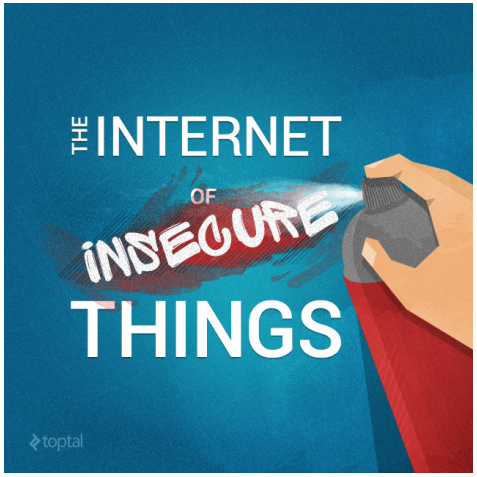
(In)Security of IoT

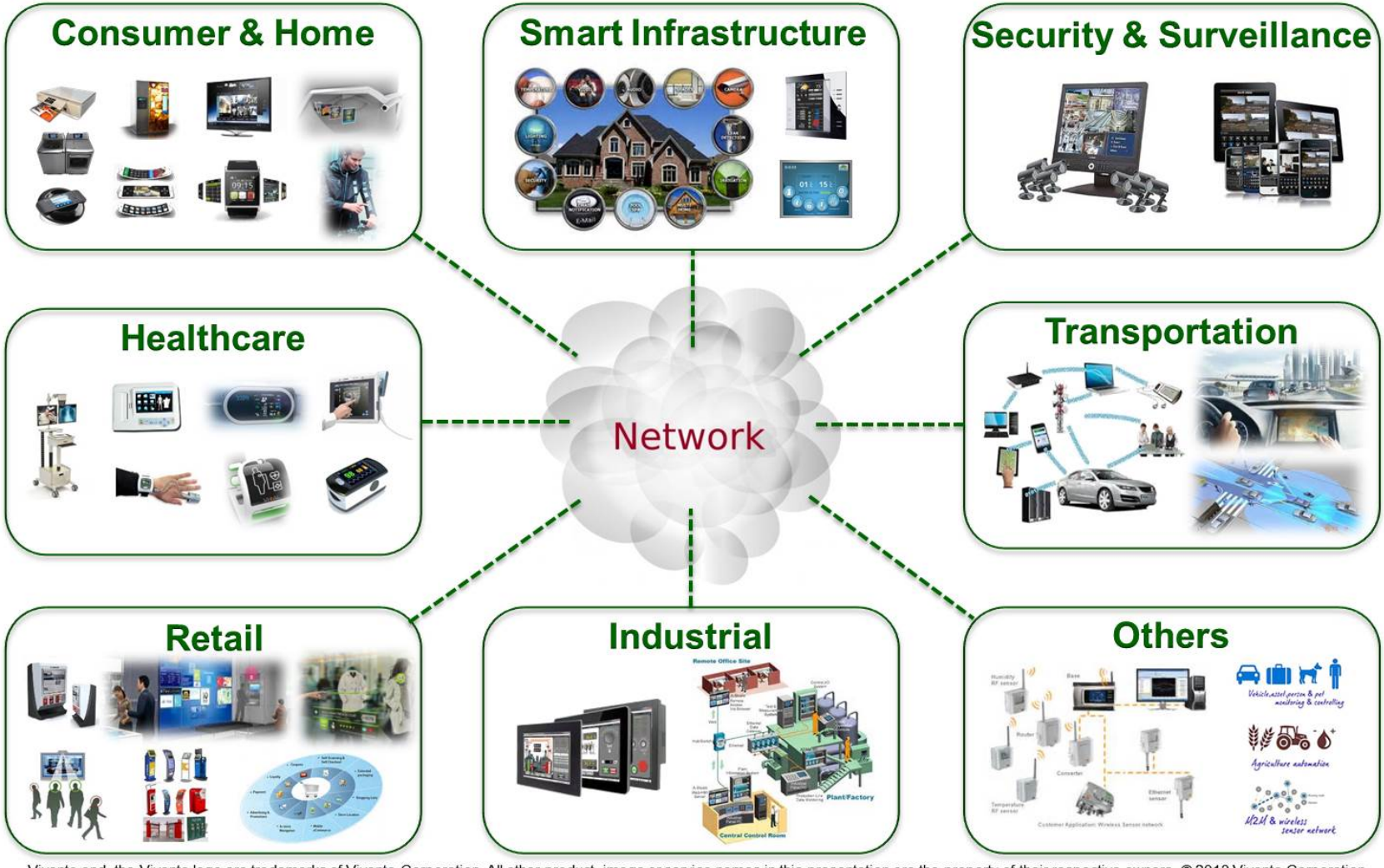


Pascal Lafourcade

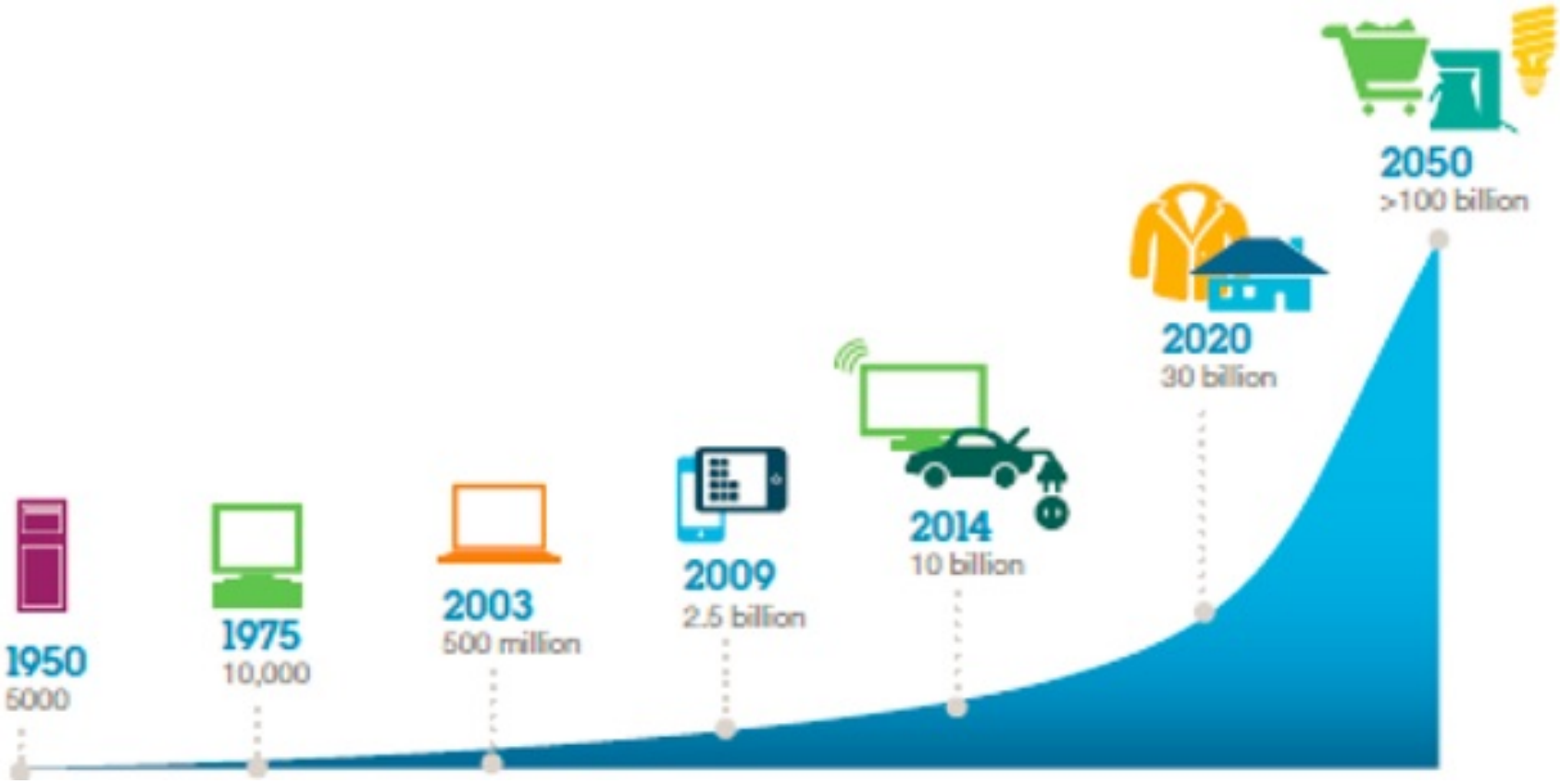
Chaire de Confiance Numérique

15th March 2016

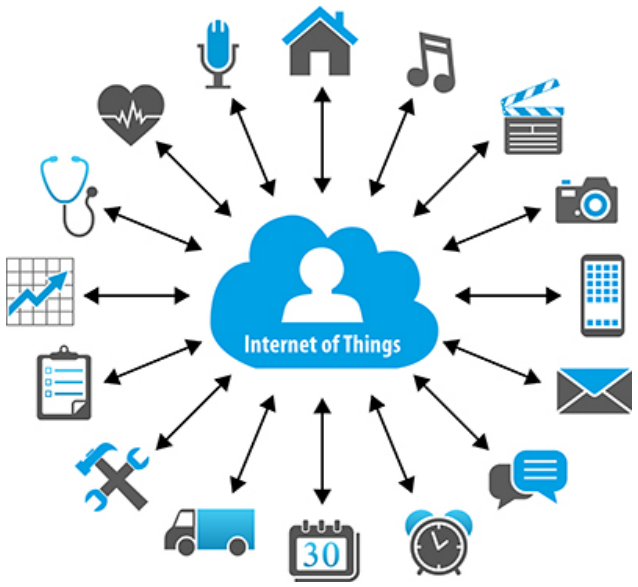
Internet of Thing (IoT)



