Towards a virtual bank for evaluating security aspects with focus on user behavior

Sven Kiljan, Harald Vranken & Marko van Eekelen

sven@kiljan.org

www.kiljan.org

July 15, 2016

NHL HOGESCHOOL

Open Universiteit

Radboud University

Introduction

- Sven Kiljan
- PhD student at Open University of the Netherlands
- Research: improving technical security in online banking

Presentation contents

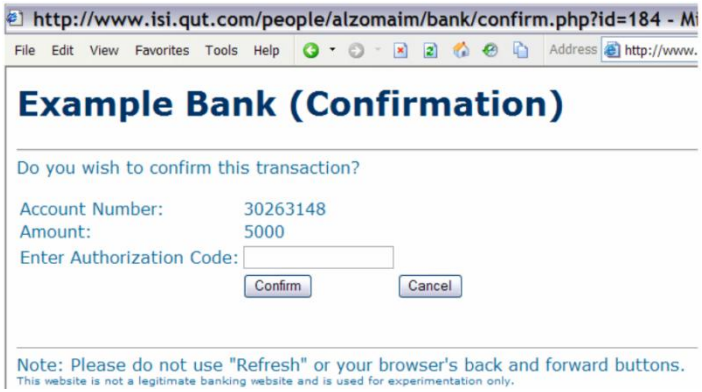
- **Problem statement and objectives**
- Design of a virtual bank and of a proof of concept
- Test case
- Resulting data
- Concluding remarks

Problem statement and objectives

- Subject: usable security in online banking
  - Specific focus: financial transaction authorization
- Research by banks
  - Closed, proprietary testing environments
  - Time constraints and limited demographical diversity due to using physical test centers
  - Results and data are shared rarely if ever

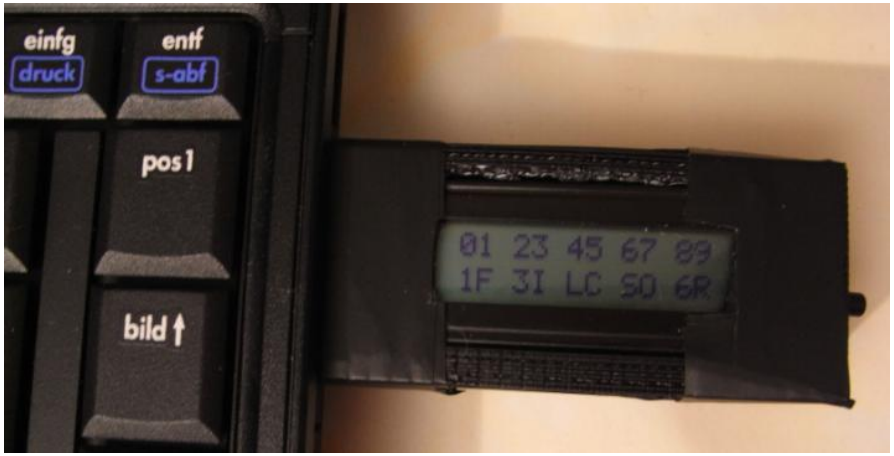
- Research by academics
  - Ad hoc testing environments
  - Limited demographical diversity (often students, teachers and other researchers, overall highly educated)
  - Results and data **are** often shared, but test environments rarely if ever

Problem statement and objectives

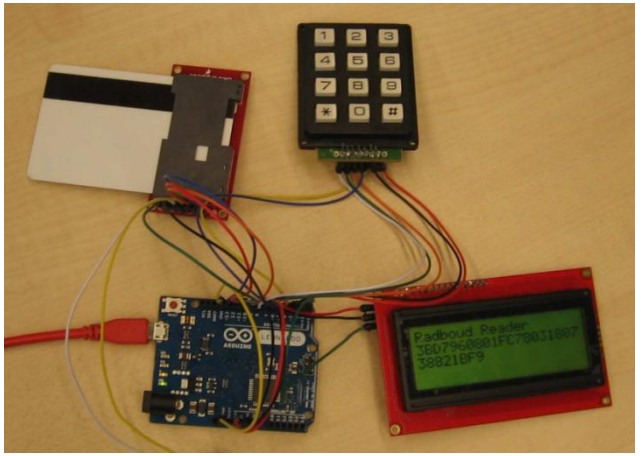


AlZomai et al. (2008)

Weigold (IBM) and Hiltgen (UBS) (2011)



Li et al. (2012)



Poll and de Ruiter (2013)

Problem statement and objectives

- Objectives

- Support more testers from a wider audience
  - Gives a better representation of the online banking population
  - More scalable and lower operational costs

- Modular and reusable code
  - Prevents reinvention of the wheel
  - Motivates researchers to share results and methods
  - Supports research repeatability

Presentation contents

- Problem statement and objectives
- **Design of a virtual bank and of a proof of concept**
- Test case
- Resulting data
- Concluding remarks

