Corroding immobilizer cryptography

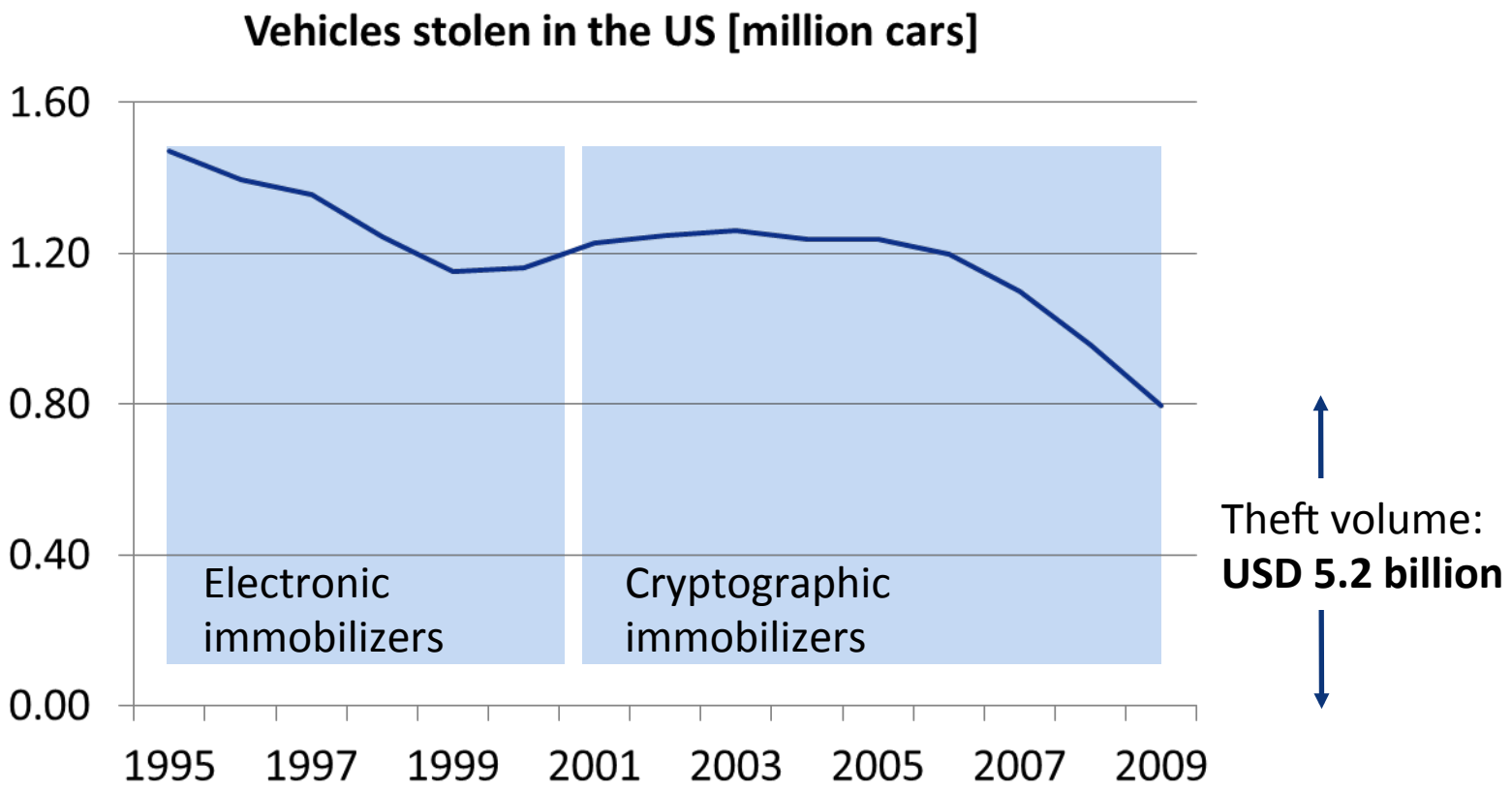
Karsten Nohl <nohl@srlabs.de>

Agenda

- **Immobilizer introduction**
- Cryptographic vulnerabilities
- Secure car protection gap

