Long Distance Relay Attack

Luigi Sportiello

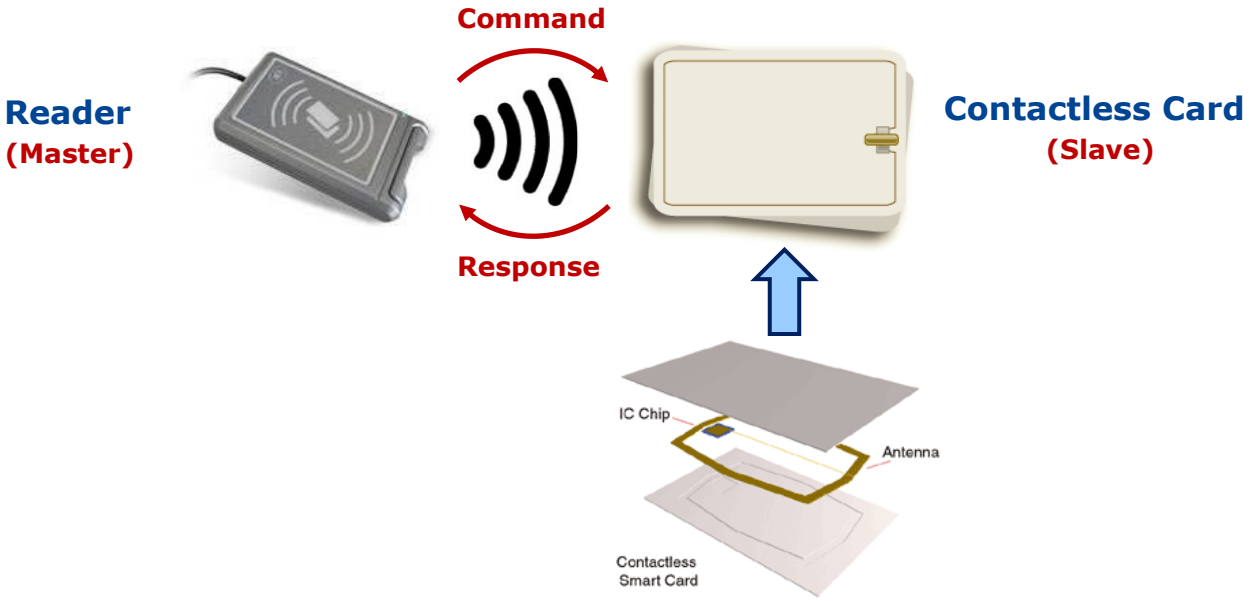
Joint Research Centre
Institute for the Protection and the Security of the Citizen

European Commission

Smart Cards

- ”Something you have”
  - Secure data storage
  - Qualify the holder for operations
- Two possible communication technologies
  - Contact
  - *Contactless*

