SYSTEM AND NETWORK ENGINEERING MSc

Research Project I

PROTECTING AGAINST RELAY ATTACKS FORGING INCREASED DISTANCE REPORTS

Xavier Torrent Gorjón
xavier.torrentgorjon@os3.nl

Supervisors:

Paul van Iterson
vanIterson.Paul@kpmg.nl

Jordi van den Breekel
vandenBreekel.Jordi@kpmg.nl

Summary

- Distance-bounding protocols
- Feasibility of the attack: study cases
  - Autonomous Cars
  - Drone MANETs (Mobile Ad-Hoc NETworks)
- Limitations of other systems
- Preventing increased distance reports
  - Behavior verification
  - Multiple distance-bounding signals
  - Distributed knowledge
- Conclusions

Summary

- Distance-bounding protocols
- Feasibility of the attack: study cases
  - Autonomous Cars
  - Drone MANETs (Mobile Ad-Hoc NETworks)
- Limitations of other systems
- Preventing increased distance reports
  - Behavior verification
  - Multiple distance-bounding signals
  - Distributed knowledge
- Conclusions

Distance-bounding protocols

- With the current implementations, closer distances cannot be faked.
  - Proof through *physical limitations*: cannot go faster than the speed of light.
  - Need for a *shared nonce* and a *fast processing* time.

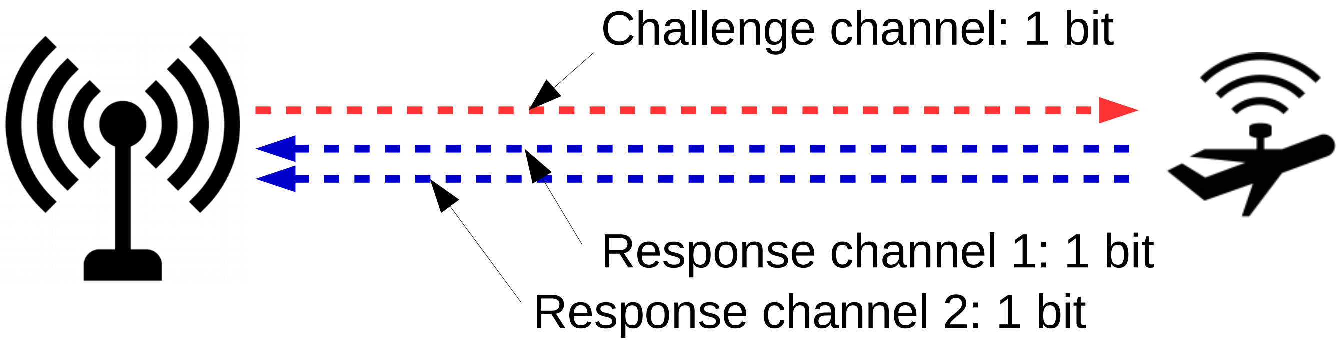

Figure 1: Distance-bounding protocol. Each challenge bit is answered with two bits: one in the communication and another one in the form of channel selection.

Distance-bounding protocols

- Current implementations can be used to prevent a wide range of attacks that attempt to fake *decreased distance* reports, generally on Access Control Systems.