Increasing Succes of IoT



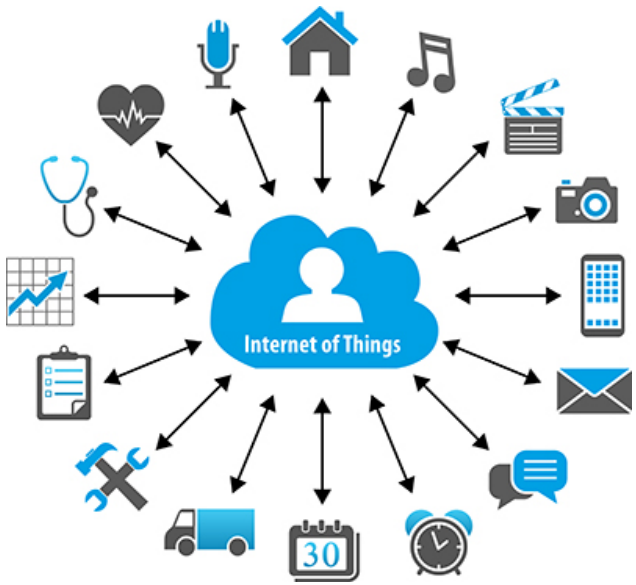
Reasons of the Succes of IOT



Technology

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

Reasons of the Succes of IOT



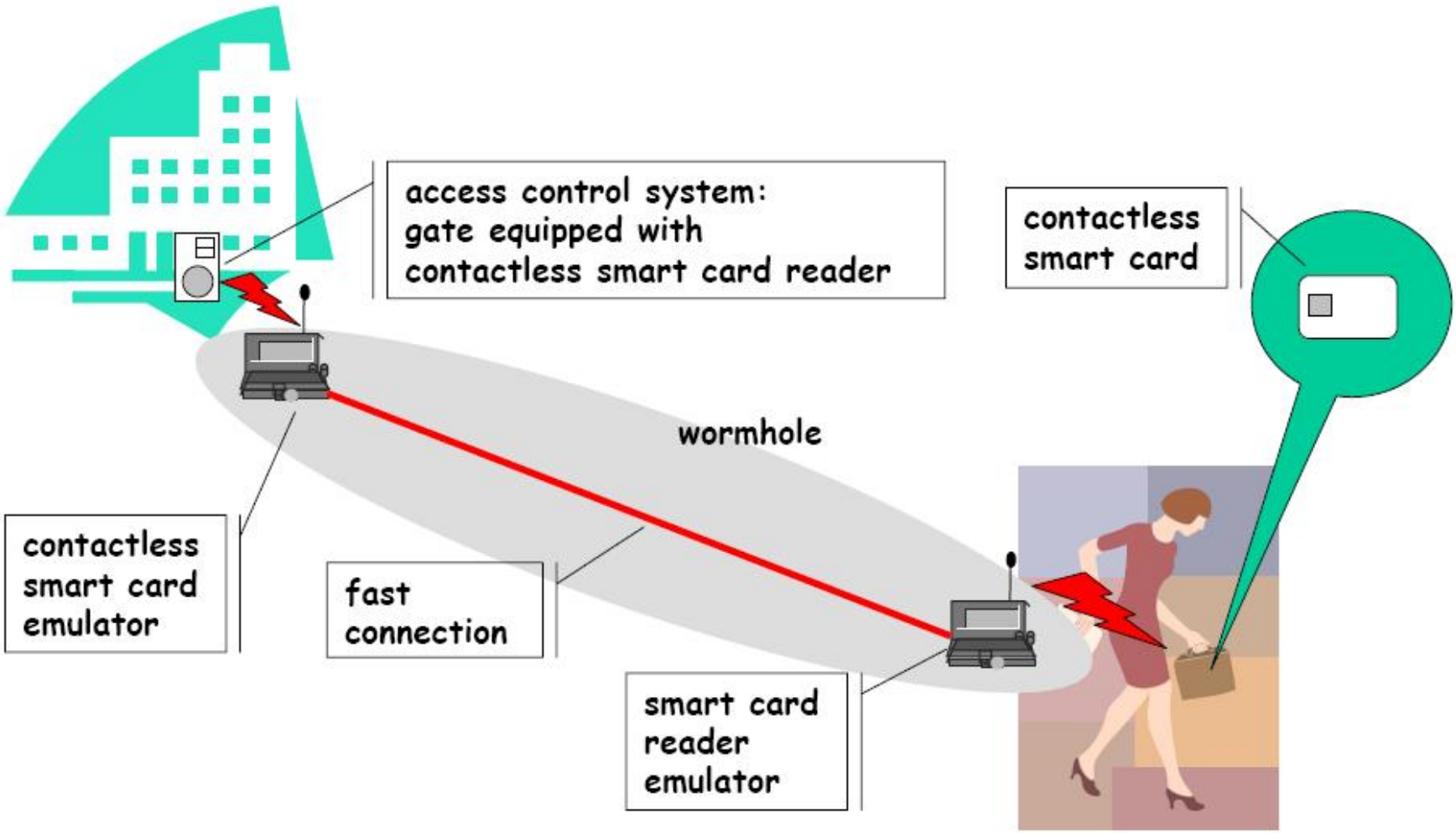
Technology

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

Usage

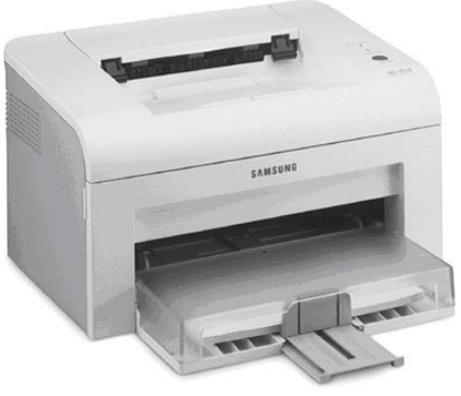
- Monitoring services
- Hyperconnectivity
- Avaibility

Wireless communications ⇒ Wormhole Attack

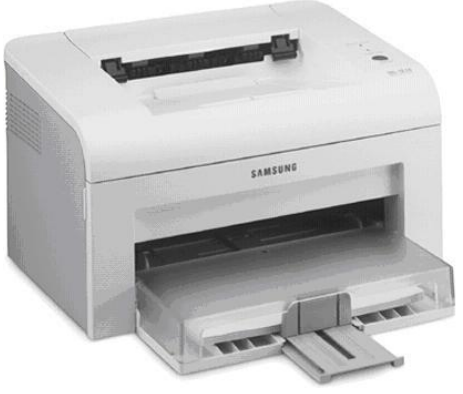


Real attacks on IoT from 2007 ...

Real attacks on IoT from 2007 ...

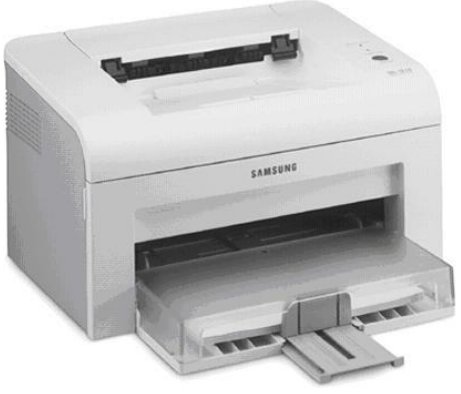


Real attacks on IoT from 2007 ...



