FONDAZIONE BRUNO KESSLER

SECURITY & TRUST

Scenari, approcci, esperienze di strong authentication pre e post direttiva PSD2

Andrea Bisegna, Roberto Carbone,
Marco Pernpruner, Giada Sciarretta, Silvio Ranise
Security & Trust Research Unit
Fondazione Bruno Kessler, Trento, Italy

Talk Tech, DedaGroup
11 marzo 2021

| Agenda

- Overview of Security Vulnerabilities Affecting the Financial Scenario
- Payment Services Directive 2 (PSD2)
- Automated Analysis of Security Protocols for the PSD2:
  - from a Design Perspective
  - from a Deployment Perspective

| Agenda

- **Overview of Security Vulnerabilities Affecting the Financial Scenario**
- Payment Services Directive 2 (PSD2)
- Automated Analysis of Security Protocols for the PSD2:
  - from a Design Perspective
  - from a Deployment Perspective

| Security Vulnerabilities

Android malware can steal Google Authentic

A new version of the "C
Authenticator app and

Cerberus banking Trojan source code released for free to cyberattackers

An auction designed to net the developer of the Android malware $100,000 failed.

Android Malware Gains 2FA Tokens, Screen

TrickBot bypassing 2FA

Malicious TrickMo app seen deployed in many for now, but broader use is

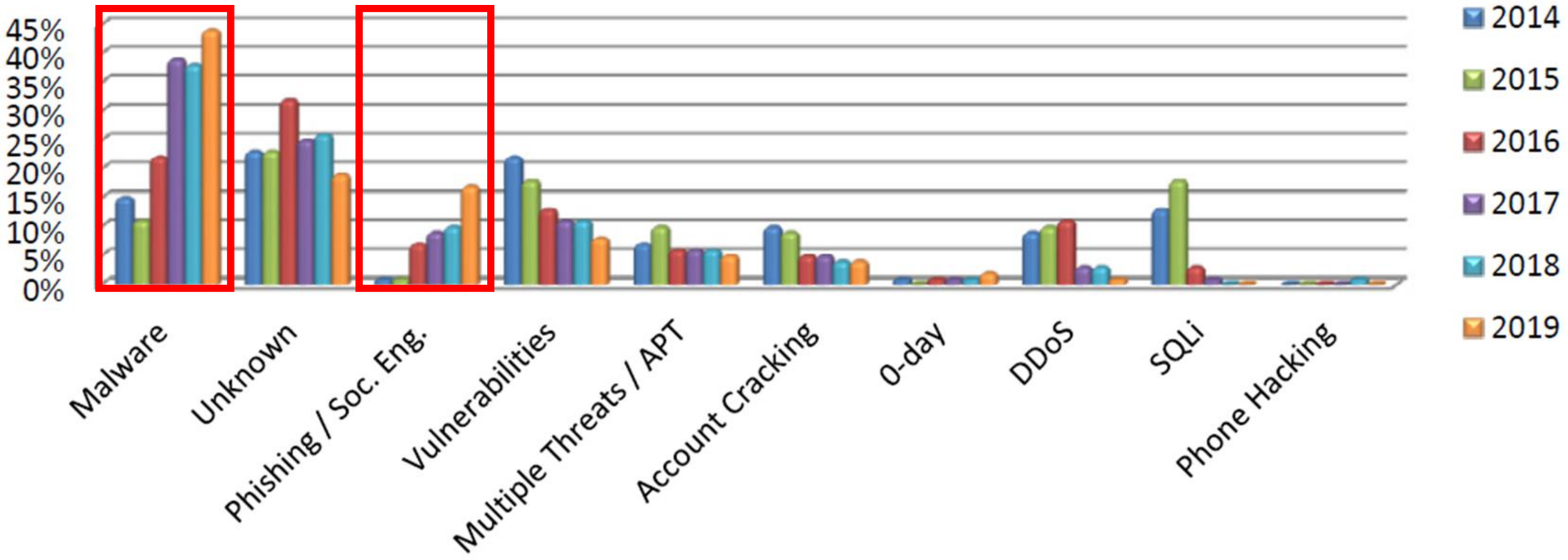
New 'Alien' malware can steal passwords from 226 Android apps

Most targets are banking apps, but Alien can also show phishing pages for social, instant messaging, and cryptocurrency apps.

id

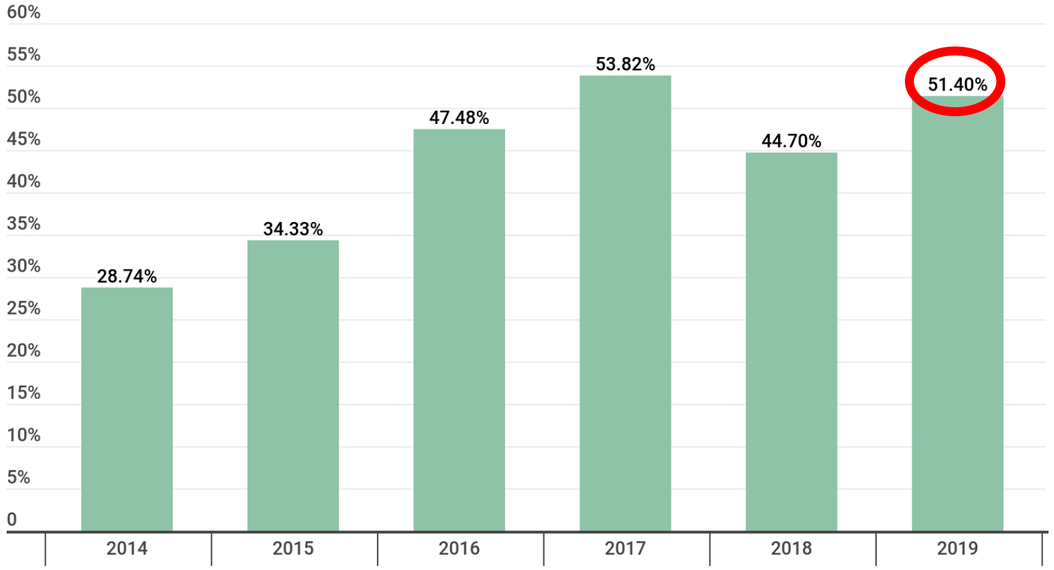
passwords and two-factor codes

Security Vulnerabilities
Techniques

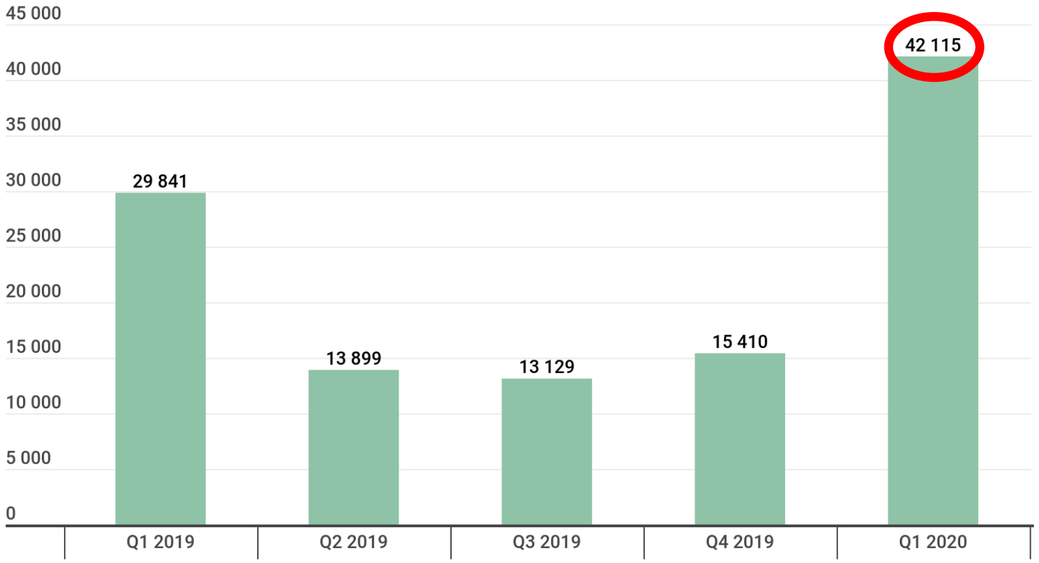


© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

Security Vulnerabilities
Financial Phishing and Malware

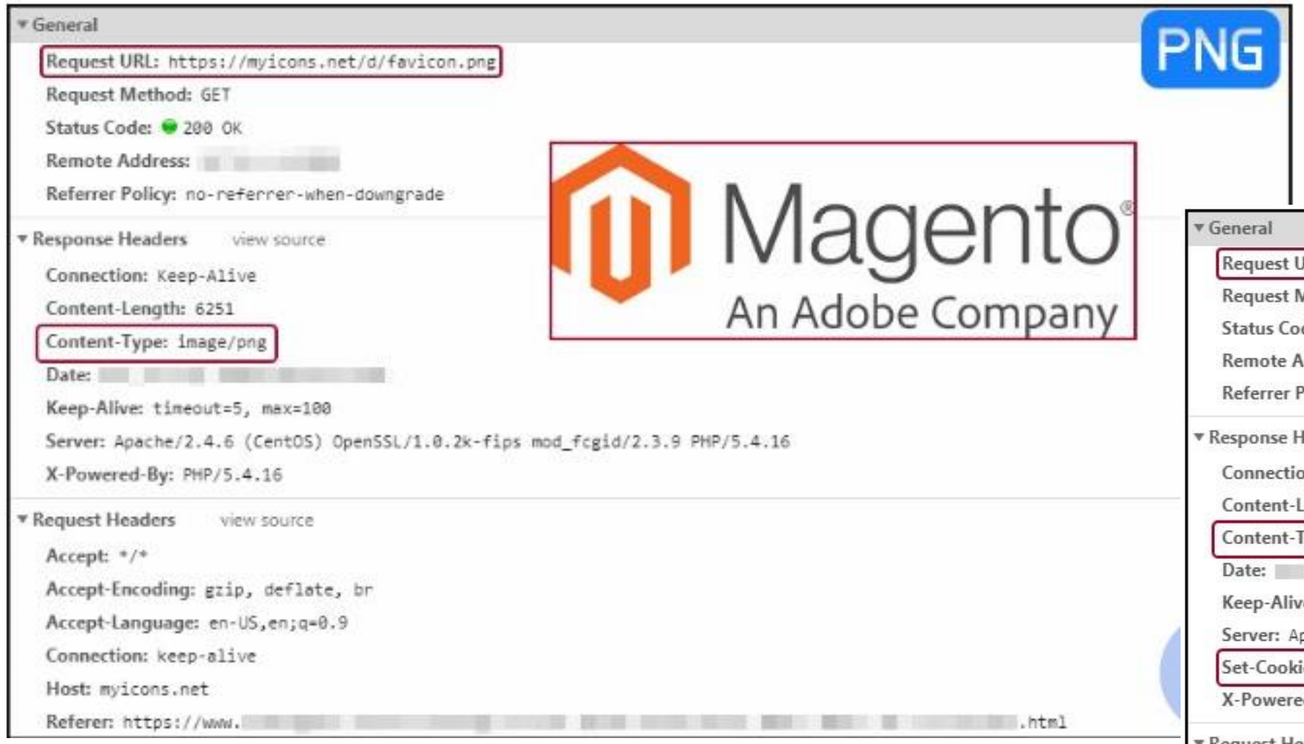


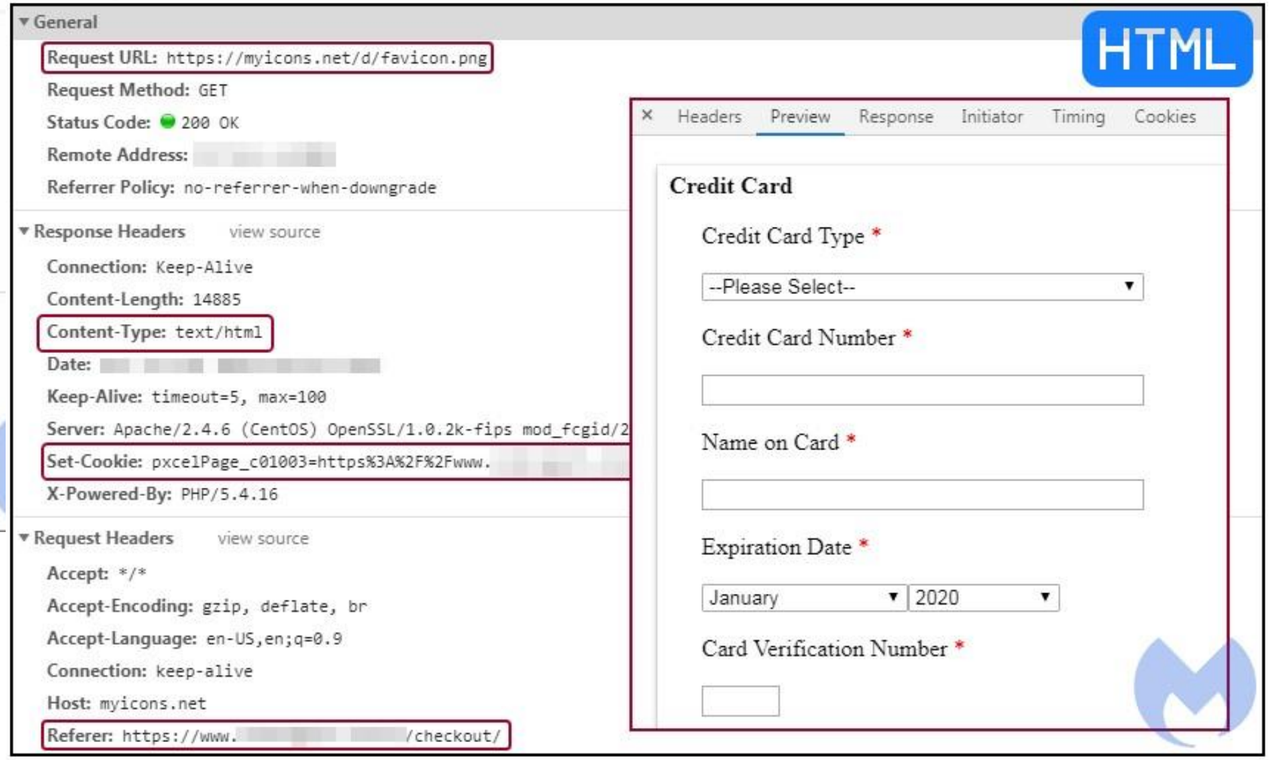
The percentage of financial phishing attacks (from overall phishing attacks) detected by Kaspersky, 2014-2019



Number of installation packages of mobile banking trojans detected by Kaspersky, Q1 2019 – Q1 2020