The idea of a ‘virtual bank’ to test with

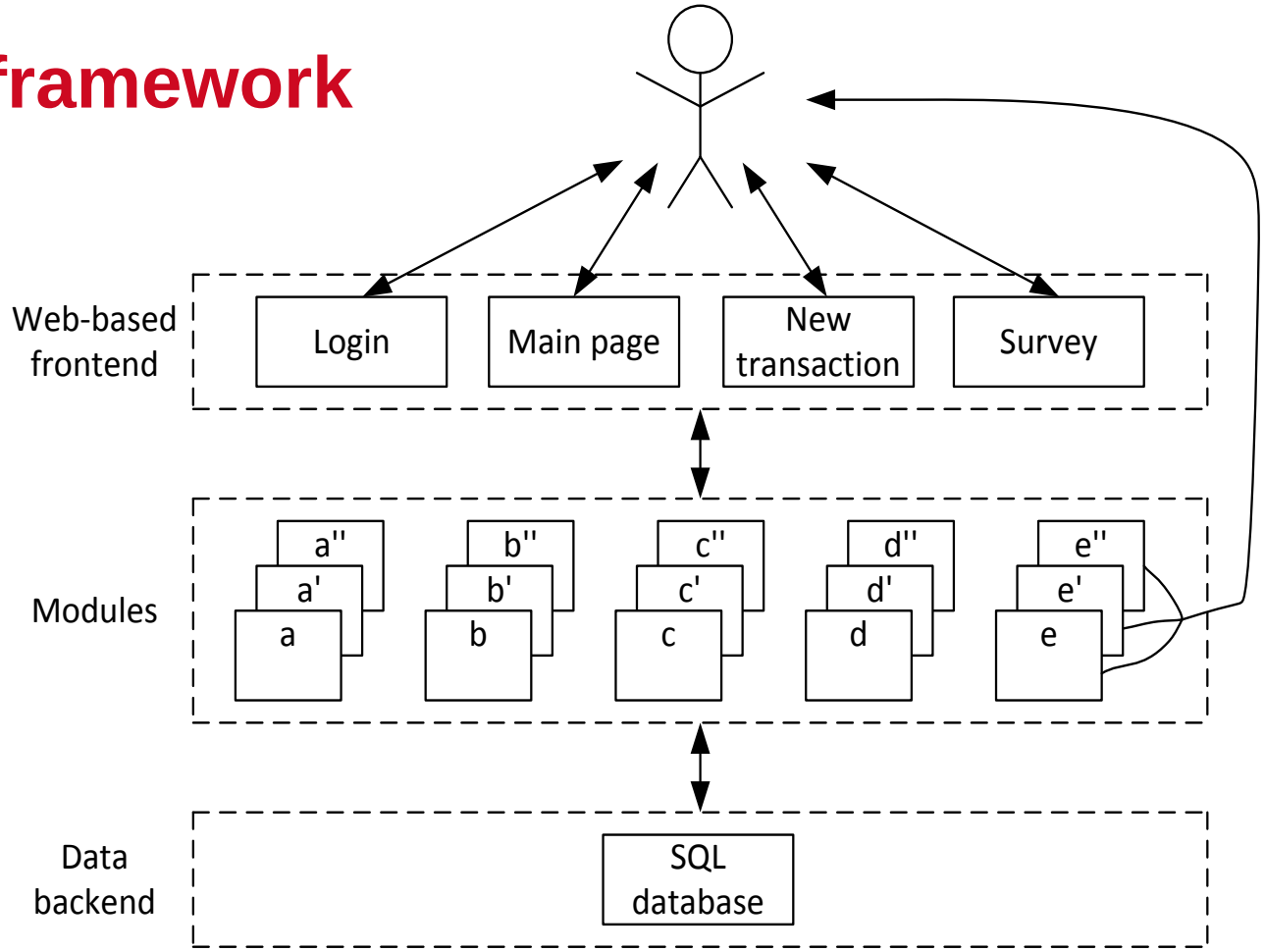
- Allow ‘real life’ circumstances for participants to test new online banking techniques by using the Internet
  - Not limited by geographical location
  - Not limited by number of test seats
  - Comes closer to representing ‘real’ online banking

- Measure user objective actions
- Measure user’s subjective perceptions (through surveys)

- Scope: login authentication and transaction authorization

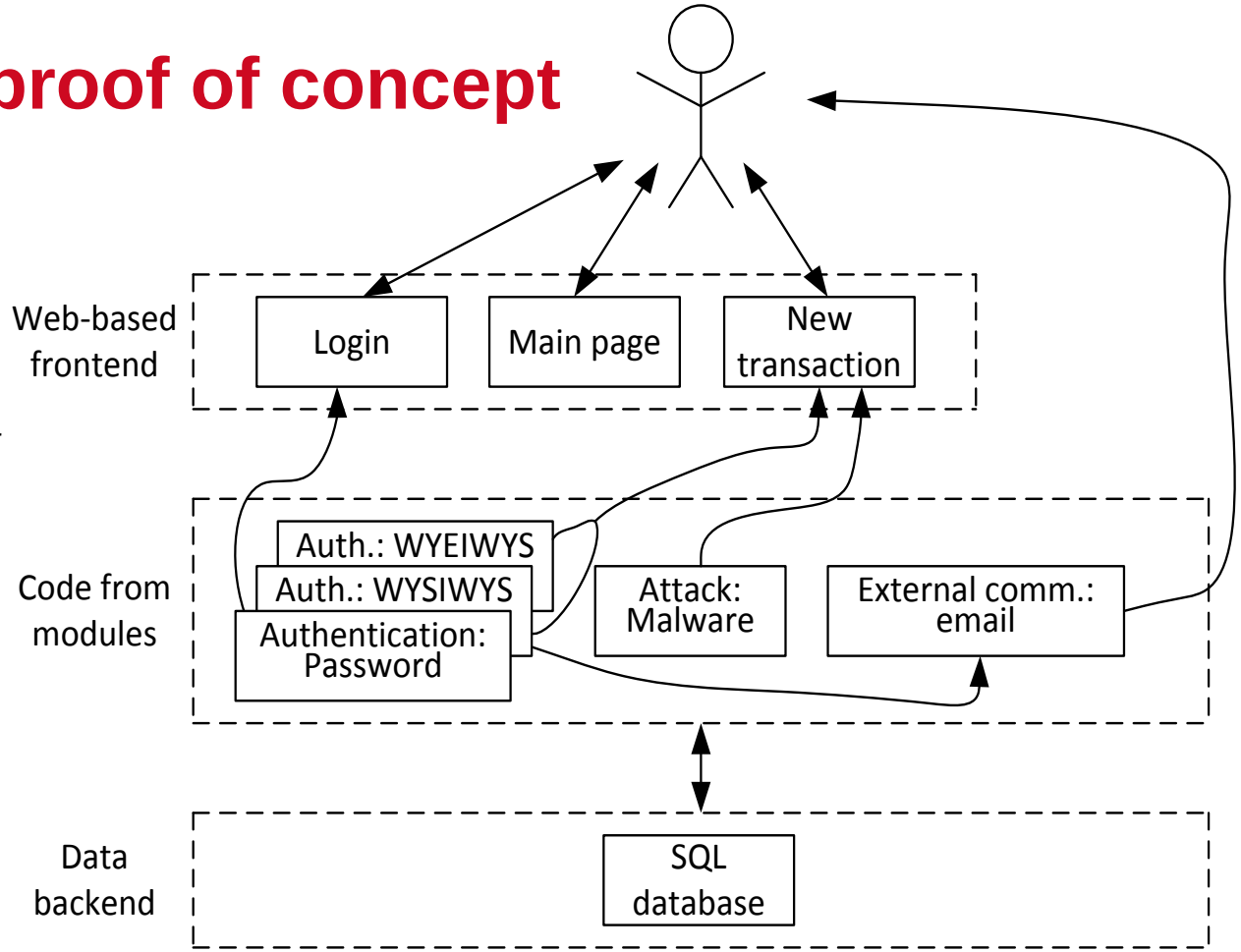
Designing a framework

- Modular
  - User authentication
  - Transaction authorization
  - Simulated online banking attacks
  - External communication
  - External survey tool connectivity
  - ...