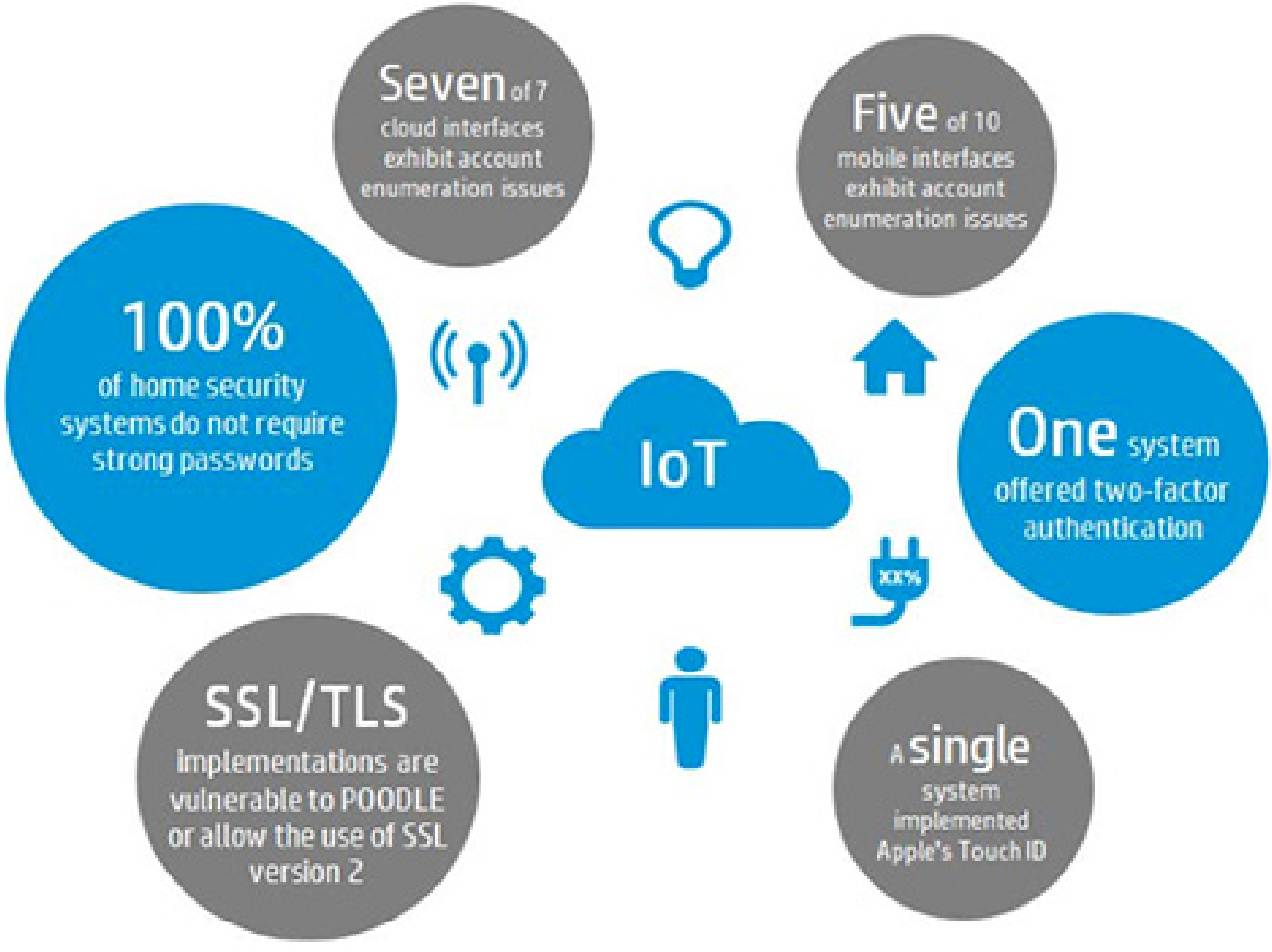
Real attacks on IoT from 2007 ...



Séminaire Confiance numérique : 7 avril 14h00 Amphi B IUT

Insecurity of IoT by HP in 2015



POODLE: Padding Oracle On Downgraded Legacy Encryption

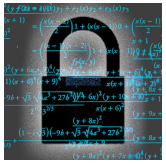
TOP 10: Vulnerabilities of IoT

1. Insecure Web Interface (weak passwords, account protection)
2. Unsufficient Authtneitcation/Authorization
3. Insecure Newtork Services (ports open, DoS)
4. Lack of Transport Encryption
5. Privacy Concerns (leak of personal informations)
6. Insecure Cloud interfaces
7. Insecure Mobile Interfaces
8. Insufficient Security Configurability
9. Insecure Software/Firmeware
10. Poor Physical Security

`https://www.owasp.org/images/8/8e/Infographic-v1.jpg`

How to Secure IoT

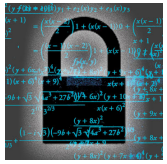
Cryptography:



- Primitives: RSA, Elgamal, AES, DES, SHA-3 ...
- Protocols: Distributed Algorithms

How to Secure IoT

Cryptography:



- Primitives: RSA, Elgamal, AES, DES, SHA-3 ...
- Protocols: Distributed Algorithms

Properties:

- Secrecy,
- Authentication,
- Privacy
- Non Repudiation ...

How to Secure IoT

Cryptography:

- Primitives: RSA, Elgamal, AES, DES, SHA-3 ...
- Protocols: Distributed Algorithms

Properties:

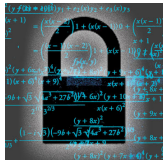
- Secrecy,
- Authentication,
- Privacy
- Non Repudiation ...

Intruders:

- Passive, active
- CPA, CCA ...

How to Secure IoT

Cryptography:



- Primitives: RSA, Elgamal, AES, DES, SHA-3 ...
- Protocols: Distributed Algorithms

Properties:

- Secrecy,
- Authentication,
- Privacy
- Non Repudiation ...

Intruders:

- Passive, active
- CPA, CCA ...

Designing such **secure** protocols is **difficult**

Is it preserving your privacy?

Is it preserving your privacy?

4096 RSA encryption

Is it preserving your privacy?

4096 RSA encryption

Environs 60 températures possibles: 35 ... 41

Is it preserving your privacy?

