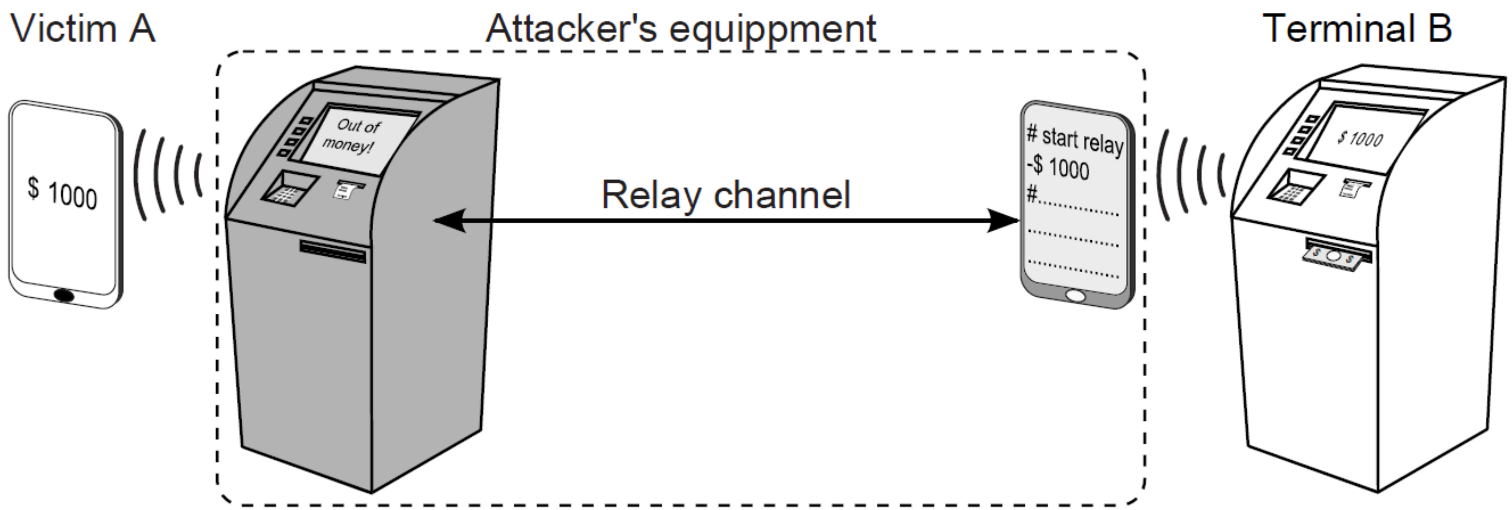
Fortune Cookies and Smartphones



Toni Perković

FESB, Sveučilište u Splitu, Hrvatska

Dani FESB-a, 2014

Motivation

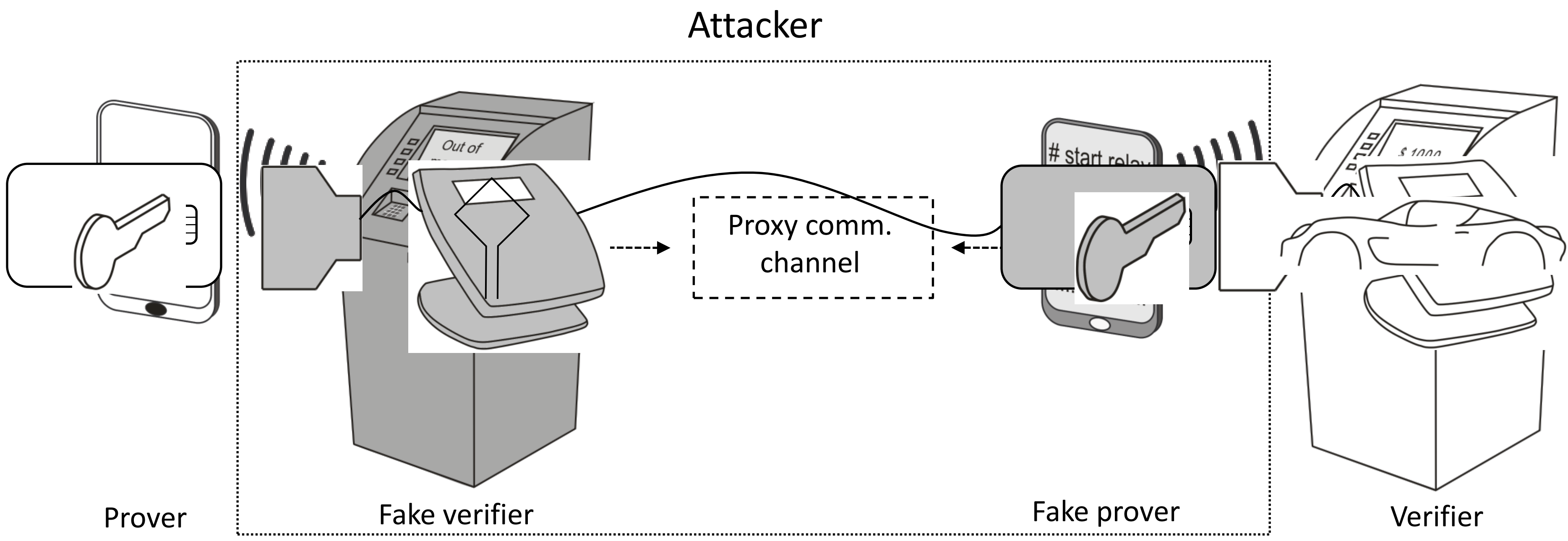
- Mobile payments
- Google + NFC = Google wallet

- AT&T + Verizon + T-Mobile = Isis

- NRC + QR codes

- La Caixa uses contactless terminals with NFC
- Zoosh uses ultrasound
- All these technologies are vulnerable to mafia fraud attack

Motivation: Mafia-fraud attack



- Solutions to counter relay attacks
- RF distance bounding [6, 7]:
  - – require modification of existing hardware
  - – focused on a specific technology (e.g. RFID)
- Paradigm on unrelayable channels by Stajano et al. [8]
  - – highly impractible

[6] A. Francillon, B. Danev, S. Capkun. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. NDSS, 2011
[7] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis. Practical NFC peer-to-peer relay attack using mobile phones. RFIDSec'10
[8] F. Stajano, F.-L. Wong and B. Christianson, Multichannel Protocols to Prevent Relay Attacks, Financial Cryptography and Data Security, FC'10, 4–19, 2010.