Designing a proof of concept

- Purpose:
  - Test feasibility
  - Collect relevant data
  - Analyze data
- Static



Presentation contents

- Problem statement and objectives
- Design of a virtual bank and of a proof of concept
- **Test case**
- Resulting data
- Concluding remarks

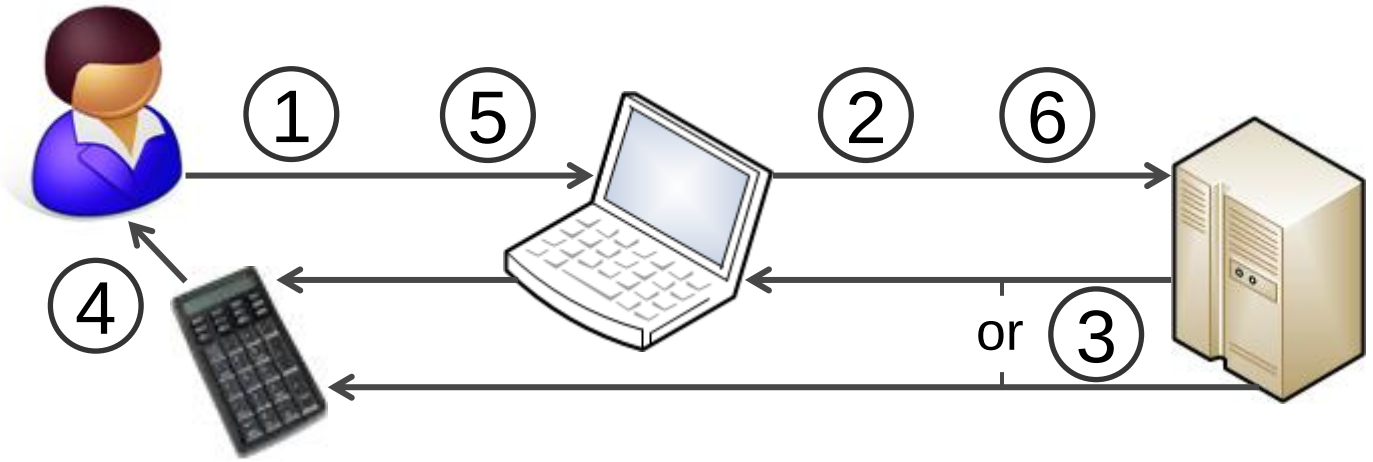
Test case

- Research questions:
  - What are the differences in time that users need to perform actions?
  - Do users pay enough attention during critical security actions?

- Two transaction authorization schemes:
  - What You See Is What You Sign
    - Use email as a simulated secure out-of-band channel
    - Allows for simulated attacks that test the user's vigilance
  - Nothing (control group)

Test case
Scheme: What You See Is What You Sign

- An authorization scheme that allows users to securely verify information received earlier by banks



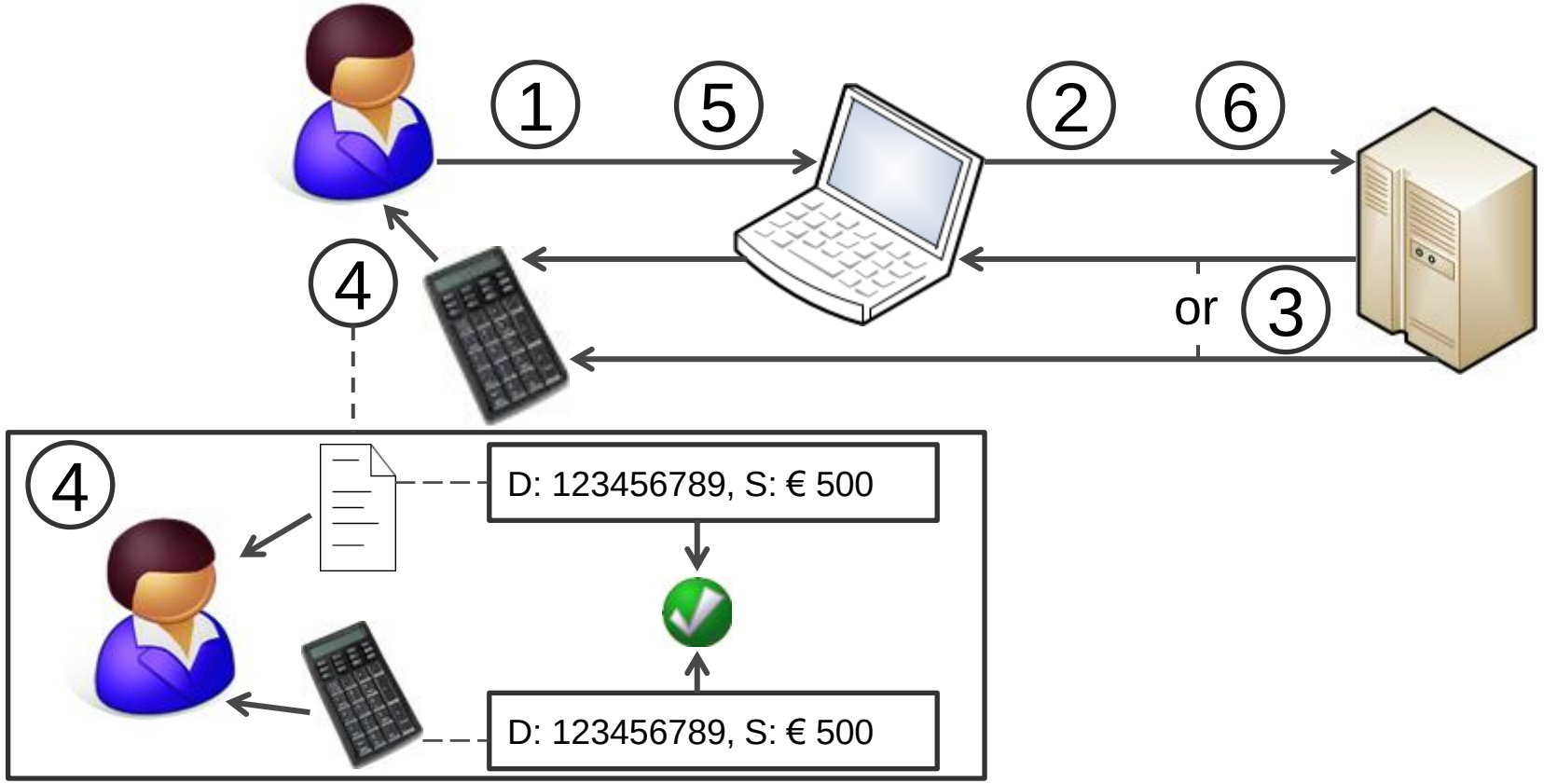
1 2 Critical transaction information (insecure)

