Automotive Cyber Security: Lessons Learned and Research Challenges

SPIDA Keynote Talk

Flavio Garcia
University of Birmingham

Joint work with

Roel Verdult, David Oswald, Timo Kasper, Josep Balasch, Baris Ege, Pierre Pavlides…

The automotive industry has undergone a major transformation

Mechanical

Digital

Shift in Responsibility and Culture

Mechanical

OEMs traditionally shift responsibility to Tier 1 Suppliers

Testing:

Software

EULA: This software is provided “as is” without warranty of any kind… The entire risk arising out of use or performance of the this SOFTWARE remains with the user.

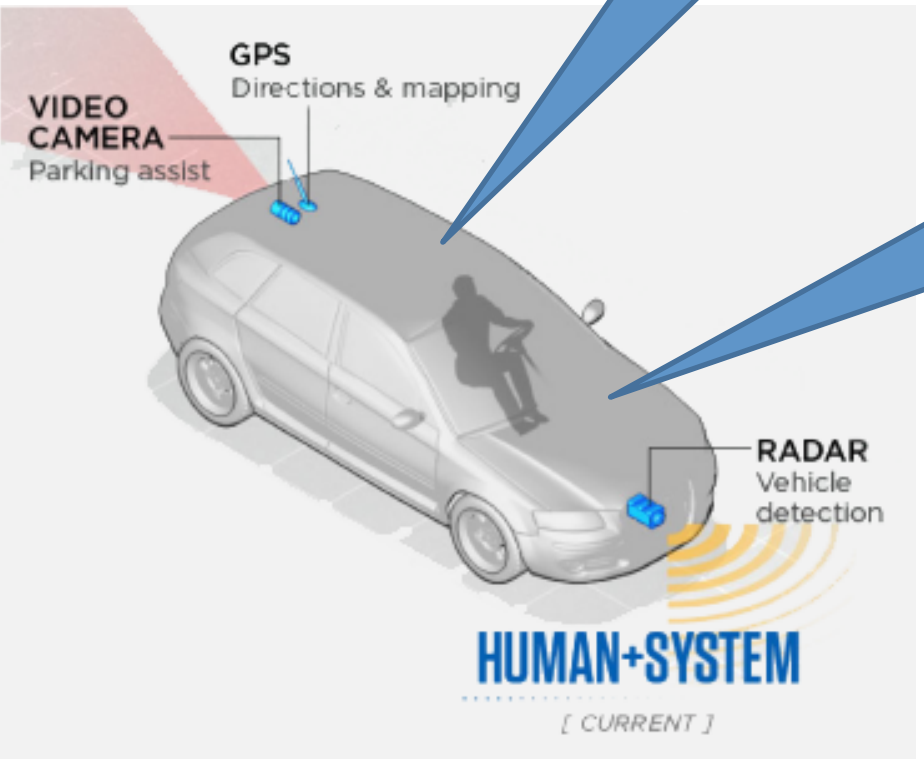
Release now patch later

Current Vehicles

- 3G
- Bluetooth
- WiFi

- Outdated firmware
- Weak firmware protection
- No source code

- ~50 ECUs (Electronic Control Units)

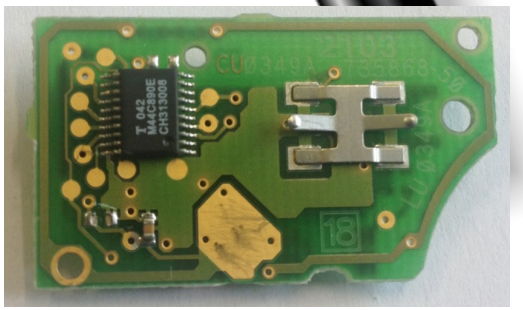


How is this all going so far?

- Not great
- Security is a “Market for Lemons” (and everyone is selling rotten ones)
- We lack an open discussion and more **transparency** about security (weaknesses)
- We need better security engineering
- I’ll give a few examples of this next.
  - Let’s have a look at **car keys**

Immobilizer (Immo

- Passive RFID at 1 5 kHz
- Prevents hot-wi ng



Remote Keyless Entry (RKE)

- Active UHF transmitter (315 / 433 / 868 MHz)
- Unidirectional
- Sometimes integrated with immobilizer chip (“hybrid”), sometimes separate

Main immobiliser chips used (2012-15)

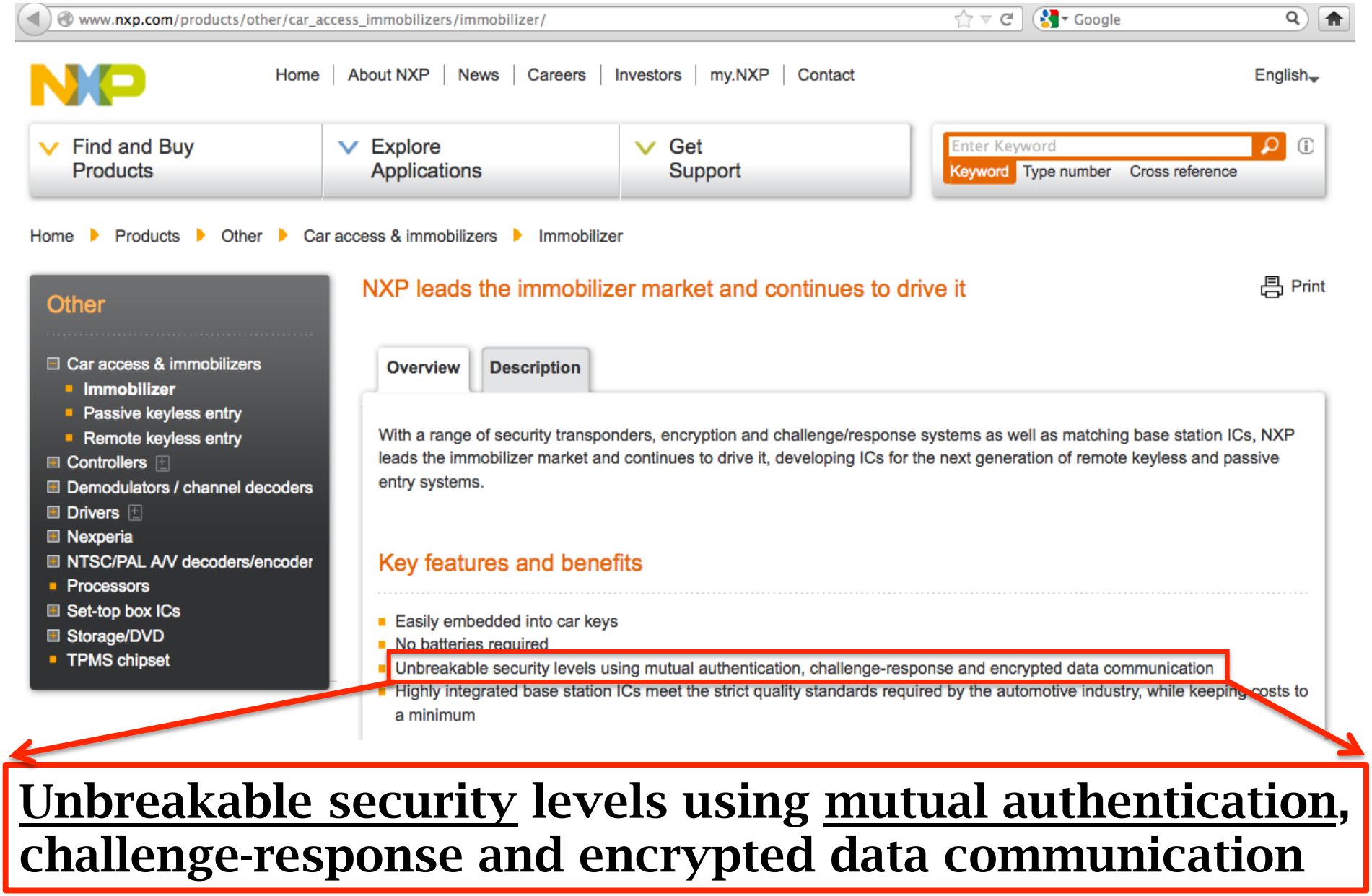
- TI's DST (**40**-bit key)
  - "Security Analysis of a Cryptographically-Enabled RFID Device" Bono et al. [Usenix Security'05]
- NXP's Hitag2 (**48**-bit key)
  [Usenix Security'12]
- EM's Megamos Crypto (VAG) (**96**-bit key)
  [~~Usenix Security'13~~]
  [Usenix Security'15]

Hitag2 Usage

Makes & Models (2012)

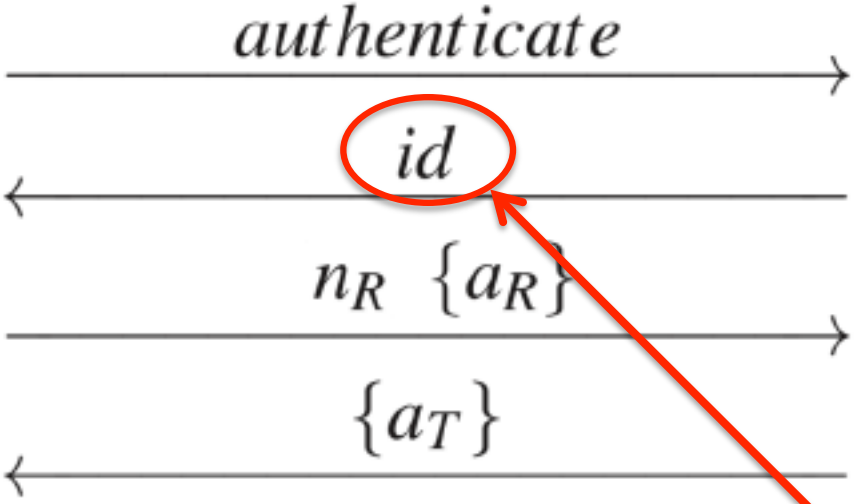
Make	Models
Acura	CSX, MDX, RDX, TL, TSX
Alfa Romeo	156, 159, 166, Brera, Giulietta, Mito, Spider
Audi	A8
Bentley	Continental
BMW	**Serie 1**, 5, 6, 7, all bikes
Buick	Enclave, Lucerne
Cadillac	BLS, DTS, Escalade, SRX, STS, XLR
Chevrolet	Avanlache, Caprice, Captiva, Cobalt, Equinox, Express, HHR Impala, Malibu, Montecarlo, Silverado, Suburban, Tahoe Trailblazer, Uplander
Chrysler	300C, Aspen, Grand Voyager, Pacifica, Pt Cruiser, Sebring Town Country, Voyager
Citroen	**Berlingo**, C-Crosser, C2, **C3**, **C4**, C4 Picasso, **C5**, C6, C8 Nemo, Saxo, Xsara, Xsara Picasso
Dacia	Duster, **Logan**, Sandero
Daewoo	Captiva, Windstorm
Dodge	Avenger, Caliber, Caravan, Charger, Dakota, Durango Grand Caravan, Journey, Magnum, Nitro, Ram
Fiat	500, Bravo, Croma, Daily, Doblo, Fiorino, Grande Punto Panda, Phedra, Ulysse, Scudo
GMC	Acadia, Denali, Envoy, Savana, Siera, Terrain, Volt, Yukon
Honda	Accord, **Civic**, CR-V, Element, Fit, Insight, Stream, Jazz, Odyssey, Pilot, Ridgeline, most bikes
Hummer	H2, H3