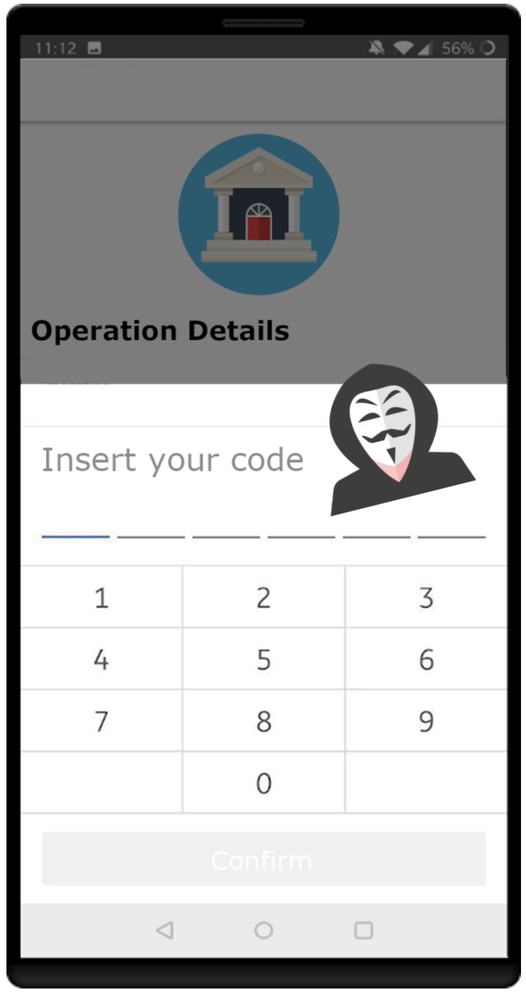
Security Vulnerabilities
Skimming



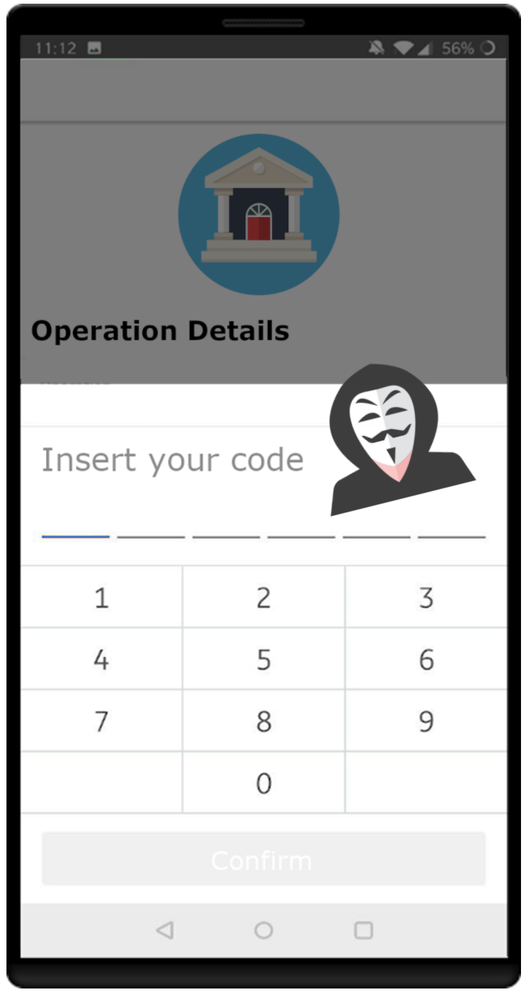


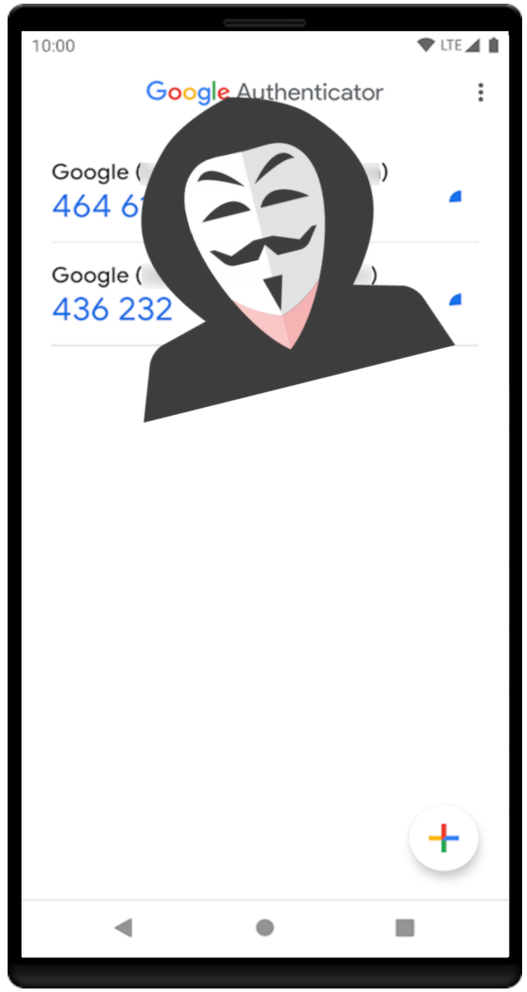
Source: https://blog.malwarebytes.com/threat-analysis/2020/05/credit-card-skimmer-masquerades-as-favicon/

Security Vulnerabilities
TrickBot



Security Vulnerabilities
TrickBot





| Agenda

- Overview of Security Vulnerabilities Affecting the Financial Scenario
- **Payment Services Directive 2 (PSD2)**
- Automated Analysis of Security Protocols for the PSD2:
  - from a Design Perspective
  - from a Deployment Perspective

| Payment Services Directive (PSD2)

Directive (EU) 2015/2366 regarding payment services in the internal market.

Open Banking

Fostering the birth of new innovative solutions
built around financial institutions

Security

Improving the security of e-banking protocols

Payment Services Directive (PSD2)

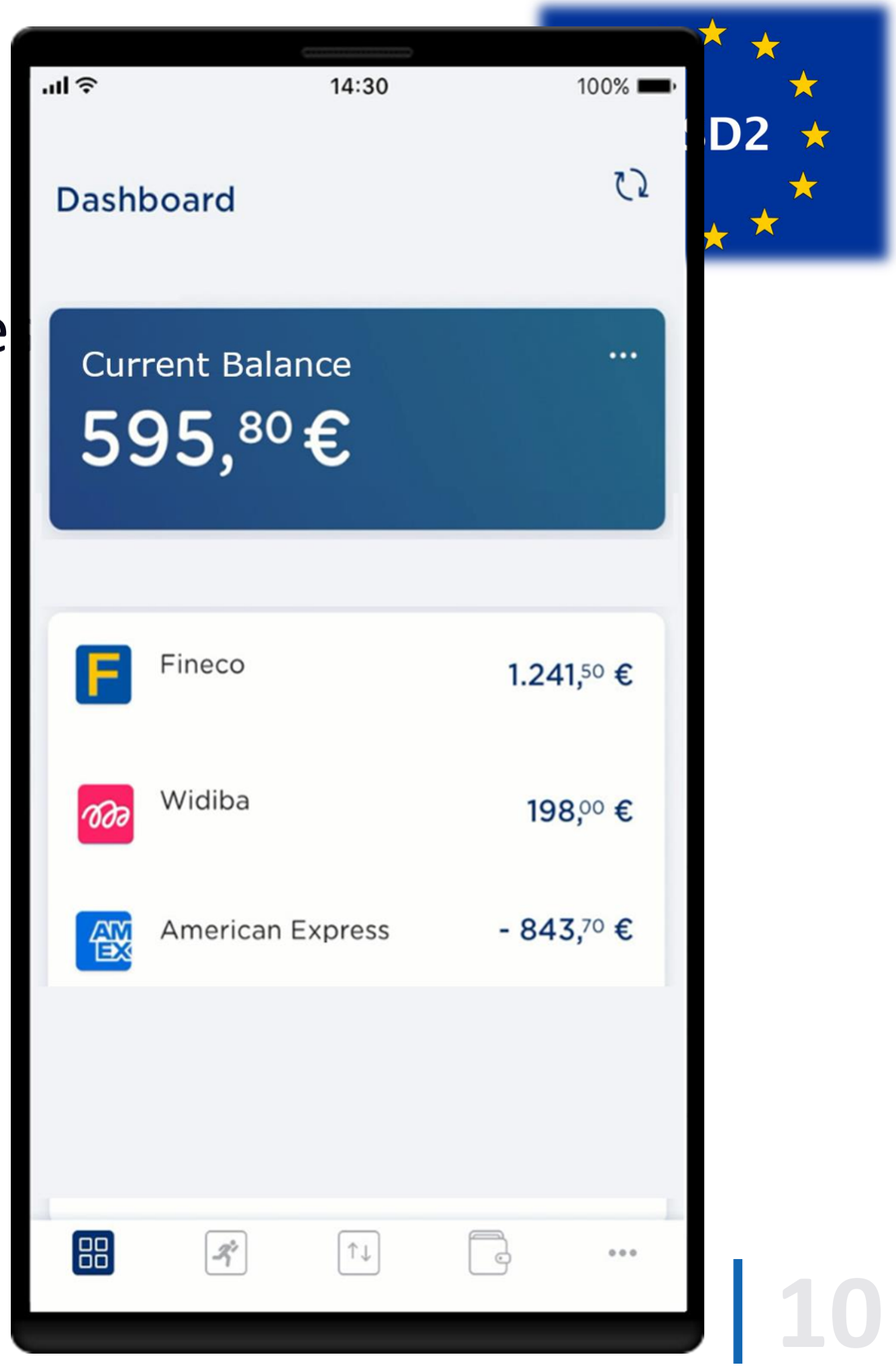
Directive (EU) 2015/2366 regarding payment service

Open Banking

Fostering the birth of new innovative solutions built around financial institutions

Security

Improving the security of e-banking protocols



FONDAZIONE BRUNO KESSLER
ICT CENTER FOR COMMUNICATION AND INFORMATION TECHNOLOGY
ST SECURITY & TRUST

| Payment Services Directive (PSD2)

Directive (EU) 2015/2366 regarding payment services in the internal market.

Open Banking

Fostering the birth of new innovative solutions built around financial institutions

Strong Customer Authentication (SCA)

Security

Improving the security of e-banking protocols

Dynamic Linking

Payment Services Directive (PSD2)
Strong Customer Authentication (SCA)

Authentication relying on more than a single *authentication factor:*

Images source: https://appspicket.com/the-next-generation-in-2fa-technology/

Payment Services Directive (PSD2)
Strong Cus

Authenticati

Actions	SCA required?
Balance inquiry	Depends on the case
Consultation of payment history of past 90 days	Depends on the case
Payments to trusted beneficiaries	Depends on the case
Recurrent payments with same amount and same payee	Depends on the case
Payments not exceeding € 30	Depends on the case
Payments exceeding € 30	Always

Images source: https://appspicket.com/the-next-generation-in-2fa-technology/

Payment Services Directive (PSD2)
Dynamic Linking

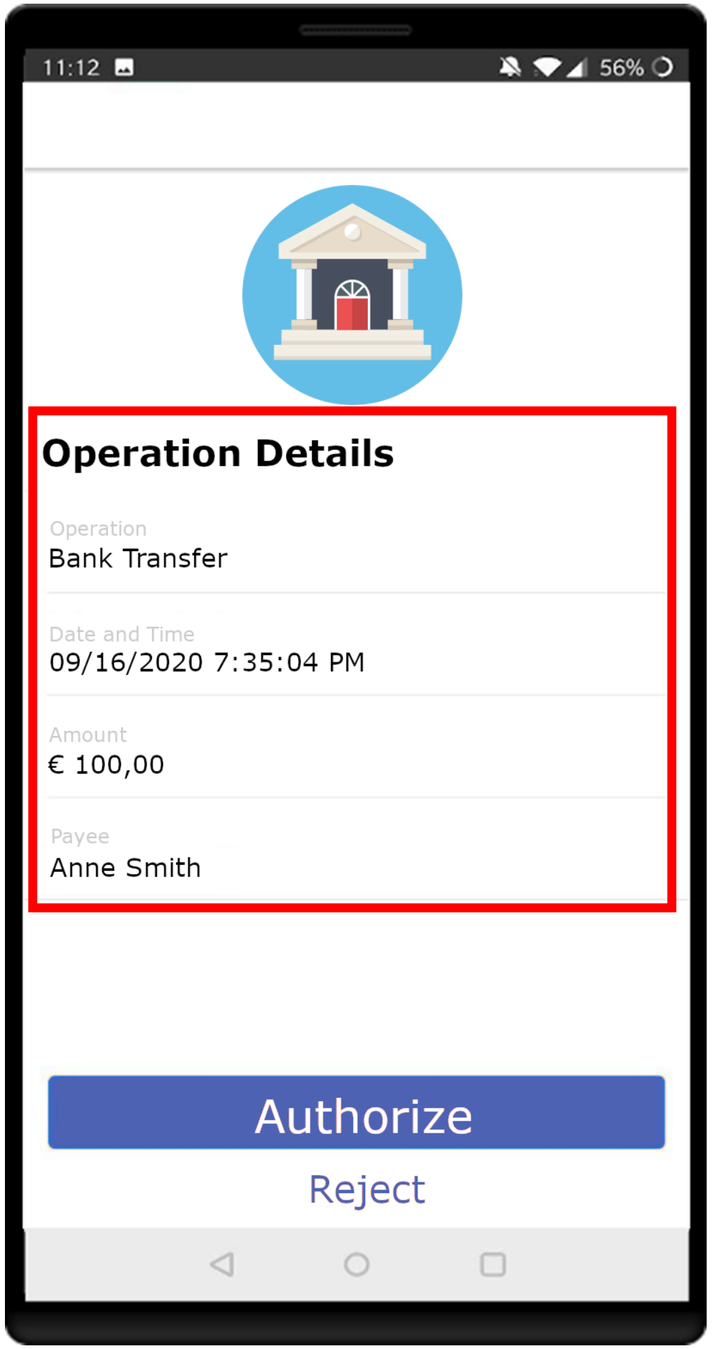
During a transaction, the *authentication code* must be strongly connected with the ongoing operation.

Transfer no.	AA/1234
Payer Name	John Smith
Payee Name	Anne Smith
Payee IBAN Code	IT12T1234512345123456789012
Amount	100,00 EUR

authentication code

Payment Services Directive (PSD2)
Dynamic Linking

Moreover, the user is always displayed the operations' details before the authorization.