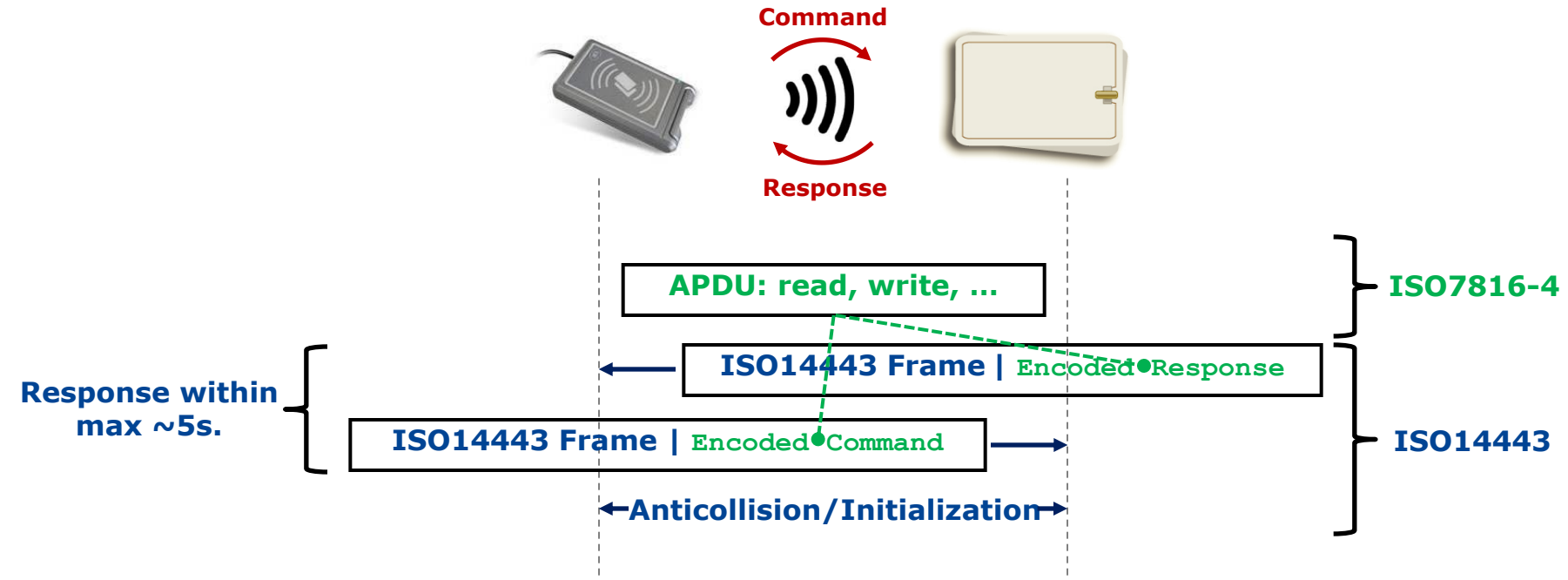
Contactless Smart Cards



- Some characteristics:
  - quick interactions
  - working distance: typically few cm

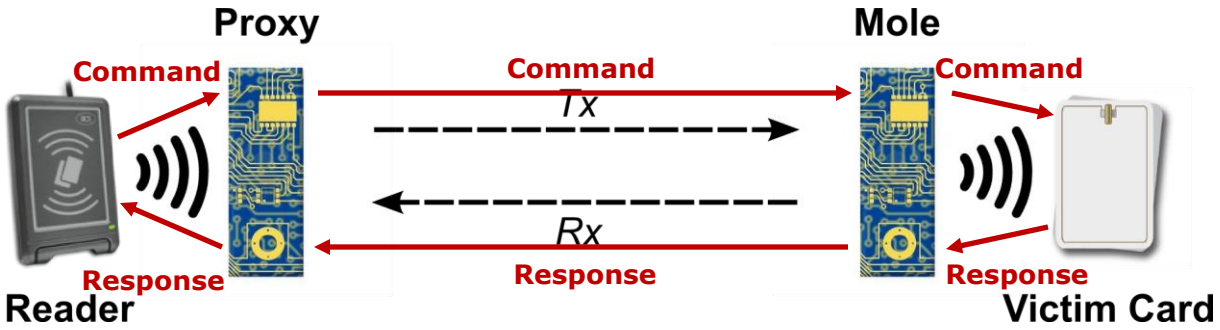
Reader-Card Communication Protocol

- ISO 14443 (+ ISO 7816-4) common solution for many contactless smart card
- Some time constraints during the communication



Relay Attack Against a Contactless Smart Card

- Two devices are needed:
  - Proxy: emulates a contactless smart card
  - Mole: acts as reader nearby the victim card
- Communication channel between Proxy and Mole