Make	Models
	Grandeur, **I30**, Matrix, Santafe, Sonata, Terracan, Tiburon Tucoson, Tuscanti
Isuzu	D-Max
Iveco	35C11, Eurostar, New Daily, S-2000
Jeep	Commander, Compass, Grand Cherokee, Liberty, Patriot Wrangler
Kia	Carens, Carnival, Ceed, Cerato, Magentis, Mentor, Optima Picanto, Rio, Sephia, Sorento, Spectra, Sportage
Lancia	Delta, Musa, Phedra
Mini	Cooper
Mitsubishi	380, Colt, Eclipse, Endeavor, Galant, Grandis, L200 Lancer, Magna, Outlander, Outlander, Pajero, Raider
Nissan	Almera, **Juke**, **Micra**, Pathfinder, Primera, Qashqai, Interstar Note, Xterra
Opel	Agila, Antara, Astra, Corsa, Movano, Signum, Vectra Vivaro, Zafira
Peugeot	**106**, **206**, 207, **307**, 406, 407, 607, 807, 1007, 3008, 5008 Beeper, Partner, **Boxer**, RCZ
Pontiac	G5, G6, Pursuit, Solstice, Torrent
Porsche	Cayenne
Renault	**Clio**, Duster, **Kangoo**, **Laguna II**, Logan, Master **Megane**, Modus, Sandero, **Trafic**, Twingo
Saturn	Aura, Outlook, Sky, Vue
Suzuki	Alto, Grand Vitara, Splash, Swift, Vitara, XL-7
Volkswagen	Touareg, Phaeton



Unbreakable security levels using mutual authentication, challenge-response and encrypted data communication

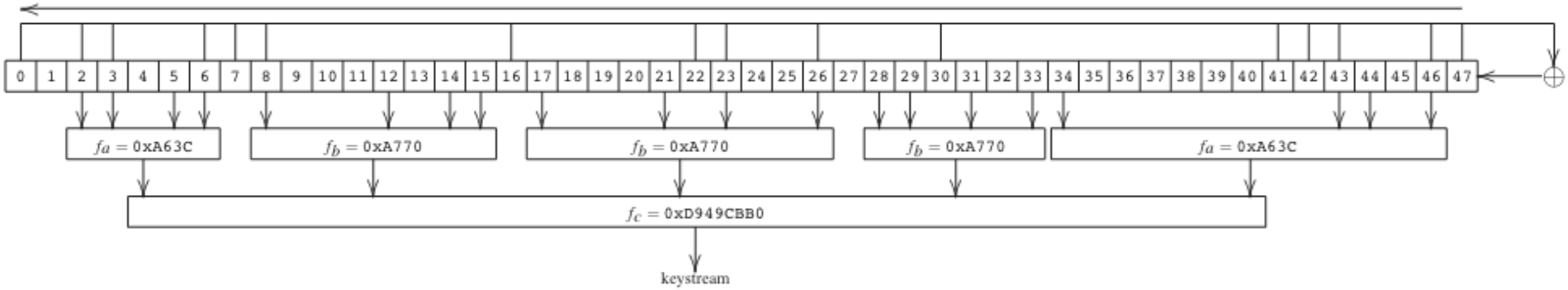
Hitag2 Authentication Protocol



id = 32-bit identifier
nR = reader nonce
{aR} = encrypted reader answer
{aT} = encrypted transponder answer

- No transponder nonce
- No mutual authentication

Hitag2 Cipher



- **48 bit internal state (LFSR stream a_0a_1…)**

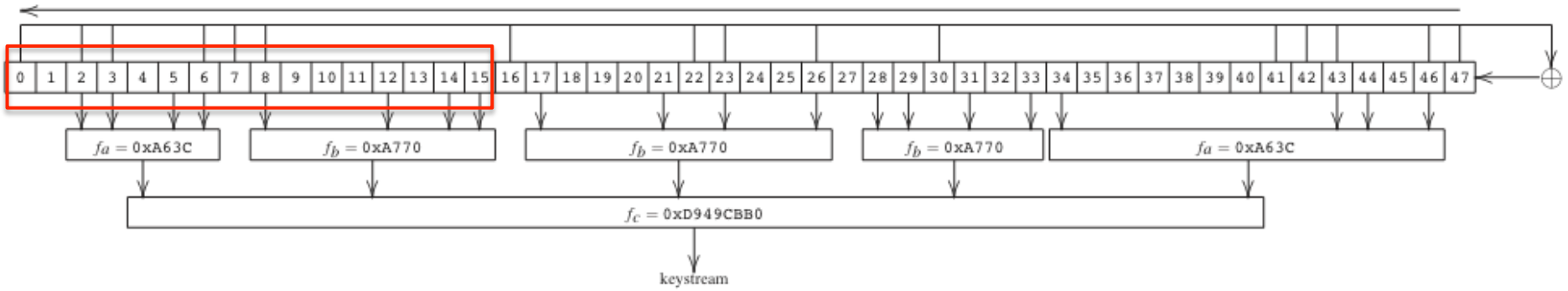
  $a_0 \ldots a_{31} = id_0 \ldots id_{31}$

  $a_{32} \ldots a_{47} = k_0 \ldots k_{15}$

  $a_{48+i} = k_{16+i} \oplus \{nr\}_i \oplus f(a_i \ldots a_{47+i}) \quad \forall i \in [0,31]$

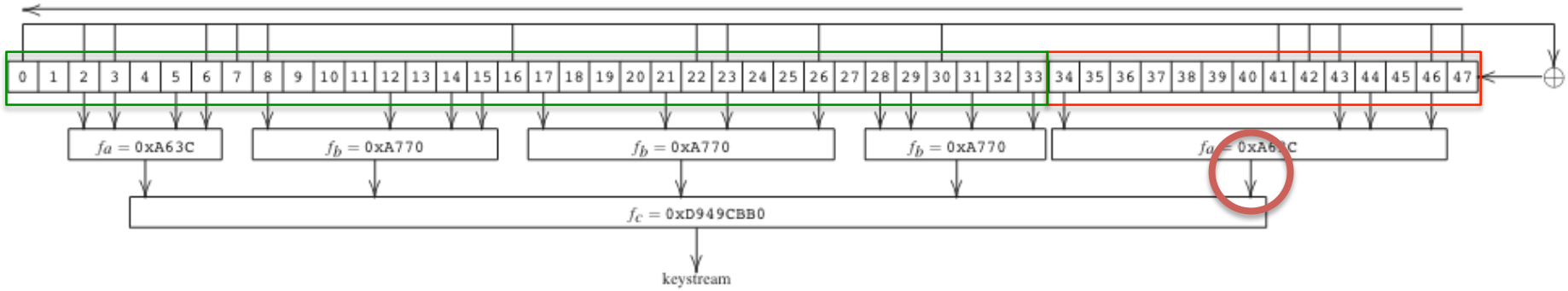
  Initialized LFSR = $a_{32} \ldots a_{79}$

Hitag2 Cipher



- Dependencies between sessions
  - Reader nonce (n_R) is **only 32 bits**
  - **$LFSR_0$…$LFSR_{15}$ are fixed over all sessions, regardless of n_R**

Hitag2 Cipher



- Filter function weakness
  - **4 bits cover 14 bits of the internal state**
  - In 8 of the 32 configurations, the output of f_c is **not** influenced by the last (rightmost) input bit
  - **With probability ¼ the output is determined by the first 34 bits of the LFSR – "Golden Property"**

Cryptanalytic Attack

- Gather 136 authentication attempts from the car **(~1 minute)**
- Use first cipher weakness to combine different reader nonces
- Try for every 2^{34} cipher state **(~5 minutes)**
  - ¼ of the 136 traces (≈34) have the "Golden Property"
  - Test if first keystream bit of {ar} is consistent
  - Verify handful of candidate keys against another trace
- **Total attack time is 360 seconds**
  - This motivates the title of our Usenix'12 paper

  "Gone in 360 Seconds: Hijacking with Hitag2"

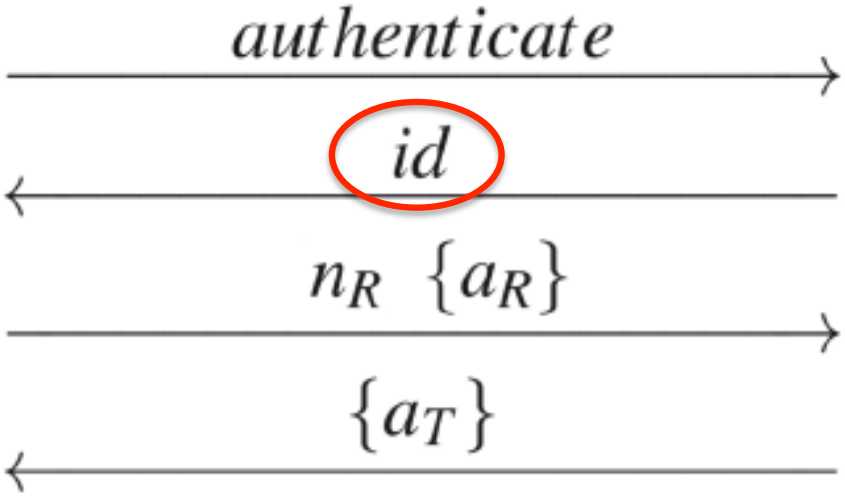
Immobilizer Demo

Responsible disclosure

- Notified the chip manufacturer NXP 6 months ahead of publication
  - NXP Verified and acknowledged our findings
  - Collaborated constructively by discussing mitigating measures
- Immobilizer based on AES cost only a couple dollars more
- NXP: the attack does not work in a car-only scenario

Is this attack car-only?

