A quoi servent les protocoles délimiteurs de distance

pascal.lafourcade@uca.fr

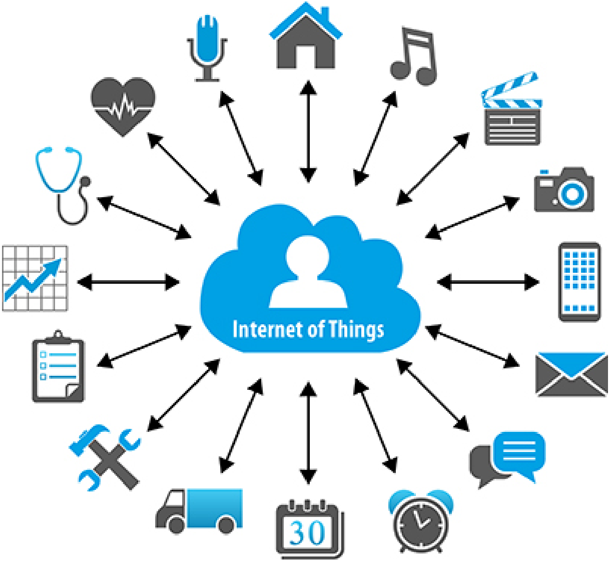
UNIVERSITÉ Clermont Auvergne

CLERMONT'ECH

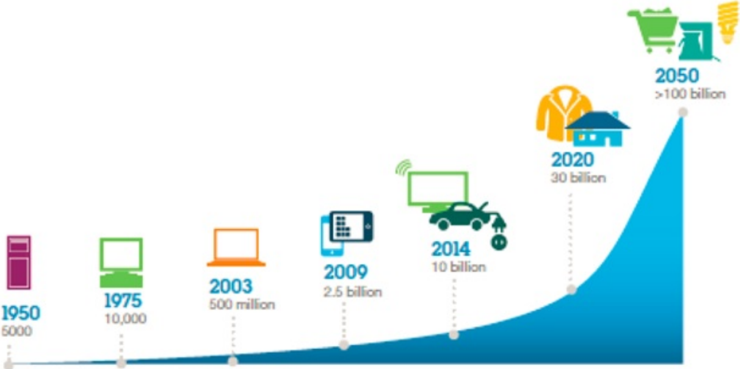
LIMOS

14 Septembre 2017

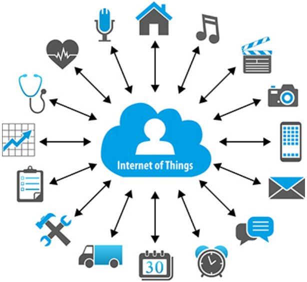
IoT



IoT


1950
5000
1975
10,000
2003
500 million
2009
2.5 billion
2014
10 billion
2020
30 billion
2050
>100 billion

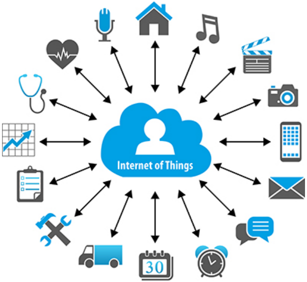
Reasons of the Succes of IOT



Usage

- Monitoring services
- Hyperconnectivity
- Avaibility
- Open data

Reasons of the Succes of IOT



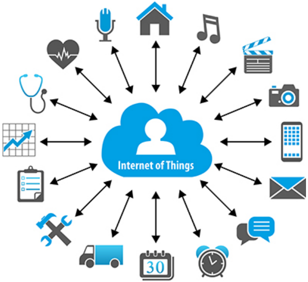
Usage

- Monitoring services
- Hyperconnectivity
- Avaibility
- Open data

Technology

- Wireless Communications :
  Wifi, 3G, 4G, Bluethooth, Sigfox ...
- Batteries
- CPU
- Sensors
- Price

Reasons of the Succes of IOT



Usage

- Monitoring services
- Hyperconnectivity
- Avaibility

Security ?