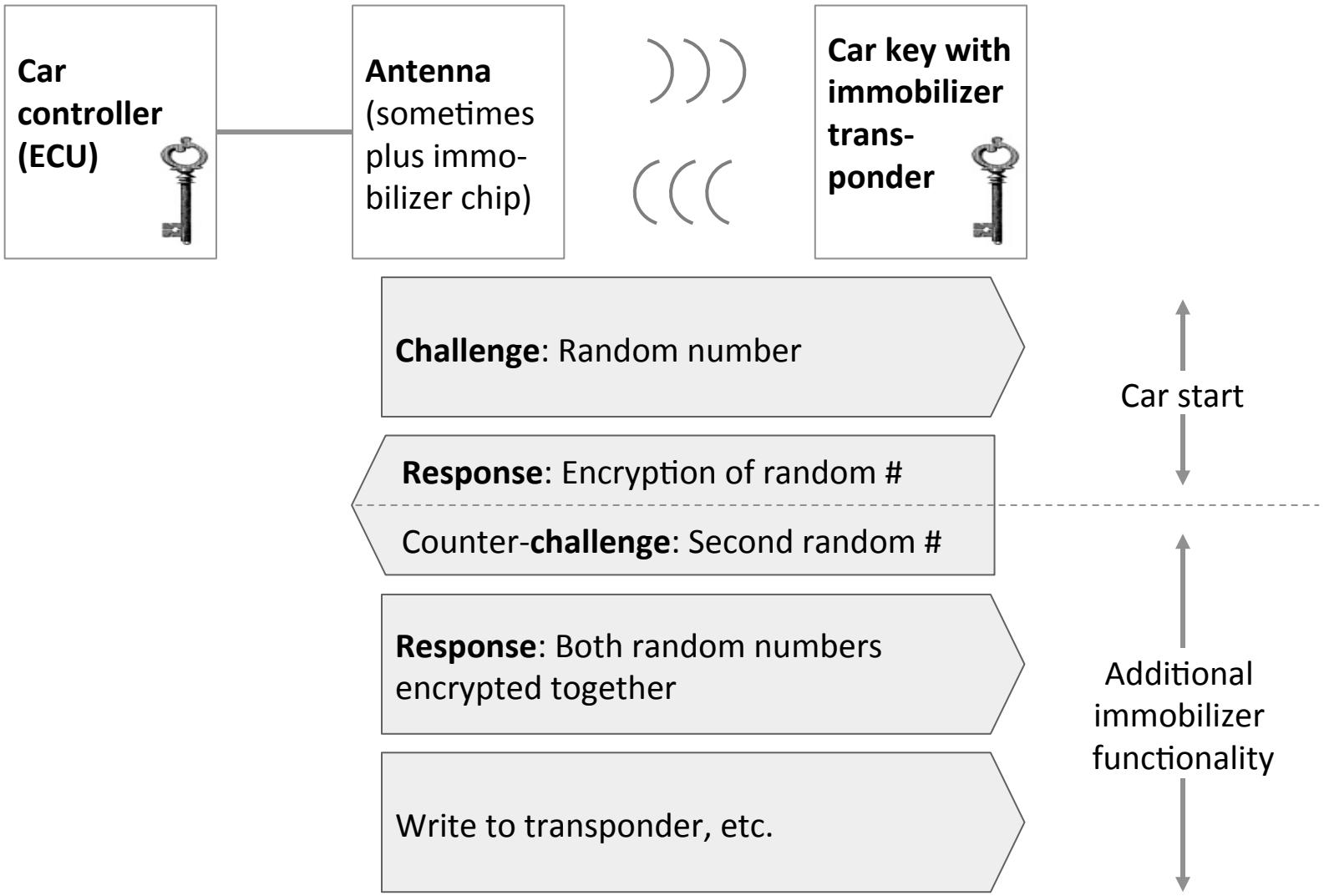
Immobilizers are the first application of IT security to cars