Use Case
Before PSD2

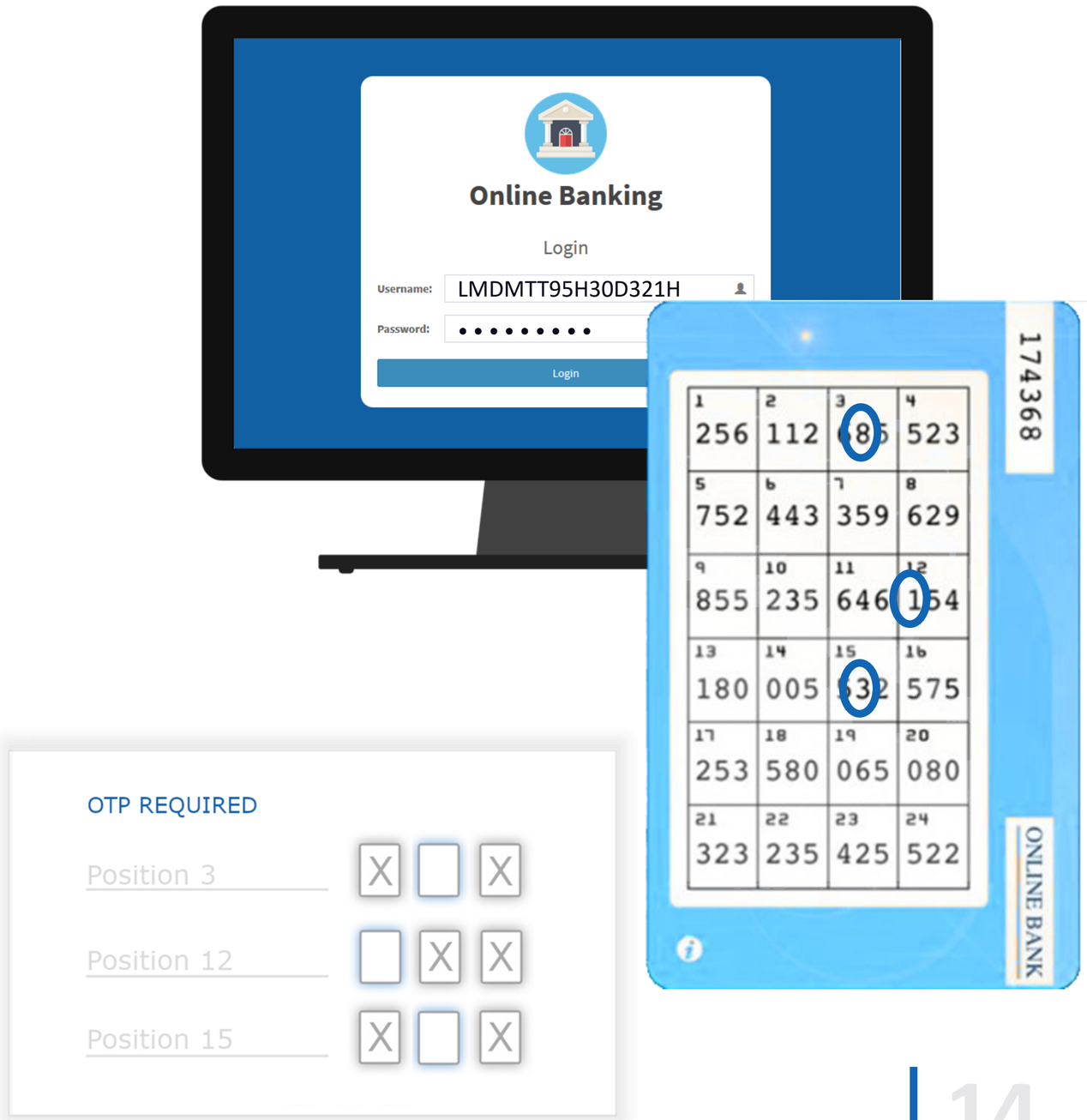
Before PSD2

1. The user authenticates on the online banking through credentials and performs an operation.

Use Case
Before PSD2

Before PSD2

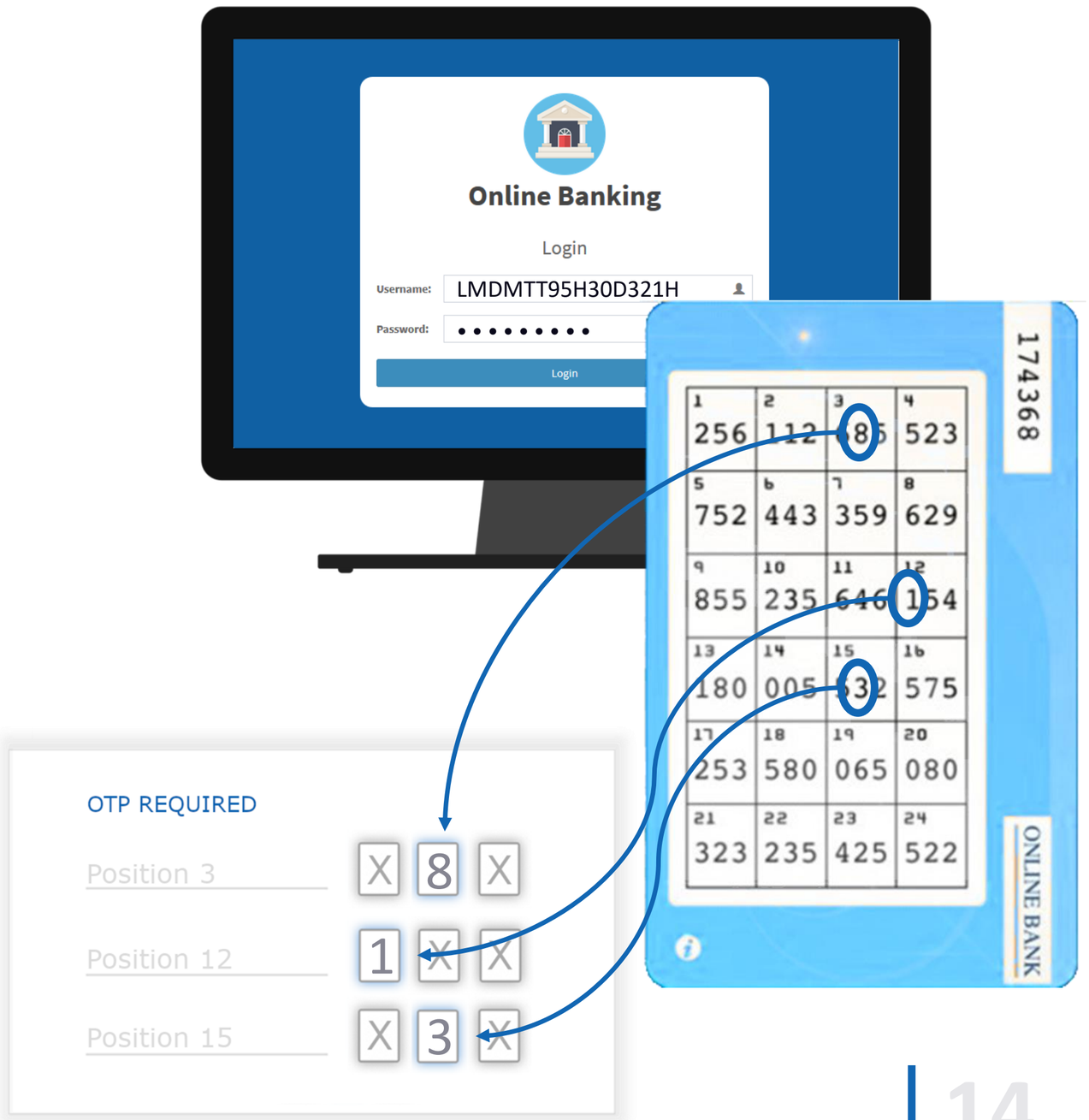
1. The user authenticates on the online banking through credentials and performs an operation.
2. The user generates a code through the matrix.



Use Case
Before PSD2

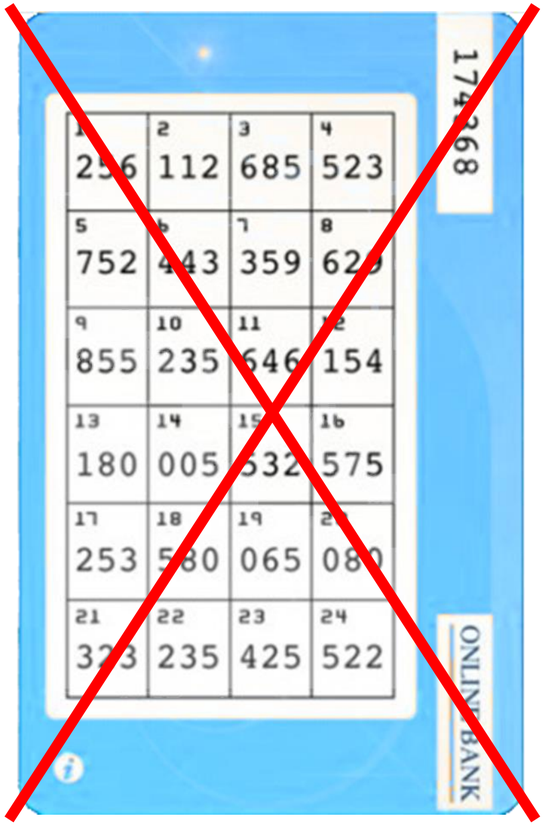
Before PSD2

1. The user authenticates on the online banking through credentials and performs an operation.
2. The user generates a code through the matrix.
3. The user inserts the code in the online page to authorize the operation.



Payment Services Directive (PSD2)
Not Compliant Solutions

1. The authentication code is not connected with the ongoing operation.



2. Users cannot be aware of which operation they are about to authorize.

Use Case
After PSD2

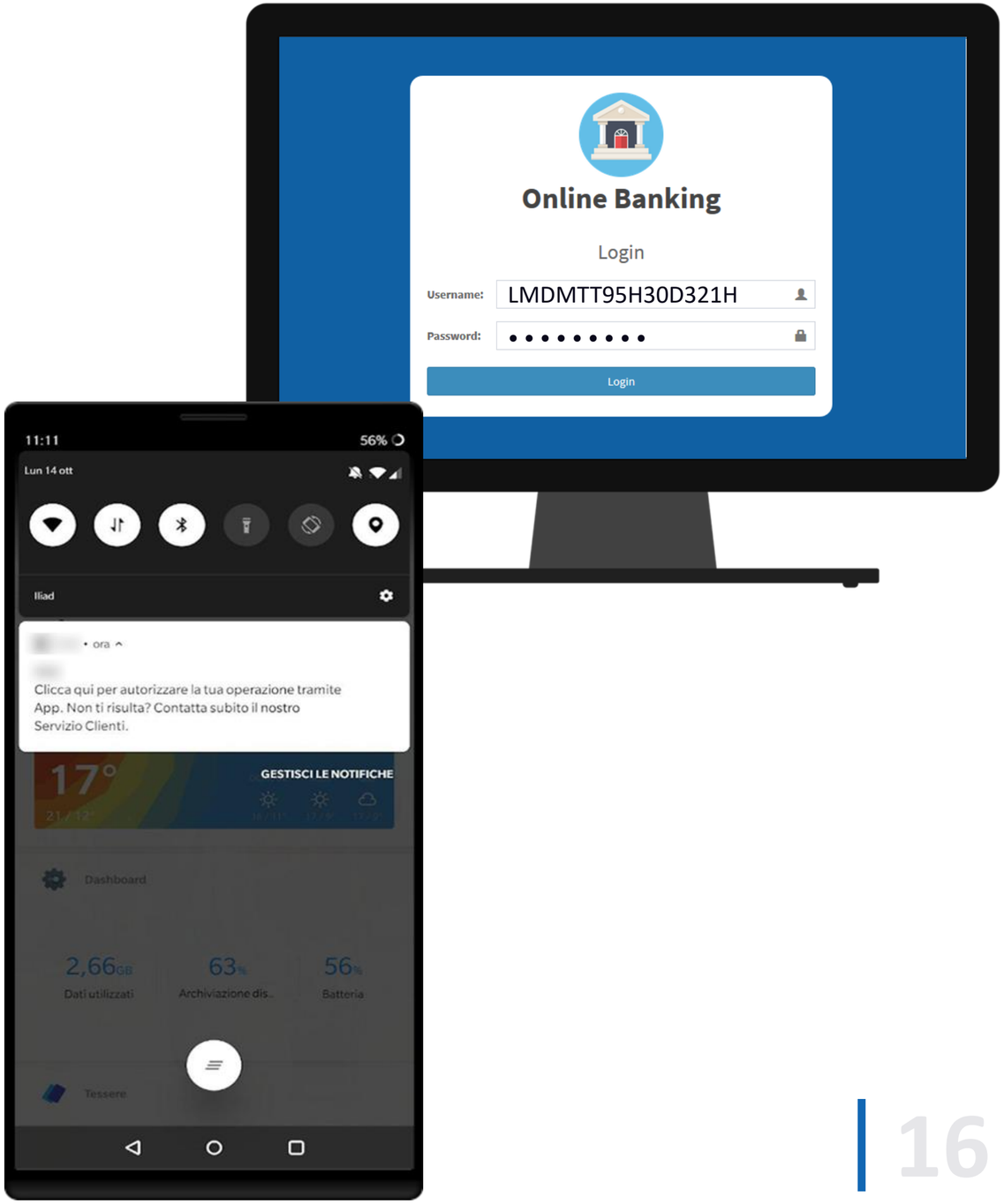
After PSD2

1. The user authenticates on the online banking through credentials and performs an operation.

Use Case
After PSD2

After PSD2

1. The user authenticates on the online banking through credentials and performs an operation.
2. The user receives a *push notification* that, once opened, details the ongoing operation.