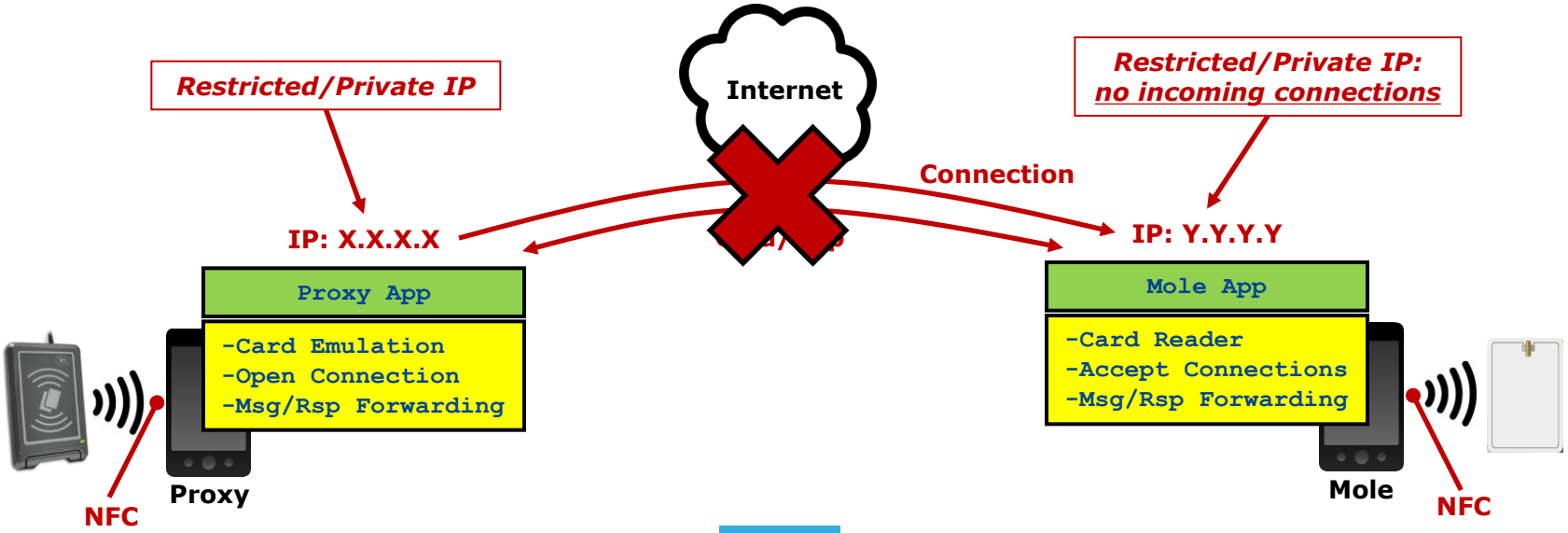
Relay Attack: Our Aim

- Relay attacks against contactless smart cards are not new
  - Some experiments featured with specific hardware modules
  - Lab conditions with short distances

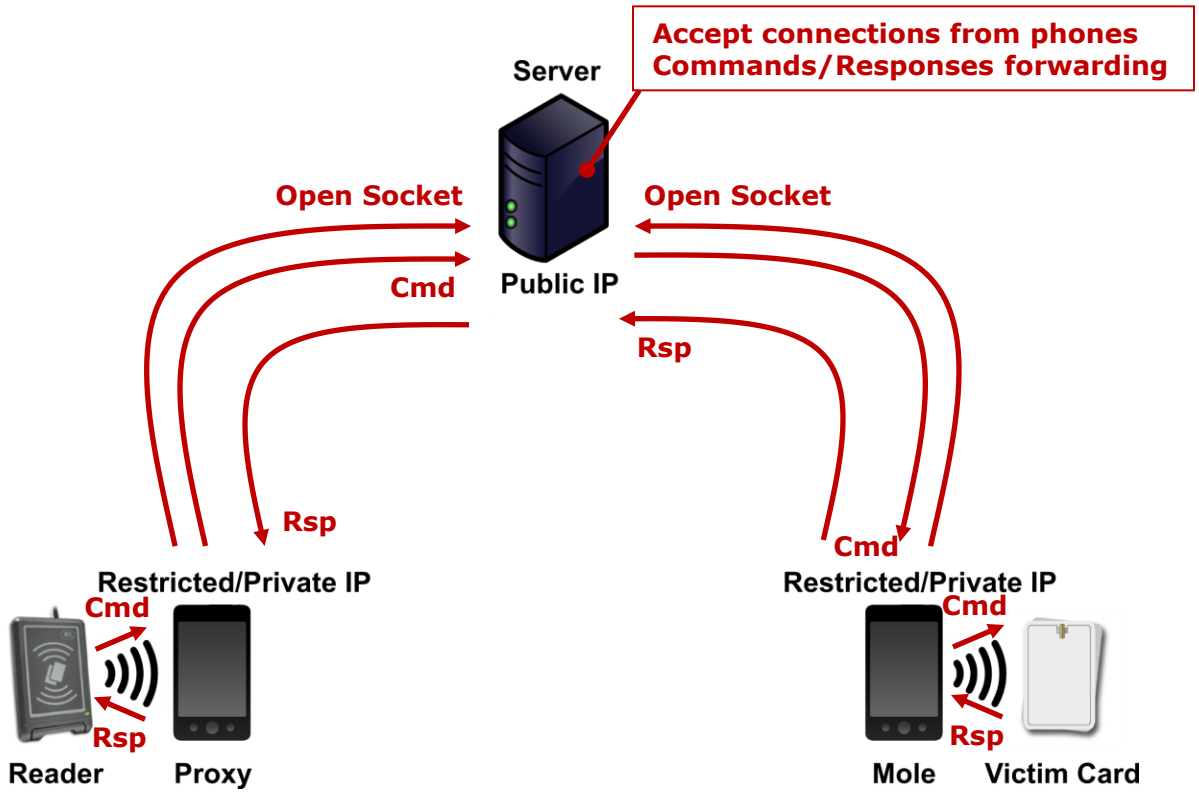
- Our proof of concept:
  - Long distance attack (>10Km)
  - In dynamic conditions (no constraints on devices positions)