- Not quite – due to whitelisting of transponder id
- Remember:



Whitelist:

id_1	k_1
id_2	k_2
id_3	k_3

We will **revisit** this point later on…

Megamos Crypto Usage (2013)

Make	Models
Alfa Romeo	147, 156, GT
Audi	A1, A2, A3, **A4 (2000)**, A6, **A8 (1998)**, Allroad, Cabrio, Coupé, Q7, S2, S3, S4, S6, S8, **TT (2000)**
Buick	Regal
Cadillac	CTS-V, SRX
Chevrolet	Aveo, Kalos, Matiz, Nubira, Spark, Evanda, Tacuma
Citroën	**Jumper (2008)**, Relay
Daewoo	Kalos, Lanos, Leganza, Matiz, Nubira, Tacuma
DAF	CF, LF, XF
Ferrari	California, 612 Schaglietti
Fiat	Albea, Doblò, Idea, Mille, Multipla, Palio, **Punto (2002)**, Seicento, Siena, **Stilo (2001)**, **Ducato (2004)**
Holden	Barina, Frontera
Honda	Accord, Civic, CR-V, FR-V, HR-V, Insight, **Jazz (2002, 2006)**, Legend, Logo, S2000, Shuttle, Stream
Isuzu	Rodeo
Iveco	Eurocargo, Daily
Kia	Carnival, Clarus, Pride, Shuma, Sportage
Lancia	Lybra, Musa, Thesis, Y
Maserati	Quattroporte
Opel	Frontera
Pontiac	G3
Porsche	911, 968, Boxster
Seat	Altea, Córdoba, **Ibiza (2014)**, Leon, Toledo
Skoda	**Fabia (2011)**, Felicia, Octavia, Roomster, Super, Yeti
Ssangyong	Korando, Musso, Rexton
Tagaz	Road Partner
Volkswagen	Amarok, Beetle, Bora, Caddy, Crafter, Cross Golf, Dasher, Eos, Fox, Gol, **Golf (2006, 2008)**, Individual, Jetta, Multivan, New Beetle, Parati, Polo, Quantum, Rabbit, Saveiro, Santana, **Scirocco (2011)**, Touran, **Tiguan (2010)**, Voyage, **Passat (1998, 2005)**, Transporter
Volvo	C30, **S40 (2005)**, S60, S80, **V50 (2005)**, V70, XC70, XC90, XC94

Tag Memory layout (from datasheet)

Block	Content	Denoted by
0	user memory	$um_0 \ldots um_{15}$
1	user memory, lock bits	$um_{16} \ldots um_{29} l_0 l_1$
2	device identification	$id_0 \ldots id_{15}$
3	device identification	$id_{16} \ldots id_{31}$
4	crypto key	$k_0 \ldots k_{15}$
5	crypto key	$k_{16} \ldots k_{31}$
6	crypto key	$k_{32} \ldots k_{47}$
7	crypto key	$k_{48} \ldots k_{63}$
8	crypto key	$k_{64} \ldots k_{79}$
9	crypto key	$k_{80} \ldots k_{95}$
10	pin code	$pin_0 \ldots pin_{15}$
11	pin code	$pin_{16} \ldots pin_{31}$
12	user memory	$um_{30} \ldots um_{45}$
13	user memory	$um_{46} \ldots um_{61}$
14	user memory	$um_{62} \ldots um_{77}$
15	user memory	$um_{78} \ldots um_{93}$

read-only
write-only
read-write

Megamos Authentication Protocol

$$id \leftarrow$$

$$n_C,\ a_C \rightarrow$$

$$a_T \leftarrow$$

id = 32-bit Tag identifier

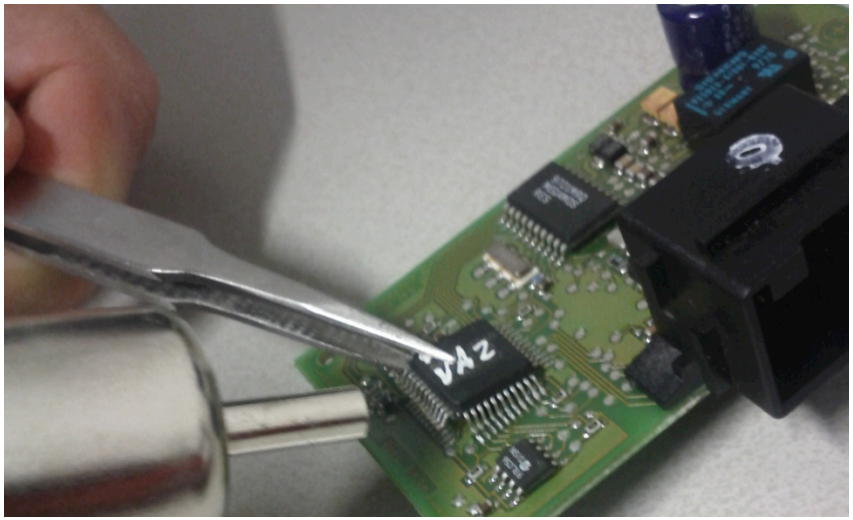
n_C = 56-bit Car nonce

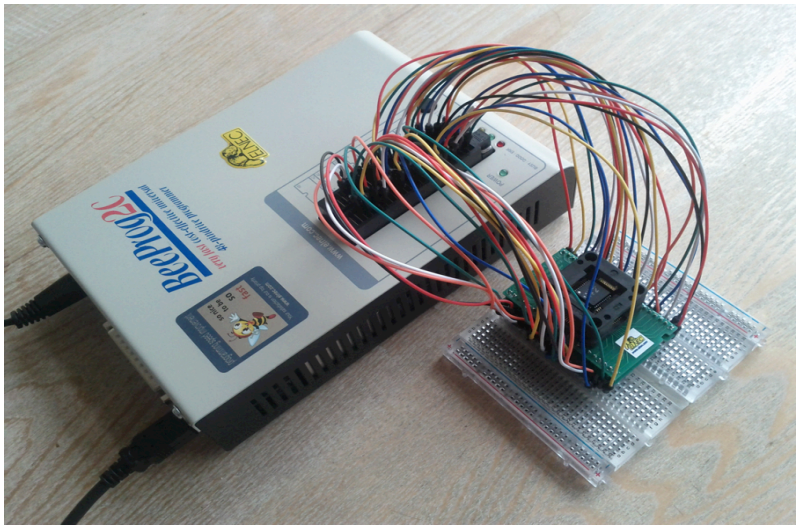
a_C = 28-bit Car authenticator (keystream)

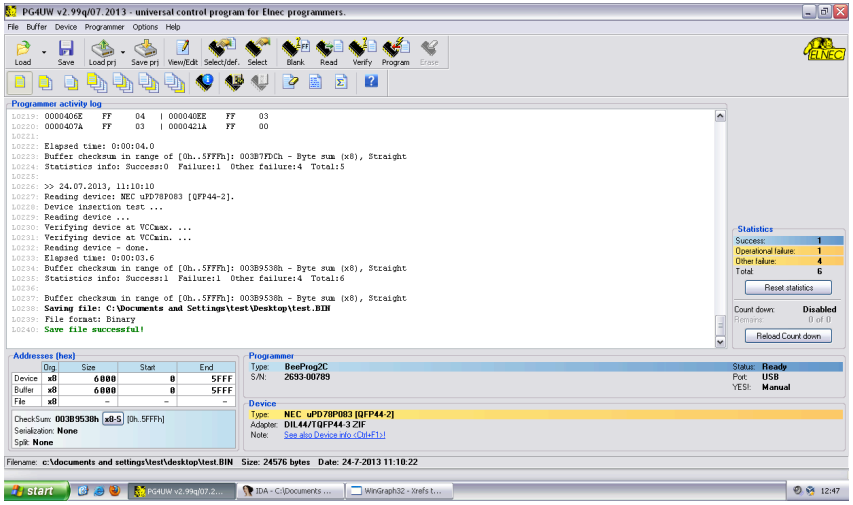
a_T = 20-bit Tag authenticator (keystream)

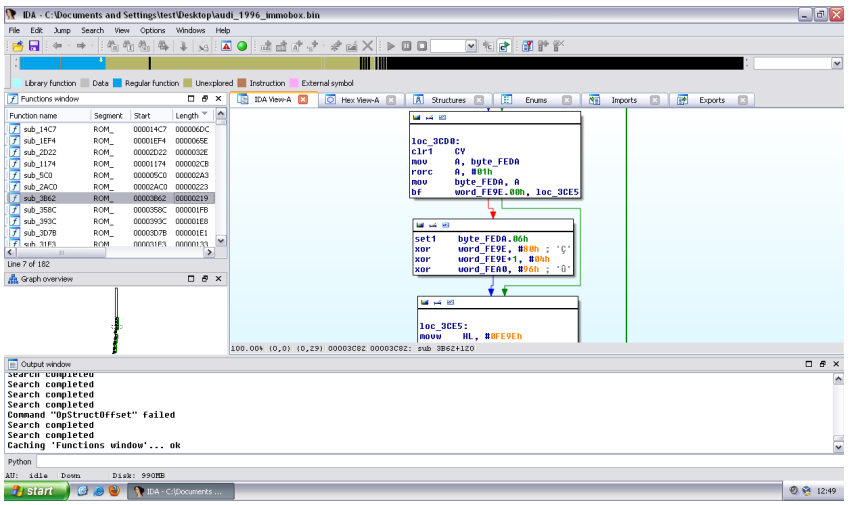
… you can read it directly from the car's ECU

