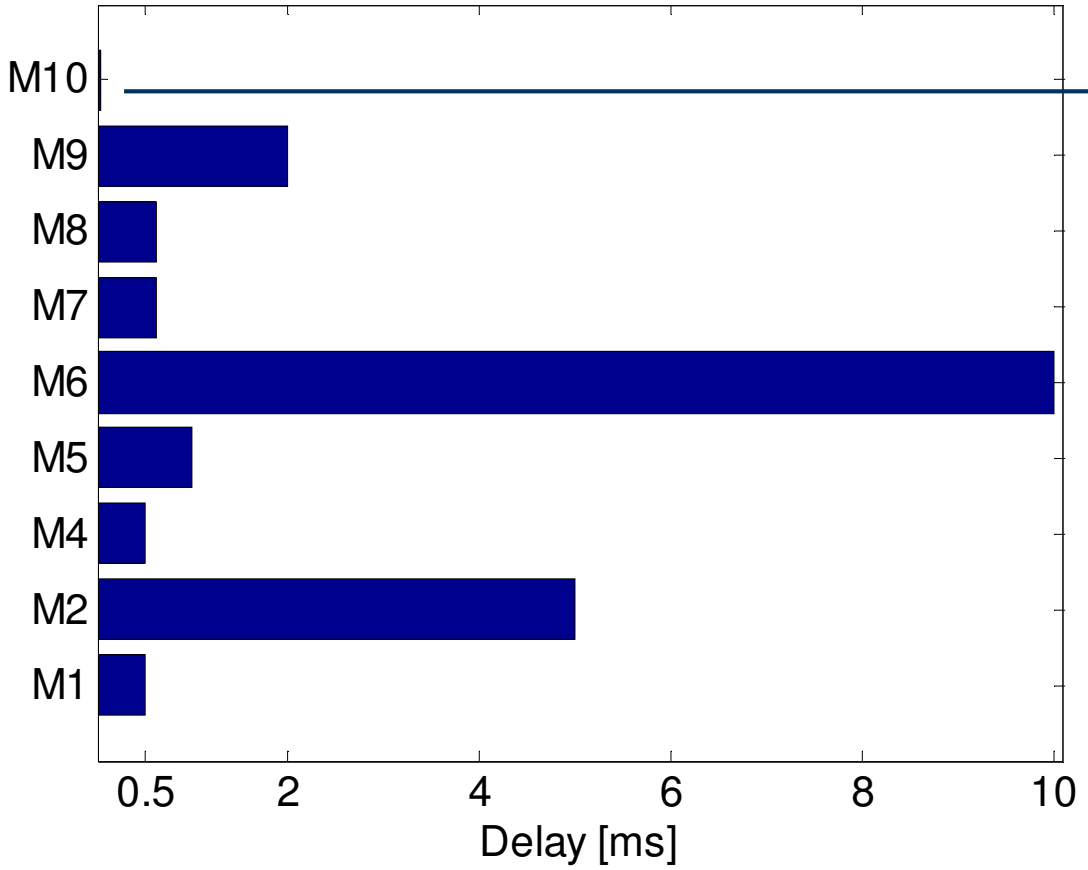
How Much Delay is Accepted by the Car ?

- The maximum distance of relay depends on
  - Acceptable delay
  - Speed of radio waves (~ speed of light)
- Possibility to relay at higher levels ?
  - E.g. relay over IP ?
- To know that we need to delay radio signals
  - Various lengths of cable: not practical
  - Scope/signal generator: too slow
  - Software Defined Radios: still too slow

Inserting a Tunable Delay

- We used a Software Defined Radio: USRP/Gnuradio
- Minimum delay 15ms
  - Samples processed by a computer
  - Delays added by the USB bus
- We modified the USRP's FPGA to add tunable delays
  - From 5µs to 10ms
  - Buffering samples on the device
  - Samples directly replayed
    - Without processing on the computer

Maximum Accepted Delay vs. Model



35 µs => 5 Km

10 ms => 1500 Km

- Non physical layer relays difficult with most models

Implications of The Attack

- Relay on a parking lot
  - One antenna near the elevator
  - Attacker at the car while car owner waits for the elevator

- Keys in locked house, car parked in front of the house
  - E.g. keys left on the kitchen table
  - Put an antenna close to the window,
  - Open and start the car without entering the house
  - Tested in practice

Additionnal Insights

- When started the car can be driven away without maintaining the relay
  - It would be dangerous to stop the car when the key is not available anymore
  - Some beep, some limit speed
- No trace of entry/start
- Legal / Insurance issues

Countermeasures

- Immediate protection mechanisms
  - Shield the key
  - Remove the battery
- Seriously reduces the convenience of use

- Long term
  - Build a secure system that securely verifies proximity

- e.g. : Realization of RF Distance bounding
  - Usenix Security 2010

Still some challenges to address before a usable system

Conclusion

- This is a simple concept, yet extremely efficient attack
  - Real world use of physical layer relay attacks
  - Relays at physical layer are extremely fast, efficient
- All tested systems so far are vulnerable
- Completely independent of
  - Protocols, authentication, encryption
- Techniques to perform secure distance measurement are required, on a budget
  - Still an open problem

Questions ?

Contact : Aurélien Francillon aurelien.francillon@inf.ethz.ch
Boris Danev bdanev@inf.ethz.ch
Srdjan Capkun capkuns@inf.ethz.ch