4096 RSA encryption

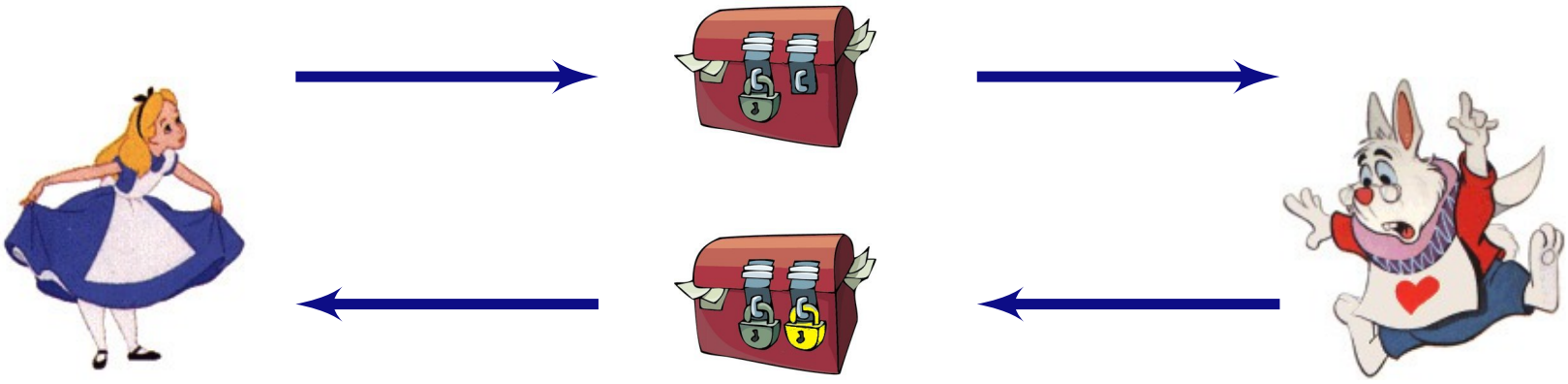
Environs 60 températures possibles: 35 ... 41