Use Case
After PSD2

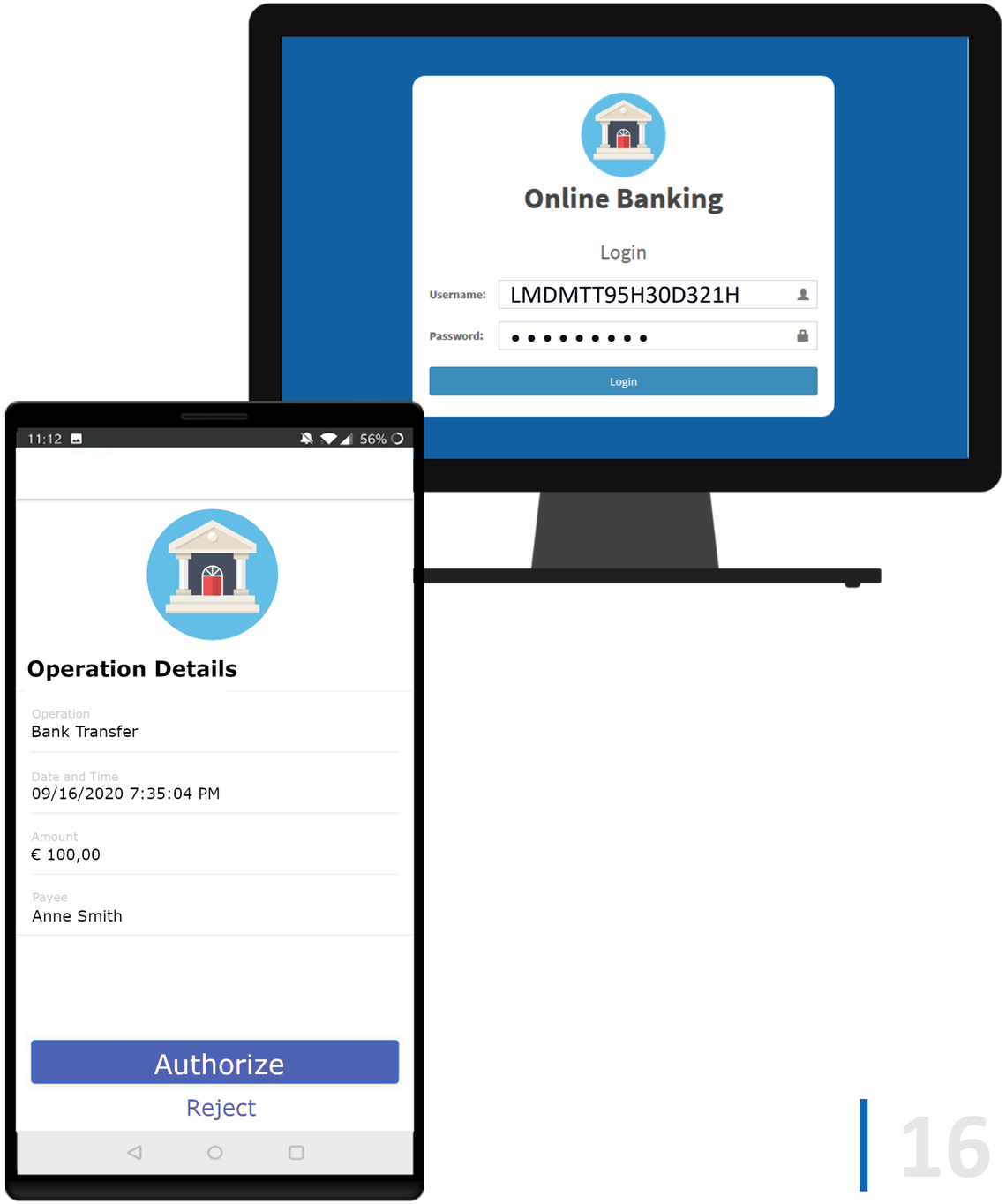
After PSD2

1. The user authenticates on the online banking through credentials and performs an operation.
2. The user receives a *push notification* that, once opened, details the ongoing operation.

Use Case
After PSD2

After PSD2

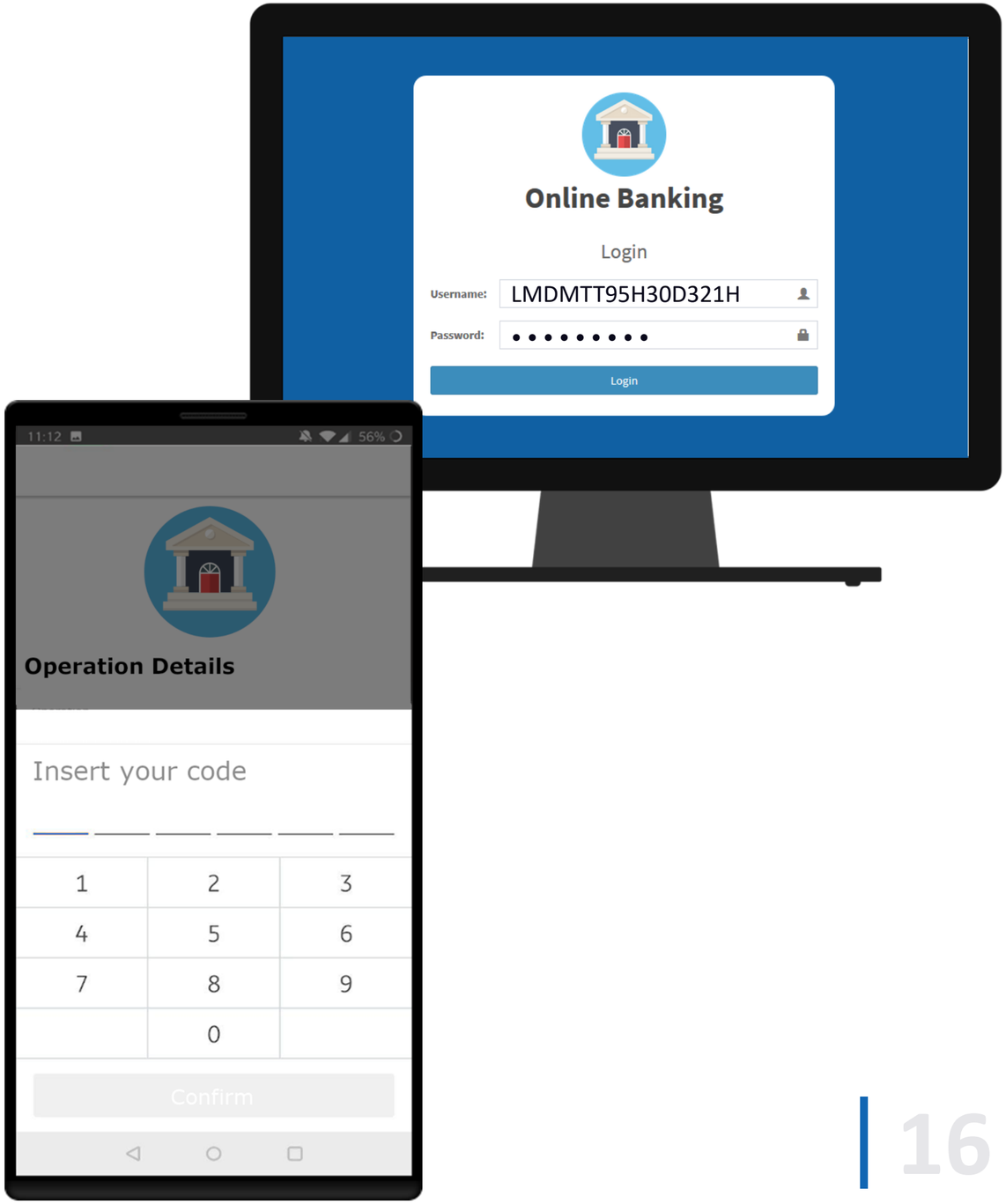
1. The user authenticates on the online banking through credentials and performs an operation.
2. The user receives a *push notification* that, once opened, details the ongoing operation.



Use Case
After PSD2

After PSD2

1. The user authenticates on the online banking through credentials and performs an operation.
2. The user receives a *push notification* that, once opened, details the ongoing operation.
3. By inserting a specific PIN, the user can authorize the operation.



Use Case
Compliance with the PSD2

Requirement	Before PSD2	After PSD2
Strong Customer Authentication	✓ Factors: credentials (K) matrix (P)	✓ Factors: credentials (K) smartphone (P)
Dynamic Linking (link between authentication code and operation)	✗ Matrices cannot generate codes linked to the ongoing operation	✓ Authentication code is bound to the ongoing operation
Dynamic Linking (information on the operation displayed to the user)	✗ Matrices cannot display any information about the ongoing operation	✓ Details on the ongoing operation are displayed after clicking on the notification

| Agenda

- Overview of Security Vulnerabilities Affecting the Financial Scenario
- Payment Services Directive 2 (PSD2)
- **Automated Analysis of Security Protocols for the PSD2:**
  - **from a Design Perspective**
  - from a Deployment Perspective

Automated Analysis of Security Protocols for the PSD2
A Two-Levels Approach

1

Security Analysis
To detect the attackers that manage to compromise the protocol

2

Risk Analysis
To evaluate the risks connected with the successful attackers detected

Automated Analysis of Security Protocols for the PSD2
A Two-Levels Approach

1

Security Analysis
To detect the attackers that manage to compromise the protocol

2

Risk Analysis
To evaluate the risks connected with the successful attackers detected

Automated Analysis of Security Protocols for the PSD2
Security Analysis

To detect the attackers that manage to compromise the protocol, we perform two different kinds of analysis:

1. **Combinatorial Analysis**: relying on attackers' capabilities on the authentication factors. It is fast and thus helps prune the set of attackers to test, but may not detect some advanced attacks.

2. **Formal Analysis**: relying on formal methods (a specification language and a model checker). It can be computationally expensive, but manages to find even more complex categories of attacks.

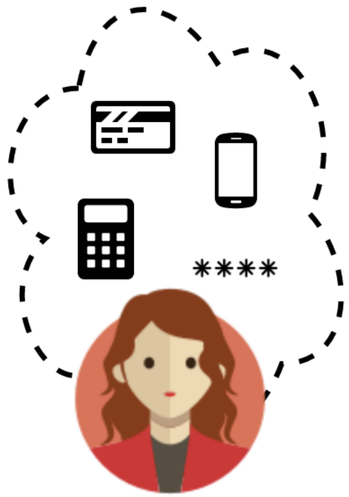
Automated Analysis of Security Protocols for the PSD2
Security Analysis

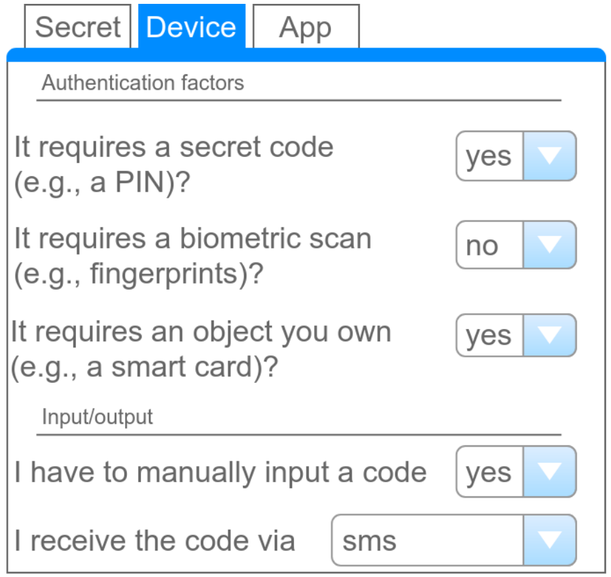
To detect the attackers that manage to compromise the protocol, we perform two different kinds of analysis:

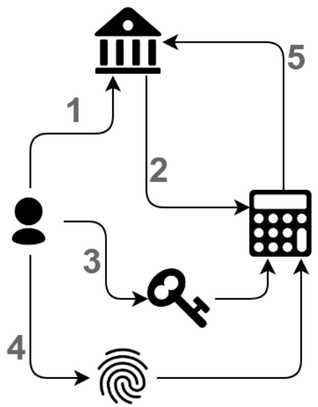
1. **Combinatorial Analysis**: relying on attackers' capabilities on the authentication factors. It is fast and thus helps prune the set of attackers to test, but may not detect some advanced attacks.

2. **Formal Analysis**: relying on formal methods (a specification language and a model checker). It can be computationally expensive, but manages to find even more complex categories of attacks.

Automated Analysis of Security Protocols for the PSD2
MuFASA





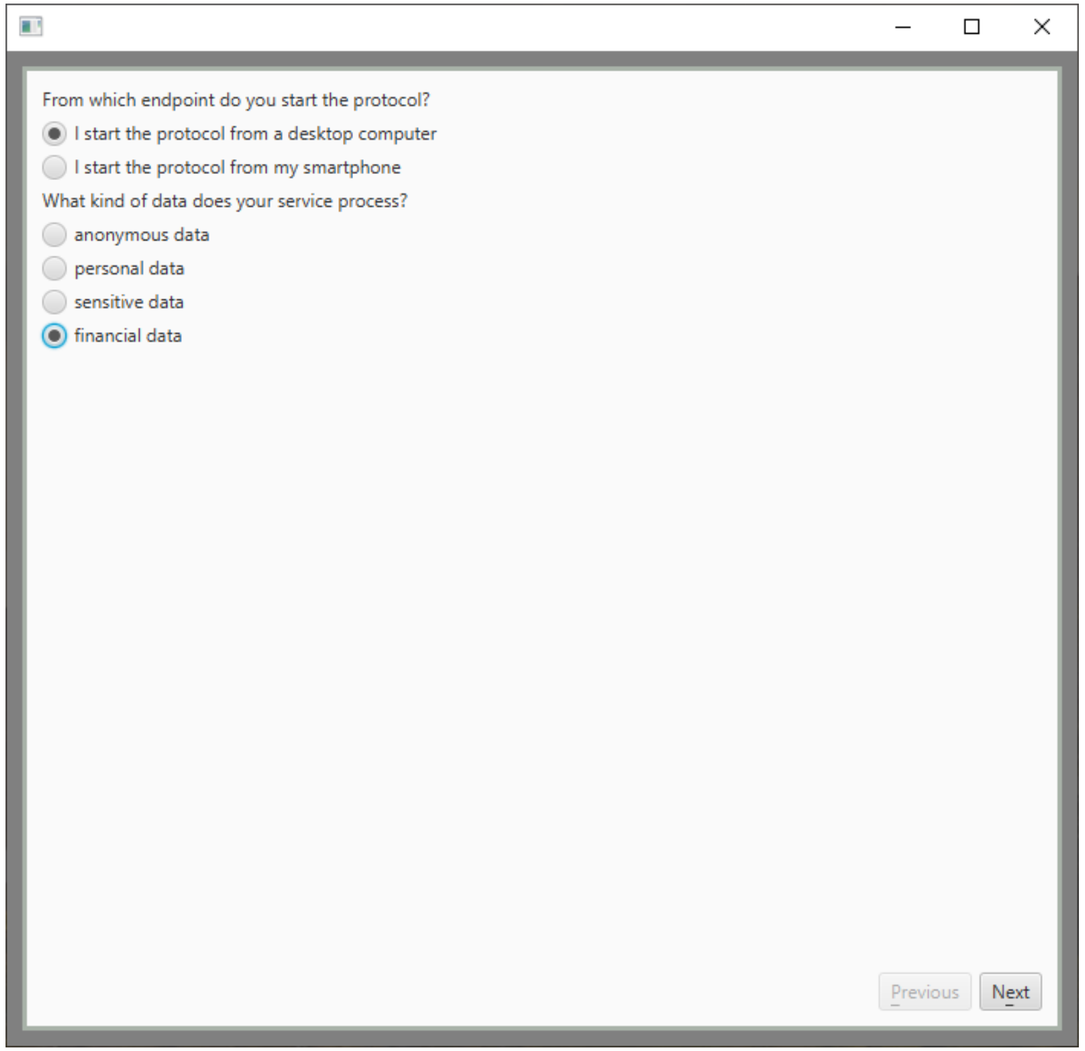


Usage	Translation	Modeling	Analysis	Reporting
Users acquire experience by running the MFA protocols	Users describe the MFA protocol through a questionnaire	Forms are translated to a MFA ML specification	Models are validated against adversaries and other specifications	Risk profile, compliance and other metrics