Relay Attack on a Mobile Phone Network

- Off-the-shelf equipment
  - Mobile phones with NFC (ISO 14443 compliant) as Proxy and Mole
- Mobile phone network for Proxy-Mole communication
  - Data network basically provided by all mobile phone network operators

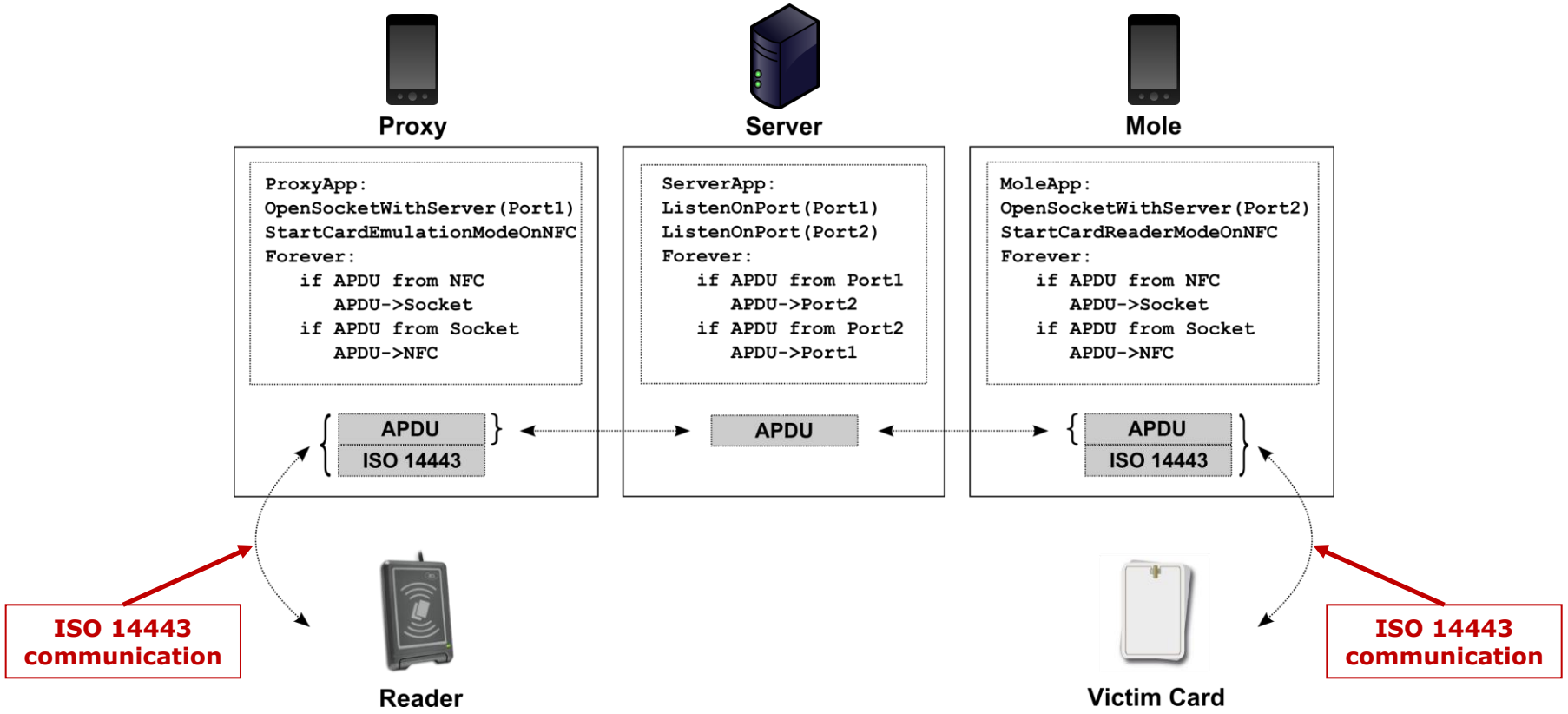


Our Relay Attack Architecture



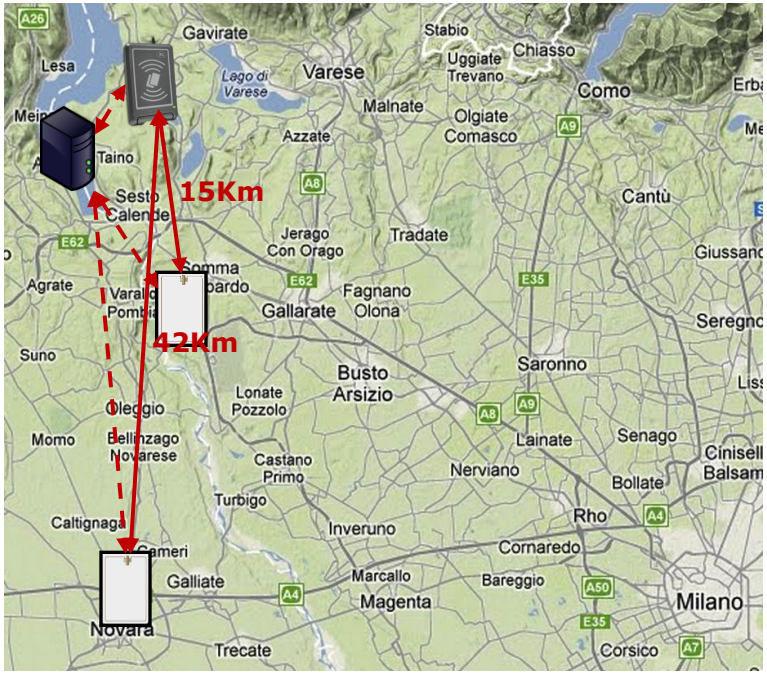