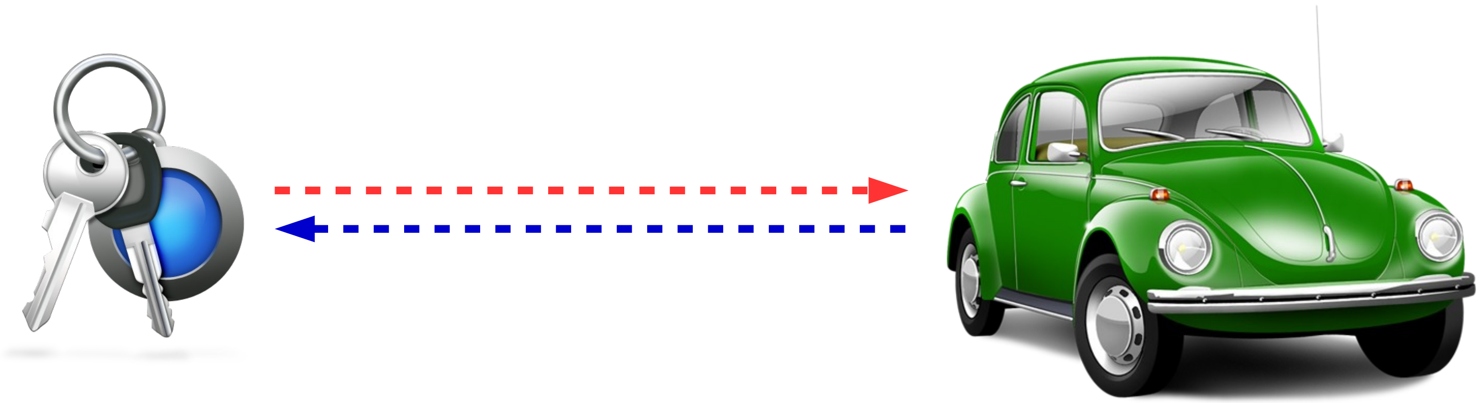

Figure 2: Distance-bounding protocols can be used to protect Passive Key Entry Systems (PKES).

Distance-bounding protocols

- However, current distance-bounding protocols *do not* prevent *increased distance* reports.
  - Physical limitations cannot be used.
  - This leads to our research questions:
    - Study the feasibility of relay attacks forging increased distance reports.
    - How can these relay attacks be prevented.

Summary

- Distance-bounding protocols
- Feasibility of the attack: study cases
  - Autonomous Cars
  - Drone MANETs (Mobile Ad-Hoc NETworks)
- Limitations of other systems
- Preventing increased distance reports
  - Behavior verification
  - Multiple distance-bounding signals
  - Distributed knowledge
- Conclusions

Feasibility of the attack: study cases

- Autonomous Cars
  - If two cars believe they are further away than they really are, they might crash.
  - Other systems might prevent this, but distance-bounding protocols could be an additional safety measure.

Figure 3: An early design of a fully autonomous car by Google.

Feasibility of the attack: study cases

- Drone MANETs I: Autonomous delivery service
  - To save costs, multiple drones could be used to carry large packages.
  - Tempering the distance awareness of these drones might cause them to lose equilibrium and fall.

Figure 4: A delivery drone by Amazon.

Feasibility of the attack: study cases

- Drone MANETs II: Area surveillance
  - Drones can be used to check areas for multiple purposes: military operations, updating maps, searching for lost people...
  - Erroneous distance reports can lead to leave areas unexplored.

Summary

- Distance-bounding protocols
- Feasibility of the attack: study cases
  - Autonomous Cars
  - Drone MANETs (Mobile Ad-Hoc NETworks)
- Limitations of other systems
- Preventing increased distance reports
  - Behavior verification
  - Multiple distance-bounding signals
  - Distributed knowledge
- Conclusions

Limitations of other systems

- It could be argued that distance-bounding protocols were not made for this purpose.
- However, other location systems present difficulties as well.

Limitations of other systems

- GPS location
- Radar detection
- Inertial Navigation System

Limitations of other systems

- GPS location
  - Can be disrupted
  - Sometimes *not reliable* even in non-dangerous environments.