Automated Analysis of Security Protocols for the PSD2

MuFASA

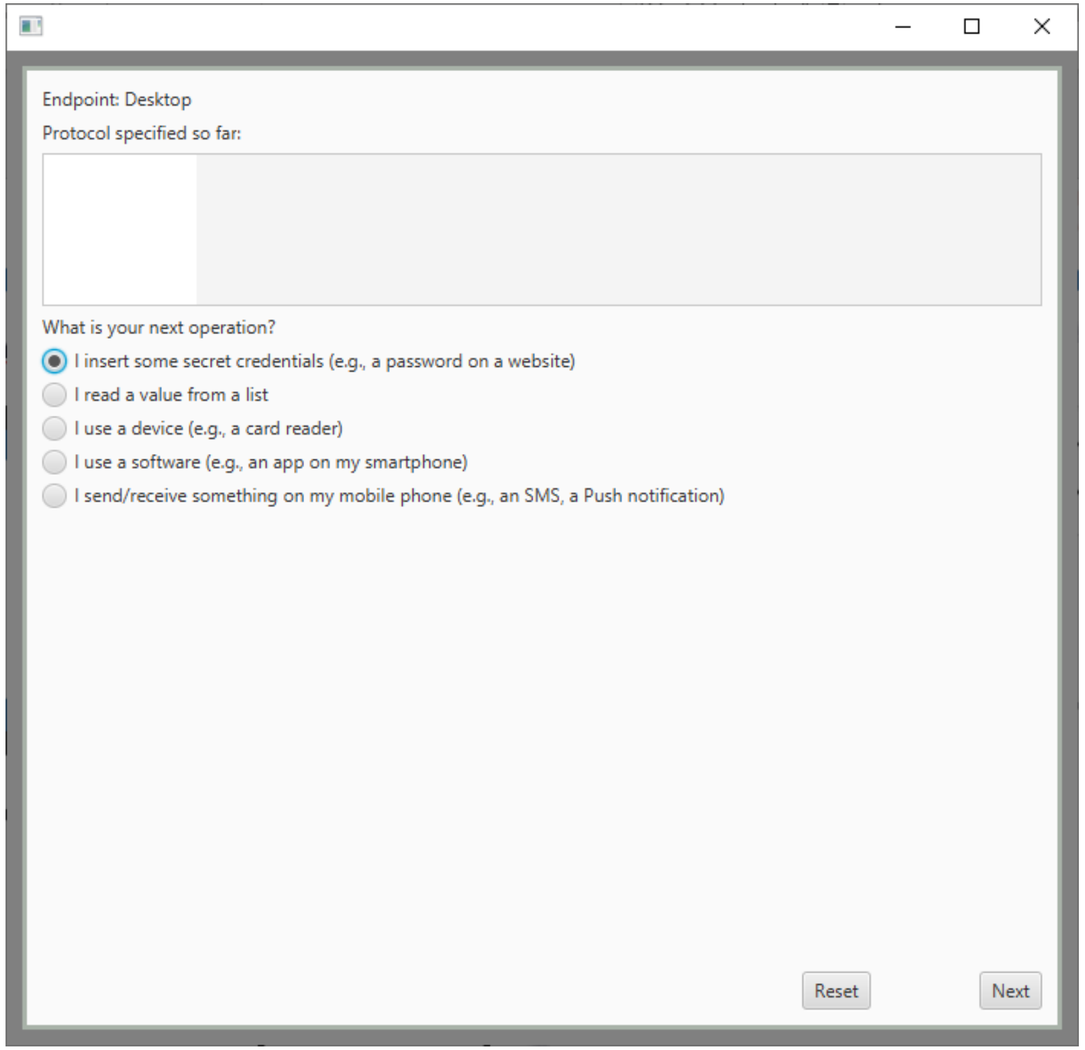
MuFASA – Translation



Automated Analysis of Security Protocols for the PSD2

MuFASA

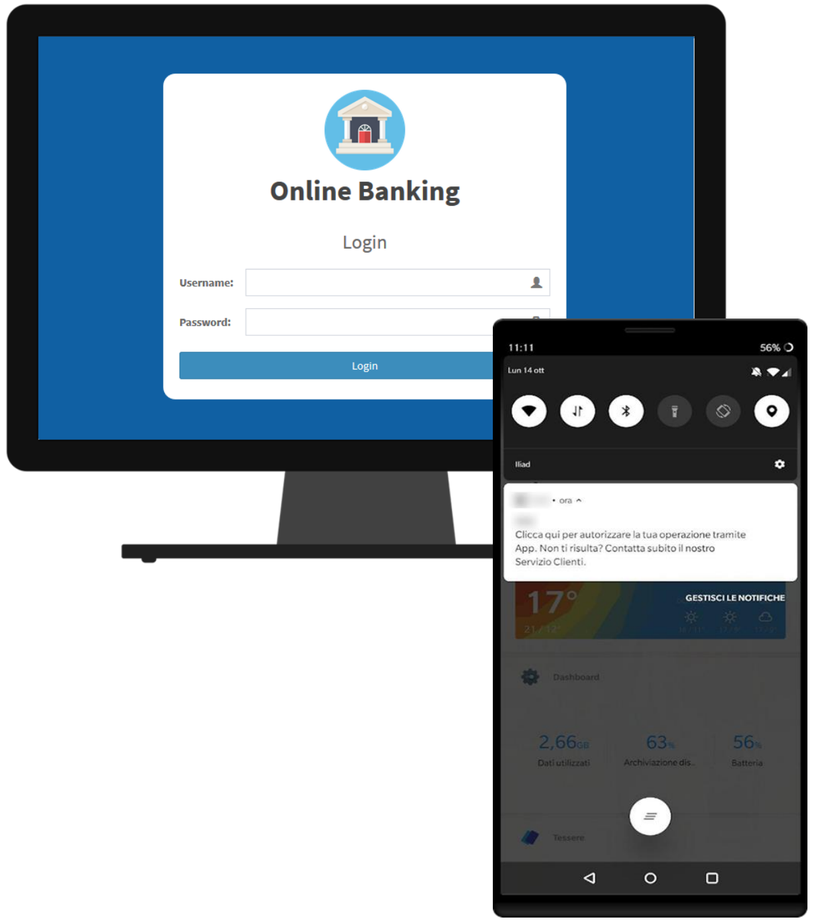
MuFASA – Translation

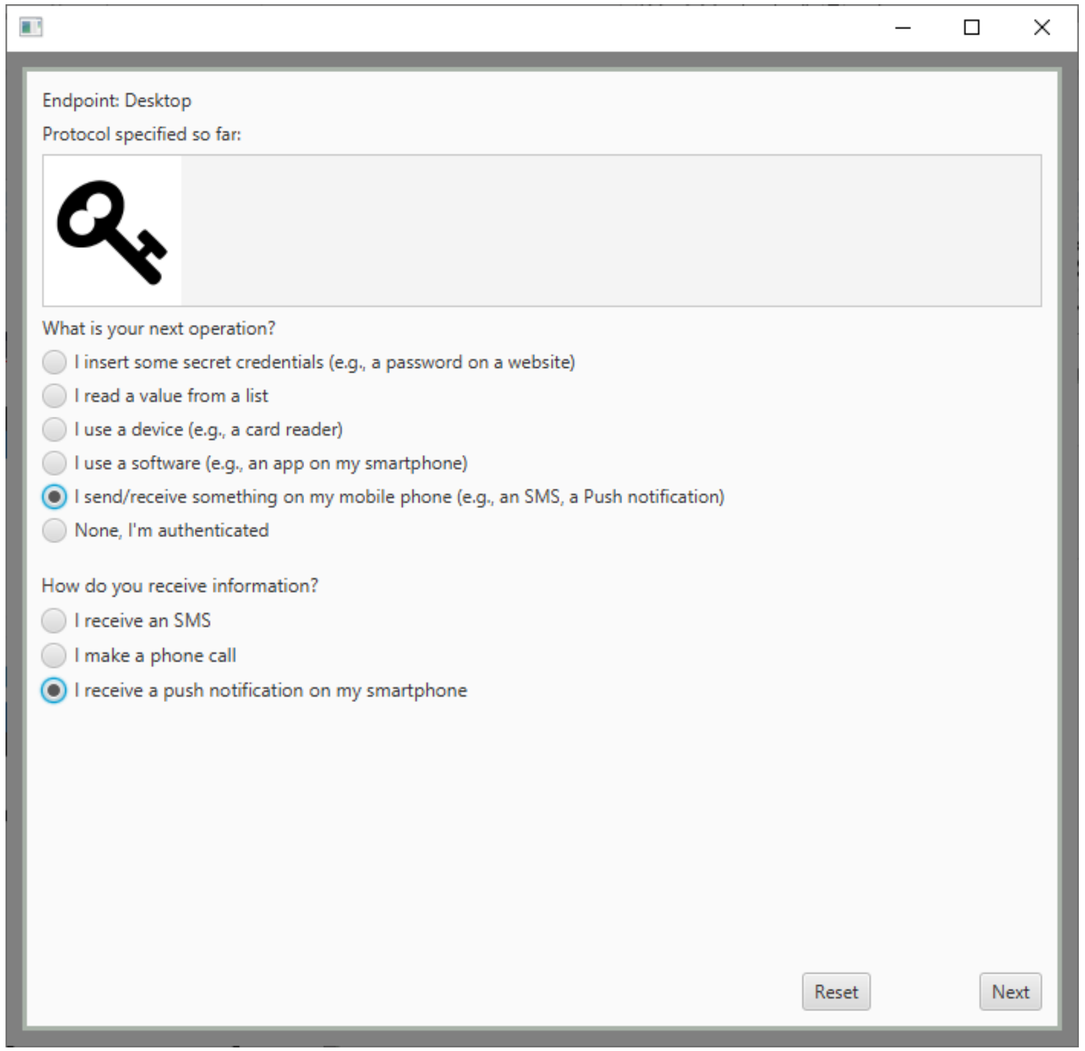


Automated Analysis of Security Protocols for the PSD2

MuFASA

MuFASA – Translation

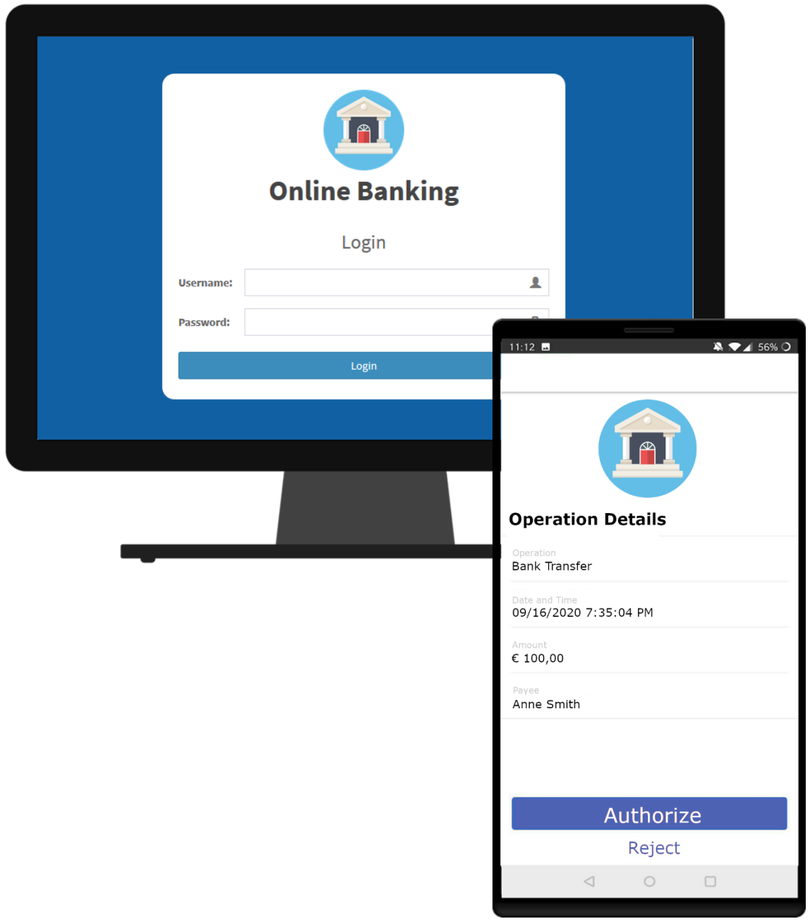


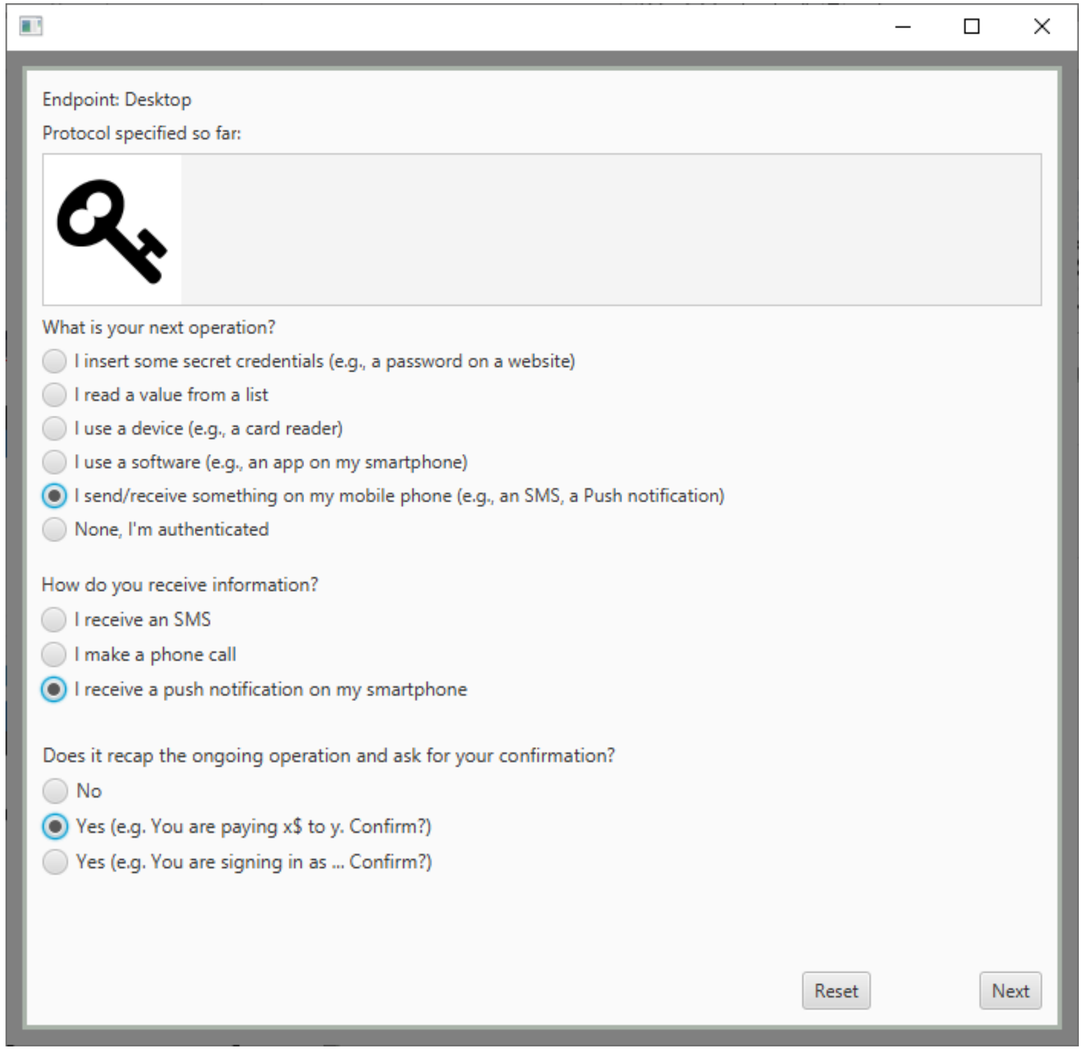


Automated Analysis of Security Protocols for the PSD2

MuFASA

MuFASA – Translation

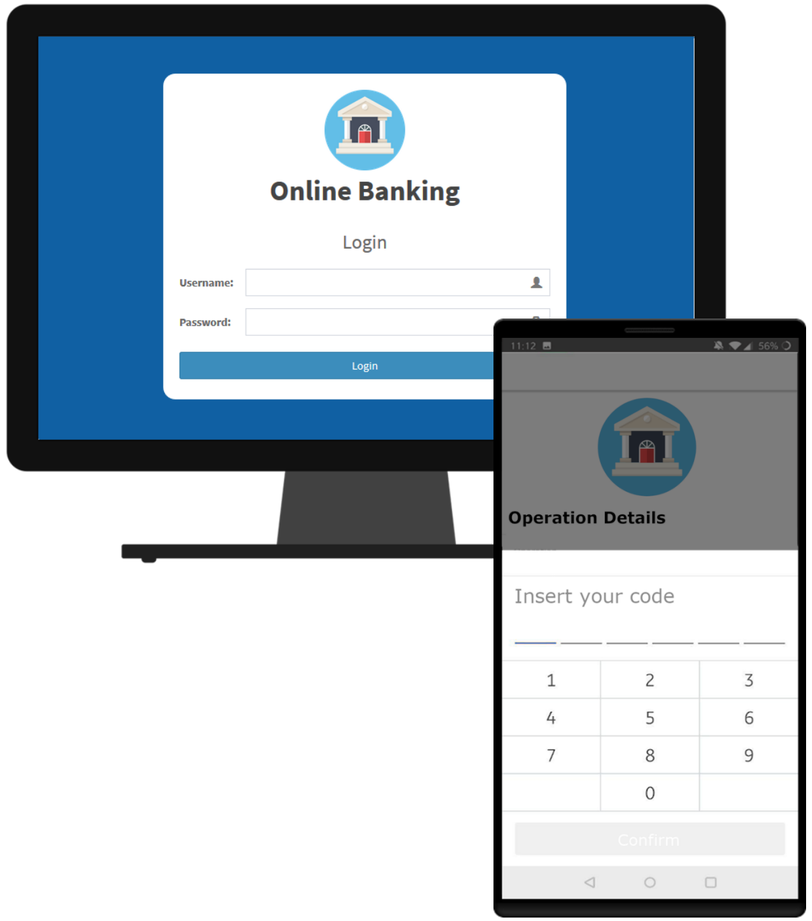


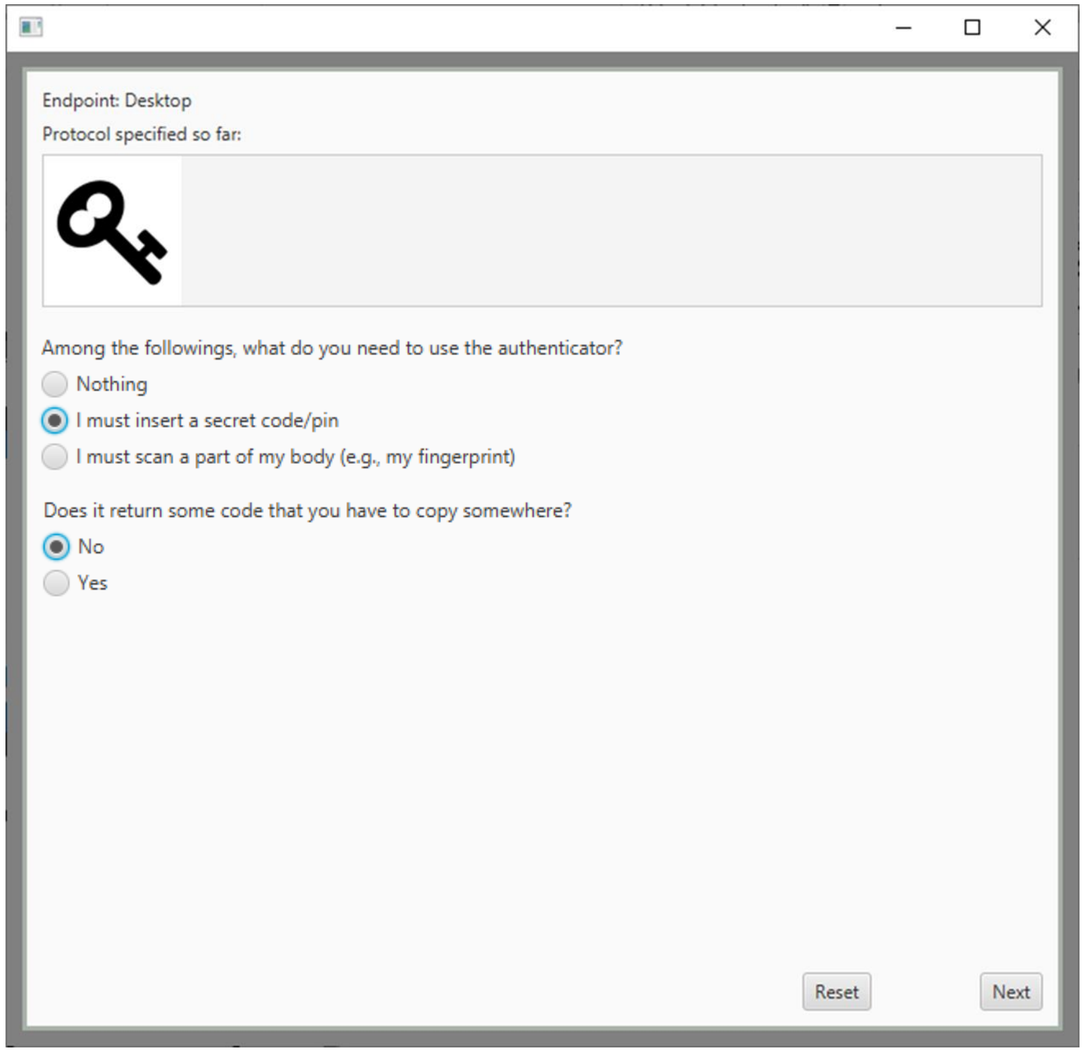


Automated Analysis of Security Protocols for the PSD2

MuFASA

MuFASA – Translation

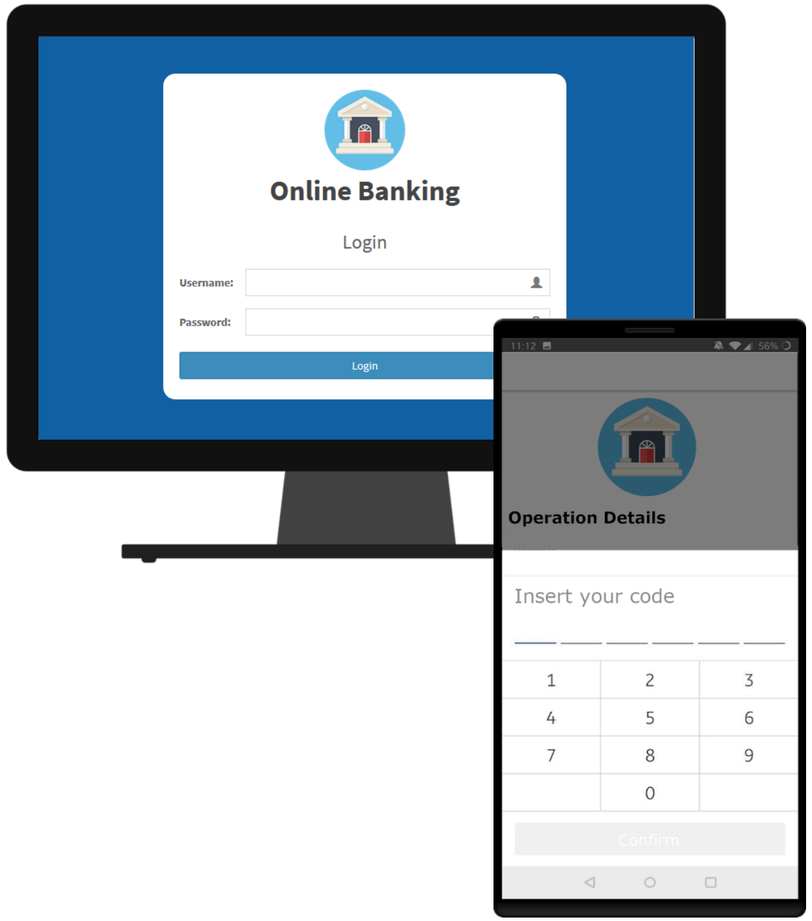


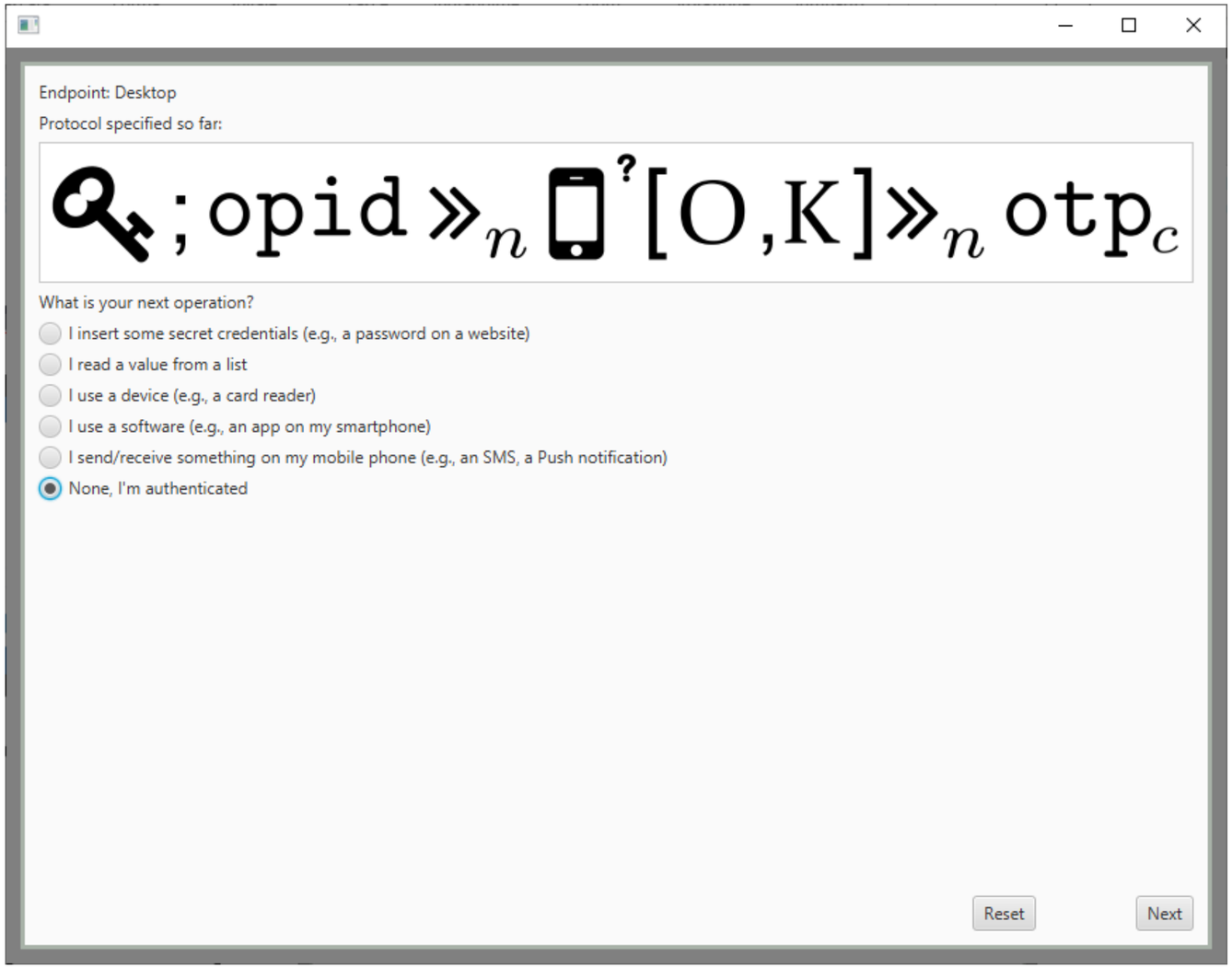


Automated Analysis of Security Protocols for the PSD2

MuFASA

MuFASA – Translation





Automated Analysis of Security Protocols for the PSD2

MuFASA

MuFASA – Modeling

Authenticators

Input/Output

$\mathtt{opid}$ $\mathtt{otp}_t$

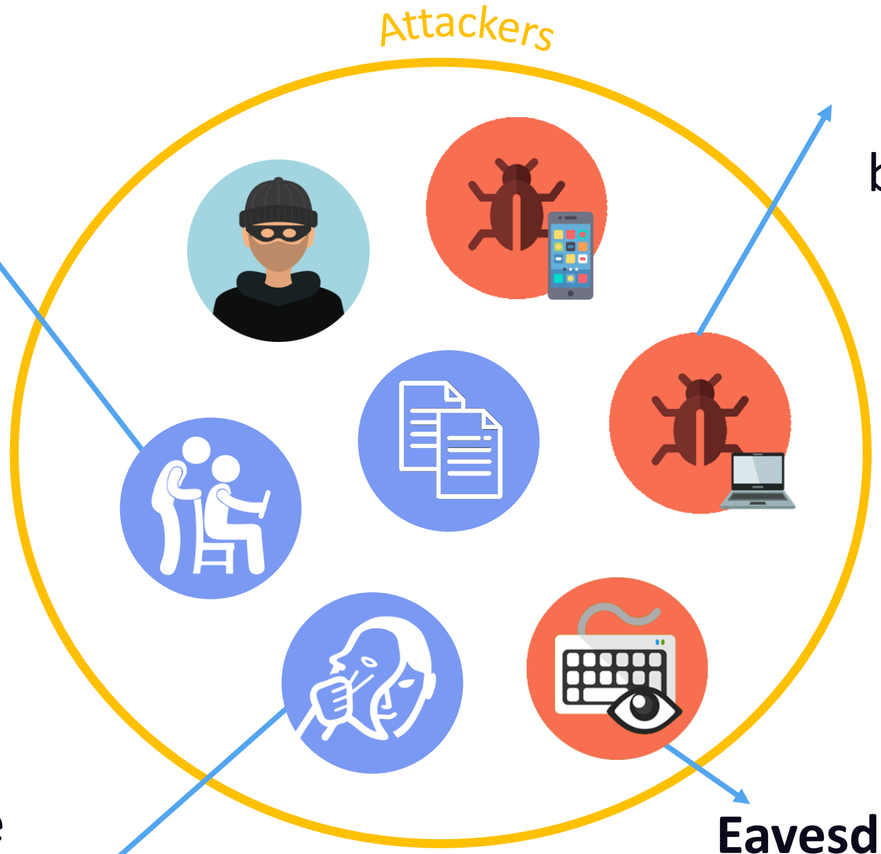
$\mathtt{otp}$ $\mathtt{otp}_c$

Communication channels

$\gg_h$ $\gg_i$ $\gg_o$ $\gg_n$ $\gg_m$

Attackers

Shoulder Surfer: compromises secrets by looking at the victim while typing



Man in the Browser: malicious application lying on the victim's browser, manages to tamper with any window or transaction

Social Engineer: deceives the victim into revealing secrets or performing operations

Eavesdropping Software: malicious application intercepting everything is typed on the keyboard

Automated Analysis of Security Protocols for the PSD2

MuFASA

MuFASA – Analysis

Before PSD2

4 single attackers

After PSD2

0 single attackers

Automated Analysis of Security Protocols for the PSD2

MuFASA

