LOCK IT AND STILL LOSE IT

ON THE (IN)SECURITY OF AUTOMOTIVE REMOTE KEYLESS ENTRY SYSTEMS

Mushary Ali Alghamdi

PROBLEM BEING ADDRESSED

Singling out the vulnerability of remote keyless entry (RKE) systems for locking and unlocking a car based on rolling codes that are major car manufacturers.

These are vulnerabilities in VW group systems and Hitag2 rolling code system

HITAG2

MOTIVATION OF RESEARCH

- The researchers were motivated by lack of research on the topic of insecurity in remote keyless entry systems.
- It was done by assessing vulnerabilities that exist in of remote keyless entry schemes used by vehicle manufacturers.

ASSUMPTIONS MADE BY AUTHORS

- All systems from VW-1 to VW-4 used by VW vehicle group used implicit authentication such that the correctness of the rolling code was checked after decryption.
- The assumption made is realistic.

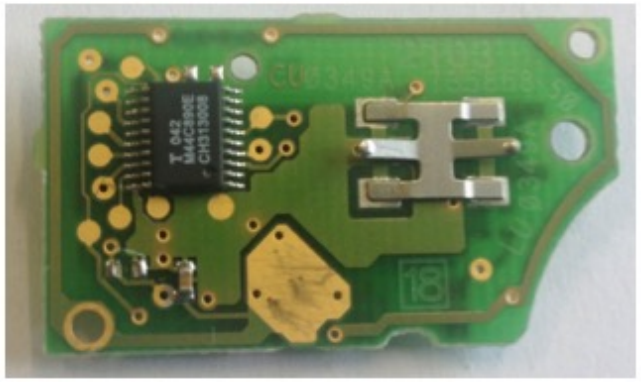


Figure 4: PCB of an older VW Group remote control using a MARC4 µC

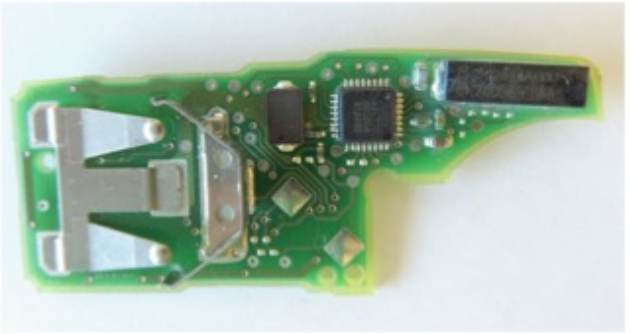
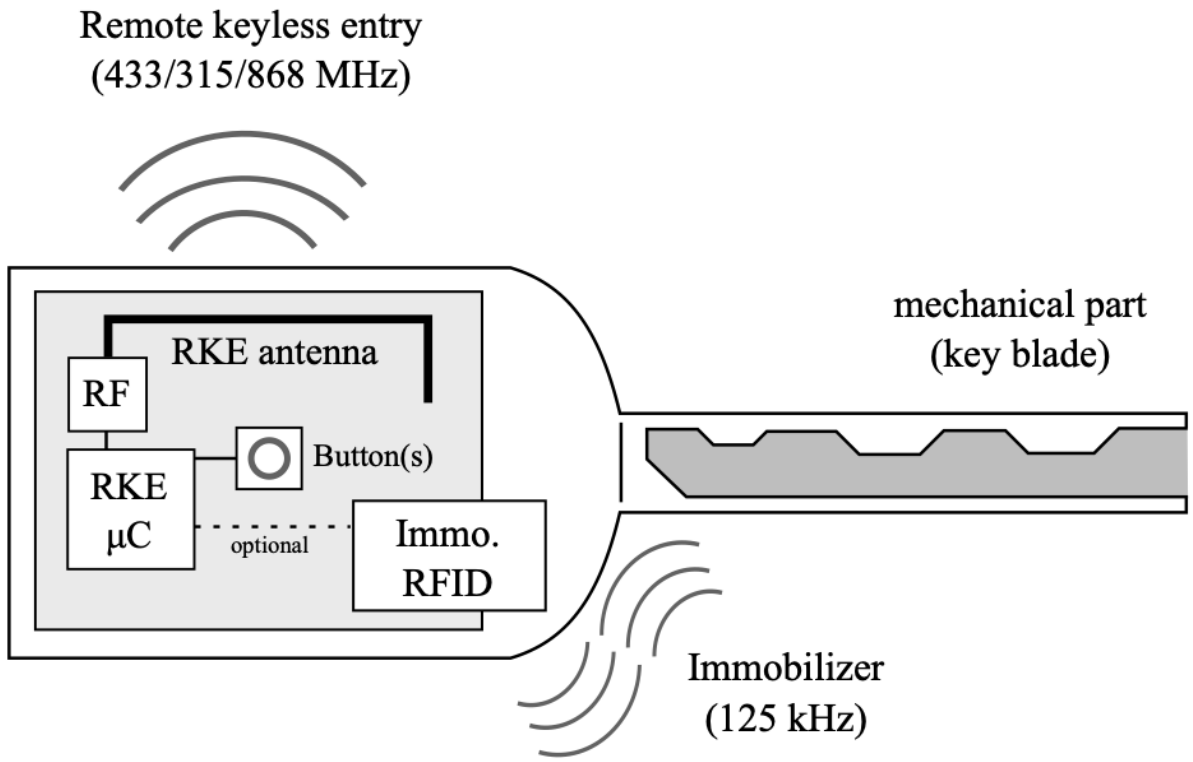