European Commission

Our Relay Attack Architecture: More Details



Relay Attack on a Geographical Scale

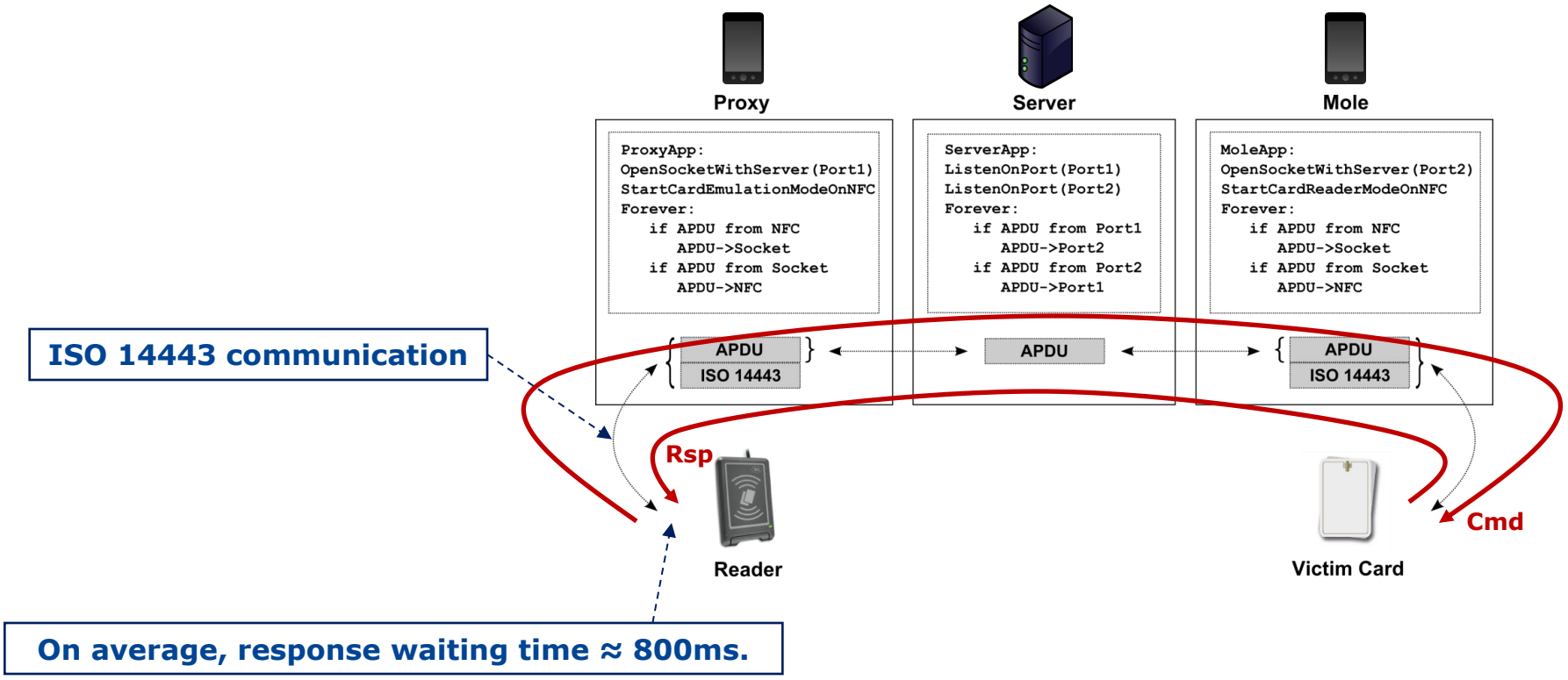
- We successfully relayed a Reader-ePassport communication over several kilometers



- Authentication protocols useless against relay attacks
- No longer possible to assume that a card is physically nearby the reader