3 4 Critical transaction information and confirmation code (secure)

5 6 Confirmation code (one-time password, so secure)

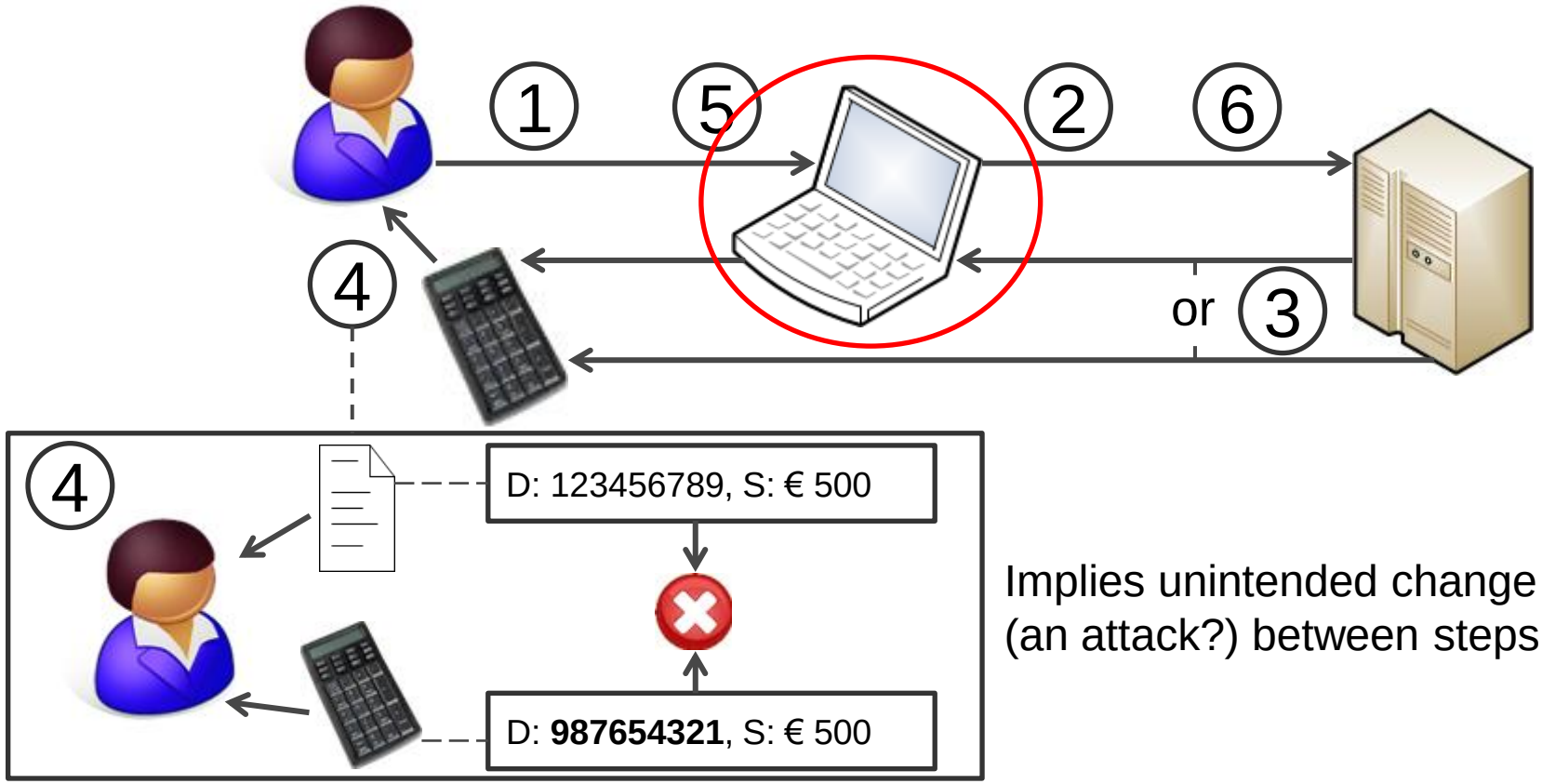
Test case
Scheme: What You See Is What You Sign

- An authorization scheme that allows users to securely verify information received earlier by banks



Test case
Scheme: What You See Is What You Sign

- An authorization scheme that allows users to securely verify information received earlier by banks