Desirable requrements

- Systems that use different communication technologies
- Minimal or no hardware changes to the existing equipment

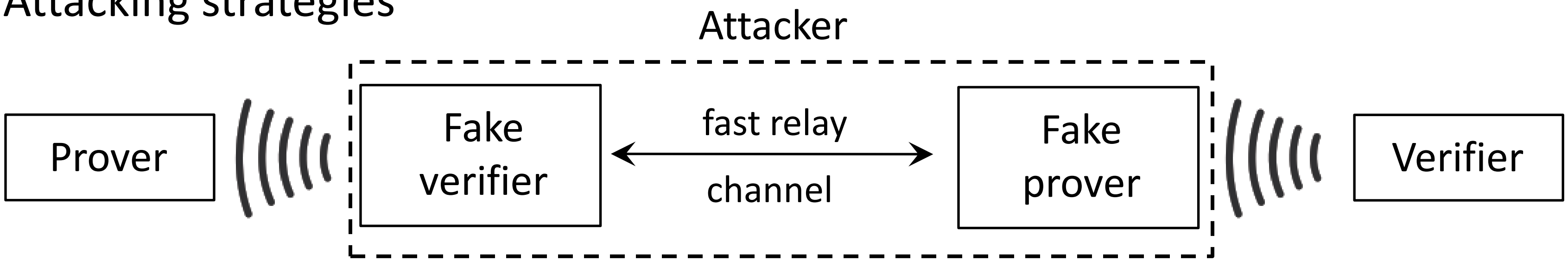
- We use the paradigm on unrelayable channels based on multichannel protocols proposed by Stajano et al. [8]:
    - unclonability
    - unsimulability
    - untransportability

- We require the properties of unclonability and untransportability to hold for only a limited time period Dt – *weakly* unrelayable channel

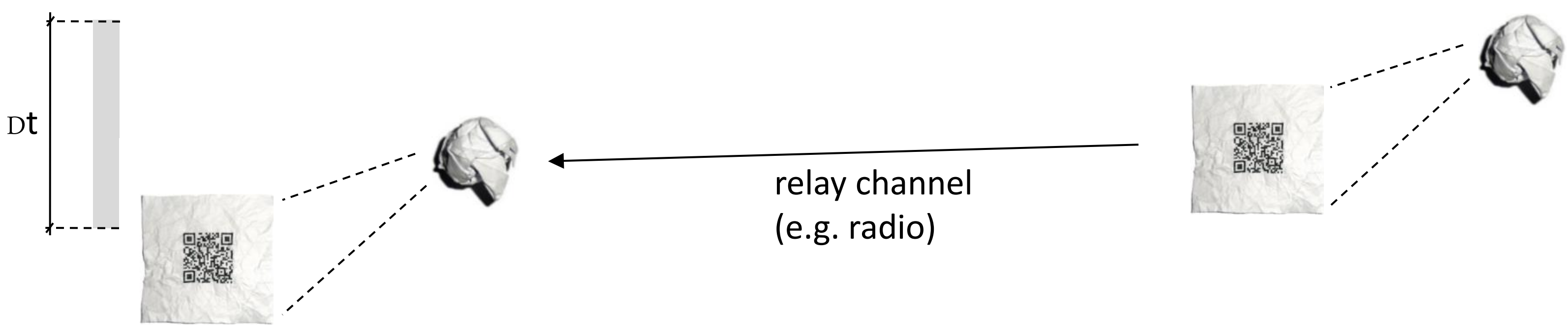
[8] F. Stajano, F.-L. Wong and B. Christianson, Multichannel Protocols to Prevent Relay Attacks, Financial Cryptography and Data Security, FC'10, 4–19, 2010.