NEC uPD78P083 has simply **no protection**









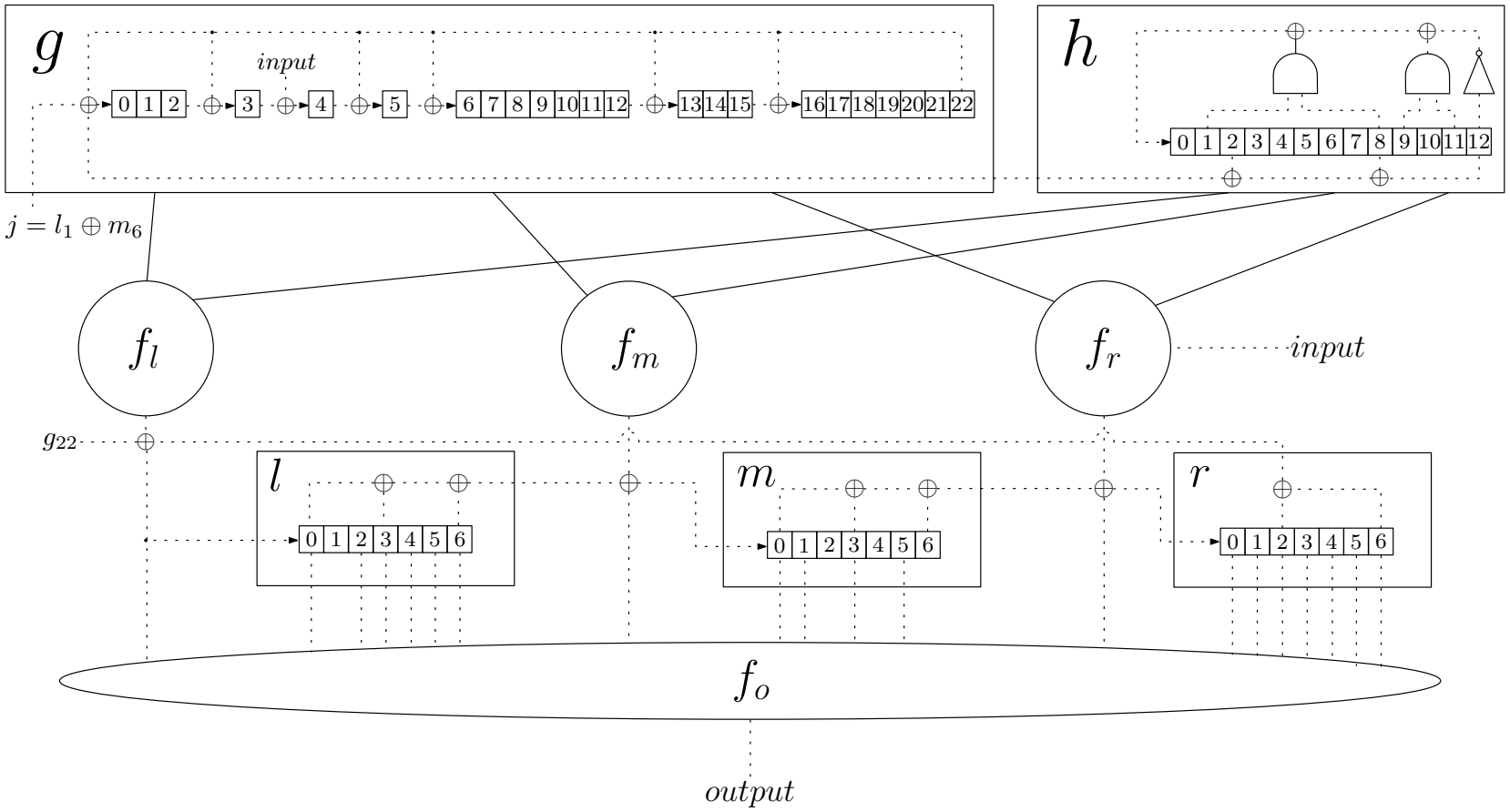
Cryptanalysis - Pre-requisites

- Requires access to the **car and the car key**
- Adversary needs to turn the ignition on twice and eavesdrop two traces

Origin	Message
Car	3
Transponder	A9 08 4D EC
Car	5
Transponder	80 00 95 13
Car	F
Transponder	AA AA AA AA AA AA AA AA
Car	6 | 3F FE 1F B6 CC 51 3F | 0^7 | F3 55 F1 A
Transponder	60 9D 6

Cryptanalysis of the cipher

The Megamos Crypto Cipher



Secret key size = 96 bits

Internal state size = 23 + 13 + 3x7 = 57 bits

Cryptanalysis of Megamos Crypto

- Total attack complexity reduced from 2^{96} to less than 2^{56} encryptions
- Takes less than two days on an FPGA
- This complexity can be further reduced by pre-computation:
  - E.g., using a 12 Terabyte table reduces the complexity to 2^{49} table lookups
  - This has some practical limitations

Partial Key-update Attack

Observations:

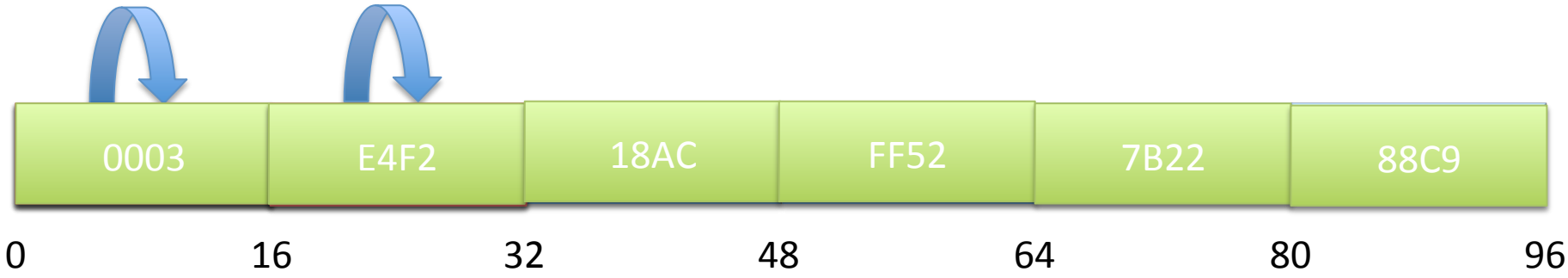
During our research, the majority of deployed tags we found were:

- Unlocked $l_0 = 0$ (writable)
- Could be unlocked with a default PIN code

Block	Content	Denoted by
0	user memory	$um_0 \ldots um_{15}$
1	user memory, lock bits	$um_{16} \ldots um_{29} l_0 l_1$
2	device identification	$id_0 \ldots id_{15}$
3	device identification	$id_{16} \ldots id_{31}$
4	crypto key	$k_0 \ldots k_{15}$
5	crypto key	$k_{16} \ldots k_{31}$
6	crypto key	$k_{32} \ldots k_{47}$
7	crypto key	$k_{48} \ldots k_{63}$
8	crypto key	$k_{64} \ldots k_{79}$
9	crypto key	$k_{80} \ldots k_{95}$
10	pin code	$pin_0 \ldots pin_{15}$
11	pin code	$pin_{16} \ldots pin_{31}$
12	user memory	$um_{30} \ldots um_{45}$
13	user memory	$um_{46} \ldots um_{61}$
14	user memory	$um_{62} \ldots um_{77}$
15	user memory	$um_{78} \ldots um_{93}$

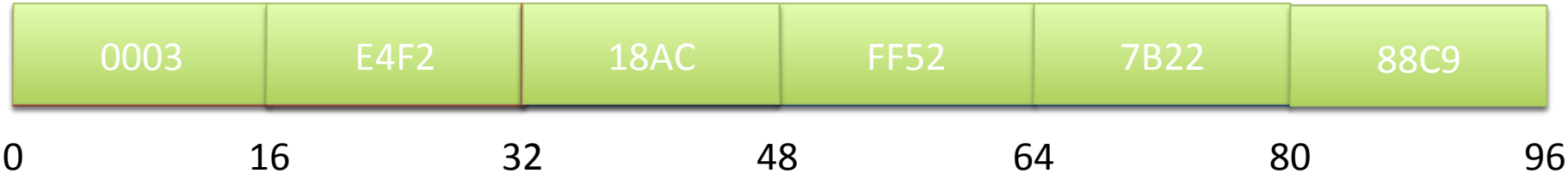
- The 96-bit secret key is written to the tag in **blocks of 16 bits** instead of being an atomic operation.

Partial Key-update Attack (simple)



- Get one authentication attempt from the car
- Guess 16 bits, write on one block then authenticate to the tag.
- If it succeeds you learn 16 key bits.
- This requires 6 x 2^{16} writes and authenticate
- Takes 25’ per block ≈ 2.5 hours in total, using a Proxmark

Partial Key-update Attack (optimized)



- Same principle but only write zeros once in the first block
- Then increment the nonce and authenticate until the tag accepts
  - **key is added to nonce** during initialisation
- Repeat for another two blocks then combine with the cryptanalytic attack searching for the remaining bits
- This attack requires 6 writes and 3×2^{16} authentications with the tag and negligible computational complexity
- The whole attack takes <30 minutes using a Proxmark III

Immobilizer Demo

Responsible disclosure

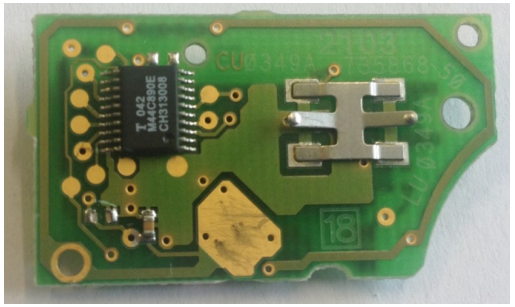
- We informed the chip manufacturer (EM) 9 months ahead of scheduled publication
- This paper was first accepted at Usenix Security'13
- VW sought an injunction from the High Court of London to prevent publication
- The High Court of London granted an interim injunction and therefore we had to withdraw the article
- We have now reached an amicable settlement without any admission of liability
- The paper was finally published at Usenix Security'15 with minor redactions

Immobilizer (Immo)

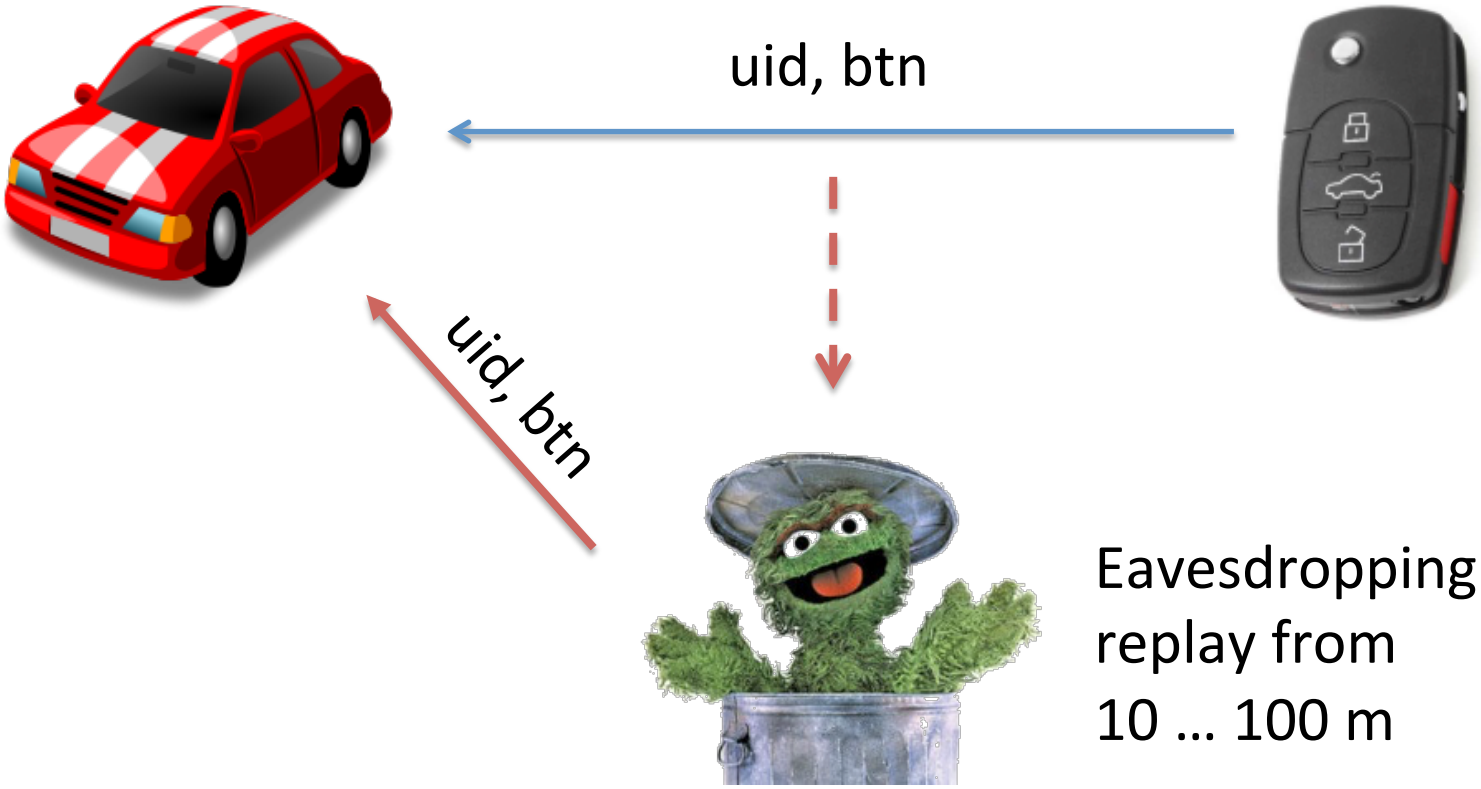
- Passive RFID at 125 kHz
- Many broken systems (DST40, Hitag2, Megamos)