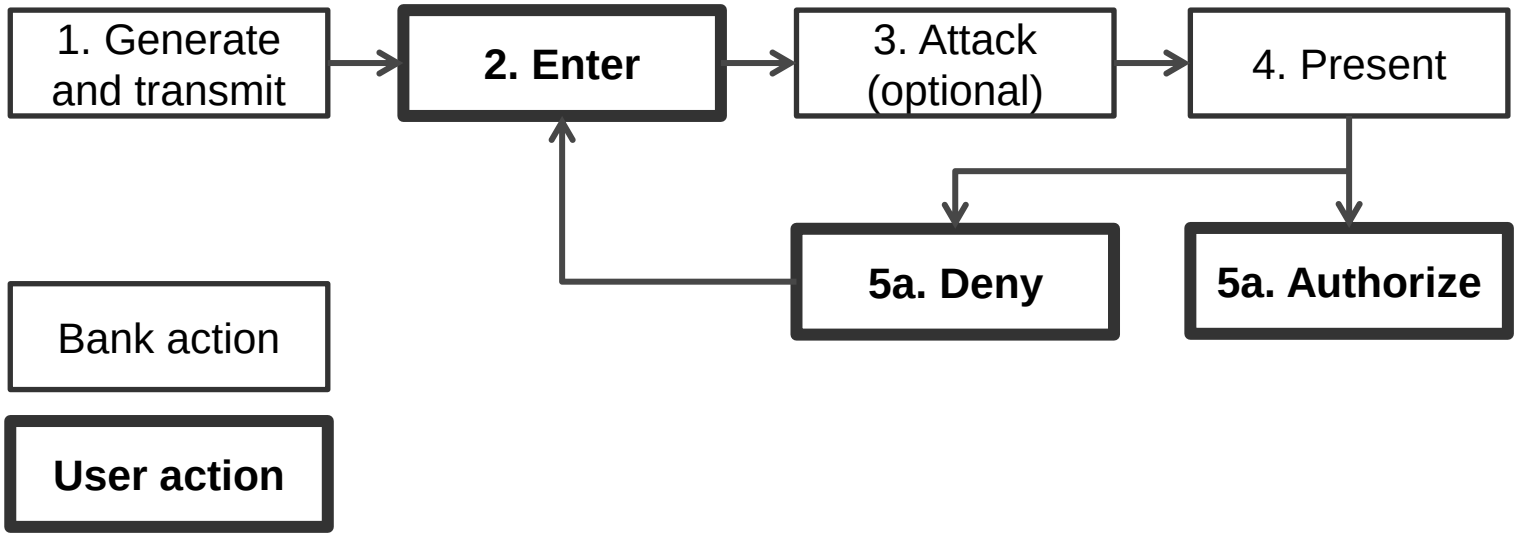


Implies unintended change
(an attack?) between steps 1 and 2.

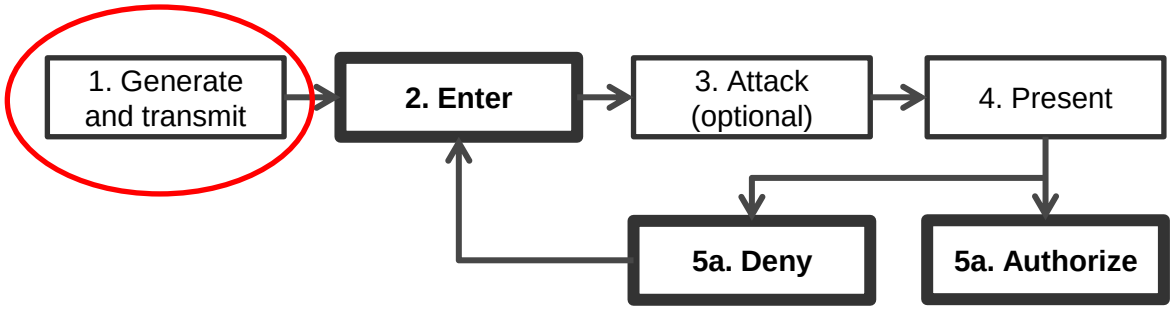
The test cycle

- Group 1: What You Enter Is What You Sign
- Group 2: Control group (no authorization method)

- Test cycle

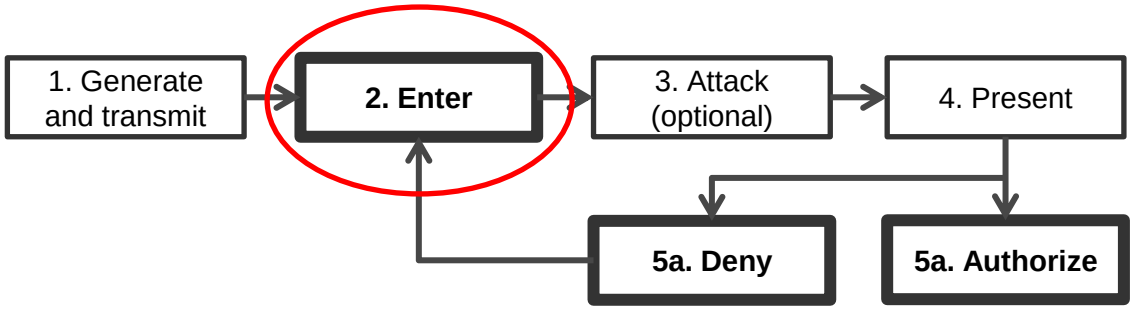


Test cycle explained




```
From: nhlbank@kiljan.org
To: <email>
Subject: Transactions to execute.

This message is part of the NHL Bank experiment, which uses a fictional
bank to test various aspects related to transaction authorization.

Dear Sir or Madam <Last Name>,

You will find information in this message to perform two transactions in
the NHL Bank online environment. The name field can have any name you can
think of.

-------------------------------------------------------
IBAN destination account: NL43 NHLB 0760 4801 68
Amount: € 260,22
-------------------------------------------------------

-------------------------------------------------------
IBAN destination account: NL10 NHLB 0693 1888 55
Amount: € 821,79
-------------------------------------------------------
```

Test cycle explained



Note: you cannot use cut, copy or paste text functions.