MuFASA – Analysis

Before PSD2

4 single attackers

After PSD2

0 single attackers

Advantages:

Security:

Dynamic Linking

- the user is aware of the ongoing operation
- the authentication code is connected with the ongoing operation and session, therefore it cannot be used anywhere nor for any other operation
- the authentication code is sent directly through the network, without requiring the user to manually enter it → attackers that intercept the code while the user is typing are mitigated

Usability: common devices are leveraged (smartphone)

Automated Analysis of Security Protocols for the PSD2

MuFASA

MuFASA – Reporting

Analysis of MFA Protocol

$;\mathtt{opid} \gg_n ?[\mathrm{O},\mathrm{K}] \gg_n \mathtt{otp}_c$

Info on the Analyzed Protocol:

- *Starting Endpoint:* Desktop
- *Number of authenticators:* 2
- *Employed authentication factors:* [K, K, O]

Protocol Complexity

- *Memory:* 2
- *Manual Operations:* 0
- *Extra Devices:* 0
- ***Complexity Score: 2***

Compliance with security requirements

- *Requirement 1:* true
- *Requirement 2:* true
- *Requirement 3:* true
- *Requirement 4:* true

Result of the resistance analysis

Base attackers: DT, AD, SS, ES, SE, MB, MM

Max number of attackers in combination: 3

Considered attackers: 63

Combinations of attackers
DT SS
ES MM
MM MB
ES DT
SS AD
ES AD
SS MM
MM SE

Automated Analysis of Security Protocols for the PSD2
Security Analysis

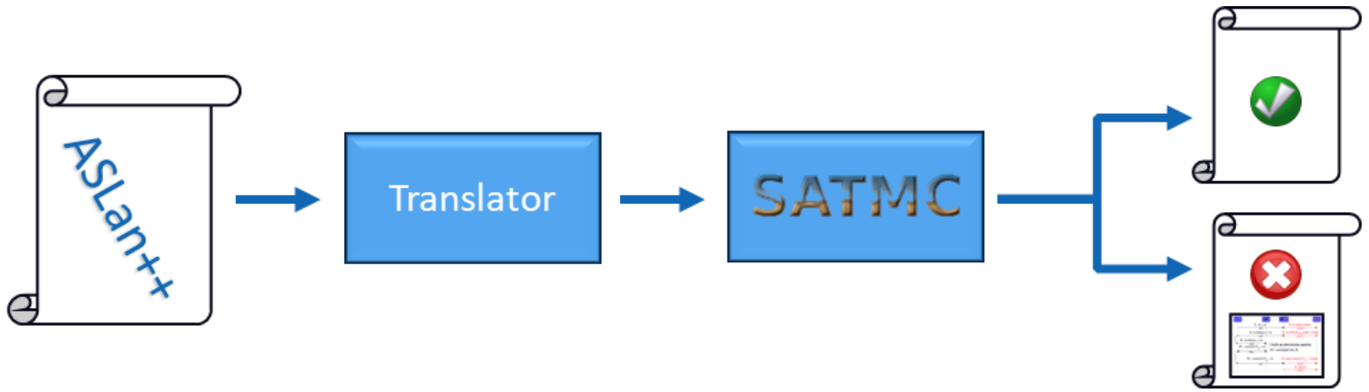
To detect the attackers that manage to compromise the protocol, we perform two different kinds of analysis:

1. **Combinatorial Analysis**: relying on attackers' capabilities on the authentication factors. It is fast and thus helps prune the set of attackers to test, but may not detect some advanced attacks.

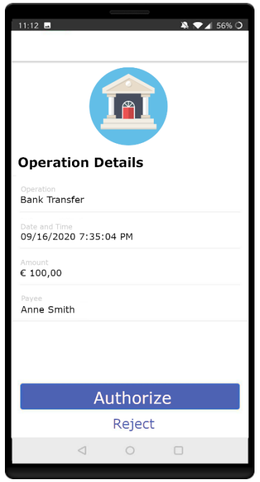
