Attacks on wireless localization
The case of PKES

Christian Müller

4 July 2012

Terms

PKE system

passive **k**eyless **e**ntry system

CID

Customer **I**dentification **D**evice

Mechanical keys

- Mechanical key & lock systems
- Immobilisers

Remote key Systems

- Button to open
- Operate at RF
- Physical key to ignite engine

Passive keyless entry systems

- Car opens when CID is in range
- Engine can be ignited if the key is in the vehicle
- Physical backup key

PKES in detail

1. Pulling handle transmits a LF-signal
2. CID wakes up and responds in RF
3. If response is correct, the vehicle opens

- Same holds for ingiting the engine
- Usually enhanced by RFID

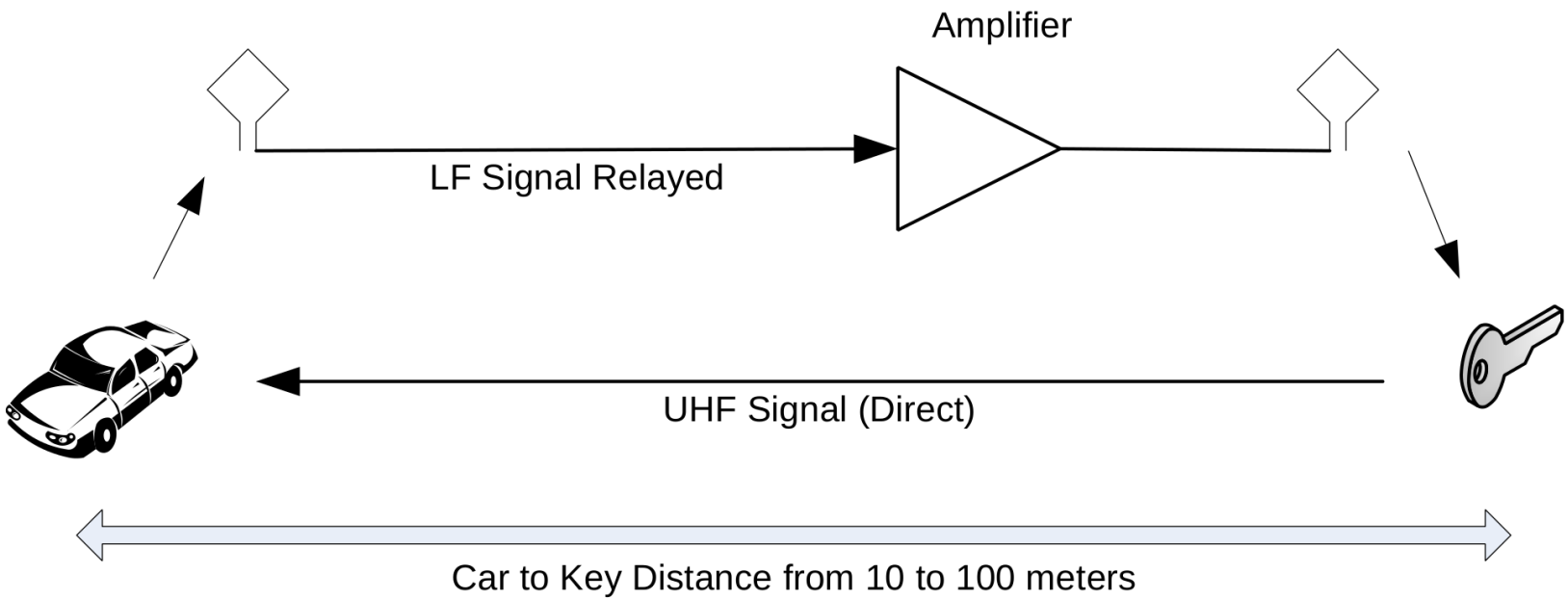
Introduction

- Relocating signal emission & reception
- Underlying problem: proper localization in wireless networks
- Circumvents higher level authentication