Weakly Unrelayable channel

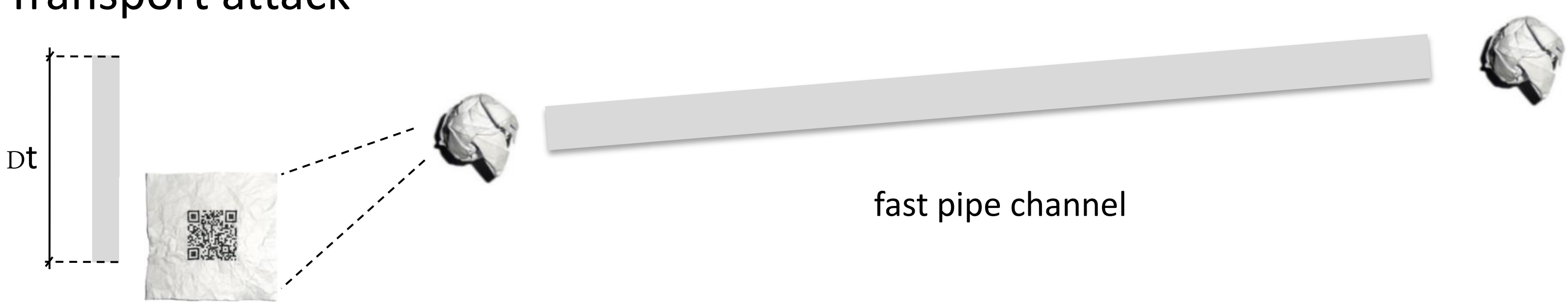
- Attacking strategies



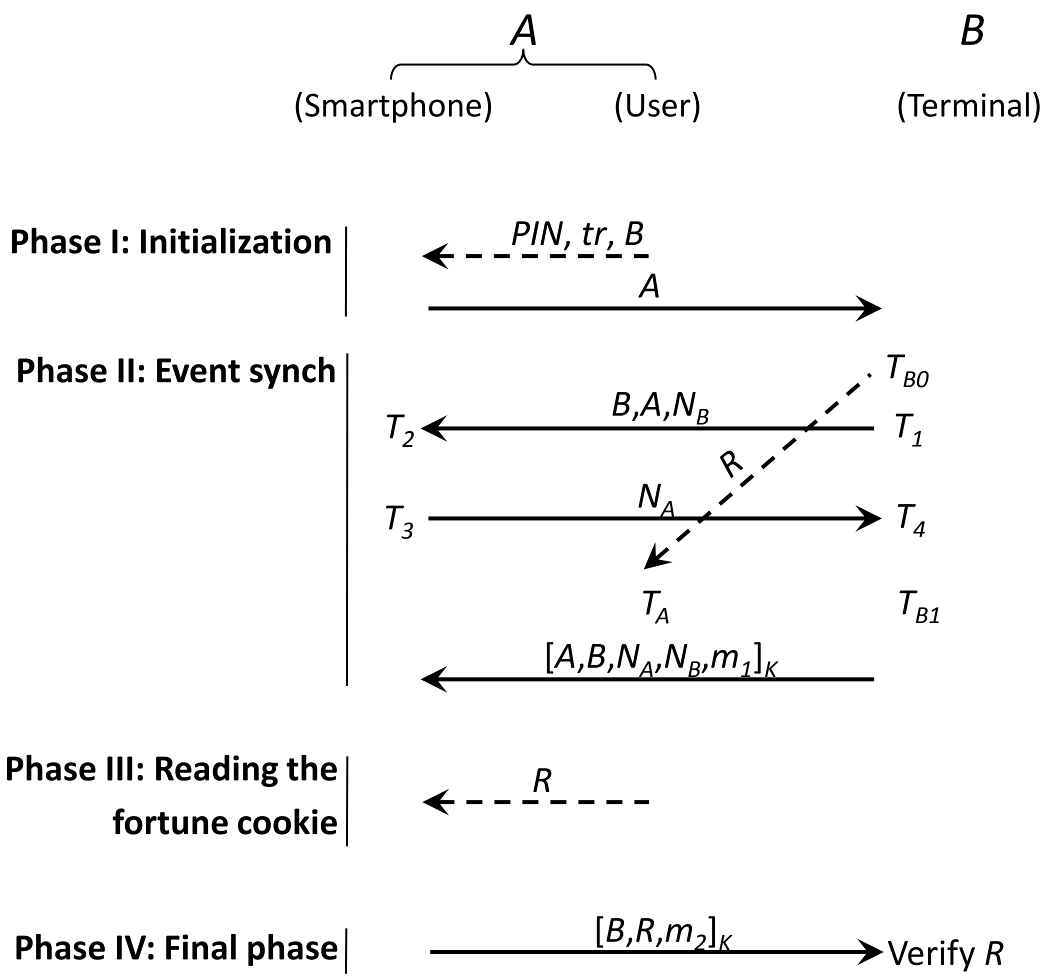
- Clone attack

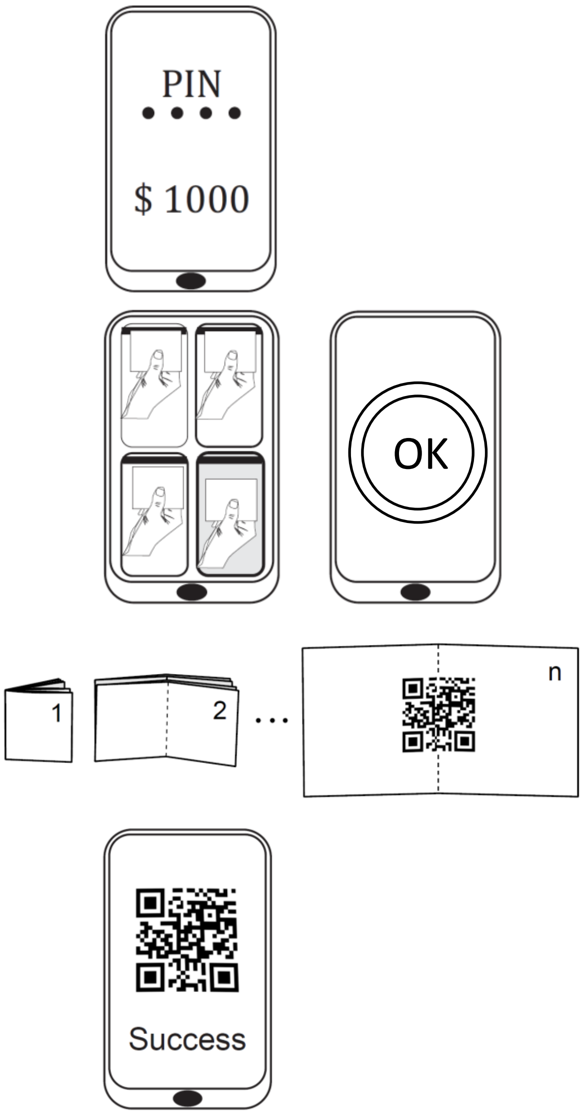


- Transport attack

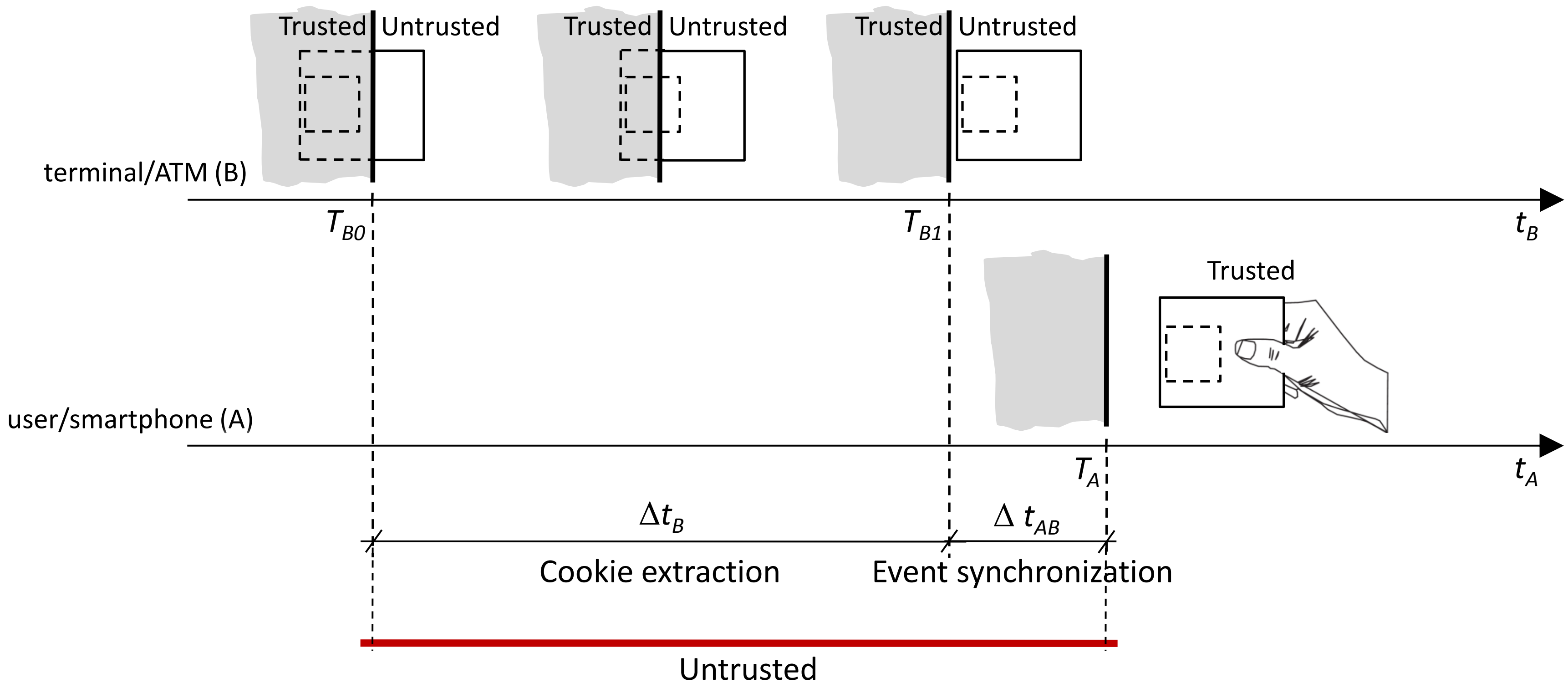