Theft went down quickly thanks to immobilizer technology

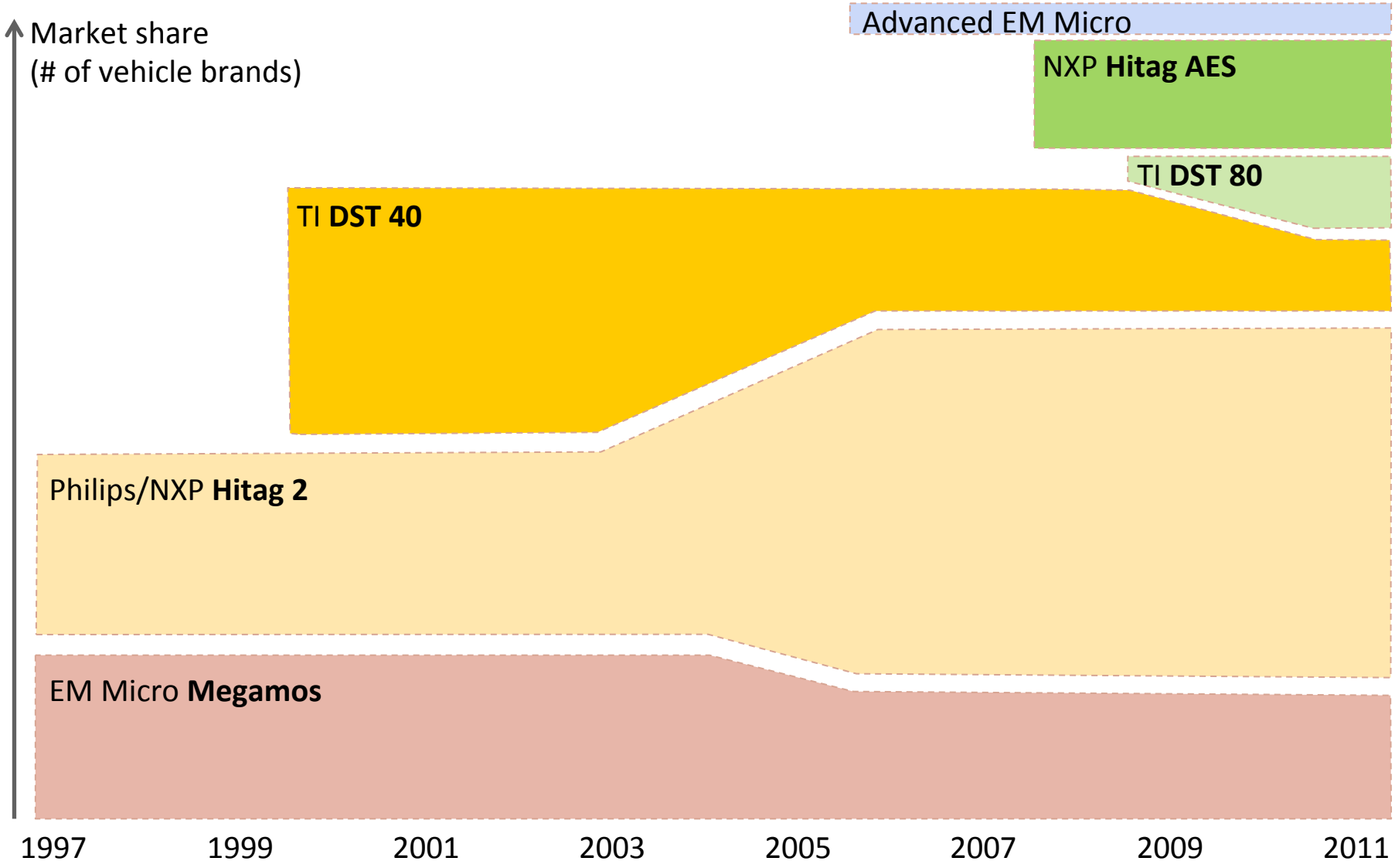


Source: Federal Bureau of Investigation's yearly crime report

Immobilizers are simple challenge-response tokens