Remote Keyless Entry (RKE)

- Active UHF transmitter (315 / 433 / 868 MHz)
- Unidirectional
- Sometimes integrated with immobilizer chip ("hybrid"), sometimes separate



History of RKE: Fix Codes



Eavesdropping and replay from 10 … 100 m

History of RKE: Rolling Codes

uid, $enc_K(ctr', btn)$

uid, $enc_K(ctr' + 1, btn)$

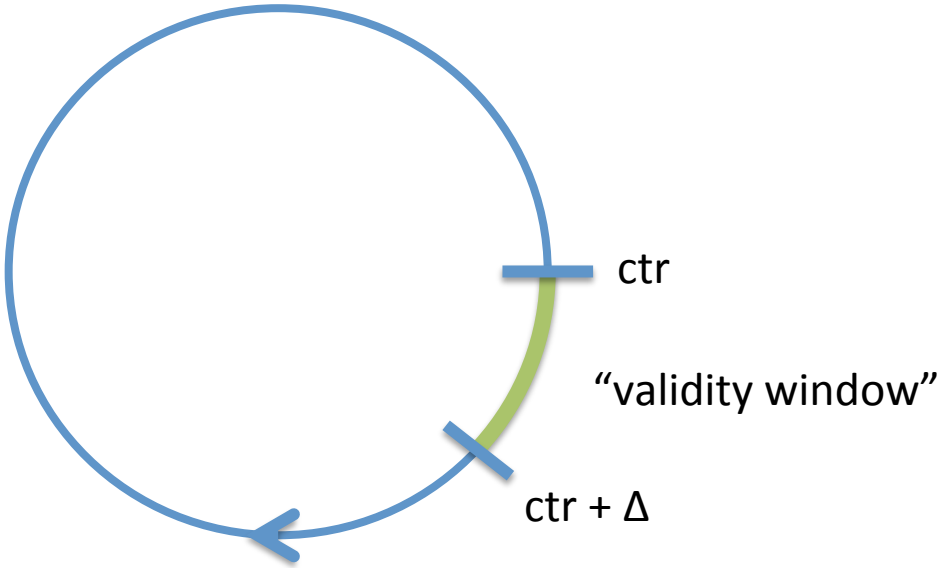
uid, $enc_K(ctr' + 2, btn)$

Decrypt ctr'

if (ctr < ctr' < ctr + Δ)

ctr := ctr'

open / close



History of RKE: Rolling Codes

uid, $enc_K(ctr', btn)$

ctr' incremented on each button press, replay fails

History of RKE: Rolling Codes

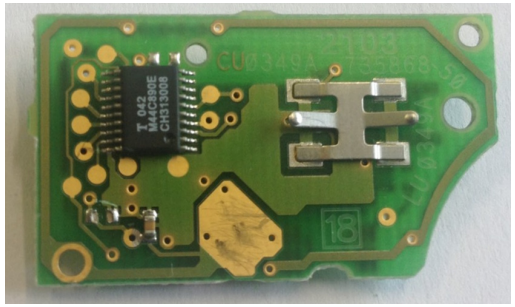
uid, $enc_K(ctr', btn)$

Option 1: Attack key management

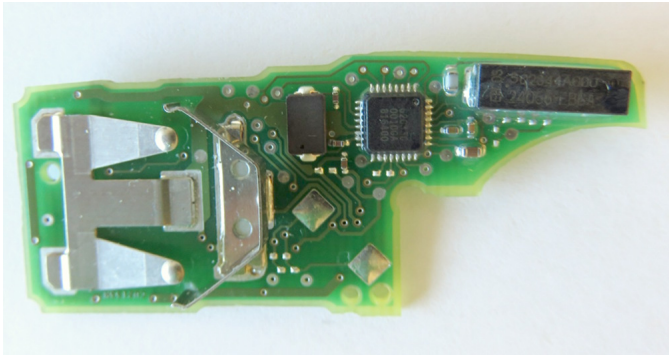
Option 2: Attack crypto

Previous Attacks on RKE

- 2007: Cryptanalysis of KeeLoq garage door openers (2^{16} plaintext/ciphertext pairs) by Biham et al.
- 2008: Side-channel attack on KeeLoq key diversification (Eisenbarth et al.)
- 2010: Relay attacks on passive keyless entry systems (Francillon et al.)
- 2014: Cesare: attack on 2000 – 05 vehicles
- 2015: “RollJam” by Spencerwhyte / Kamkar
  (had been proposed before, does not apply to most modern vehicles since button is authenticated)



Part 1: The VW Group System

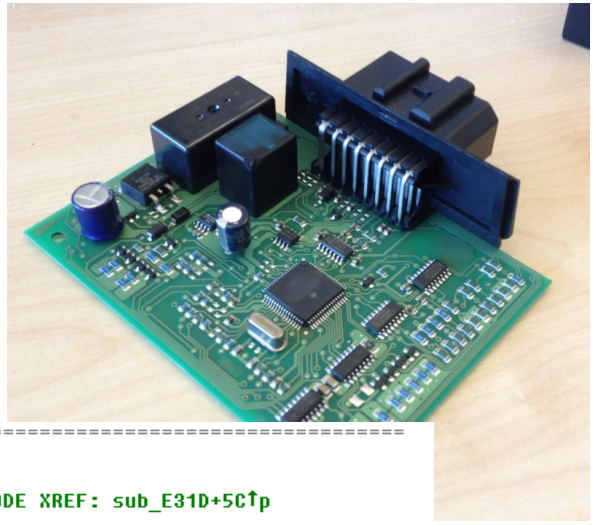


VW Group RKE

- > 10% worldwide market share
- Immobilizer (Megamos) and RKE separate for most vehicles
- Proprietary RKE system, mostly 434.4 MHz
- We analyzed vehicles between ~2000 and today
- Four main schemes (VW-1 … VW-4) studied

VW Group RKE: Analysis

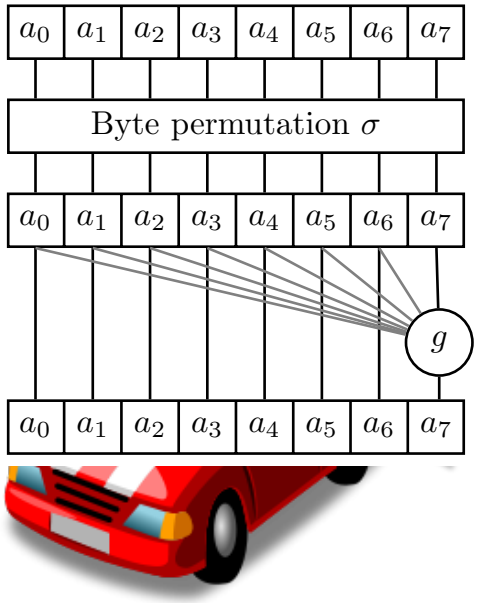
Step 2: Reverse-engineering ECUs



```
; =============== S U B R O U T I N E =======================================

sub_F5C4:                               ; CODE XREF: sub_E31D+5C↑p
                pshd
                pshx
                leas    -$C,sp
                anda    #$3F ; '?'
                clrx
                addd    #$8000
                bcc     loc_F5D2
                inx

loc_F5D2:                               ; CODE XREF: sub_F5C4+B↑j
                std     4,sp
                ldd     $14,sp
                ldx     $12,sp
                subd    $E,sp
                sbex    $C,sp
```



xample: VW-3

$AUT64_{K_3}$(uid, ctr', btn'), btn

- AUT64 is a proprietary block cipher, no trivial attacks known
- … but key K_3 is the same in **all** VW-3 vehicles
- VW-2: Same cipher, different key
- VW-1: Weak crypto (LFSR)

Example: VW-4

$XTEA_{K_4}(uid, ctr', btn'), btn$

- Used from ~ 2010 onwards
- Secure standard cipher: XTEA
- … but again one worldwide key K_4
- Adversary can clone remote by eavesdropping a single rolling code

VW RKE Demo

Affected Vehicles

- **Audi**: A1, Q3, R8, S3, TT, other types of Audi cars (e.g. remote control 4D0 837 231)
- **VW**: Amarok, (New) Beetle, Bora, Caddy, Crafter, e-Up, Eos, Fox, Golf 4, Golf 5, Golf 6, Golf Plus, Jetta, Lupo, Passat, Polo, T4, T5, Scirocco, Sharan, Tiguan, Touran, Up
- **Seat**: Alhambra, Altea, Arosa, Cordoba, Ibiza, Leon, MII, Toledo
- **Škoda**: City Go, Roomster, Fabia 1, Fabia 2, Octavia, Superb, Yeti
- **In summary:** probably most VW group vehicles between 2000 and today not using Golf 7 (MQB) platform

Intermezzo

- Cryptographic algorithms improving over time
- But: Secure crypto ≠ secure system
- Reverse engineering ECU firmware yields a few worldwide keys
- Attack highly practical and scalable
- New VW group system (MQB / Golf 7) allegedly uses diversified keys + good crypto

The Hitag2 RKE

Hitag2 in the RKE context

- Hybrid chip (Immo+RKE) uses a different secret key for both but the **same uid**
  - This can be eavesdropped from 100 m/300 ft
- **136** traces is not practical in a RKE context, so we needed to **improve** the attack

- The cipher was known so we did a black-box reverse engineering of the RKE protocol