Figure 5: PCB of a newer VW Group remote control using an unidentified µC

PROPOSED SOLUTIONS

- Remote keyless entry systems should be secured by both secure cryptographic algorithms and secure key distribution.
- Firmware update or exchange of both the respective Electronic Control Units and the vehicle key containing the remote control could be used as a temporary solution.
- Disabling and removing the remote keyless entry in a vehicle and instead use a mechanical lock.



PROOF OF HYPOTHESIS

- The researchers present vulnerabilities of remote keyless entry used by vehicle manufacturers to prove that these systems are insecure.
- They prove the hypothesis using two case studies;
  - First for VW Group vehicles
  - Second for Hitag2 rolling code scheme used in vehicles
- In the VW Group case study, they recover the cryptographic algorithms and keys from electronic control units to prove that original remotes could be cloned.
- In the Hitag2 rolling code scheme case study, they describe this scheme and present a novel correlation-based attack on this system.

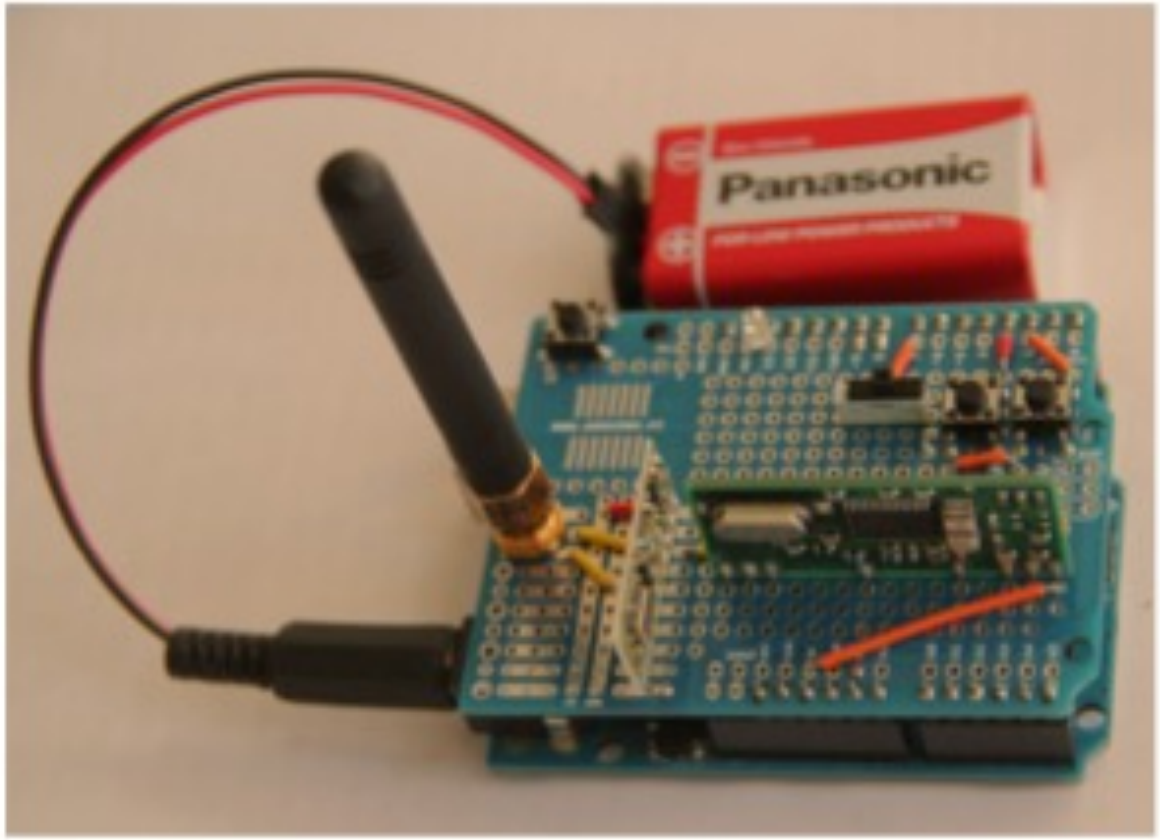


Figure 2: Arduino-based RF transceiver

MAIN RESULTS

- VW Group and the Hitag2 rolling code schemes are vulnerable to eavesdropping to clone the original remote and gain unauthorized access to the vehicle.
- VW group system vulnerabilities are caused by worldwide master keys,
- Hitag2 RKE system vulnerabilities are caused by cryptographically weak cipher
- It is possible to break VW group schemes with a single eavesdropped signal.