Authentication Protocol *Forces*



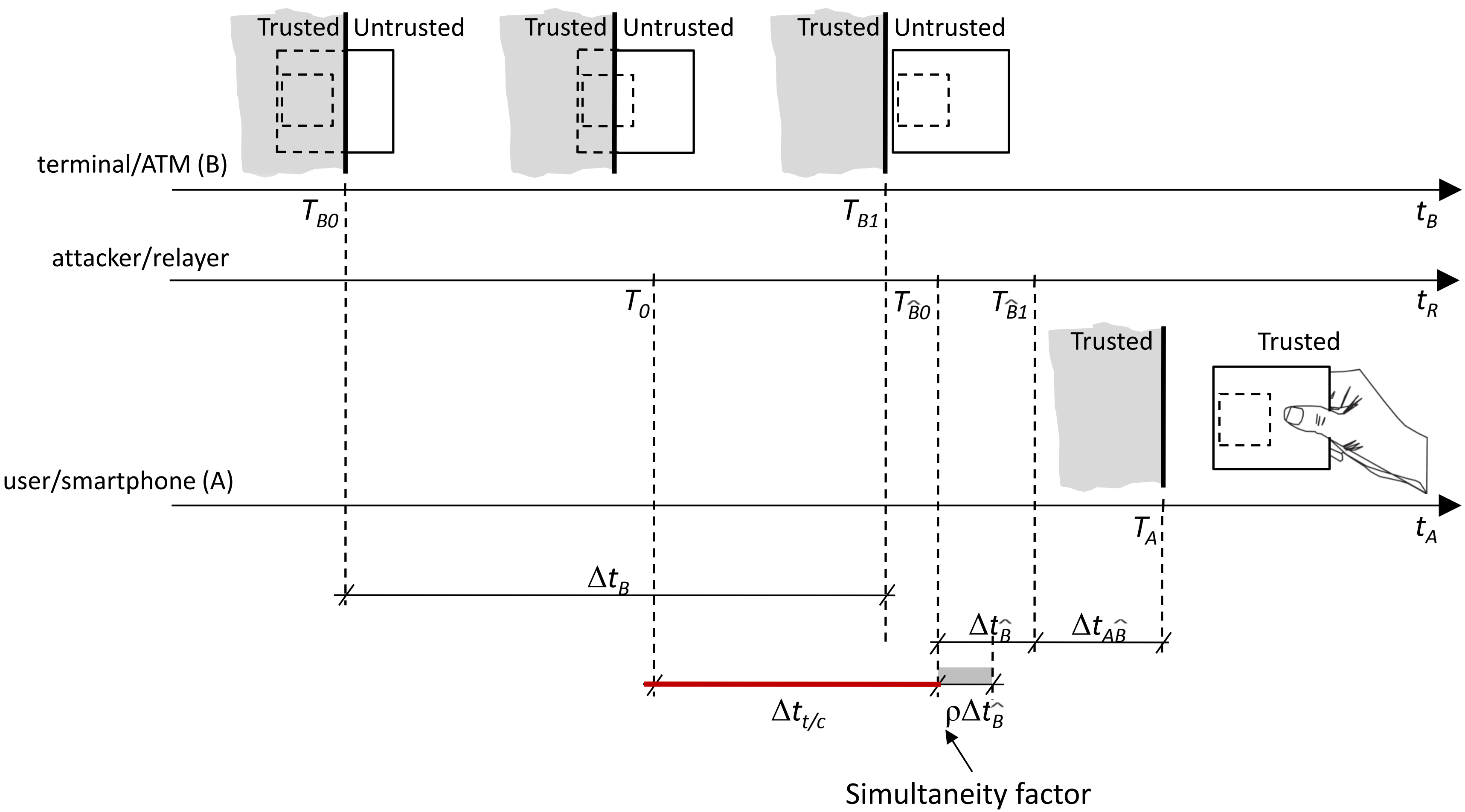


Attacker Model



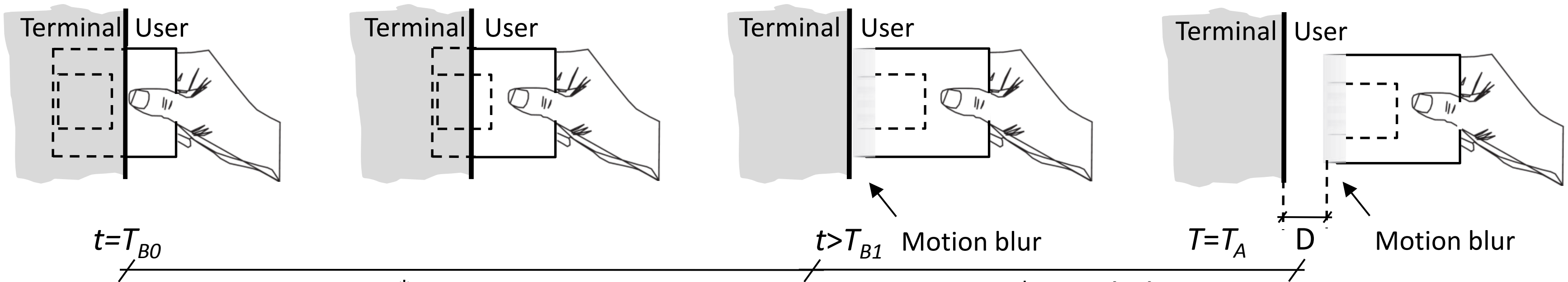
- Cookie extraction: $\Delta t_B = T_{B1} - T_{B0} \leq \Delta t_B^*$
- Event synchronization: $\Delta t_{AB} = T_A - T_{B1} \leq \Delta t_{AB}^*$