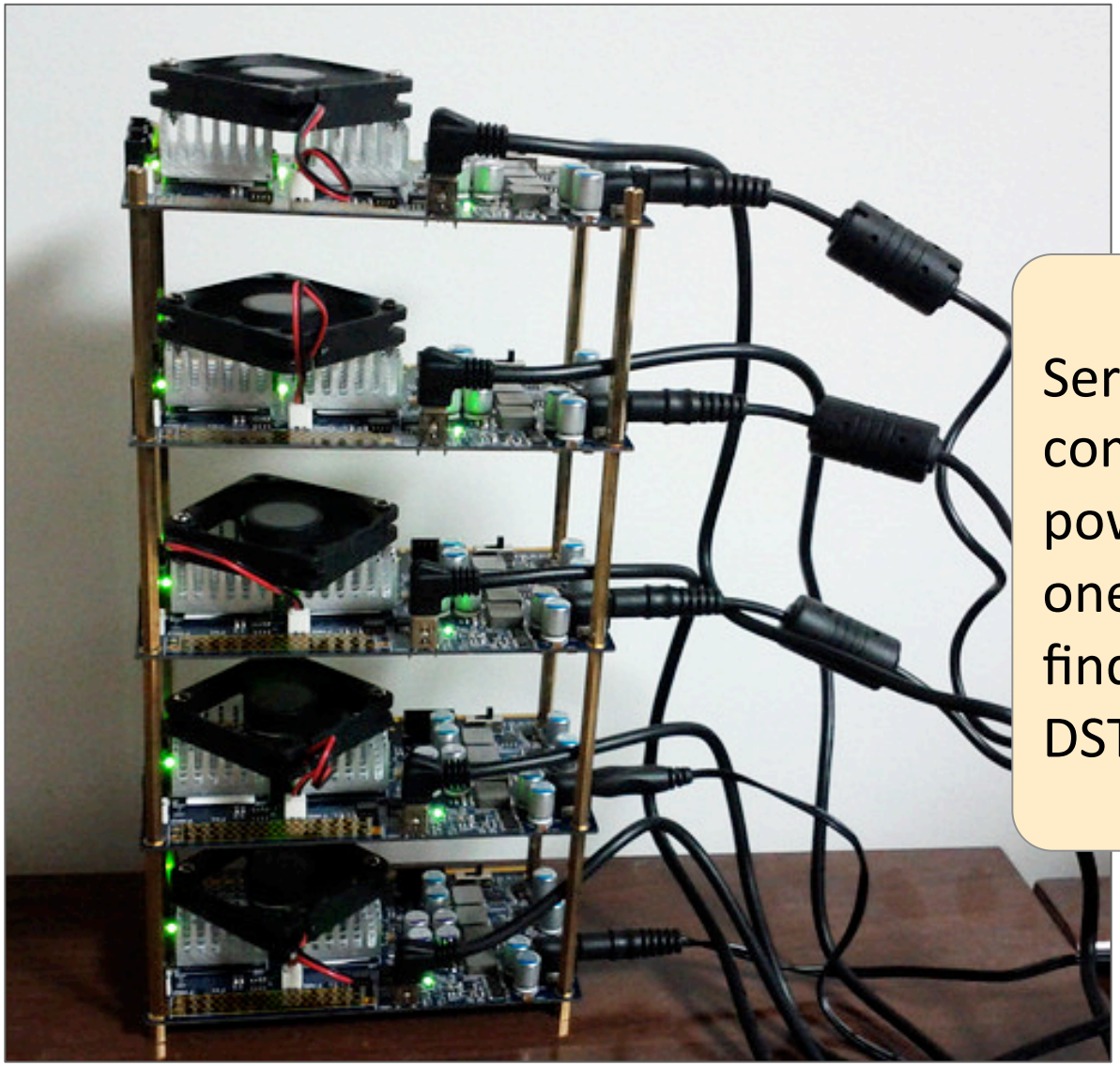
Three technologies dominate the immobilizer market



Agenda

- Immobilizer introduction
- **Cryptographic vulnerabilities**
- Secure car protection gap