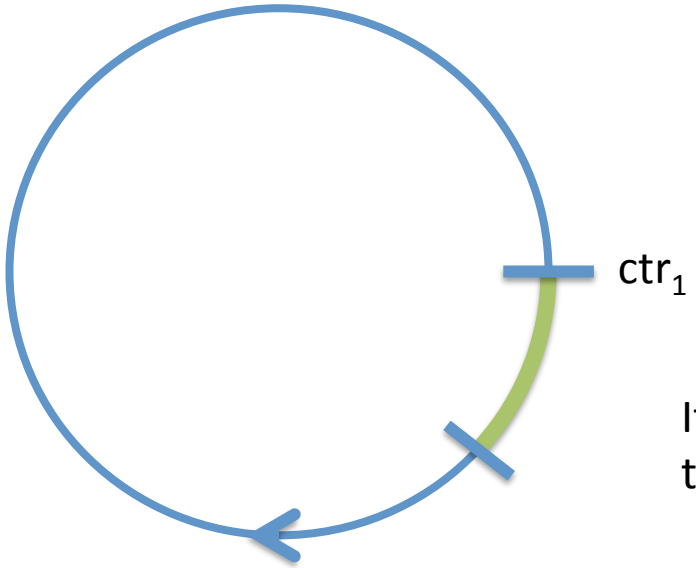
RKE protocol (simplified)

MAC_k is 32 bits of keystream

uid, btn, ctr, MAC_k, crc

Diversified keys

id_1	k_1	ctr_1
id_2	k_2	ctr_2
id_3	k_3	ctr_3

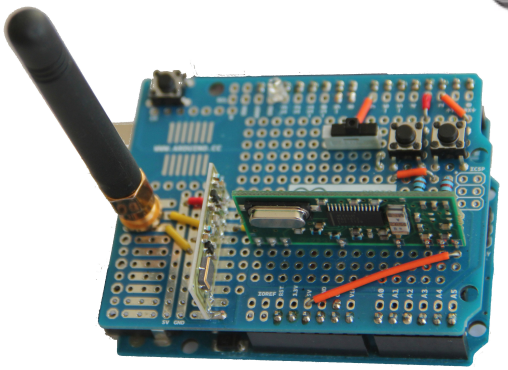


If ($ctr_1 < ctr'_1 < ctr_1 + \Delta$)
then $ctr_1 := ctr'_1$; open

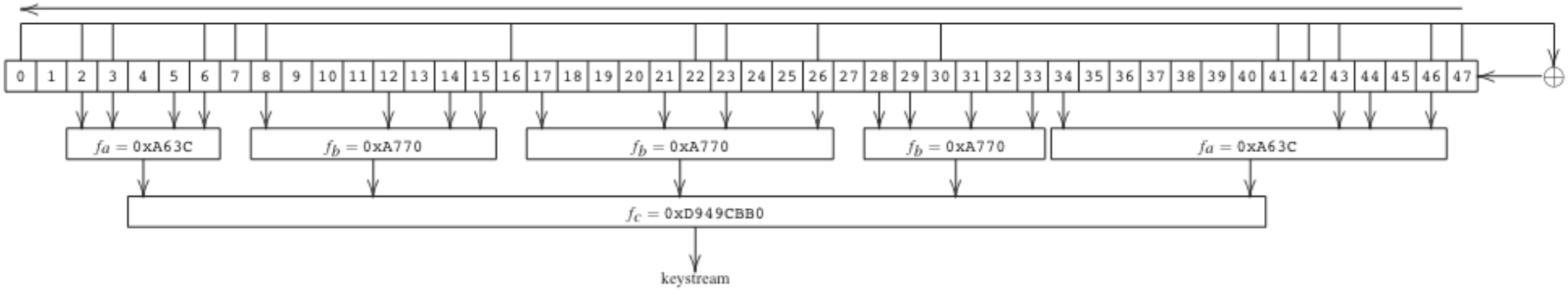
Our RKE attack requires

- ≈ 8 traces (key presses)
- Our $40 Arduino board can collect them

uid, btn, ctr, MAC_k, crc



Hitag2 Cipher



48 bit internal state (LFSR stream a_0a_1…)

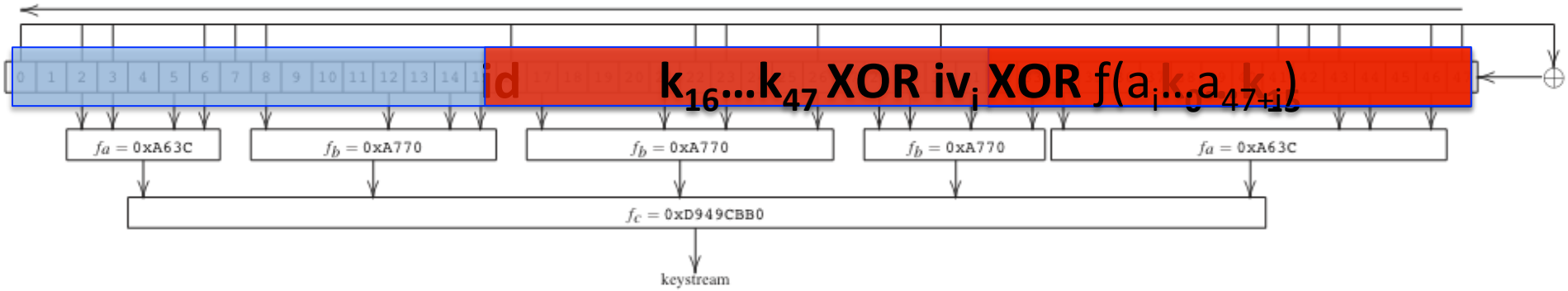
$a_0 \ldots a_{31} = id_0 \ldots id_{31}$

$a_{32} \ldots a_{47} = k_0 \ldots k_{15}$

$a_{48+i} = k_{16+i} \oplus \{data\}_i \oplus f(a_i \ldots a_{47+i}) \quad \forall i \in [0,31]$

Initialized LFSR = $a_{32} \ldots a_{79}$

Hitag2 cipher



48 bit internal state (LFSR stream a_0a_1…)

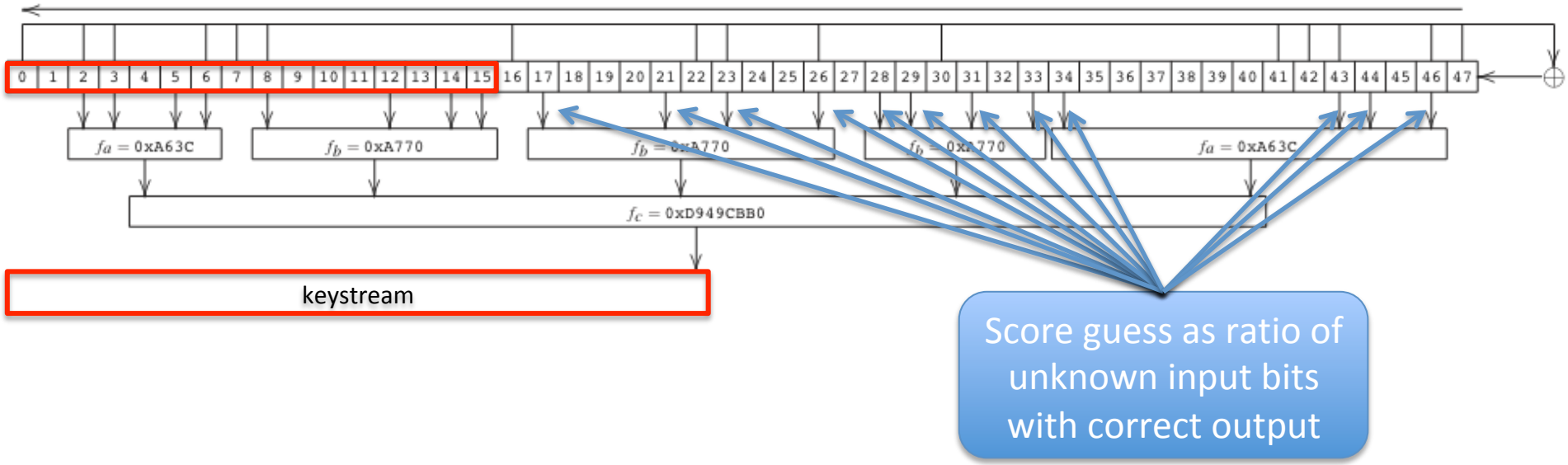
$a_0…a_{31} = id_0…id_{31}$

$a_{32}…a_{47} = k_0…k_{15}$

$a_{48+i} = k_{16+i} \oplus iv_i \oplus f(a_i…a_{47+i}) \quad \forall i \in [0,31]$

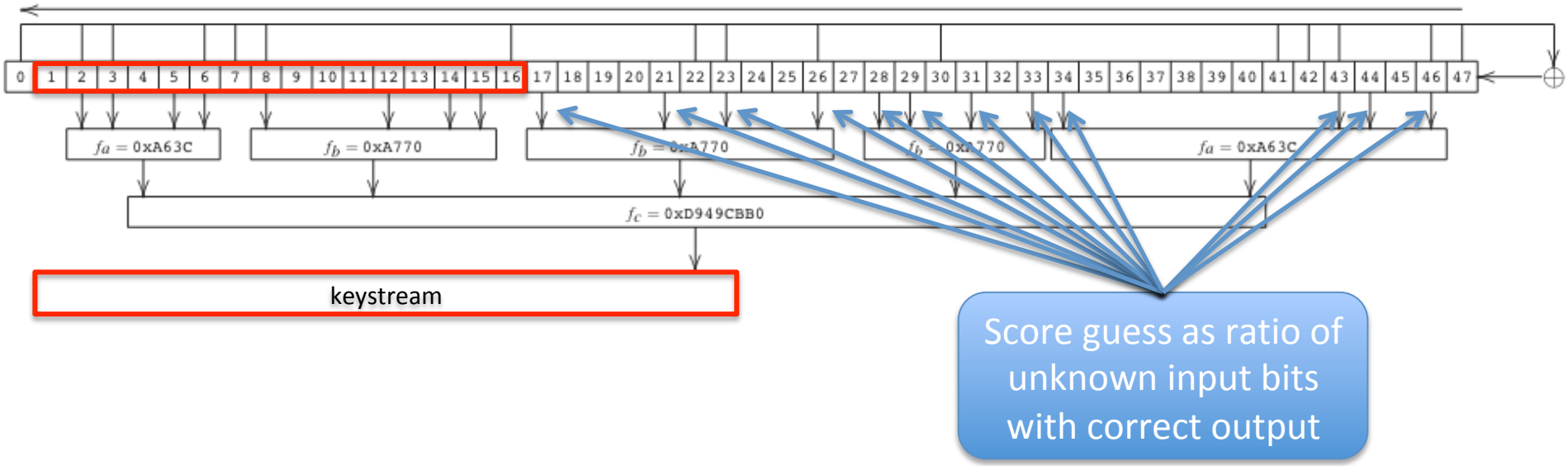
Initialized LFSR = $a_{32}…a_{79}$

A fast correlation attack on Hitag2 (simplified)

