RP2
Online Banking: Attacks & Defences

Dominic van den Ende, Tom Hendrickx

University of Amsterdam
Master of Science in System and Network Engineering
Class of 2008-2009

July 1, 2009
Research questions

- Examine the current used models of authentication and consider their strengths and flaws.
- Which methods can be used in one of the three different layers of security and compare them on points such as maturity, potential and effectivity.
- Propose new models, based on known elements in combination with the new found methods for a more secure level of authentication.
- Make a proposition of a balanced model and analyse this architecture against current trojans and speculate how future trojans may evolve if confronted with this new architecture.
Research questions

- Examine the current used models of authentication and consider their strengths and flaws.
- Which methods can be used in one of the three different layers of security and compare them on points such as maturity, potential and effectivity.
- Propose new models, based on known elements in combination with the new found methods for a more secure level of authentication.
- Make a proposition of a balanced model and analyse this architecture against current trojans and speculate how future trojans may evolve if confronted with this new architecture.
Research questions

- Examine the current used models of authentication and consider their strengths and flaws.
- Which methods can be used in one of the three different layers of security and compare them on points such as maturity, potential and effectivity.
- Propose new models, based on known elements in combination with the new found methods for a more secure level of authentication.
- Make a proposition of a balanced model and analyse this architecture against current trojans and speculate how future trojans may evolve if confronted with this new architecture.
Research questions

- Examine the current used models of authentication and consider their strengths and flaws.
- Which methods can be used in one of the three different layers of security and compare them on points such as maturity, potential and effectivity.
- Propose new models, based on known elements in combination with the new found methods for a more secure level of authentication.
- Make a proposition of a balanced model and analyse this architecture against current trojans and speculate how future trojans may evolve if confronted with this new architecture.
Level of fraud

![Graph showing yearly losses per client in Euro against the number of clients for single-factor and two-factor authentication methods. The graph indicates a higher level of fraud for single-factor authentication compared to two-factor authentication.](image)

Dominic van den Ende, Tom Hendrickx
RP2 Online Banking: Attacks & Defences
Two-factor authentication

- First factor: Something you know.
- Second factor: Something you have.
Current danger: Man-in-the-Browser attacks

FUBAR (uitdrukking) - Wikipedia
23 april 2009 ... FUBAR is een Amerikaanse afkorting, die meestal in slang of groepstaal wordt gebruikt. Ook bij soldaten wordt de afkorting gebruikt om ...

FUBAR - Wikipedia, the free encyclopedia - [ Vertaal deze pagina ]
FUBAR is an acronym that commonly means "fucked up beyond all repair," "fucked up beyond all recognition," or any of a number of similar constructions. ...

fubar: the only online bar and happy hour - [ Vertaal deze pagina ]
fubar is the first online bar and happy hour. Can you handle the fu? Join NOW (it's free!) Once
Current danger: Man-in-the-Browser attacks

SNE/OS3 Homepage [OS3 Website] - [Vertaal deze pagina]
OS3 stands for Open Standards, Open Software (which extends Open Source) and Open Security. Together these three components define Open Technology. ...FUBAR
www.os3.nl/ - 21k - In cache - Gelijkwaardige pagina's

FUBAR - Wikipedia, the free encyclopedia - [Vertaal deze pagina]
FUBAR is an acronym that commonly means "fucked up beyond all repair," "fucked up beyond all recognition," or any of a number of similar constructions. ...
en.wikipedia.org/wiki/FUBAR - In cache - Gelijkwaardige pagina's

fubar: the only online bar and happy hour - [Vertaal deze pagina]
fubar is the first online bar and happy hour. Can you handle the fu? Join NOW (it's free!) Once
Out-of-band control and authentication

- "ABN AMRO" model: E.dentifier2
- "ING" model: SMS messages
Multi-layer security

- Layer I: End-user PC
- Layer II: Extra out-of-band authentication
- Layer III: Back-office monitoring
Multi-layer security

- Layer I: End-user PC
- Layer II: Extra out-of-band authentication
- Layer III: Back-office monitoring
Multi-layer security

- Layer I: End-user PC
- Layer II: Extra out-of-band authentication
- Layer III: Back-office monitoring
Model 1: Thin server-side virtual machine
- Username
- Challenge-response token
- Secure environment
The most balanced model

Compare models using the following:

- Cost overview
- User convenience & Security
Estimated cost overview

- ING
- ABN Amro
- Model 1
- Model 2 (Models)
- Model 3
- Model 4
- Model 5

Cost p.a. in Euro

Legend:
- 100,000 users
- 1,000,000 users
- 10,000,000 users

Models:
- Model 1 - Virtual machines
- Model 2 - Hardened browser
- Model 3 - Trusteer
- Model 4 - App load from USB
- Model 5 - App run on USB

Dominic van den Ende, Tom Hendrickx

RP2 Online Banking: Attacks & Defences
Convenience & Security overview

Security questions

- The number of attacks it does not counter
- Degree of difficulty to perform possible attacks
- User skill-level/awareness dependence
- Maturity
Convenience & Security overview

Some of the user convenience questions

- The number of steps / operations for the customer
- The time needed to login and make a transaction
- The number of physical items to keep
- The familiarity with the solutions (by other sites / banks)
- Is the solution "perceived" to be secure
Convenience & Security overview

- ING
- ABN Connected
- ABN Disconnected
- Model 1
- Model 2
- Model 3
- Model 4
- Model 5

Scoring points

Security
User convenience

Models

Model 1 - Virtual machines
Model 2 - Hardened browser
Model 3 - Trusteer
Model 4 - Appl load from USB
Model 5 - Appl run on USB
Future malware threats

- Man-in-the-Middle
Server side VM-model: Future malware threats

- Man-in-the-Middle

- Large scale attack will be very difficult
- Connection speed
- Application reaction time span
Questions

Any questions?
Most of the current models not protected against Man-in-the-Browser

Thin server-side virtual machine : Our most balanced model