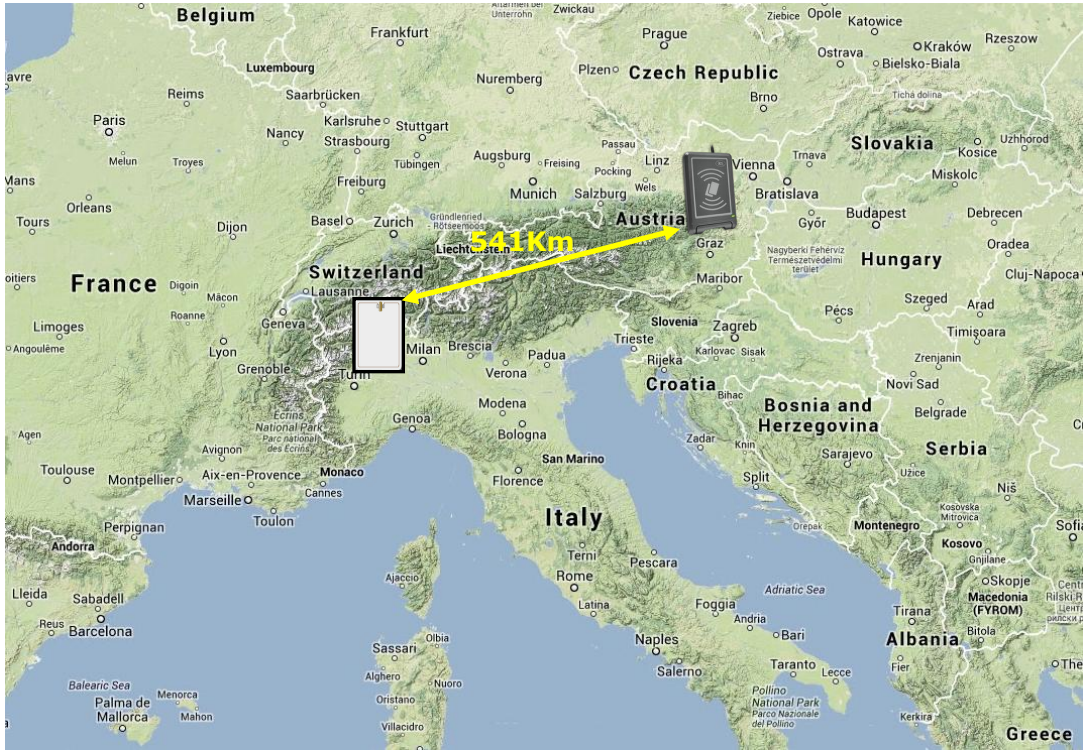
European Commission

No Timing Issues



Live Experiment: Italy-Austria Relay Attack?

- Let's try!
- (you know, things never go well in these cases... we apologize in advance…)