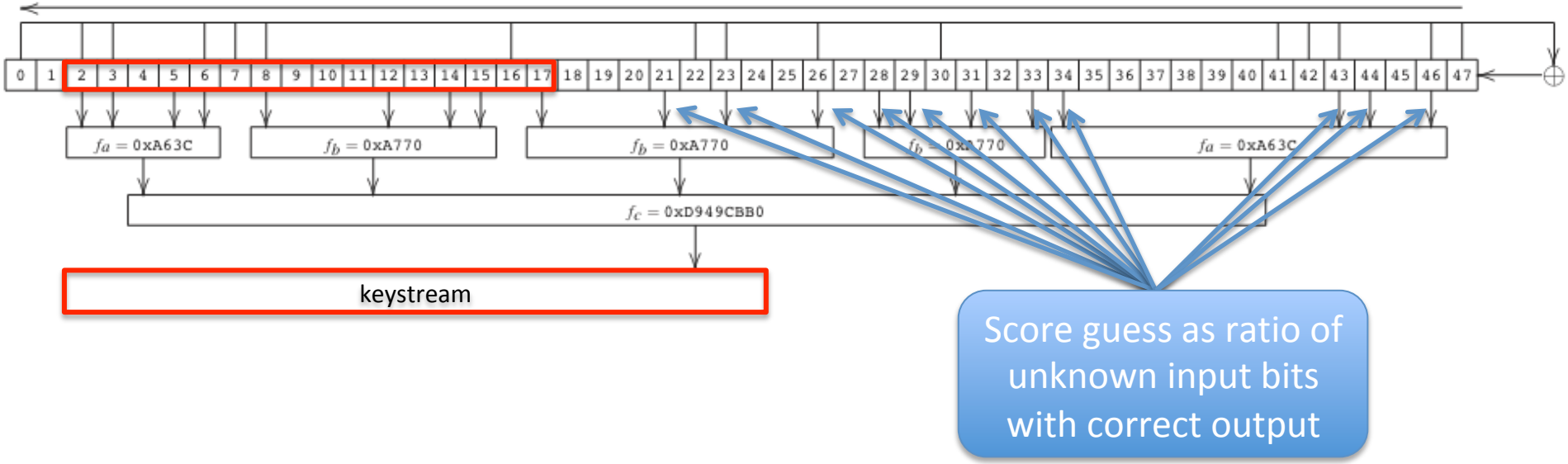


- Guess a 16-bit window value

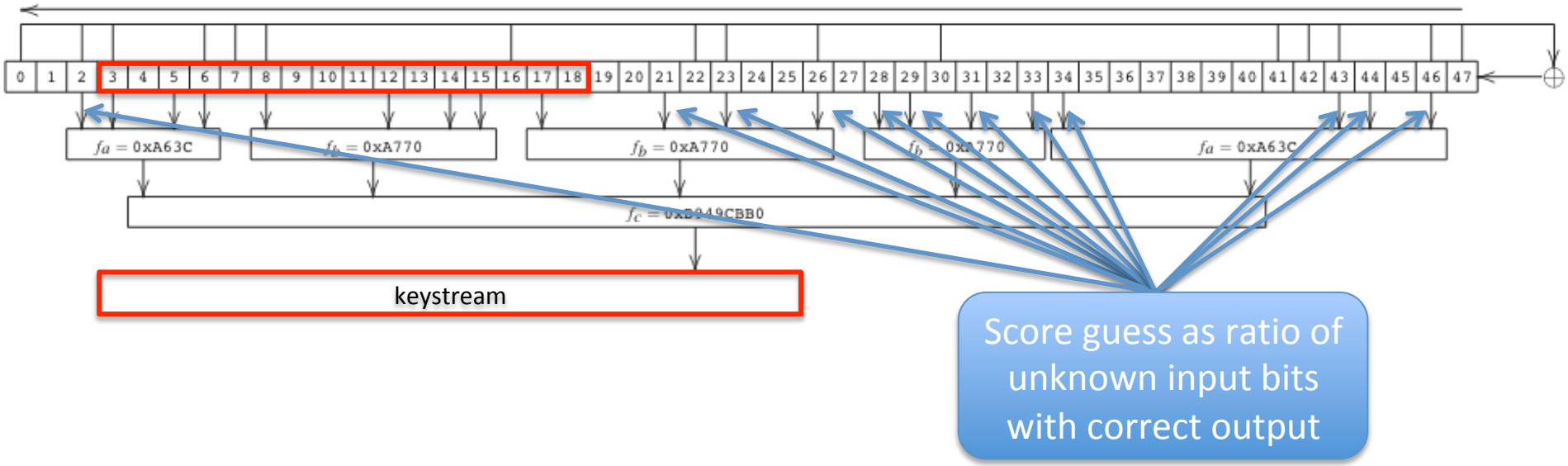
A fast correlation attack on Hitag2 (simplified)



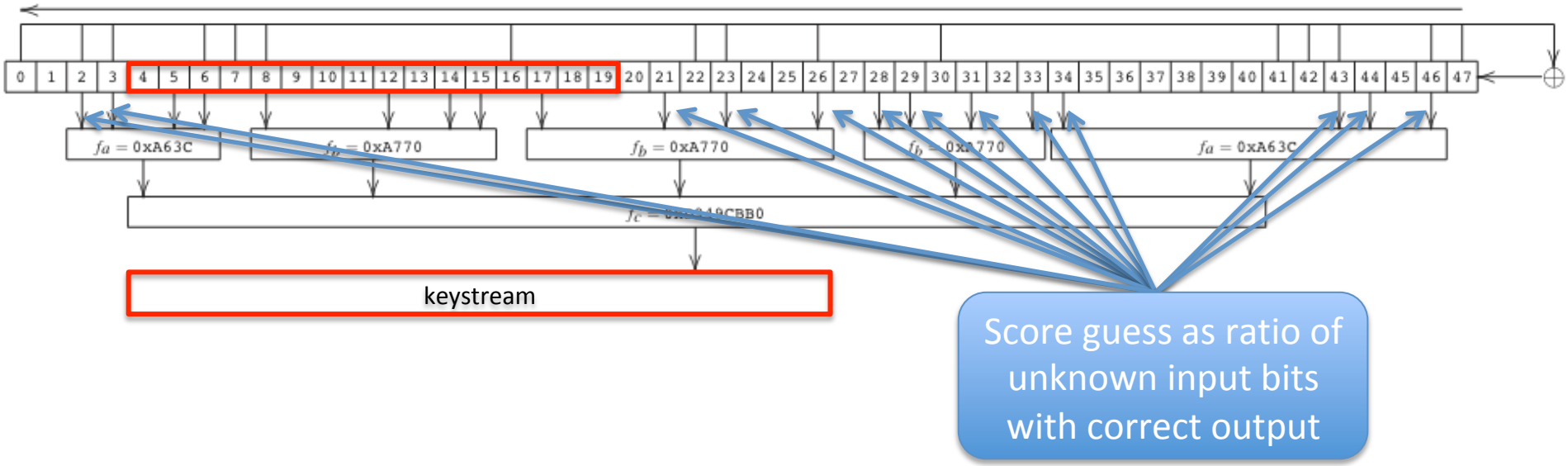
A fast correlation attack on Hitag2 (simplified)



A fast correlation attack on Hitag2 (simplified)

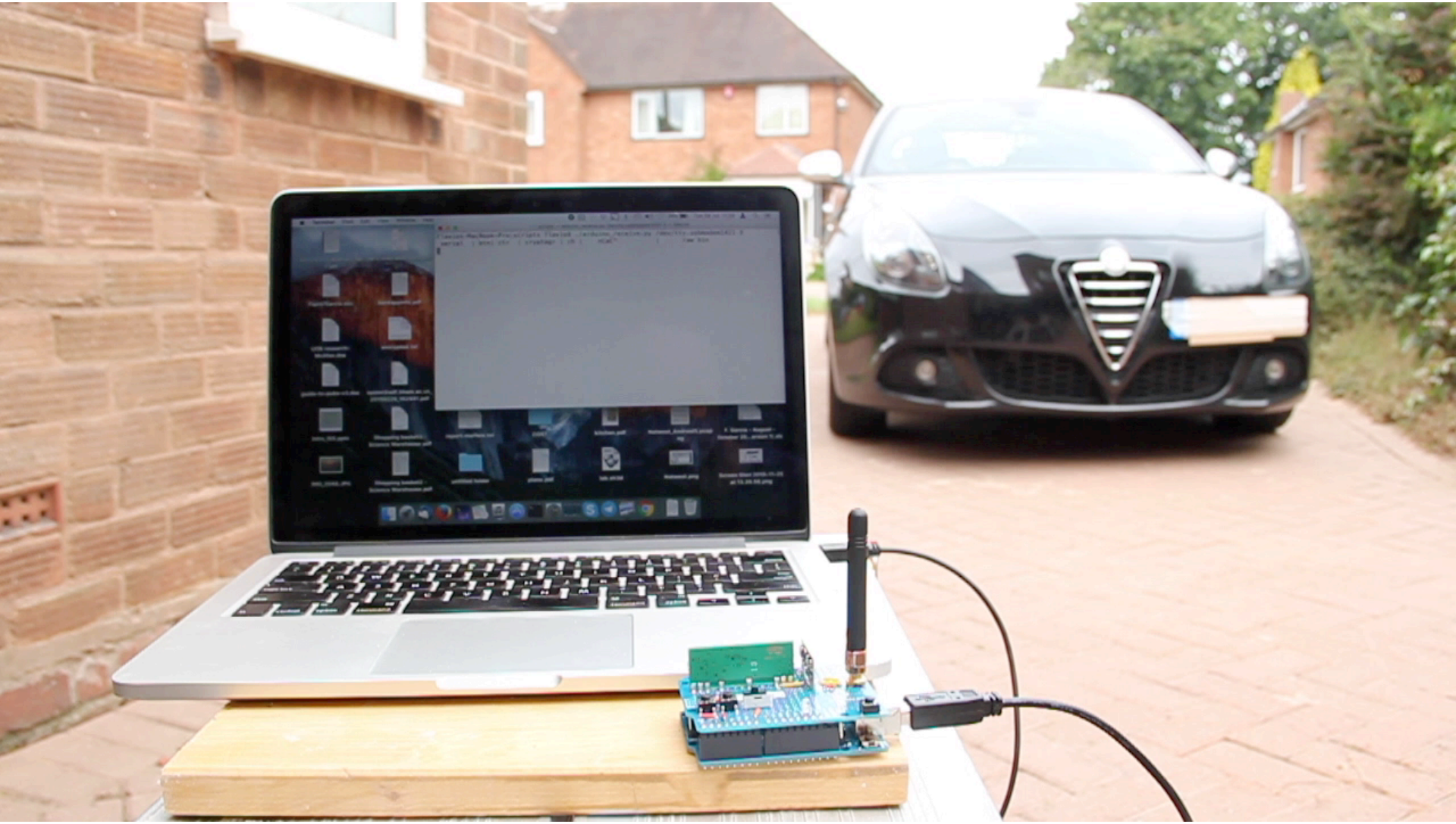


A fast correlation attack on Hitag2 (simplified)