From account:

NL64 SIMB 0933 0778 07

Amount (€):

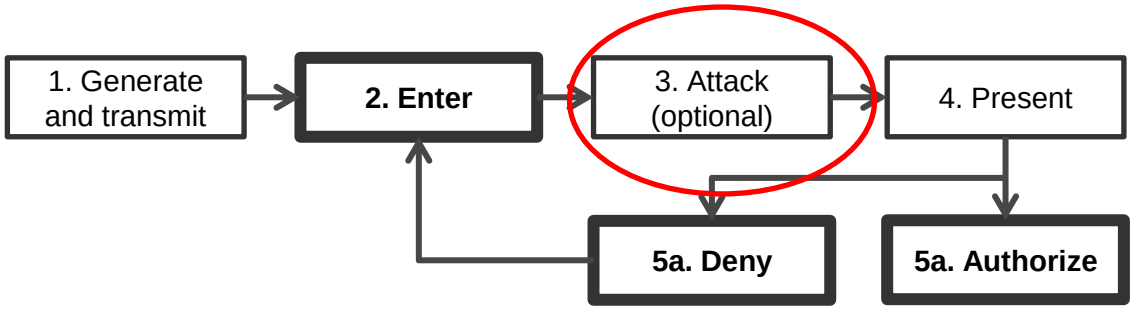
Recipient name:

Recipient account number:

Cancel

To authorization ->

Test cycle explained



Simulated attack or not? (only applies to WYSIWYS)

Original data (entered by user)

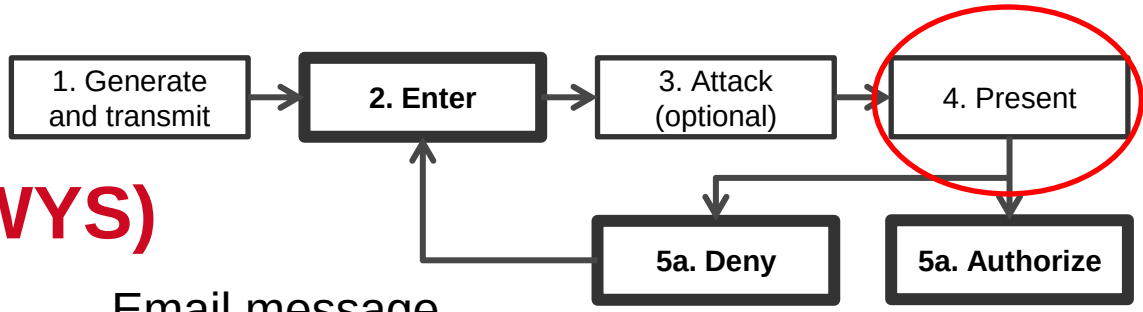
```
Amount: € 12.34
Recipient name: Recipient
To account: NL23SIMB0111882559
```

Modified data (by server)

```
Amount: € 12.34
Recipient name: Recipient
To account: NL23SIMB011188259
```

- Each has a 50% probability
- Note: this is not a realistic attack

Test cycle explained (WYSIWYS)



Browser
Insecure channel. Shows what the user entered.

Prepared transaction

From account: NL64 SIMB 0933 0778 07

Amount: € 12.34

Recipient name: Recipient

Recipient account: NL23SIMB0111882559

An email with information about the transaction and an authorization code has been sent to your email address.
Only enter the authorization code in the field below if the information on this page matches the information in the email.

Authorization code:

<-- Back to entry | Deny | Authorize

Email message
Secure channel. Shows what the bank received.

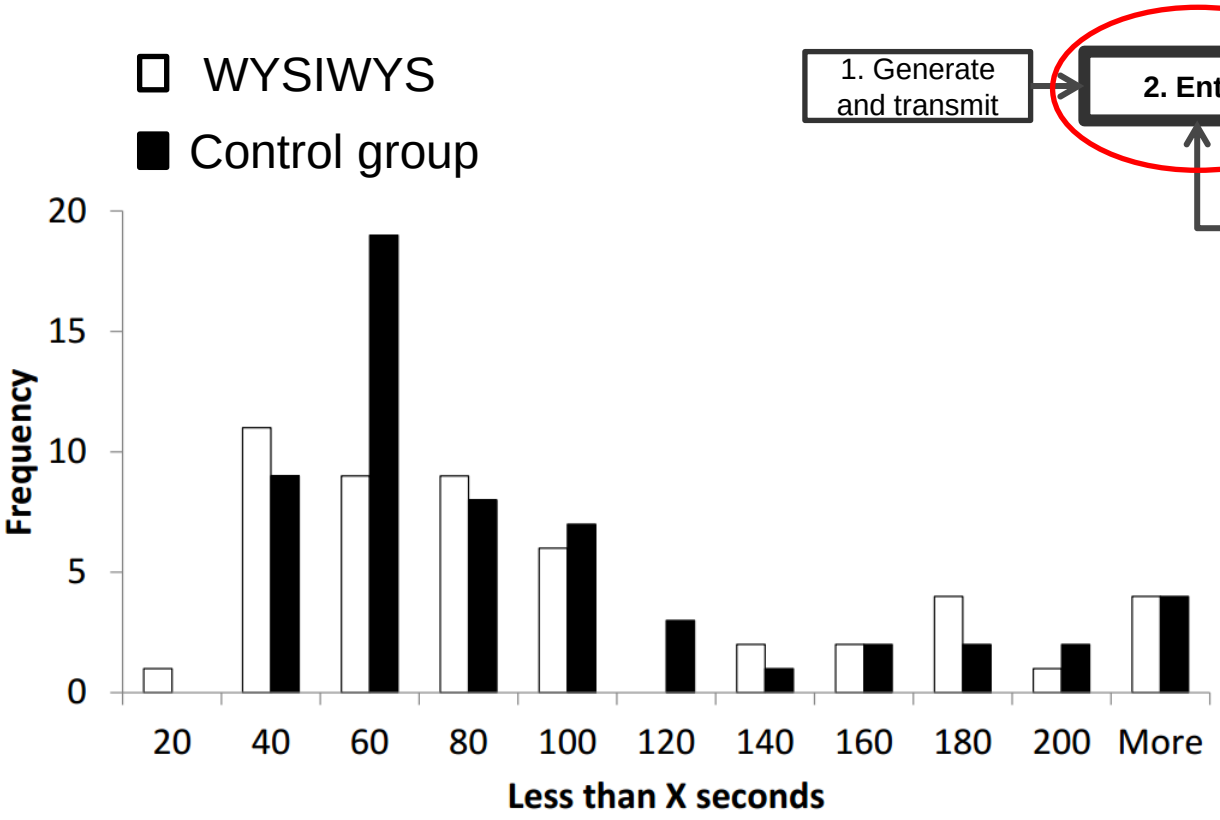
```
From: nhlbank@kiljan.org
To: <email>
Subject: Transactions to execute.

The NHL Bank received a request to transfer an
amount of money from your bank account with
IBAN NL64 SIMB 0933 0778 07. This request was
made with the following data:

            Amount: € 12.34
   Recipient name: Recipient
Recipient account: NL23SIMB0111882259

Authorization code: 170169

Please verify that the data represented in
this message matches the data that you see on
the bank's site. If the data matches, enter
the authorization code from this message on
the prepared transaction page and use the
'Authorize' button. If the data does not
match, ignore the authorization code and only
use the 'Deny' button.
```