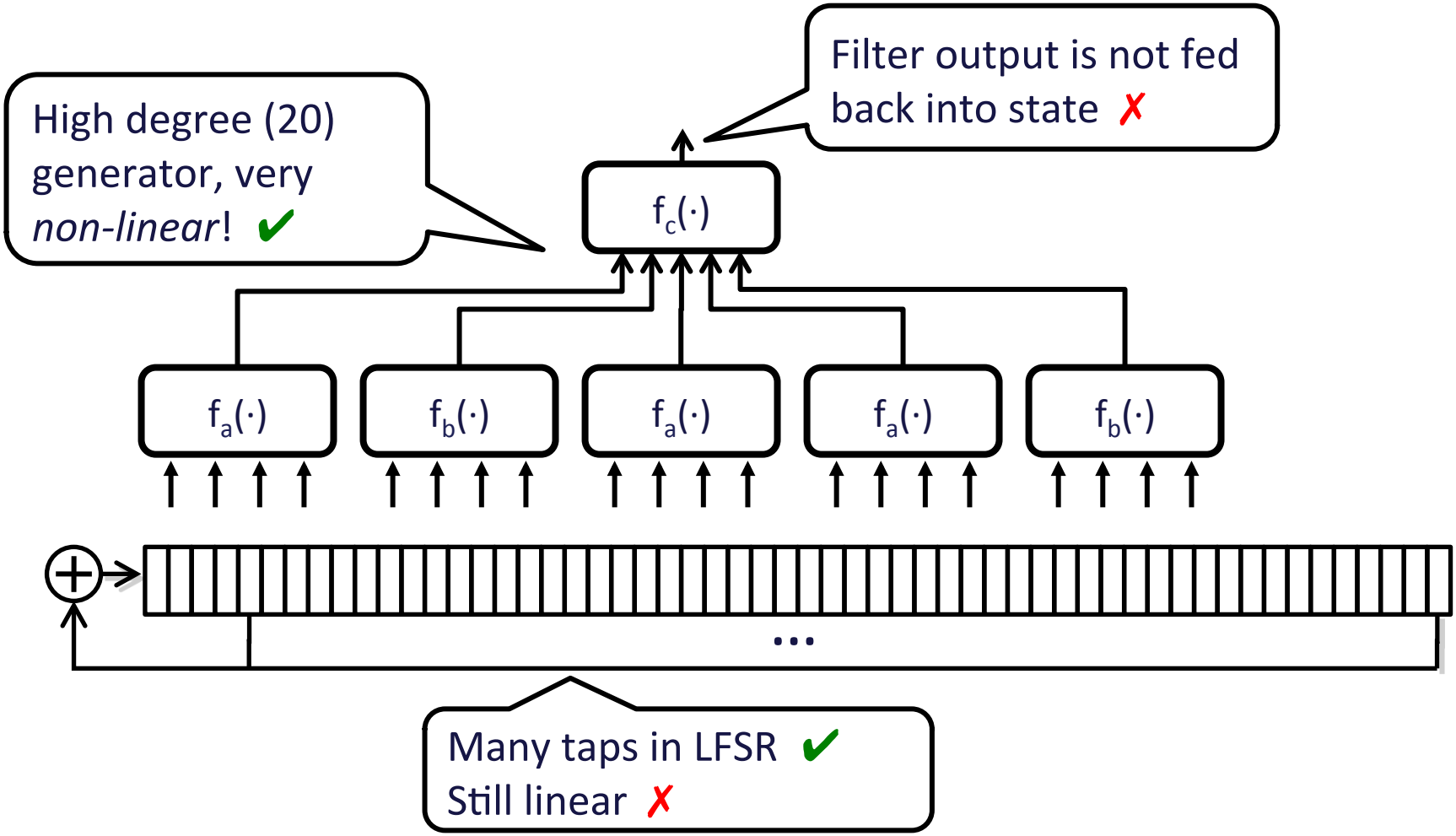
Victim 1: DST40 transponder is vulnerable to brute-force