2. **Formal Analysis**: relying on formal methods (a specification language and a model checker). It can be computationally expensive, but manages to find even more complex categories of attacks.

Automated Analysis of Security Protocols for the PSD2
Formal Analysis with ASLan++ and SATMC

```
entity IdPServer(Actor, FCMServer, EICApp, User, SPServer, Browser, EIC: agent, Ch_B2IdPS, Ch_IdPS2FCMSrv, Ch_EICApp2IdPS, Ch_IdPS2EICApp: channel) {

  symbols
    IdPCookie: cookie;
    OpId: opid;
    Request: userrequest;

  body { % of IdPServer
    select {
      on(Browser -Ch_B2IdPS-> Actor: ?Request):{
        Actor -Ch_IdPS2B-> Browser: Actor;

        select {
          on(Browser -Ch_B2IdPS-> Actor: User.?IdPCookie &
            enrollmentDB(Actor)->contains((User,?IdPCookie))):{
              OpId := fresh();
              Actor -Ch_IdPS2FCMSrv-> FCMServer: OpId.Request;

              select {
                on(EICApp -Ch_EICApp2IdPS-> Actor: OpId):{
                  Actor -Ch_IdPS2EICApp-> EICApp: OpId.Actor.SPServer;

                  select {
                    on(EICApp -Ch_EICApp2IdPS-> Actor: OpId.{OpId.Actor.SPServer}_inv(pk(EIC))):{
                      Actor -Ch_IdPS2B-> Browser: {Actor.User.SPServer}_inv(pk(Actor));
                    }
                  }
                }
              }
            }
          }
        }
      }
    }
  }
}
```

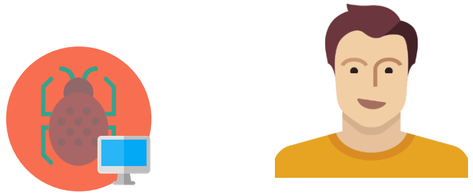


Advanced Vulnerabilities
Man in the Browser (Login)

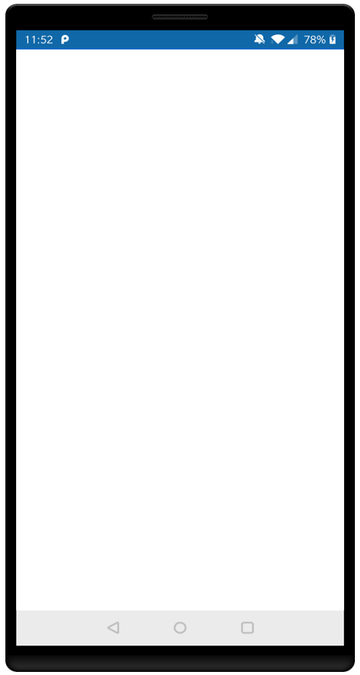


Advanced Vulnerabilities
Man in the Browser (Login)

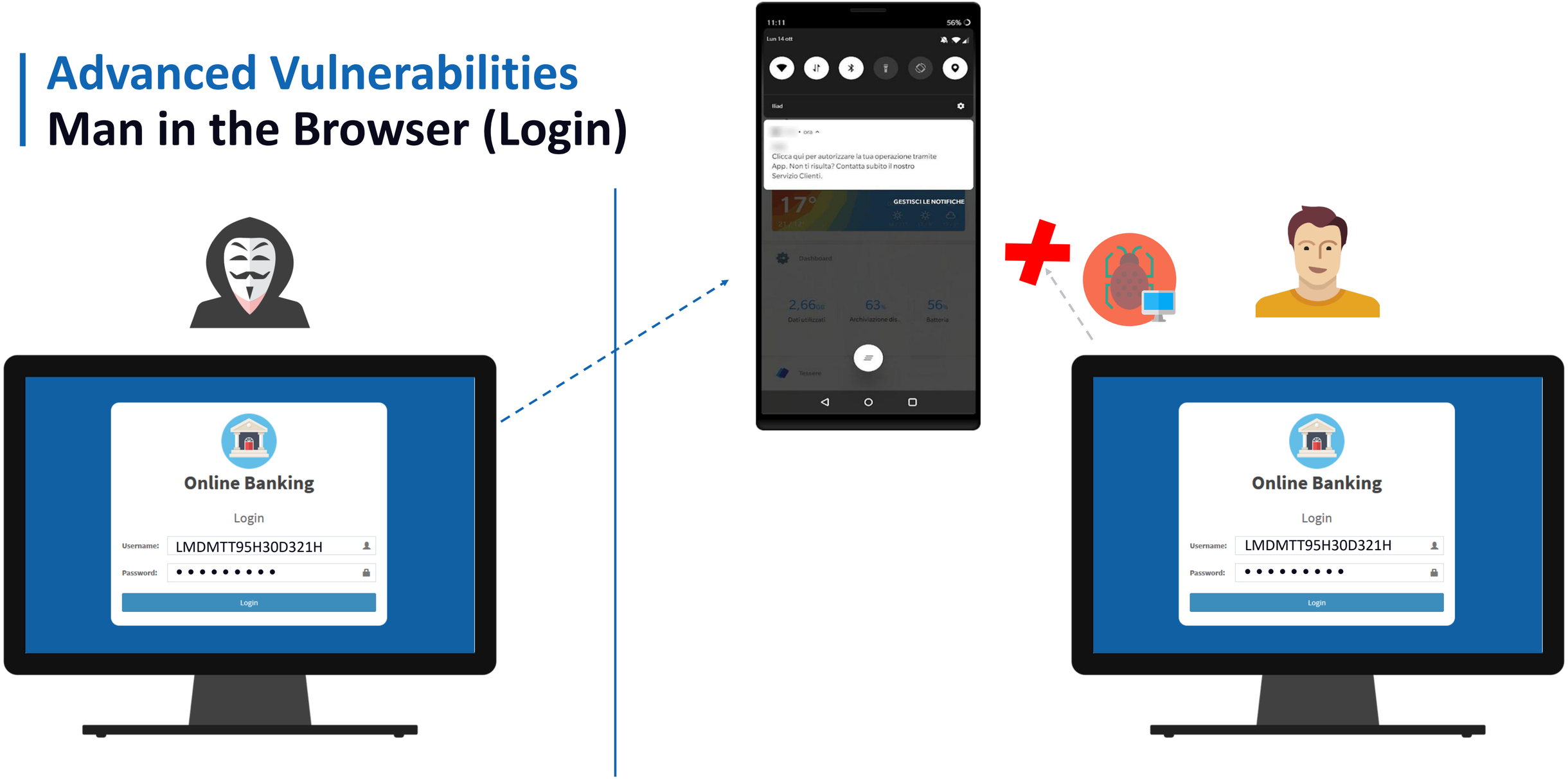
Advanced Vulnerabilities
Man in the Browser (Login)



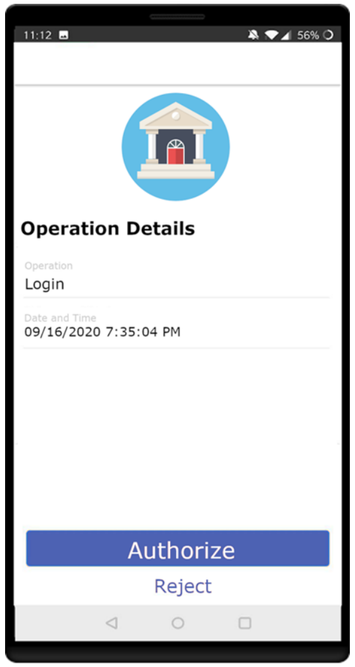
Advanced Vulnerabilities
Man in the Browser (Login)