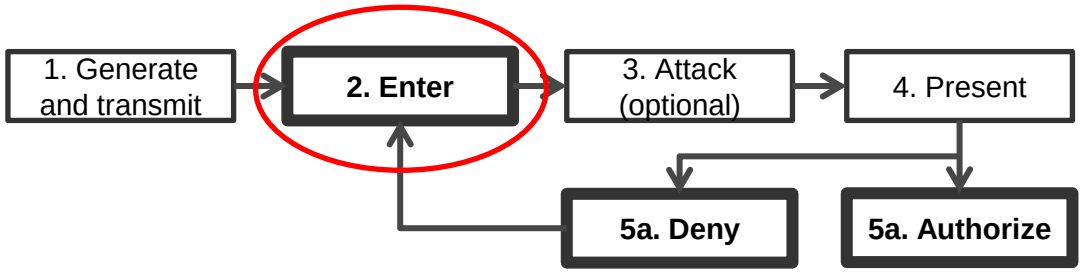
Presentation contents

- Problem statement and objectives
- Design of a virtual bank and of a proof of concept
- Test case
- **Resulting data**
- Concluding remarks

Resulting data – Time differences

- Average transaction entry times





$n_{WYSIWYS} = 49$
$n_{control} = 57$

H_0: times are equal

H_a: times are not equal

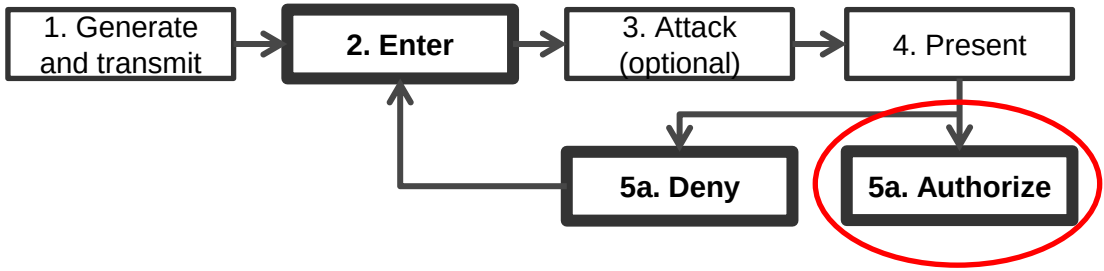
$p = 0.71$

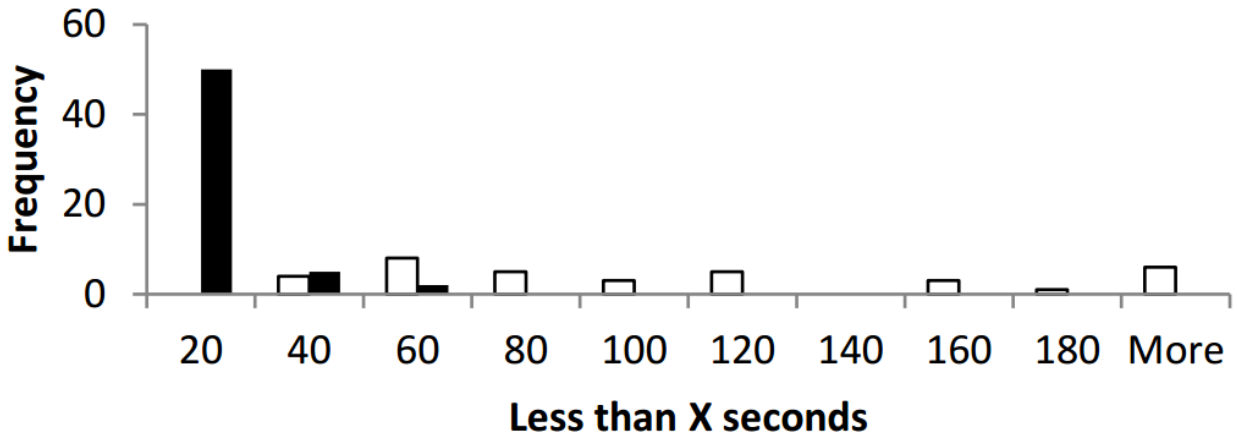
Resulting data – Time differences

- Average transaction authorization times

WYSIWYS

Control group





$n_{WYSIWYSnotattacked}$ = 35

$n_{control}$ = 57

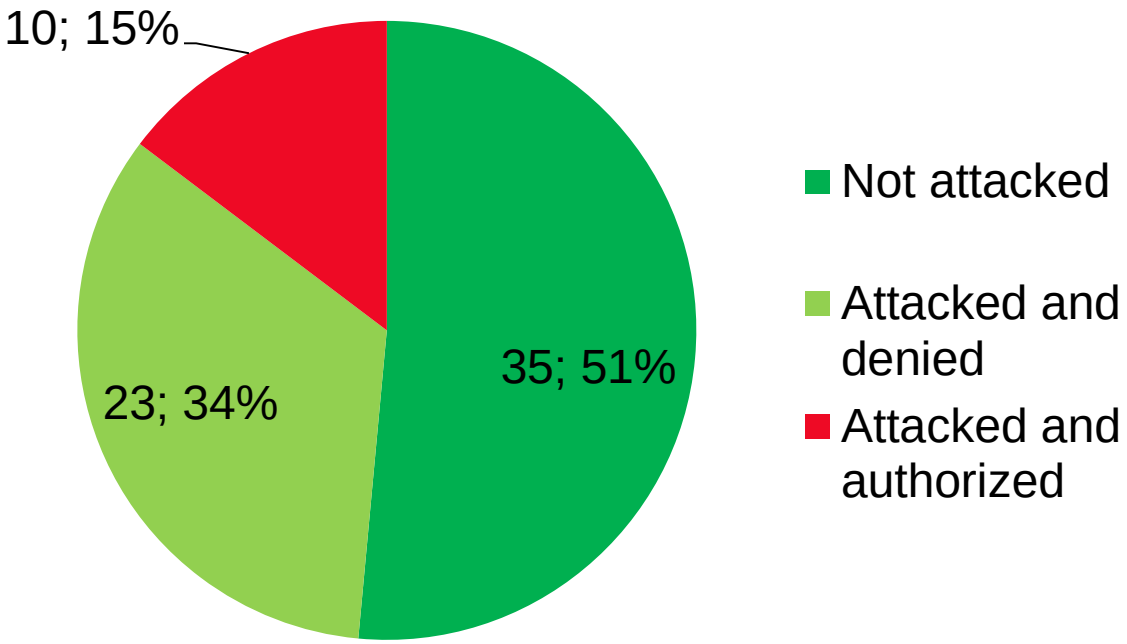
H_0: times are equal

H_a: control group needs less time

p = < 0.0001

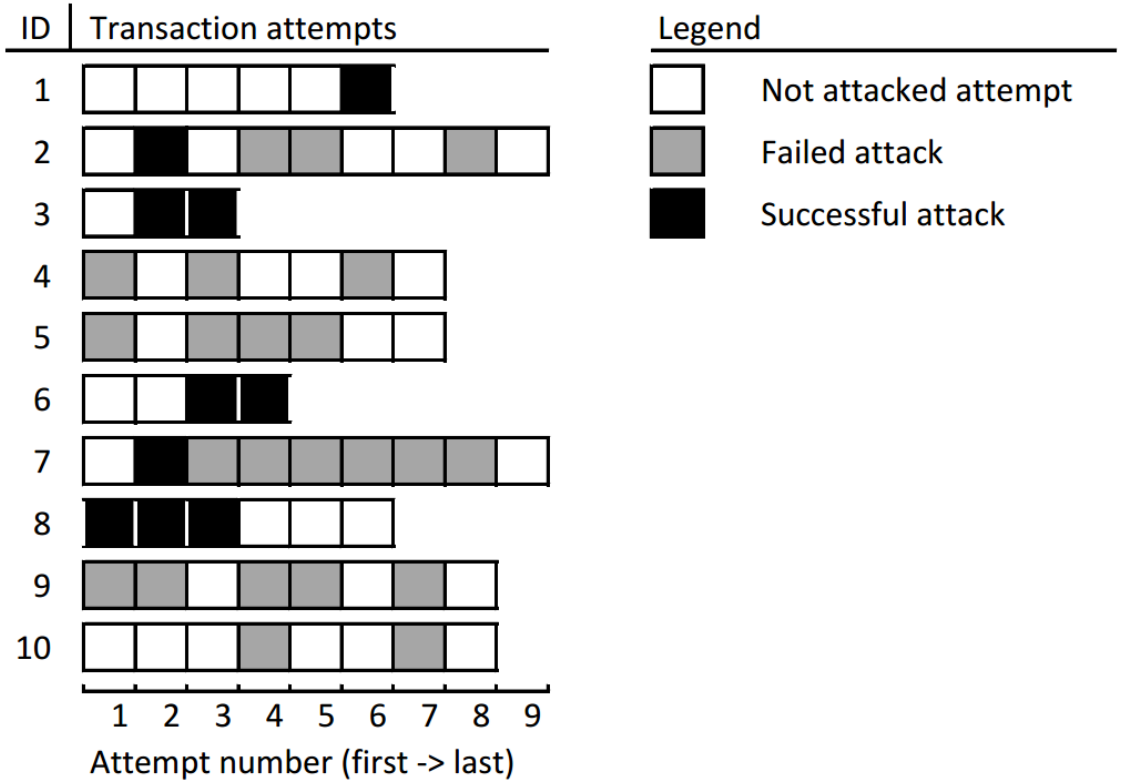
Resulting data – Attacked transactions

- What You See Is What You Sign attempts



Resulting data – Attacked transactions

- What You See Is What You Sign attempts by each participant



- Users seem to pay more attention after successfully noticing an attack

Concluding remarks

- The proof of concept could be used to retrieve useful data about a user's actions. This was done independent of the location and availability of the individual testers and over a longer period of time.

- Users seem to pay more attention in the What You See Is What You Sign transaction authorization scheme if they were previously confronted with a successful attack. Further research questions:
  - Is this effect constant?
  - How long does the period of increased attention last?
  - Are there alternatives to direct confrontation with an attack that can start and/or repeat this period?

Thank you for your attention!

- AlZomai, M., AlFayyadh, B., Jøsang, A., and McCullagh, A. (2008). An exprimental investigation of the usability of transaction authorization in online bank security systems. In *Proceedings of the sixth Australasian conference on Information security-Volume 81*, pages 65–73. Australian Computer Society, Inc.
- S. Li, A.-R. Sadeghi, S. Heisrath, R. Schmitz, and J. Ahmad, “hPIN/hTAN: A Lightweight and Low-Cost E-Banking Solution against Untrusted Computers,” in *Financial Cryptography and Data Security*, ser. Lecture Notes in Computer Science, G. Danezis, Ed. Springer Berlin Heidelberg, 2012, vol. 7035, pp. 235–249. [Online].
- Poll, E., de Ruiter, J., 2013. The Radboud Reader: A Minimal Trusted Smartcard Reader for Securing Online Transactions. In: *Policies and Research in Identity Management* - Third IFIP WG 11.6 Working Conference, IDMAN 2013, London, UK, April 8-9, 2013. Proceedings. pp. 107-120.
- T. Weigold and A. Hiltgen, “Secure confirmation of sensitive transaction data in modern Internet banking services,” in *Internet Security* (World-CIS), 2011 World Congress on, Feb 2011, pp. 125–132.