Relay Attack Timing Model



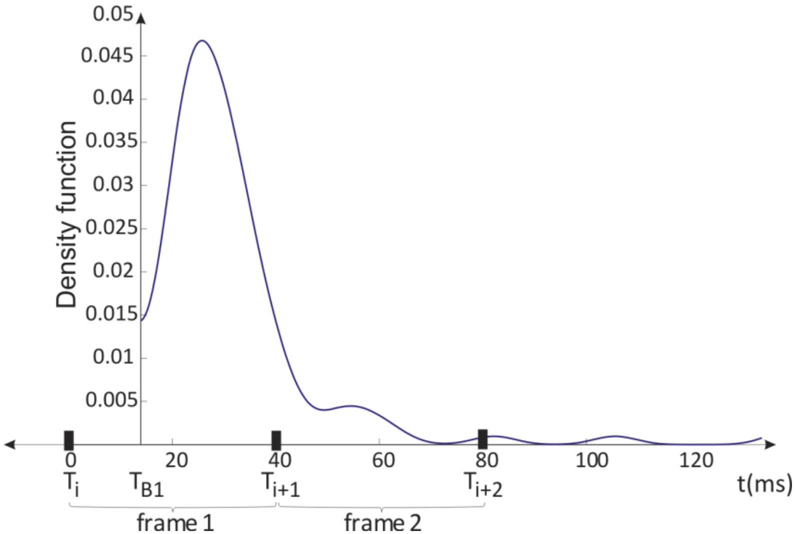
- the time window during which the attacker can mount the relaying attack:
  $\Delta t_{t/c} \leq (\Delta t^*_{AB} - \Delta t_{A\hat{B}}) + [\Delta t_B - (1-\rho)\, \Delta t_B] - (T_0 - T_{\hat{B}0})$