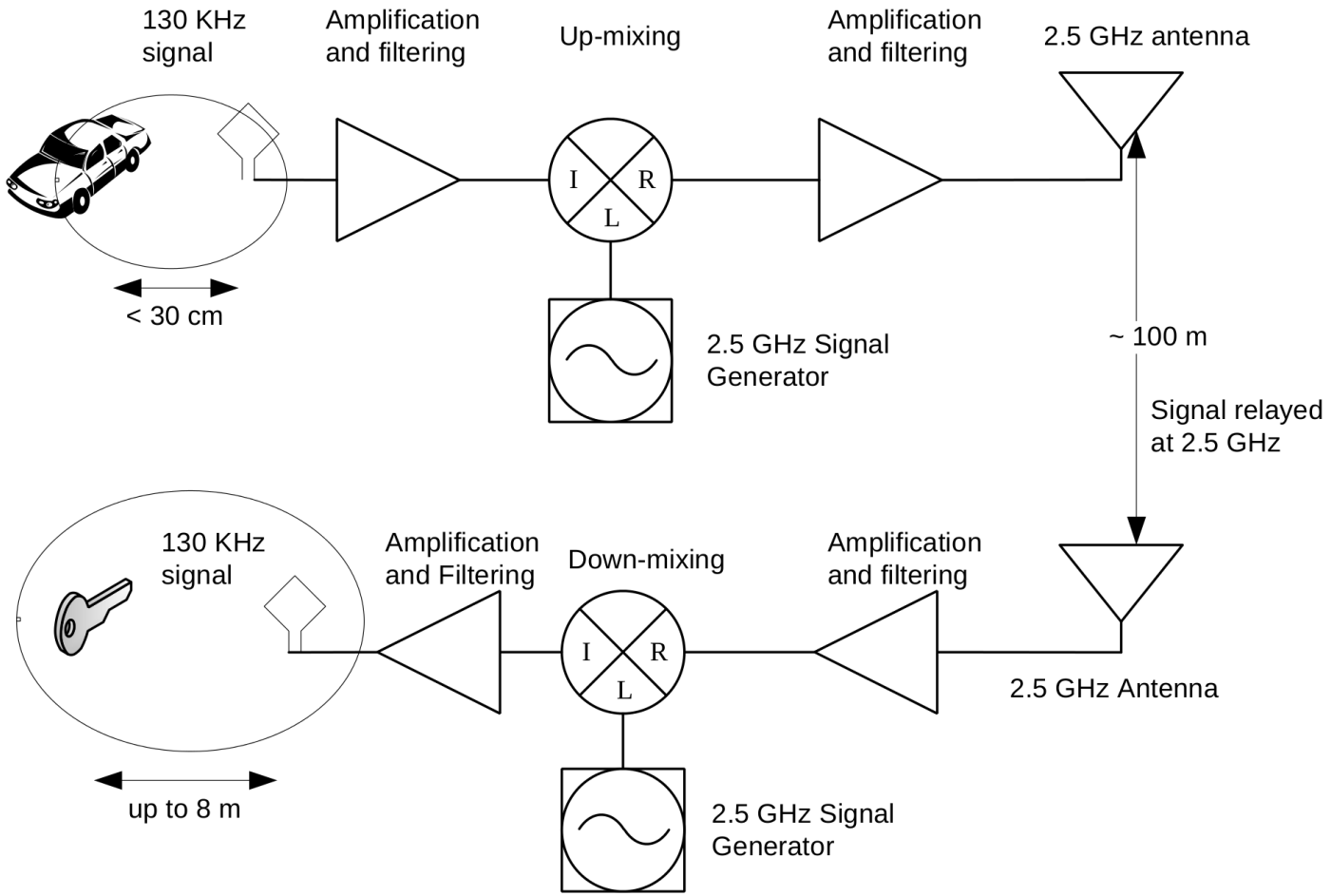
Two thieves

- Thief 1 next to the vehicle
- Thief 2 near the CID
- Relay between both thieves

Relay over the cable



Relay over the wire



This works in practice

- Simple & inexpensive
- Tested by Francillon, Danev, and Capkun [2011]
- All ten systems vulnerable

Results of tests

Car model	Maximum Delay		Key Response (std dev)		Key Response Time Spread	
1	500	µs	1782	µs (±8)	21	µs
2	5000	µs	11376	µs (±15)	47	µs
4	500	µs	-		-	
5	1000	µs	5002	µs (±4)	11	µs
6	10000-20000	µs	23582	µs (±196)	413	µs
7	620	µs	1777	µs (±12)	25	µs
8	620	µs	437	µs (±70)	162	µs
9	2000	µs	1148	µs (±243)	436	µs
10	35	µs	2177	µs (±8)	12	µs