- Hitag2 RKE system attacks require at lest four rolling codes. However selective jamming of the signal during the final checksum byte allows the attacker to quickly obtain the rolling codes required.

Manufacturer	Model	Year
Alfa Romeo	Giulietta	2010
Chevrolet	Cruze Hatchback	2012
Citroen	Nemo	2009
Dacia	Logan II	2012
Fiat	Punto	2016
Ford	Ka	2009, 2016
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

CONCLUSIONS

- VW Group systems and Hitag2 rolling code scheme are vulnerable to cloning the original remote control.
- The use of remote keyless entry (RKE) systems for locking and unlocking a car puts the owner of the vehicle at a risk of theft of belongings left in a car and theft of vehicle components.

THOUGHTS ABOUT THE PAPER

- The paper informatively exposes vulnerabilities the remote keyless entry (RKE) systems in VW group systems and Hitag2 rolling code.
- It proves that using remote keyless entry (RKE) systems for locking and unlocking a car exposes the vehicle to risks.
- The paper expresses solutions including disabling and removing the remote keyless entry in a vehicle and instead use a mechanical lock.

SMART KEY VS TRADITIONAL KEY

QUESTIONS?

THANK YOU FOR YOUR TIME

SOURCES

1. Garcia, F. D., Oswald, D., Kasper, T., & Pavlides, P. (2016). Lock It and Still Lose It—on the ({In) Security} of Automotive Remote Keyless Entry Systems. In *25th USENIX security symposium (USENIX Security 16)*. https://doi.org/10.5555/3241094.3241166
2. https://surelockkey.com/blog/the-different-types-of-car-keys/