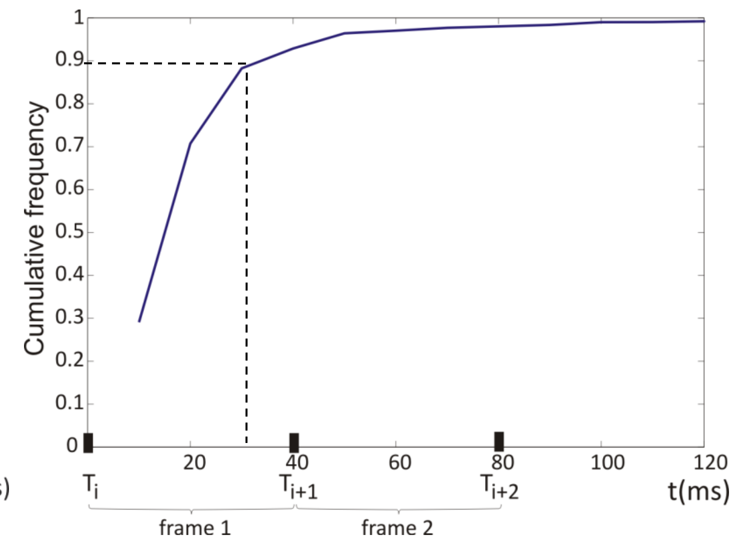
Relay Attack Timing Model



$\Delta t_B^* = T_{B1} - T_{B0} \lesssim 120$ ms

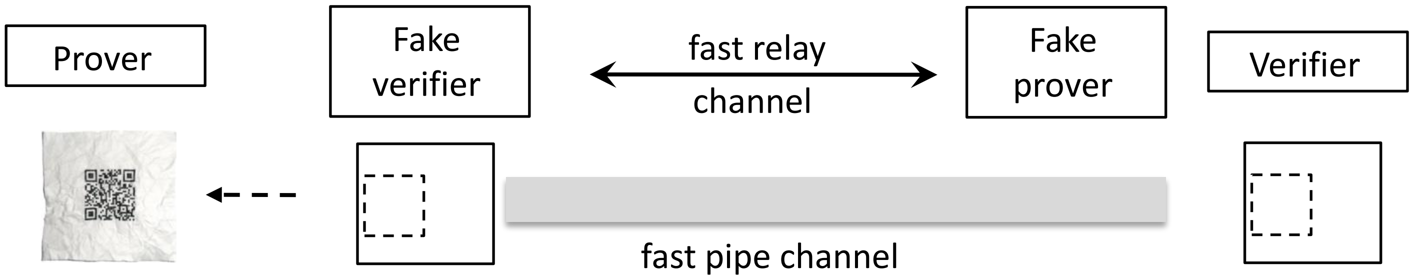
$\Delta t_{AB}^* = \Delta t(D) + \Delta t_f \lesssim 70$ ms





$$
\begin{aligned}
\Delta t_{AB} &= T_A - T_{B1} \\
&= \left(\left\lceil \frac{T_{B1} - T_i + \Delta t(D)}{\Delta t_f} - \alpha_D \right\rceil + \alpha_D \right) \Delta t_f + T_i - T_{B1} \\
&\leq \left(\frac{T_{B1} - T_i + \Delta t(D)}{\Delta t_f} - \alpha_D + 1 + \alpha_D \right) \Delta t_f + T_i - T_{B1} \\
&= \Delta t(D) + \Delta t_f \ .
\end{aligned}
$$

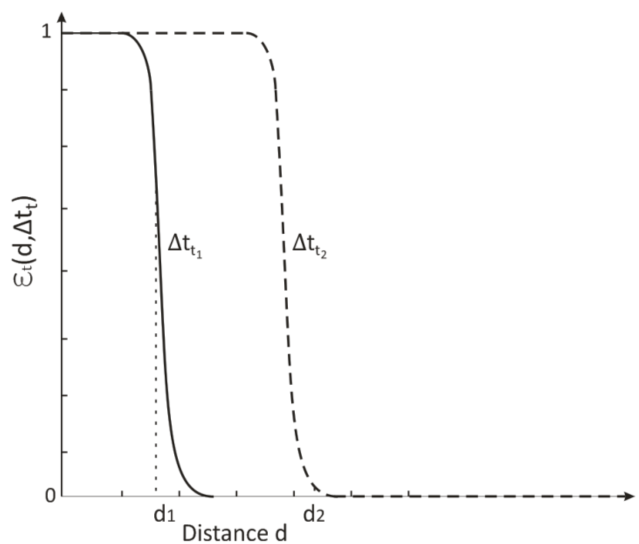
Weak Untransportability



- Transport attack: $\Delta t_t \leq (\Delta t^*_{AB}\text{-}\Delta t_B)$=70 ms-25 ms=45ms
- Airbag inflates within approximately 60-80 ms
- Accessing an application to a secure element on a NFC-enabled phone takes 50-80 ms
- With "bang-bang" strategy the cookie can travel the maximum distance *d* within Δt_t

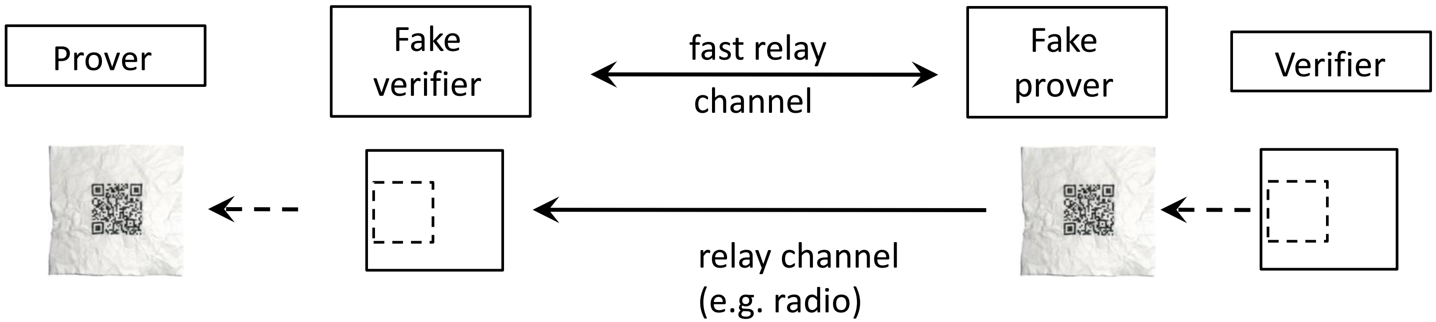
$$d(\Delta t_t)=\begin{cases} v_m(\Delta t_t - v_m/a) & \text{for } v_m<a\Delta t_t/2 \\ a\,\Delta t_t^2/4, & \text{otherwise} \end{cases}$$