$$\{35\}_{pk}, \{35, 1\}_{pk}, \ldots, \{41\}_{pk}$$

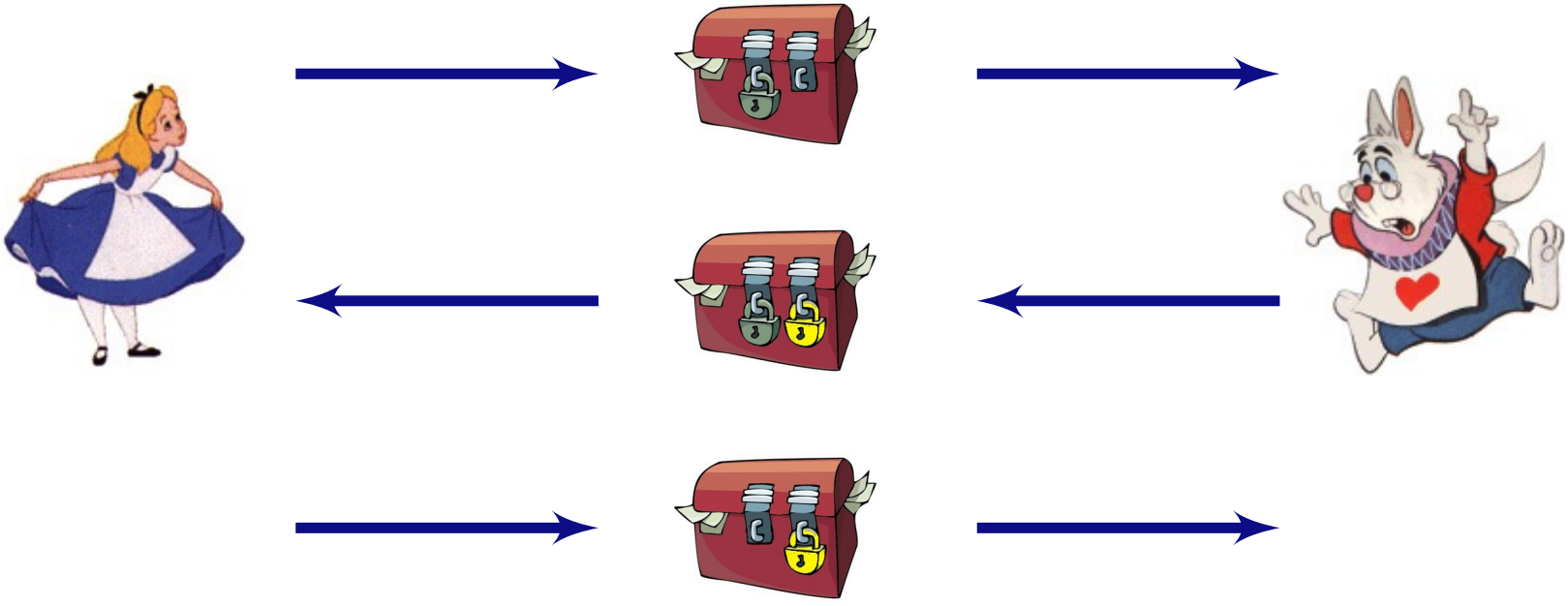
3-Pass Shamir

3-Pass Shamir

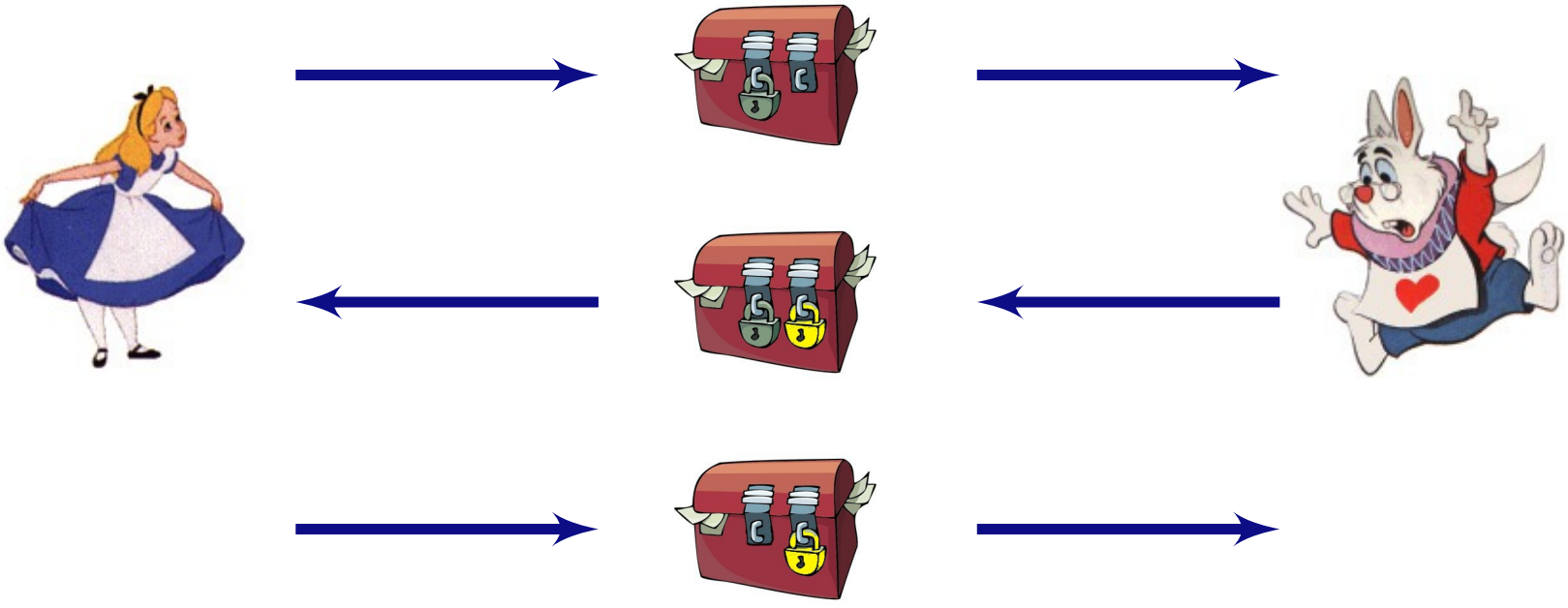
3-Pass Shamir



3-Pass Shamir



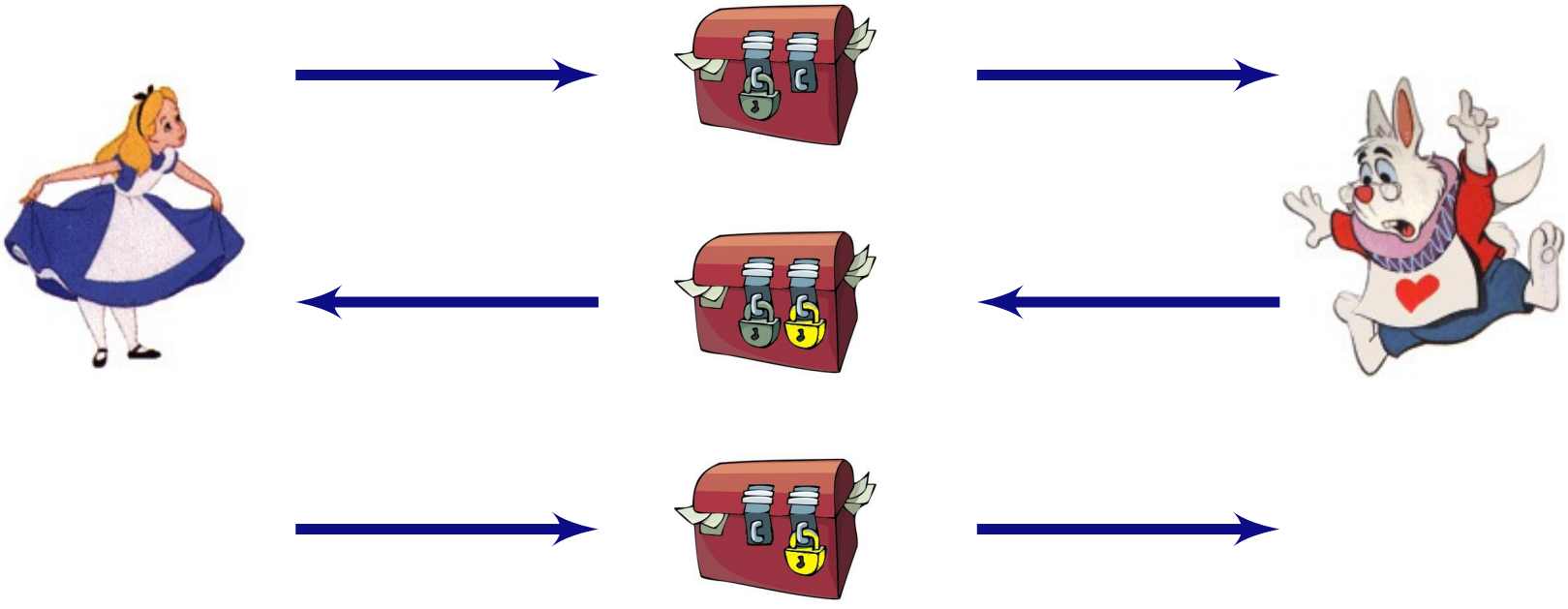
3-Pass Shamir



Abstract Representation

$$1 \quad A \quad \rightarrow \quad B \quad : \quad \{m\}_{K_A}$$

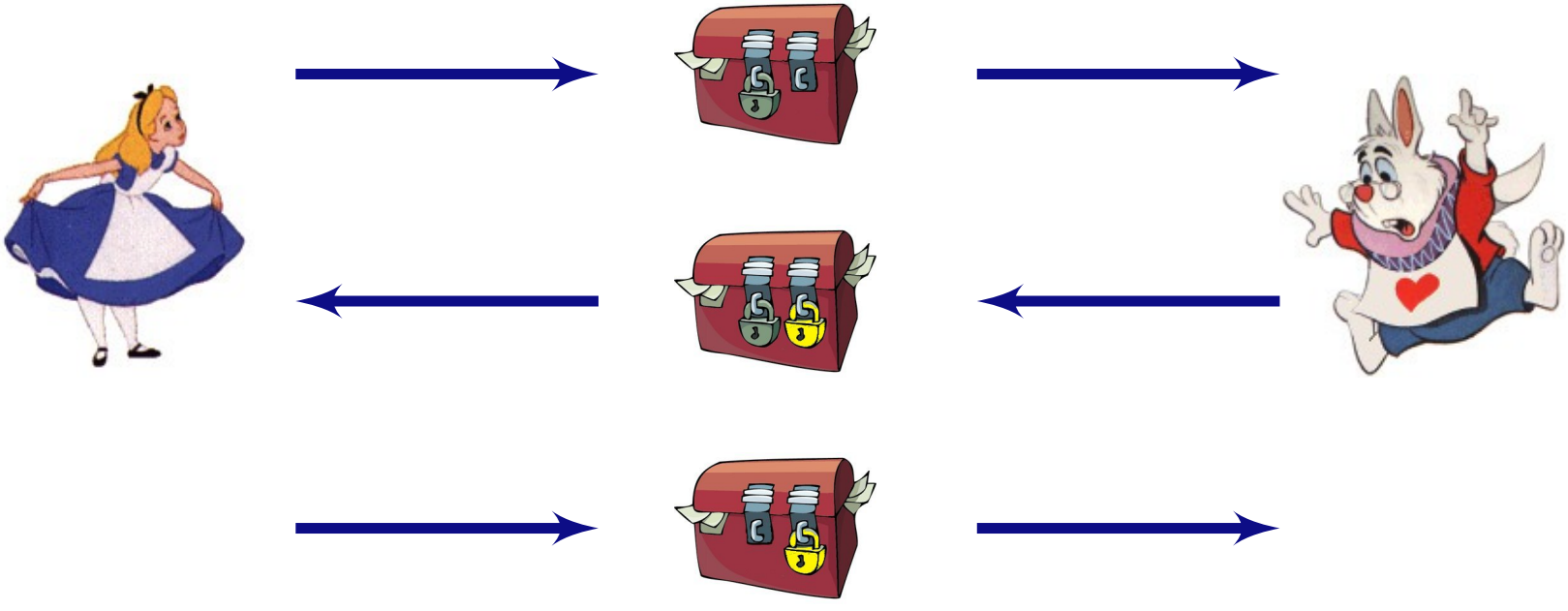
3-Pass Shamir



Abstract Representation

$$
\begin{array}{llcll}
1 & A & \rightarrow & B & : \{m\}_{K_A} \\
2 & B & \rightarrow & A & : \{\{m\}_{K_A}\}_{K_B}