Serious FPGA computing power takes one hour to find secret DST40 key

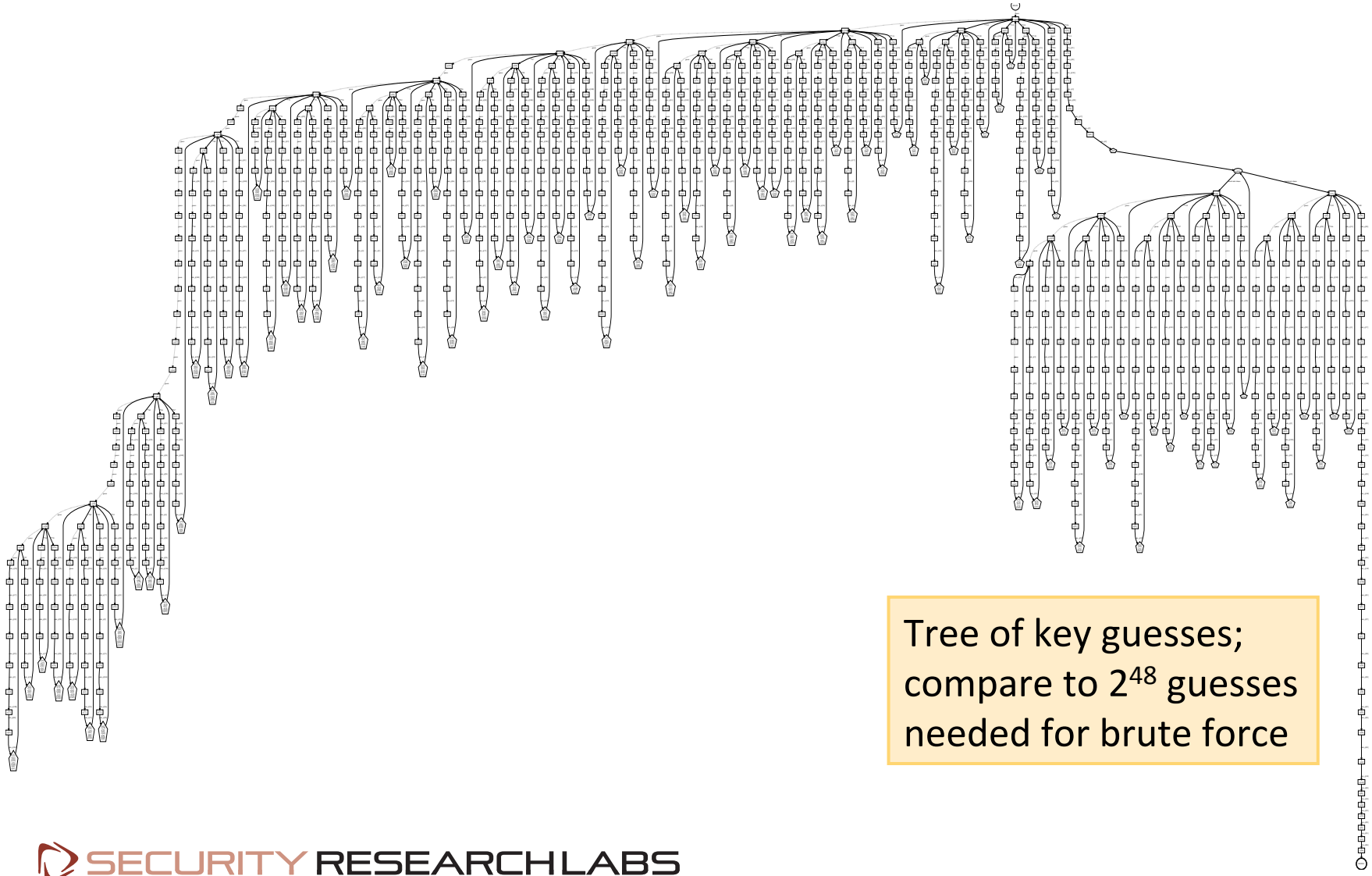
Victim 2: Hitag2 is vulnerable to cryptanalysis (1/2)

Hitag2 cipher violates several stream cipher design principles



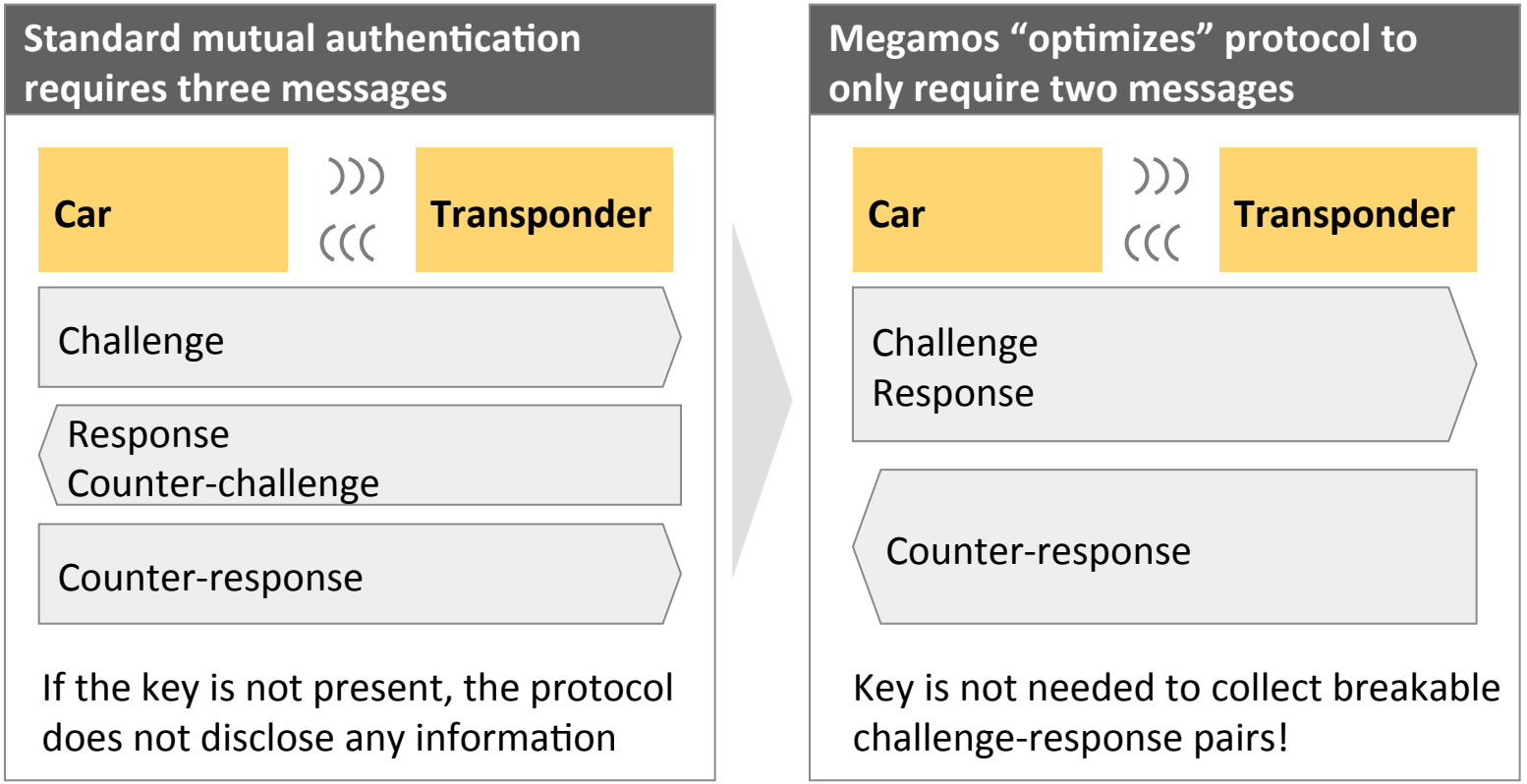
Victim 2: Hitag2 is vulnerable to cryptanalysis (2/2)