- Open data

Technology

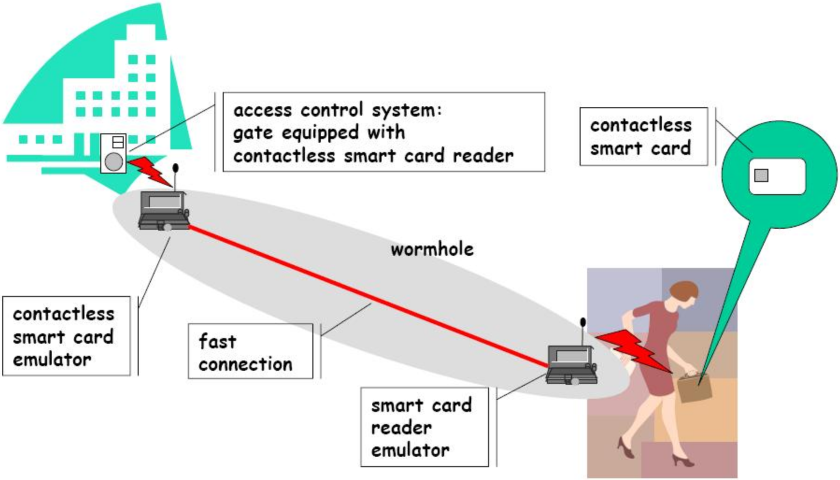
- Wireless Communications :
  Wifi, 3G, 4G, Bluethooth, Sigfox ...
- Batteries
- CPU
- Sensors
- Price

Proximity Devices Everywhere

Proximity Devices Everywhere

What security do we want ?

“Wormhole Attack”

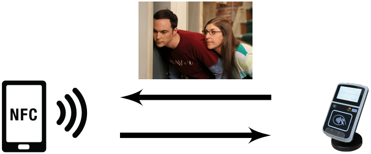


Video

- Buy two Zürich transports ticket

Intruder : Eavesdropper VS Curious Verifier

Eavesdropper

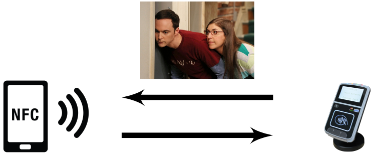


Prover P

Verifier V

Intruder : Eavesdropper VS Curious Verifier

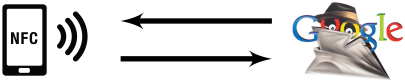
Eavesdropper



Prover P

Verifier V

Curious Verifier

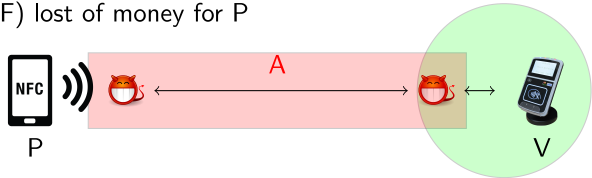


Prover P

Verifier V

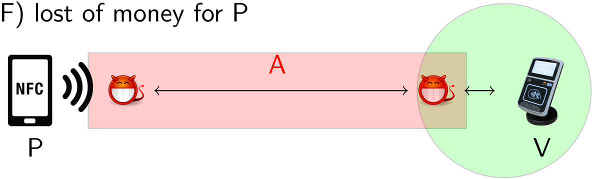
Properties : Threats against honest provers

Mafia Fraud (MF) lost of money for P

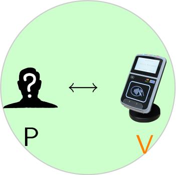


Properties : Threats against honest provers

Mafia Fraud (MF) lost of money for P

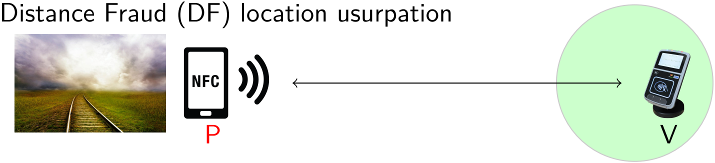


User tracking



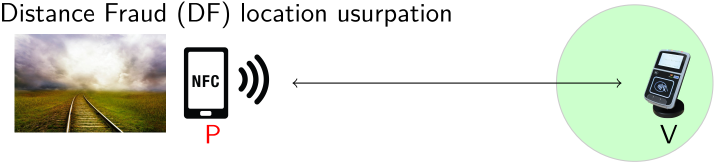
Properties : Threats with malicious Provers