\end{array}
$$

3-Pass Shamir

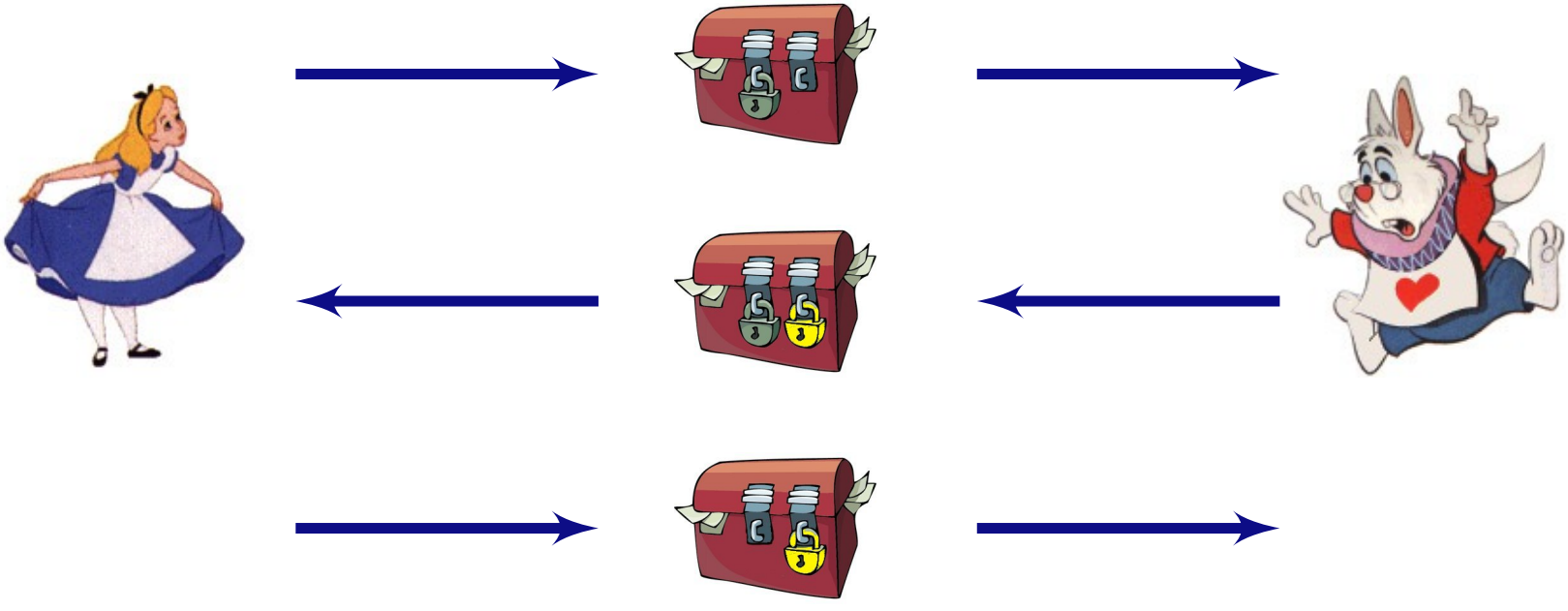


Abstract Representation

$$\begin{array}{llllll} 1 & A & \rightarrow & B & : & \{m\}_{K_A} \\ 2 & B & \rightarrow & A & : & \{\{m\}_{K_A}\}_{K_B} = \{\{m\}_{K_B}\}_{K_A} \end{array}$$

Commutative Encryption

3-Pass Shamir



Abstract Representation

$$
\begin{array}{llllll}
1 & A & \rightarrow & B & : & \{m\}_{K_A} \\
2 & B & \rightarrow & A & : & \{\{m\}_{K_A}\}_{K_B} = \{\{m\}_{K_B}\}_{K_A} \\
3 & A & \rightarrow & B & : & \{m\}_{K_B}
\end{array}
$$

Commutative Encryption

Logical Attack on Shamir 3-Pass Protocol (I)

Perfect encryption one-time pad (Vernam Encryption)

$\{m\}_k = m \oplus k$

XOR Properties (ACUN)

- $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ **A**ssociativity
- $x \oplus y = y \oplus x$ **C**ommutativity
- $x \oplus 0 = x$ **U**nity
- $x \oplus x = 0$ **N**ilpotency

Logical Attack on Shamir 3-Pass Protocol (I)

Perfect encryption one-time pad (Vernam Encryption)

$\{m\}_k = m \oplus k$

XOR Properties (ACUN)