SAT solving ("smart brute force") solves Hitag2 system of equations in minutes



Tree of key guesses; compare to 2^{48} guesses needed for brute force

Victim 3: Megamos uses insecure challenge-response protocol



Attack surface	▪ Key cloning	▪ Key cloning when car is present ▪ Car theft with no access to key!

Immobilizer weaknesses are actively being exploited

Car transponder duplication machines

Agenda

- Immobilizer introduction
- Cryptographic vulnerabilities
- **Secure car protection gap**

Cars have security issues far beyond cryptographic design of immobilizers

	Cryptographic best practice			Actual method of car theft
	Key length	Cipher strength	Protocol strength	
DST 40				**Vulnerabilities in car controller are used to program new keys; typically over CAN bus**
DST 80				
Hitag 2				
Hitag 3				
Hitag AES				
Megamos				Unclear if electronic theft occurs

Video: Car theft through car controller exploit

Source: YouTube user EdilockLtd

“Insecure” smartphones have more advanced protection than car controllers

Protection

- ✓ Available
- ✓ Ineffective
- ✗ Not available

Protection area	Best practice		
Hardware	Secure boot	✗	✓
	Hardware key store	✗	✓
	Debug modes disabled	✗	✓
OS	Sandboxing	✗	✓
	Memory randomization	✗	✓
	Signature validation	✓	✓
Software	Modern programming language	✗	✓
	Source code analysis	✗	✓

Wide-scale car hacking is just about to start

Car security is weak

- Immobilizers were the first IT security application in cars
- All popular systems have stark design deficiencies, violating long-standing best practices
- Further weaknesses that are commonly used for car theft arise from insecure car controller implementations

Protection demand grows

- Cars quickly add new applications that need to be protected:
  - Remote assistance (OnStar, mbrace)
  - In-car Wi-Fi
  - Extensible entertainment system
- The security of these new systems often relies on the same car controllers that are already known to be weak

Wide-scale car hacking expected

- Cars provide large attack surface (academia and thieves have shown this repeatedly)
- As soon as meaningful attack incentives emerge, cars will be easy prey
- Car manufacturers have two strategic mitigation options:

a. Keep cars dumb and simple and thereby attack incentives away

b. Strongly invest in security expertise to find and fix design and implementation bugs

Take-aways

- Immobilizers, the first application of IT security to cars, are flawed in their design and implementation
- New attack incentives will be exploited quickly, as attack tools against core components already exist
- The time to prepare all critical car components for the onslaught of hackers is *now*

Questions?

Karsten Nohl <nohl@srlabs.de>