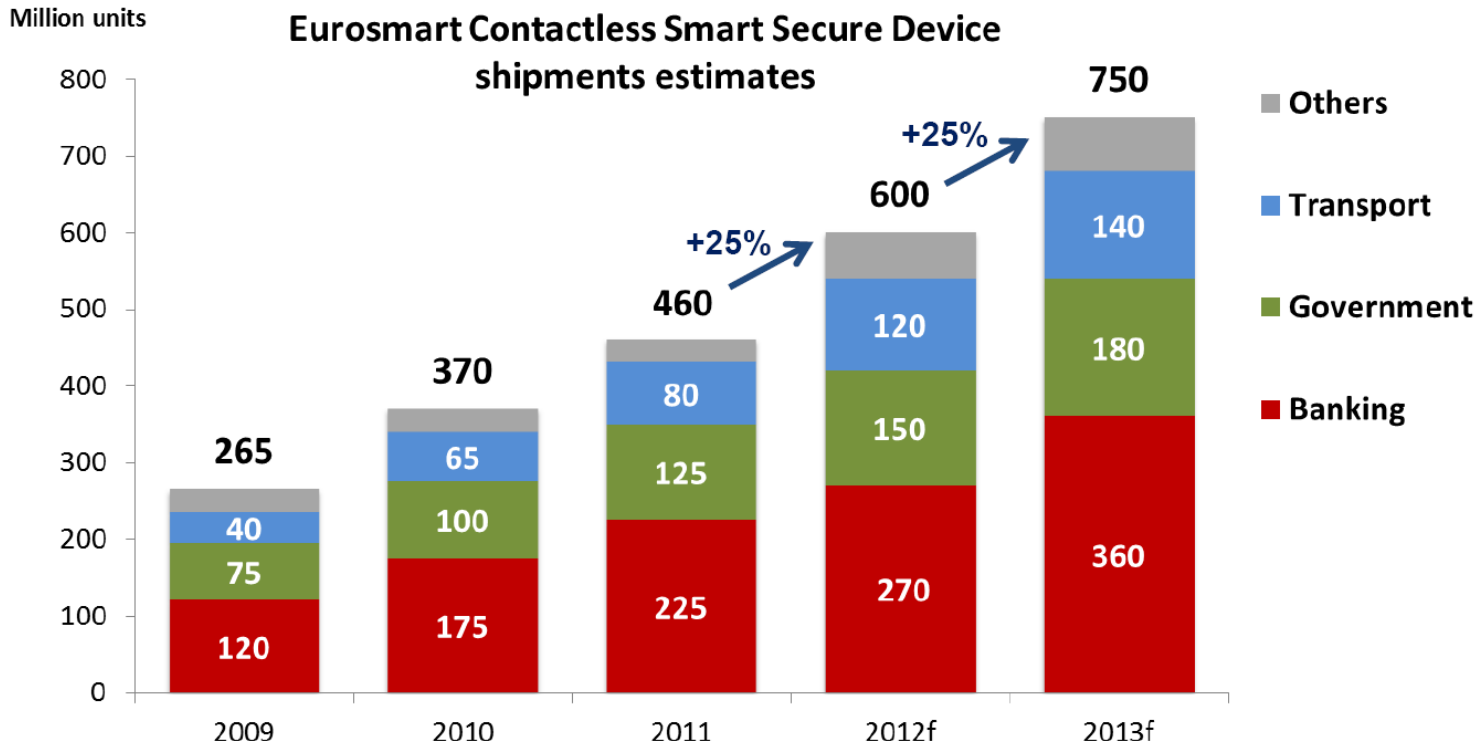


Contactless Smart Card Applications

- Government (e.g., identification)
- Banking (e.g., electronic payments)
- Transport (e.g., tickets)
- Access control
- Loyalty programs
- ...

European Commission

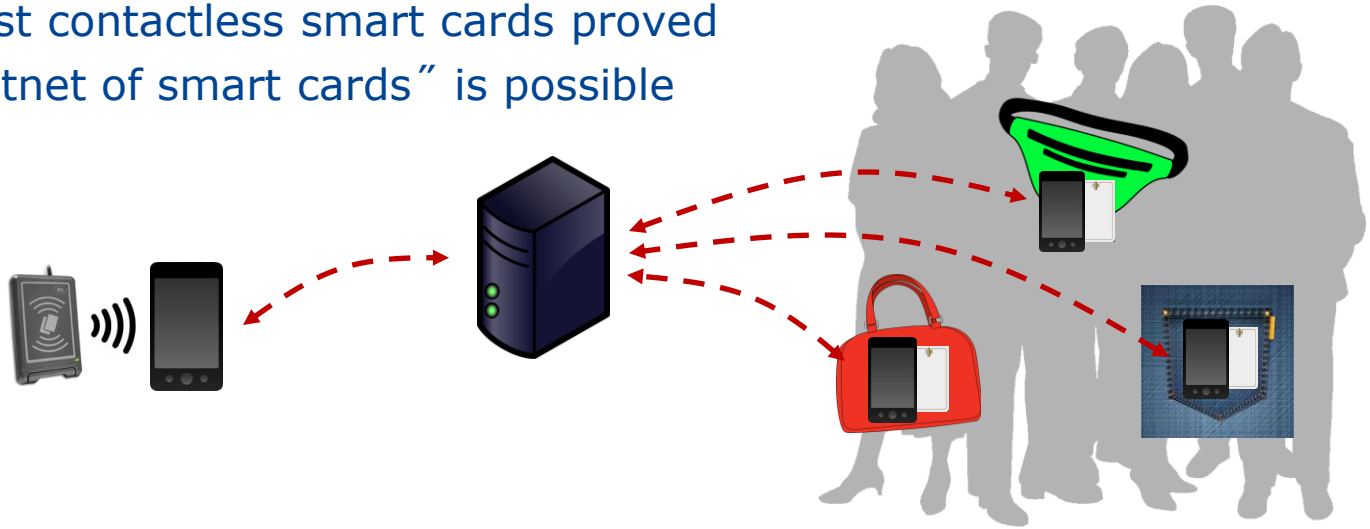
Market Figures



Source: EUROSMART The Voice of the Smart Security Industry

Conclusions

- Long distance relay attack in dynamic conditions against contactless smart cards proved
- A ″botnet of smart cards″ is possible



- Practical countermeasures:
  - Access codes (e.g., MRZ, PIN)
  - Shielding

European Commission

Thank you for your attention!

Joint Research Centre