Table: Experimentally tested maximum delay, key response time and spread per model, from Francillon et al. [2011]

Results of tests

- Attack works on all systems
- For “convenient” attack, amplification is required
- Relay can be established over long distances

Scenarios

- Supermarket
- Office

Implications

- Steal the car

Implications

- Steal the car
- Access to the vehicle
  $\rightarrow$ "Experimental Security Analysis of a Modern Automobile" by Koscher et al. [2010]

short term

- Fall back to mechanical keys

short term

- Fall back to mechanical keys

long term

- Highlight action on the CID

short term

- Fall back to mechanical keys

long term

- Highlight action on the CID

long term

- Multi channel [Stajano et al., 2010]
- Distance bounding protocols [Brands and Chaum, 1994]

Multichannel communication

- Use two frequencies or types of media
- Makes relaying more difficult
- More difficult to implement

Distance bounding protocols

- Be quick
- Be strict on timing
- Has vulnerabilities

Distance bounding protocol

1. A generates a nonce
2. A sends nonce in reverse bitorder to B and starts timer
3. B will respond with the xored nonce in correct bit order
4. A stops timer upon receiving of the correctly xored nonce
5. A deduces distance from time-of-flight

Summary

- PKE systems are vulnerable to relay attacks
- Attacks can be performd easily
- Solutions are at hand, but not free from vulnerabilities

Literature

A.I. Alrabady and S.M. Mahmud. Some attacks against vehicles' passive entry security systems and their solutions. *Vehicular Technology, IEEE Transactions on*, 52(2):431 – 439, march 2003. ISSN 0018-9545. doi: 10.1109/TVT.2003.808759.

Stefan Brands and David Chaum. Distance-bounding protocols. In Tor Helleseth, editor, *Advances in Cryptology — EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 344–359. Springer Berlin / Heidelberg, 1994. ISBN 978-3-540-57600-6. URL http://dx.doi.org/10.1007/3-540-48285-7_30. 10.1007/3-540-48285-7_30.

S. Capkun and J.-P. Hubaux. Secure positioning in wireless networks. *Selected Areas in Communications, IEEE Journal on*, 24(2):221 – 232, feb. 2006. ISSN 0733-8716. doi: 10.1109/JSAC.2005.861380.

Jolyon Clulow, Gerhard Hancke, Markus Kuhn, and Tyler Moore. So near and yet so far: Distance-bounding attacks in wireless networks. In Levente Buttyán, Virgil Gligor, and Dirk Westhoff, editors, *Security and Privacy in Ad-Hoc and Sensor Networks*, volume 4357 of *Lecture Notes in Computer Science*, pages 83–97. Springer Berlin / Heidelberg, 2006. ISBN 978-3-540-69172-3. URL http://dx.doi.org/10.1007/11964254_9. 10.1007/11964254_9.

Aurélien Francillon, Boris Danev, and Srdjan Capkun. Relay attacks on passive keyless entry and start systems in modern cars. *IACR Cryptology ePrint Archive*, 2011, 2011. URL http://dx.doi.org/10.3929/ethz-a-006708714.

Yih-Chun Hu, A. Perrig, and D.B. Johnson. Wormhole attacks in wireless networks. *Selected Areas in Communications, IEEE Journal on*, 24(2):370 – 380, feb. 2006. ISSN 0733-8716. doi: 10.1109/JSAC.2005.861394.

Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage. Experimental security analysis of a modern automobile. In *Security and Privacy (SP), 2010 IEEE Symposium on*, pages 447 –462, may 2010. doi: 10.1109/SP.2010.34.

P. Schaller, B. Schmidt, D. Basin, and S. Capkun. Modeling and verifying physical properties of security protocols for wireless networks. pages 109 –123, july 2009. ISSN 1063-6900. doi: 10.1109/CSF.2009.6.

Frank Stajano, Ford-Long Wong, and Bruce Christianson. Multichannel protocols to prevent relay attacks. 6052: 4–19, 2010. URL http://dx.doi.org/10.1007/978-3-642-14577-3_4. 10.1007/978-3-642-14577-3_4.

Questions?

Thank you!

Thank you for your attention!