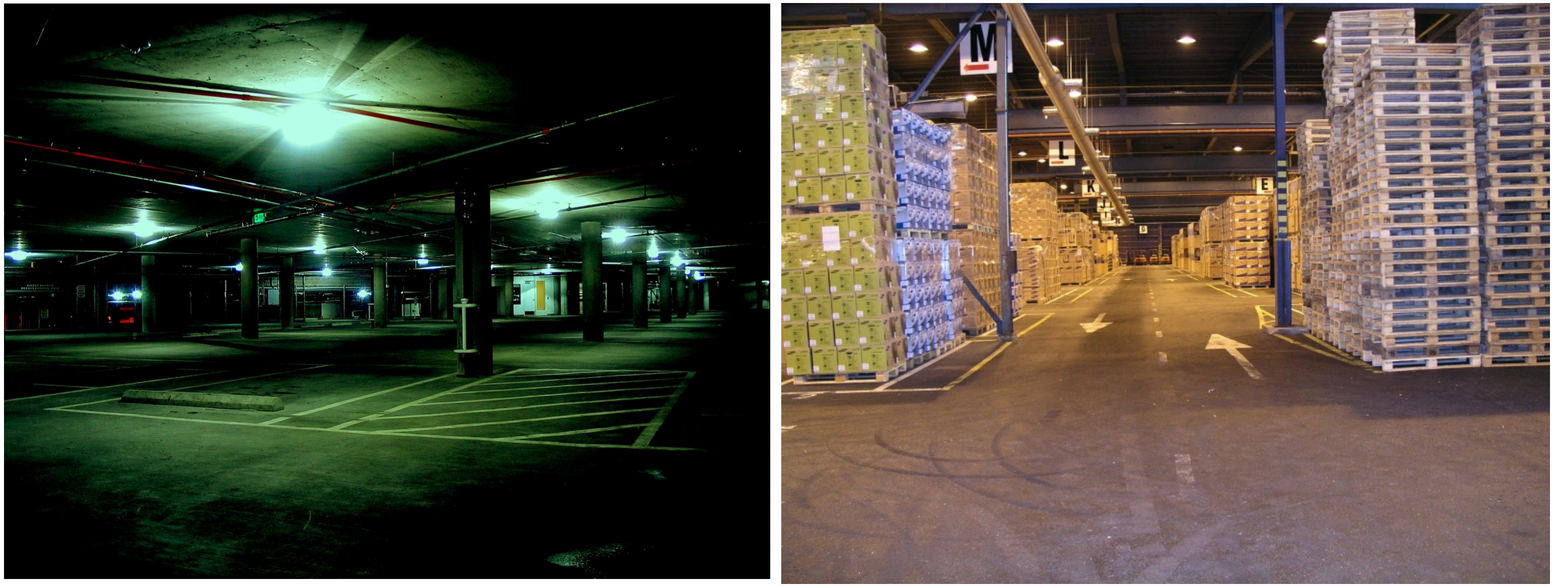

Figure 5: GPS requires unobstructed line of sight with satellites to work. This limits its usability inside buildings or underground.

Limitations of other systems

- Radar detection
  - Systems could attempt to *physically detect* attackers
  - Problem: stealth technology *surpasses* anti-stealth technology in the current state of the art

Figure 5: The US F117 is a 13m wide airplane, but under the radar it appears to have the same size as a bird.

Limitations of other systems

- Inertial navigation system
  - Fits perfectly our purpose, but it cannot be reliably used as a stand-alone positioning system due its accuracy. This may change in the future.

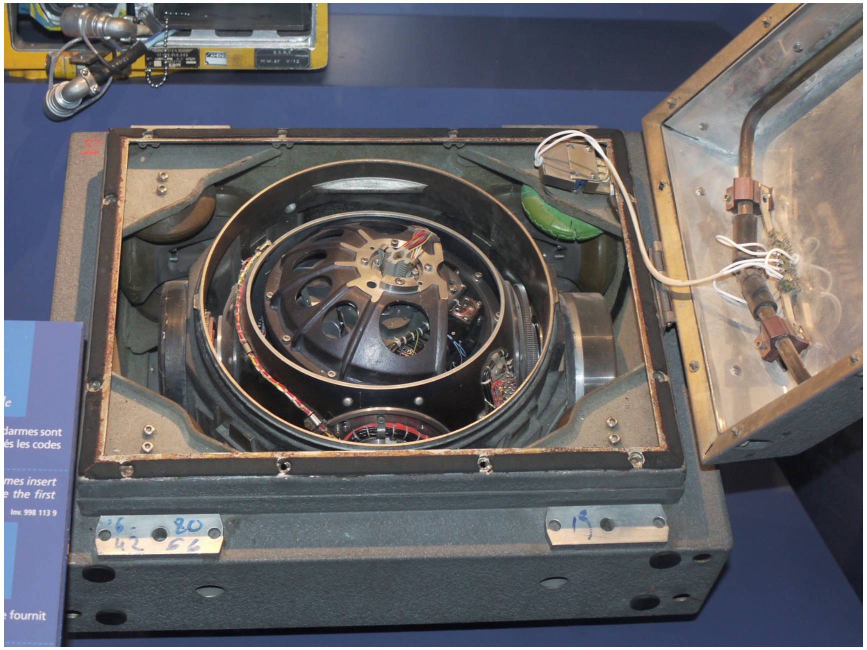

Figure 6: An Inertial Navigation System used by the French army.