a=200 G $\quad v_m$=70 m/s $\quad d(\Delta t_t)$=1.01 m



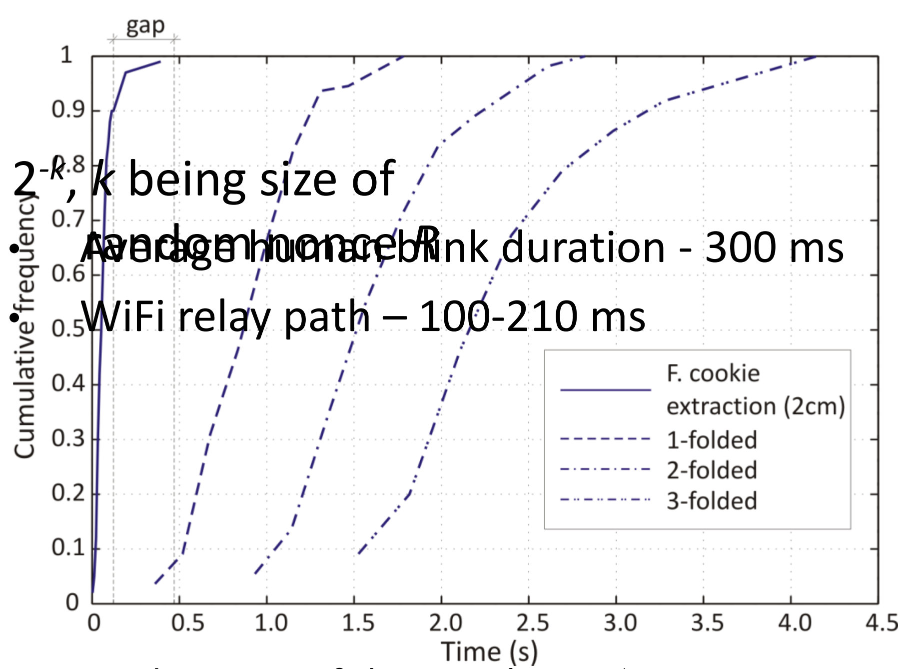
Advantage of the attacker $\varepsilon_t(d, \Delta t_t)$

Weak Uncloneability



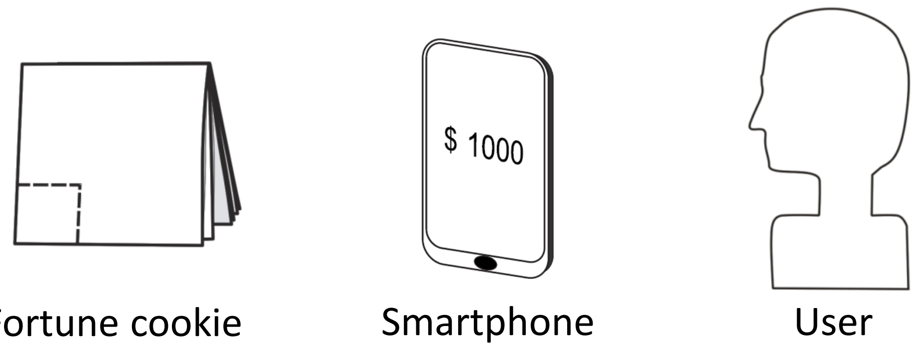
- Clone attack: $\Delta t_c \leq (\Delta t^*_{AB} - \Delta t_{AB}) + \Delta t^*_B = 70\text{ ms} - 0\text{ ms} + 120\text{ ms} = 190\text{ms}$
- Timewise it is more optimal to launch the cloning attack (45ms vs 190 ms)

- Naive guessing attacker → 2^{-k}, k being size of random nonce R
- Very strong X-Ray attacker →
  - Average human blink duration - 300 ms
  - WiFi relay path – 100-210 ms
- Realistic cloning attacker
- Powerful realistic cloning attacker

