Car security: remote keyless "entry and go"

Dick Visser and Jarno van de Moosdijk

June 2009

Mechanical key

- Ignition locks since 1919
- Door locks since late 1920s
  - RFID immobiliser since 1993

Remote keyless entry (RKE)

- Remote control for doors
- Since 1983
- 315 / 433.92 / 868 MHz
- Keys have to be associated to the car
- Encryption
  - KeeLoq cipher

Passive keyless entry (PKE)

- Doors open/close without user intervention
- Since 1990
- Same frequencies
- Same encryption
  - Often combined with “keyless go”

Future systems

- Lots of development
- Mostly flashy concept car stuff
- Integration is the “key”
  - Payment systems, multimedia, user prefs

Research questions

- What requirements should RKE/PKE adhere to?
- Which systems are available and do they meet these requirements?

Research questions

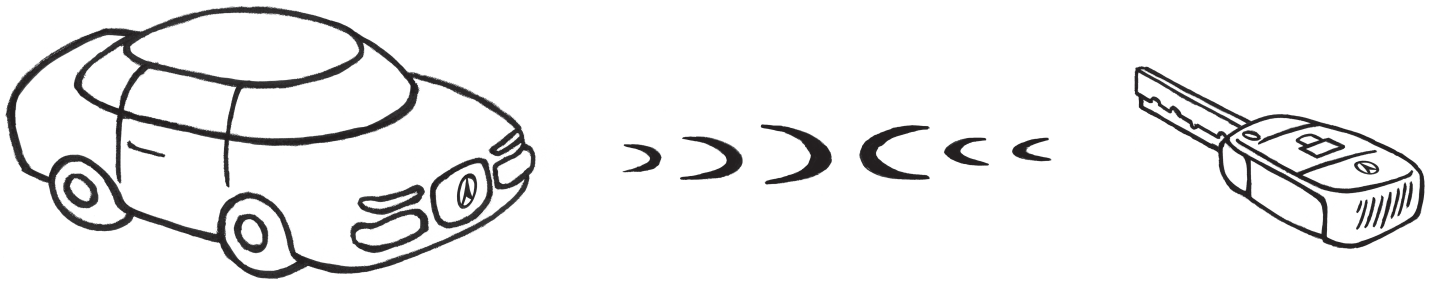
- What requirements should RKE/PKE adhere to?
- Which systems are available and do they meet these requirements?
- What requirements should the key order procedure adhere to?
- What are current order procedures and do they meet these requirements?

Method

- Defining requirements & threats analysis
- Interviewing car dealers, importers, key manufacturers
- Examining car key fobs
- Assessing current systems and procedures

System architecture

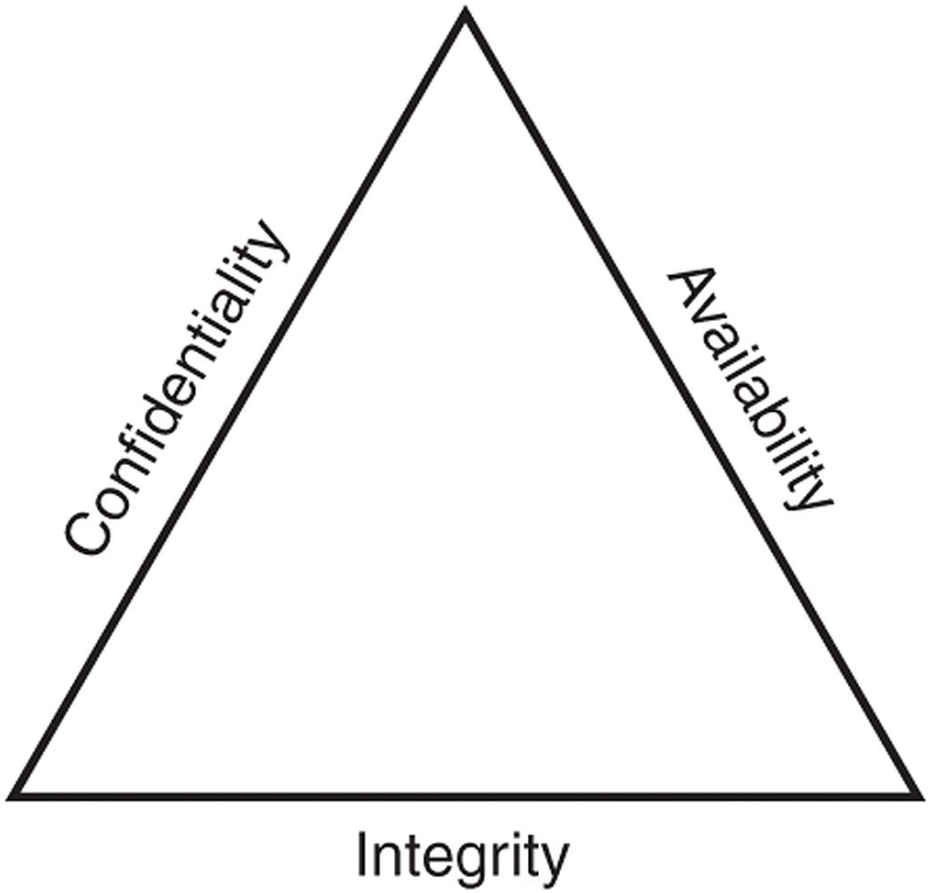
Parts of the car access process



System architecture

Parts of the new/spare key order procedure

CIA Triad



STRIDE threat model (Microsoft)

- **S**poofing identity
- **T**ampering with data
- **R**epudiation
- **I**nformation disclosure
- **D**enial of service
- **E**levation of privilege

CIA vs STRIDE

	Confidentiality	Accountability	Authenticity	Authorisation	Data integrity	Availability
Spoofing identity			✓			
Tampering with data					✓	
Repudiation		✓				
Information disclosure	✓					
Denial of service						✓
Elevation of privilege				✓		

Threat demo

Real world DoS demo

Establishing requirement sets

Apply CIA/STRIDE to car access procedure items
Examples:

- Key/car should use authentication (S car/key)
- Cars should log all lock status changes (R - car)
- Key-car communication should not leak information (I - medium)

Establishing requirement sets

Applied CIA/STRIDE to key order procedure
Examples:

- Keys should be shipped to static address (S)
- Four-eye principle (R)
- Online key learning (R,E)

Highlights

General:

- Huge amount of different systems (brand/model/version/year...)
- Smaller set of chipset manufacturers
- Kerckhoffs' principle is used by no one

Highlights

"If everything, except the key, is known, a car would become unsecure very soon due to the fast growing computing power of IT technology compared to automotive technology and their life cycle."

Highlights

General:

- Huge amount of different systems (brand/model/version/year...)
- Smaller set of chipset manufacturers
- Kerckhoffs' principle is used by no one
- Investigating order procedures was less problematic

Highlights

Car access process:

- All use proprietary black box systems
- No one uses key authentication/authorisation
- Majority of ECUs do not log which key changed lock status

Highlights

Key order/learning procedure:

- All dealers require ID + proof of ownership
- None of them use four-eye principle
- Only few brands use online learning/logging
- Third party key manufacturers all use plain text HTTP

Recommendations

1. Car industry should honour Kerckhoffs' principle
2. Keys should use authentication
3. Cars and keys should use logging
4. All manufacturers should use online learning/logging
5. Third parties should use HTTPS

Further research

1. Relay attack PoC
2. Security certification
3. Cryptanalysis/reverse engineering
4. DoS/User awareness test

Questions?