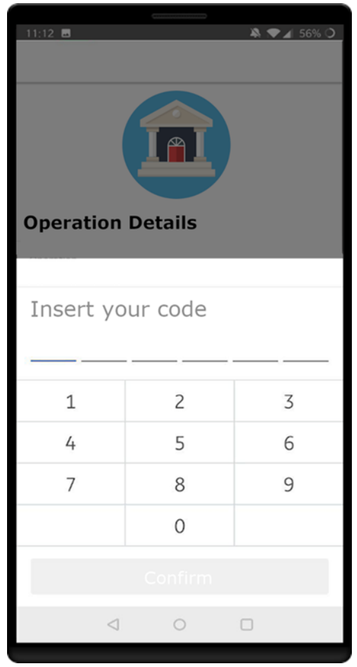
Advanced Vulnerabilities
Man in the Browser (Login)



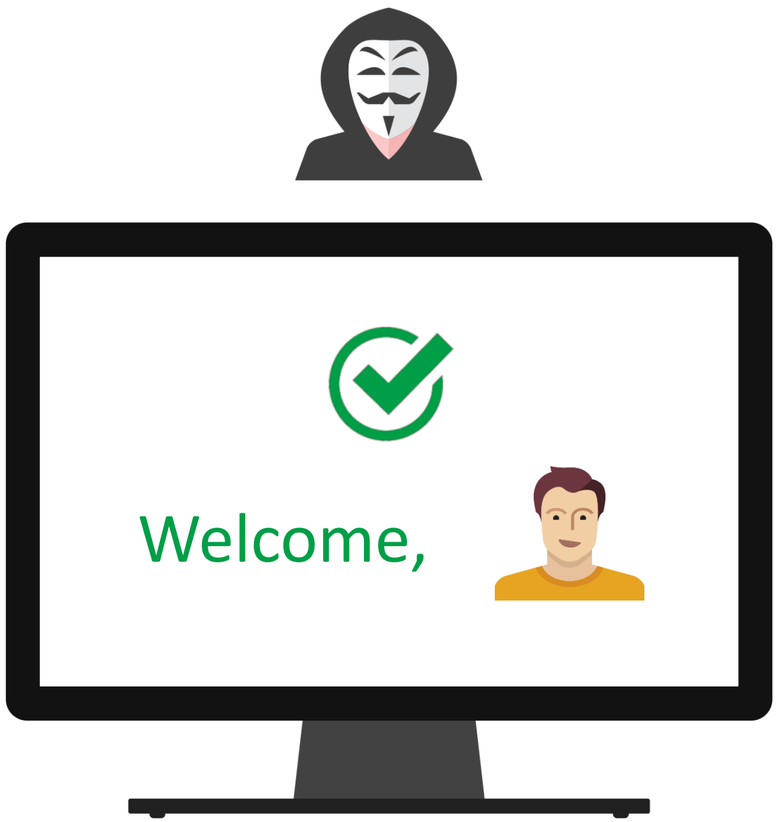
Advanced Vulnerabilities
Man in the Browser (Login)

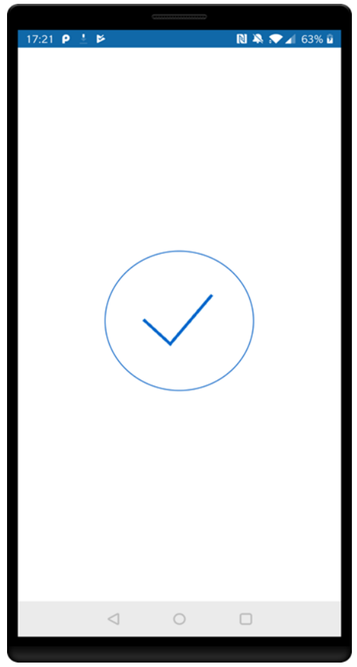


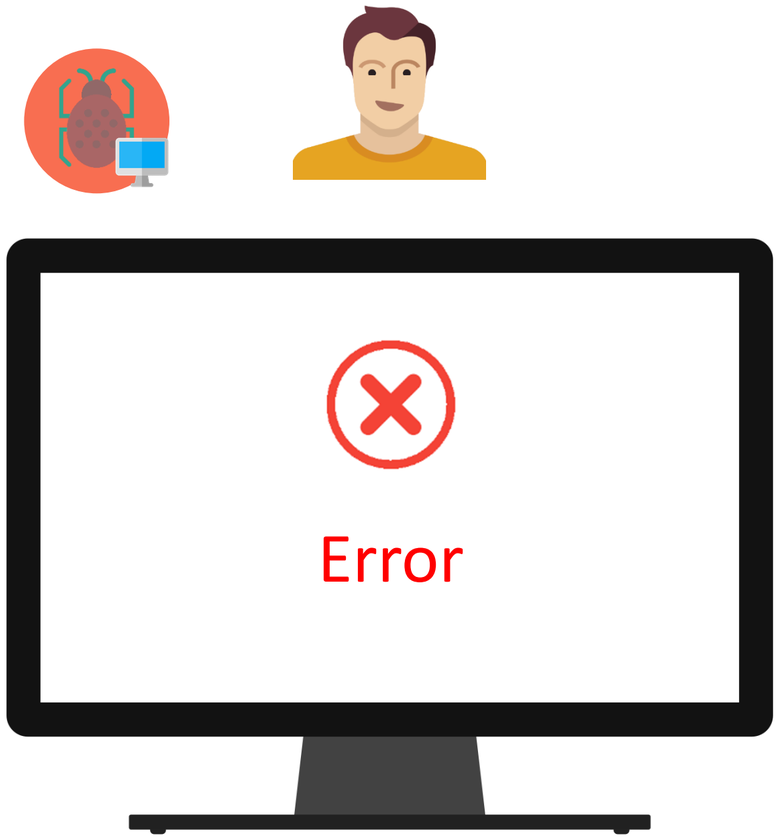
Advanced Vulnerabilities
Man in the Browser (Login)



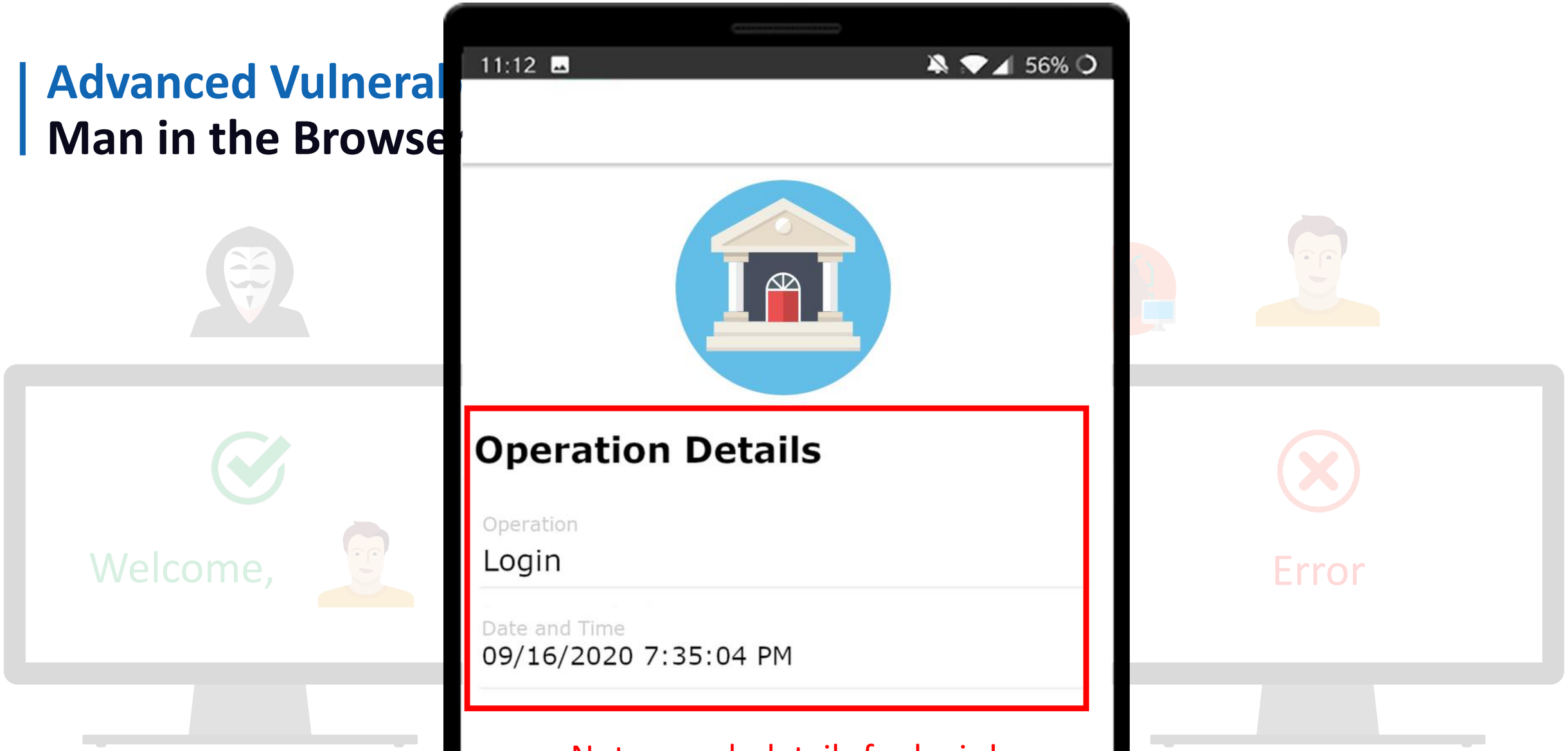
Advanced Vulnerabilities
Man in the Browser (Login)



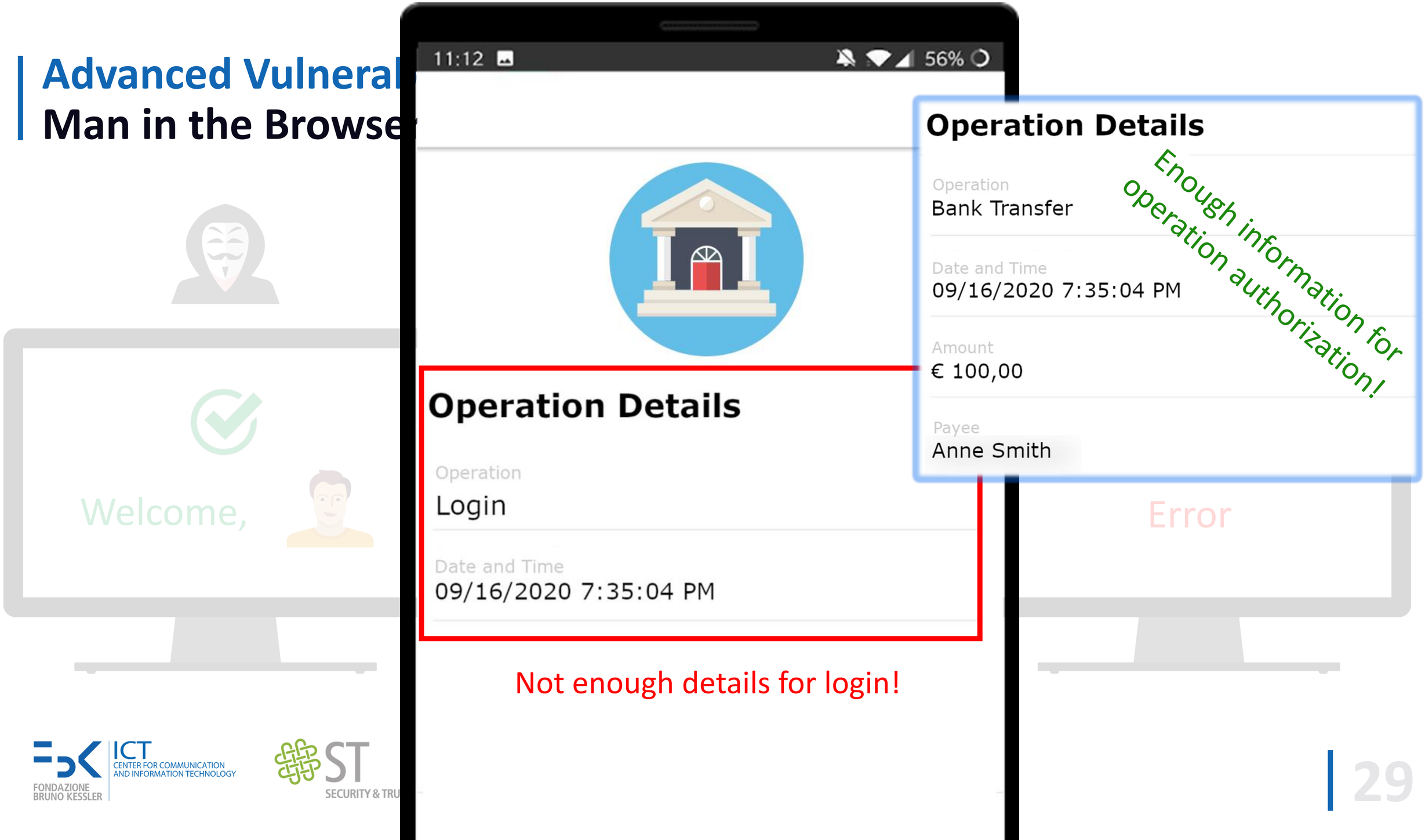




Advanced Vulnerabi
Man in the Browse



Advanced Vulnerabi
Man in the Browse



Automated Analysis of Security Protocols for the PSD2
A Two-Levels Approach

1

Security Analysis
To detect the attackers that manage to compromise the protocol

2

Risk Analysis
To evaluate the risks connected with the successful attackers detected

Automated Analysis of Security Protocols for the PSD2

Risk Analysis with OWASP Risk Rating Methodology

Likelihood

Impact

Risk = Likelihood × Impact

Probability of an attack happening

Consequences in case of the attack was successful

Automated Analysis of Security Protocols for the PSD2

Risk Analysis with OWASP Risk Rating Methodology

		Likelihood		
		Low	*Medium*	*High*
Impact	*Low*	Note	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	Critical

Risk = Likelihood × Impact

Probability of an attack happening

Consequences in case of the attack was successful

Automated Analysis of Security Protocols for the PSD2
Risk Analysis with OWASP Risk Rating Methodology

Result of the resistance analysis

Base attackers: DT, AD, SS, ES, SE, MB, MM

Max number of attackers in combination: 3

Considered attackers: 63

Combinations of attackers	Likelihood	Impact	Risk
DT SS	MEDIUM	MEDIUM	MEDIUM
ES MM	LOW	HIGH	MEDIUM
MM MB	LOW	HIGH	MEDIUM
ES DT	LOW	MEDIUM	LOW
SS AD	LOW	MEDIUM	LOW
ES AD	LOW	MEDIUM	LOW
SS MM	LOW	MEDIUM	LOW
MM SE	LOW	MEDIUM	LOW