Distance Fraud (DF) location usurpation

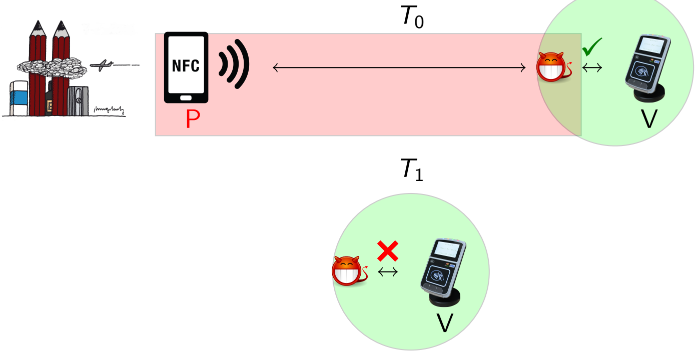


Properties : Threats with malicious Provers

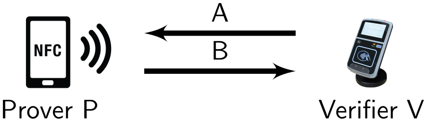
Distance Fraud (DF) location usurpation



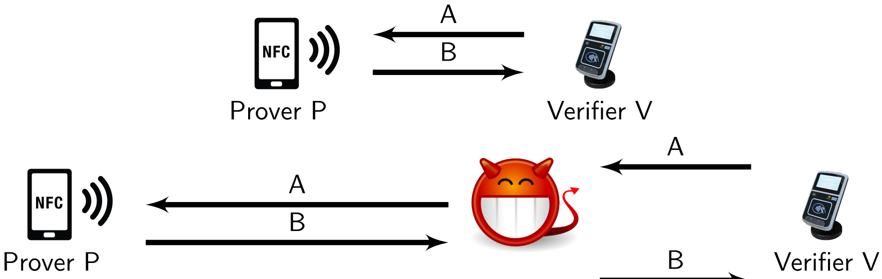
Terrorist Fraud(TF) lost of money for V



Distance Bounding Idea



Distance Bounding Idea



A

B

Prover P

Verifier V

A

A

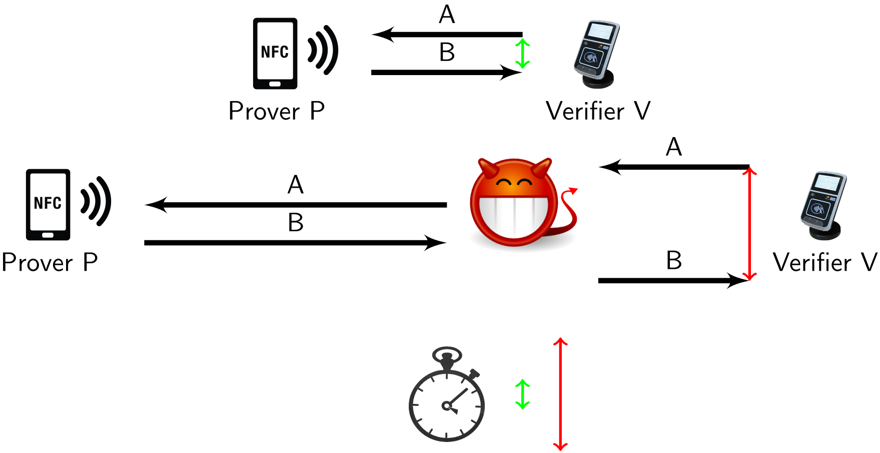
B

B

Prover P

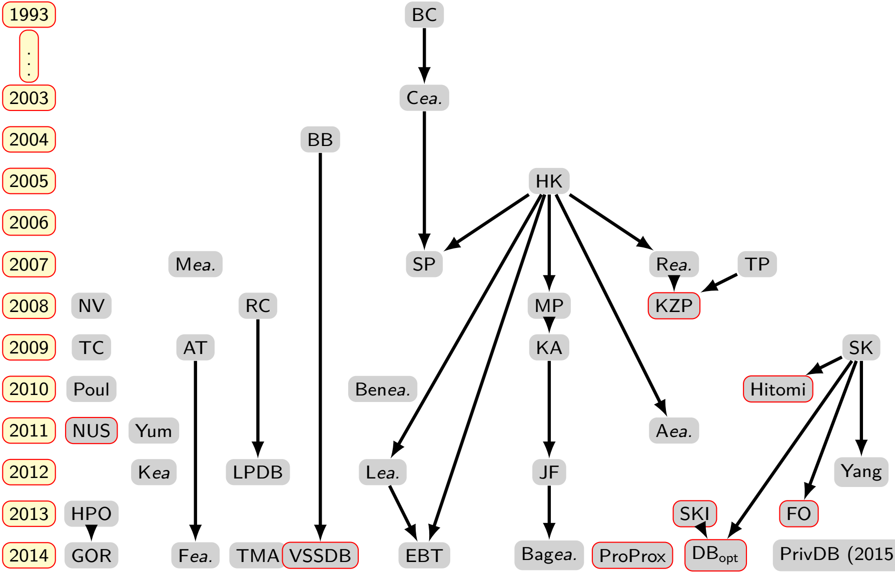
Verifier V

Distance Bounding Idea



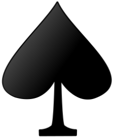
Solution against MF : Distance Bounding (Brands and Chaum, 1991)

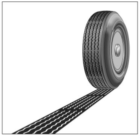
Survey : 42 protocols from 1993 to 2015.



Conclusion

- Designing secure IoT is difficult
- Distance Bounding can help to improve security
- We propose SPADE and TREAD, two new secure DB protocols





Thank you for your attention !

Questions ?