Summary

- Distance-bounding protocols
- Feasibility of the attack: study cases
  - Autonomous Cars
  - Drone MANETs (Mobile Ad-Hoc NETworks)
- Limitations of other systems
- Preventing increased distance reports
  - Behavior verification
  - Multiple distance-bounding signals
  - Distributed knowledge
- Conclusions

Preventing increased distance reports

- Behavior verification
  - Similar idea to Intruder Detection System on networking environments.
  - Attempt to detect sudden changes in the received data, such as *signal strength* or *large variations* on the reported locations.

Preventing increased distance reports

- Multiple distance-bounding signals
  - Original distance-bounding only attempts to check if a reporter is inside or outside a certain range.
  - Use multiple distance-bounding signals to obtain approximate location, not only distance.

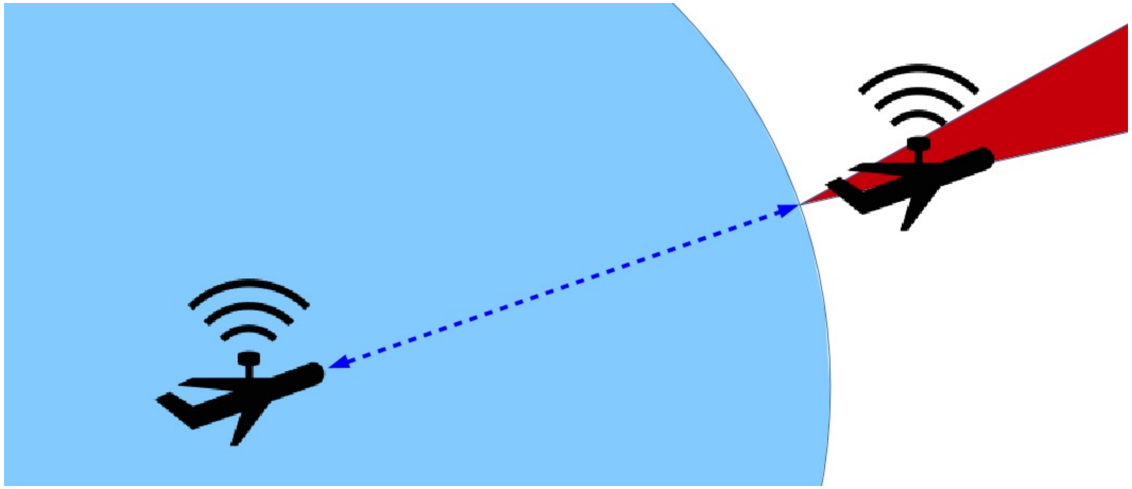

Figure 7: Multiple signals difficult attacks on the system, as attackers need to coherently fake multiple distances. However, distance in a straight line is still easy to fake.

Preventing increased distance reports

- Distributed knowledge
  - Instead of relying only on its own measurement, a node could also ask for the measurements of other nodes.
  - It would be extremely difficult for an attacker to fake multiple different distances at the same time.

Summary

- Distance-bounding protocols
- Feasibility of the attack: study cases
  - Autonomous Cars
  - Drone MANETs (Mobile Ad-Hoc NETworks)
- Limitations of other systems
- Preventing increased distance reports
  - Behavior verification
  - Multiple distance-bounding signals
  - Distributed knowledge
- Conclusions

Conclusions

- Most of the systems discussed are not employed nowadays but they are a *latent problem*.
- Lower-distance bound cannot rely on physical limitations for its security: *difficult to achieve perfect security*.
- Proposed solutions -specially a combination of them- reduce the changes of performing an attack without the system noticing it.

Questions?