- Discard overall low scoring guesses
- Increase window size by one
- Repeat
- Takes ~**1 minute** on a laptop to recover the key

Hitag2 RKE Attack Demo



Vehicles we tested using Hitag2 RKE

Manufacturer	Model	Year
Alfa Romeo	Giulietta	2010
Citroen	Nemo	2009
Dacia	Logan II	2012
Fiat	Punto	2016
Ford	Ka	2009,
Lancia	Delta	2009
Mitsubishi	Colt	2004
Nissan	Micra	2006
Opel	Vectra	2008
Opel	Combo	2016
Peugeot	207	2010
Peugeot	Boxer	2016
Renault	Clio	2011
Renault	Master	2011
Opel	Astra H	2008
Opel	Corsa D	2009
Fiat	Grande Punto	2009

Responsible disclosure

- We contacted VW Group in Dec 2015 and NXP Semiconductors in Jan 2016
- In general: good cooperation/ communication
- Many manufacturers are migrating to better chips
- NXP has AES-based products

Car key Summary

- 1 trace is enough for all 4 VW RKE systems
- 4 traces are enough to bypass Hitag2 immo
- ~8 traces for Hitag2 RKE

- This research may explain several mysterious theft cases/insurance claims without signs of forced entry

sign in search jobs more UK edition

theguardian
website of the year

home › tech UK world politics sport football opinion culture business all

Hacking

Millions of cars at risk as keyless entry systems can be hacked, report says

Cars that use Volkswagen's remote keyless entry system are vulnerable to theft using equipment costing £30, researchers claim

WIRED

A New Wireless Hack Can Unlock 100 Million Volkswagens

ANDY GREENBERG SECURITY 08.10.16 4:29 PM

A NEW WIRELESS HACK CAN UNLOCK 100 MILLION VOLKSWAGENS

SHARE
SHARE 14408
TWEET
PIN 41
COMMENT 21
EMAIL

The Washington Post

Sign In Subscribe

ch

Your car's keyless entry syst might help hackers unlock i

By Andrea Peterson August 12

the INQUIRER

Whitepapers Industry Voice SMB Spotlight Newsletter

News Artificial Intelligence Internet of Things Open Source All sections

Security

100 million Volkswagen cars vulnerable to wireless hack due to 20-year-old flaw

Car maker says 'there is no 100 per cent guarantee for security'

Carly Page
@CarlyPage_
12 August 2016

3 Comments

SECURITY RESEARCHERS have revealed that 100 million cars made by Volkswagen (VW) are vulnerable to hacks that could let thieves unlock them remotely through a wireless signal.

A duo of **computer experts at the University of Birmingham**, Flavio Garcia and David Oswald, have uncovered two flaws in VW's keyless entry systems that could

WHITEPAPERS

The new standard in wireless networks and supporting the future needs of clients

802.11n is certainly not dead and whilst manufacturers are still recommending 802.11n deployments, enterprise IT managers should give some thought…

NETS

A holistic view of application performance

Enterprise organisations are constantly being asked to do more work with fewer people, as the size and complexity of infrastructure…

NETS

Driving fundamental change in the way that IT organisations need to function

NBC NEWS HOME TOP VIDEOS DECISION 2016 ONGOING: ORLANDO NIGHTCLUB MASSACRE

U.S. WORLD LOCAL POLITICS HEALTH TECH SCIENCE POP CULTURE BUSINESS INVESTIGATIONS SPORTS MORE NIGHTLY NEWS TOD

BUSINESS AUG 11 2016, 11:58 AM ET

Millions of VW's Cars Can Be Hacked V Cheap Device, Experts Show

by REUTERS

SHARE

Tens of millions of vehicles sold by Volkswagen over the past 20 years are vulnerable to theft because keyless entry systems can be hacked using cheap technical devices, according to European researchers.

Computer security experts at the University of Birmingham in England have published a paper outlining how they were able to clone VW remote keyless entry controls by eavesdropping nearby when drivers press their key fobs to open or lock up their cars.

▶ **Volkswagen to pay US auto dealers restitution after emissions scandal** 0:22

Vehicles vulnerable to this attack include most Audi, VW, Seat and Skoda models sold since 1995 and many of the approximately 100 million VW Group vehicles on the road since then, the researchers said. The flaw was found in car models as recent as the Audi Q3, model year 2016, they added.

BBC Sign in News Sport Weather

NEWS

Home UK World Business Politics Tech Science Health

Technology

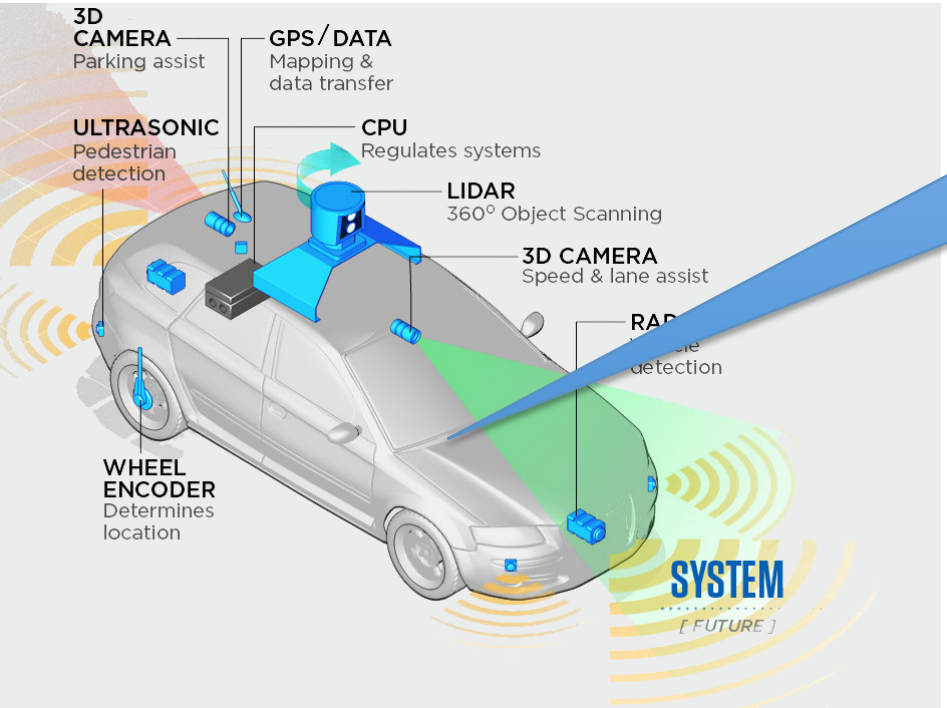
'Millions' of Volkswagen cars can unlocked via hack

By Chris Baraniuk
Technology reporter

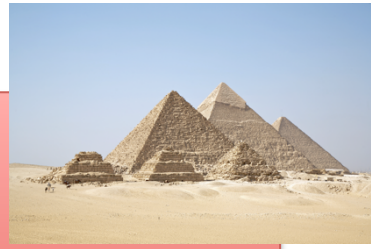
12 August 2016 | Technology

The problem affects many millions of cars, according to researchers

Connected and Autonomous Vehicles



- 100s of ECUs
- 100s million lines of code
- Sensors + fusion algorithms
- V2V, V2I communication
- No driver
- Summon your car with an app?



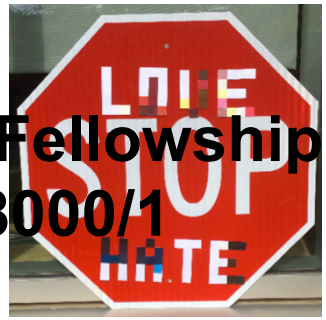
Goal

To secure the vehicle's attack surfaces

Research Challenges

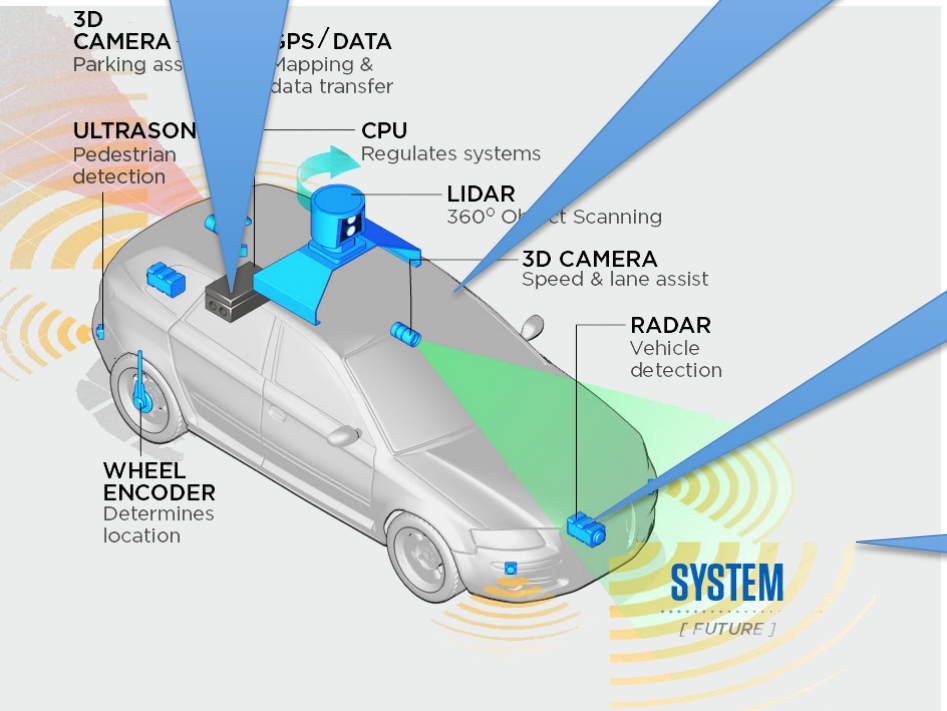
Securing ECU firmware
- Epsilon firmware updates
- Side-channel and fault resilience

Automated security testing tools
- Protocol State Fuzzing
- Static analysis + machine learning



EPSRC Fellowship EP/R008000/1

Securing Sensors
- Radar
- Lidar
- MEMS (accelerometer)
- Cameras
- Underlying fusion algorithms



Hardware anchored V2X
- Authentication + privacy
- Low-latency crypto

Thanks for your attention!