- $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ **A**ssociativity
- $x \oplus y = y \oplus x$ **C**ommutativity
- $x \oplus 0 = x$ **U**nity
- $x \oplus x = 0$ **N**ilpotency

Vernam encryption is a commutative encryption :

$$\{\{m\}_{K_A}\}_{K_I} = (m \oplus K_A) \oplus K_I = (m \oplus K_I) \oplus K_A = \{\{m\}_{K_I}\}_{K_A}$$

Logical Attack on Shamir 3-Pass Protocol (II)

Perfect encryption one-time pad (Vernam Encryption)

$\{m\}_k = m \oplus k$

Shamir 3-Pass Protocol

$$
\begin{array}{llll}
1 & A & \rightarrow & B: \quad m \oplus K_A \\
2 & B & \rightarrow & A: \quad (m \oplus K_A) \oplus K_B \\
3 & A & \rightarrow & B: \quad m \oplus K_B
\end{array}
$$

Passive attacker :

$m \oplus K_A \qquad m \oplus K_B \oplus K_A \qquad m \oplus K_B$

Logical Attack on Shamir 3-Pass Protocol (II)

Perfect encryption one-time pad (Vernam Encryption)

$\{m\}_k = m \oplus k$

Shamir 3-Pass Protocol

$$
\begin{array}{llcll}
1 & A & \rightarrow & B: & m \oplus K_A \\
2 & B & \rightarrow & A: & (m \oplus K_A) \oplus K_B \\
3 & A & \rightarrow & B: & m \oplus K_B
\end{array}
$$

Passive attacker :

$$m \oplus K_A \oplus m \oplus K_B \oplus K_A \oplus m \oplus K_B = m$$

Second Example

Needham Schroeder Key Echange 1976

$$A \rightarrow B : \{A, N_A\}_{Pub(B)}$$

$$B \rightarrow A : \{N_A, N_B\}_{Pub(A)}$$

$$A \rightarrow B : \{N_B\}_{Pub(B)}$$

- Use cryptography
- Small programs
- Distributed

Cryptography is not sufficient !

Example : Needham Schroeder Key Echange

$$A \rightarrow B : \{A, N_A\}_{Pub(B)}$$

$$B \rightarrow A : \{N_A, N_B\}_{Pub(A)}$$

$$A \rightarrow B : \{N_B\}_{Pub(B)}$$

Cryptography is not sufficient !

Example : Needham Schroeder Key Echange

$$A \to B : \{A, N_A\}_{Pub(B)}$$
$$B \to A : \{N_A, N_B\}_{Pub(A)}$$
$$A \to B : \{N_B\}_{Pub(B)}$$

Broken 17 years after, by G. Lowe

$$A \to I : \{A, N_A\}_{Pub(I)} \qquad I \to B : \{A, N_A\}_{Pub(B)}$$
$$A \leftarrow I : \{N_A, N_B\}_{Pub(A)} \qquad I \leftarrow B : \{N_A, N_B\}_{Pub(A)}$$
$$A \to I : \{N_B\}_{Pub(I)} \qquad I \to B : \{N_B\}_{Pub(B)}$$

Cryptography is not sufficient !

Example : Needham Schroeder Key Echange

$$A \to B : \{A, N_A\}_{Pub(B)}$$
$$B \to A : \{N_A, N_B\}_{Pub(A)}$$
$$A \to B : \{N_B\}_{Pub(B)}$$

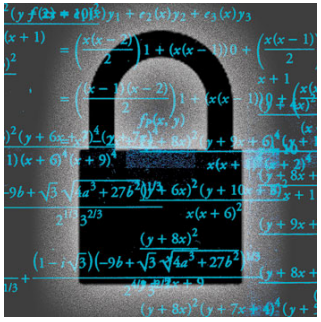
Broken 17 years after, by G. Lowe

$$A \to I : \{A, N_A\}_{Pub(I)} \qquad I \to B : \{A, N_A\}_{Pub(B)}$$
$$A \leftarrow I : \{N_A, N_B\}_{Pub(A)} \qquad I \leftarrow B : \{N_A, N_B\}_{Pub(A)}$$
$$A \to I : \{N_B\}_{Pub(I)} \qquad I \to B : \{N_B\}_{Pub(B)}$$

Computer-Aided Security

Formal Verification Approaches

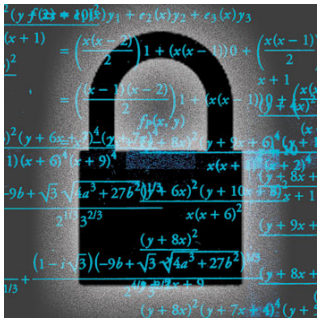
Designer



Attacker

Formal Verification Approaches

Designer

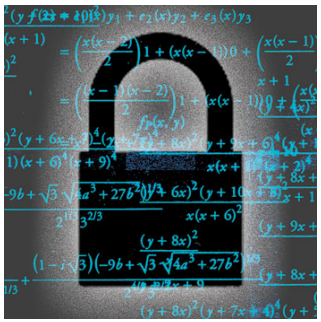


Attacker

Security Team

Formal Verification Approaches

Designer



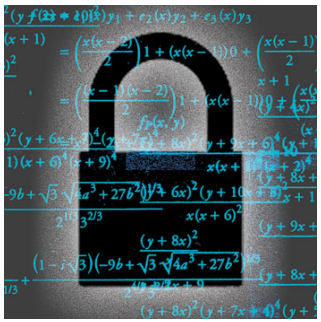
Attacker

Give a proof

Security Team

Formal Verification Approaches

Designer



Attacker

Give a proof

Find a flaw

Security Team

Security Challenges for IoT

Data exchanged should be protected.

Security Properties

- Data Integrity
- Data Confidentiality
- Data Privacy
- Authentication
- Non-repudiation
- Avaibility

5 Things to Bring Home

1. Severals **security challenges** in IoT
2. Security has to be taken **at the design** of IoT
3. Designing secure protocols is **difficult**
4. **Tradeoff** between security, battery, CPU and price.
5. **Formal methods** can **help** you for designing secure protocols

Protocol + *Properties* + *Intruder* ⇒ *Security*

Thanks for your attention

Questions ?