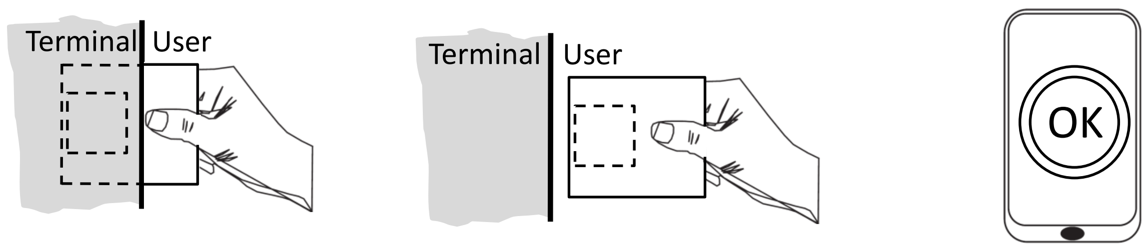


Advantage of the attacker $\varepsilon_c(\Delta t_c)$

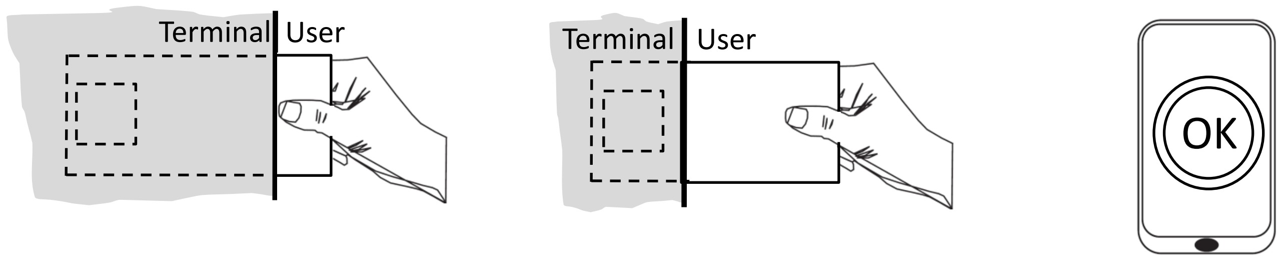
Unsimulabilty



- A successful simulability attack buys the attacker an extra time
- Example: Longer fortune cookie size
- No attack



- Attack



- We managed to trick 25 percent of users
- Advantage of the attacker: $\varepsilon_S(\varepsilon_t(d,\Delta t_t)+ \varepsilon_c(\Delta t_c))$

The Main Secrurity Result

Definition 1.

We say that a given protocol, executed between two honest parties A and B, is (d,ε) mafia fraud resistant, if the following holds except for the probability ε: a honest party B accepts to provide the service at time instant $(t + \Delta t_s)$ **only if** (1) a honest party A (e.g., the user) has requested that service from B during period $[t; t+\Delta t_s)$, and (2) A and B have been within the distance d of each other during that period

- Δt_s – allowable session duration
- k – size of the random nonce
- q – number of oracle calls
- $\varepsilon_t(\cdot)$ – probability of successful transport attack
- $\varepsilon_c(\cdot)$ – probability of successful cloning attack
- $\varepsilon_s(\cdot)$ – probability of successful simulability attack

Theorem 1.

The Forces protocol is (d,e) - mafia fraud resistant, with

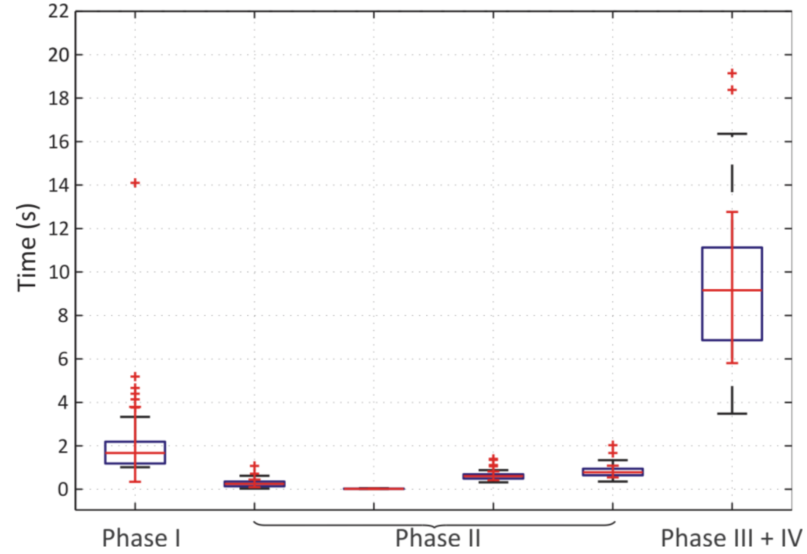
$\varepsilon \leq q[(q+1)2^{-k} + \varepsilon_t(d, \Delta t_t) + \varepsilon_c(\Delta t_c) + \varepsilon_S(\varepsilon_t(d,\Delta t_{out}) + \varepsilon_c(\Delta t_{out}))]$

User Performance Study

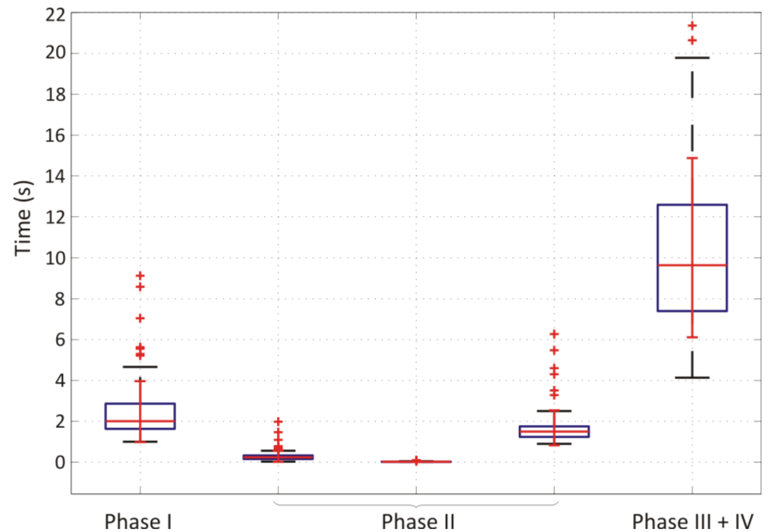
Implementation

- Tests with 58 users
- Small execution times
- Aveage times around 13 seconds
- Small error rates

Pushbutton-based event-synchronization



Camera-based event-synchronization



Conclusion

- Design of a completely new protocol secure against relay attacks developed for finantial transactions based on a paradigm of unrelayable channels,
- Formal proof of the protocol,
- Extensive user performance study on 54 users,
- The proposed solution has a reasonably low execution time (around 13 seconds on average), minimal error rate and is easy to understand,

Thank you for your attention!