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.

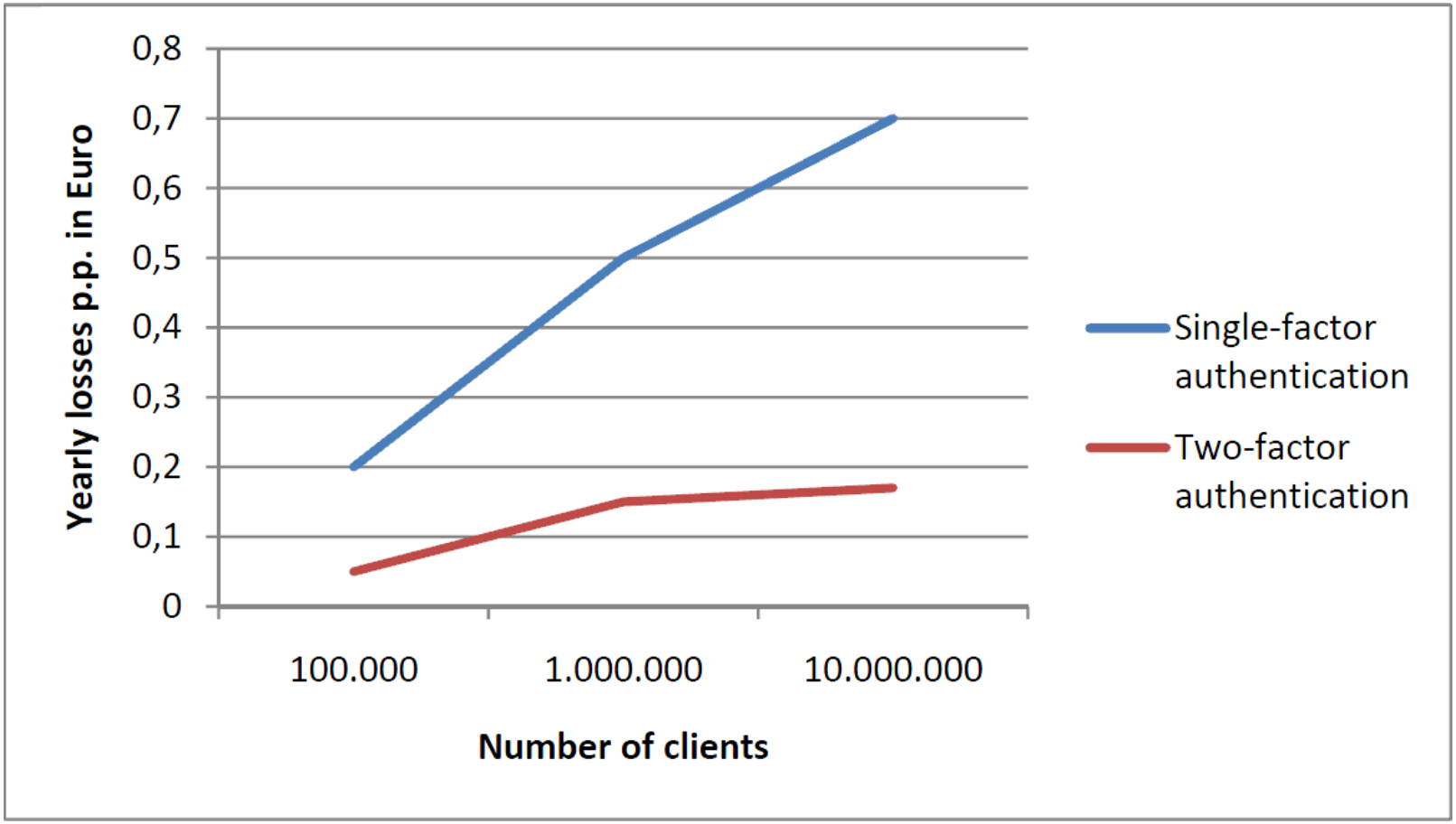
Research questions

- 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



Two-factor authentication

- First factor: Something you know.
- Second factor: Something you have.

Current danger: Man-in-the-Browser attacks

Current danger: Man-in-the-Browser attacks

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

Next generation models

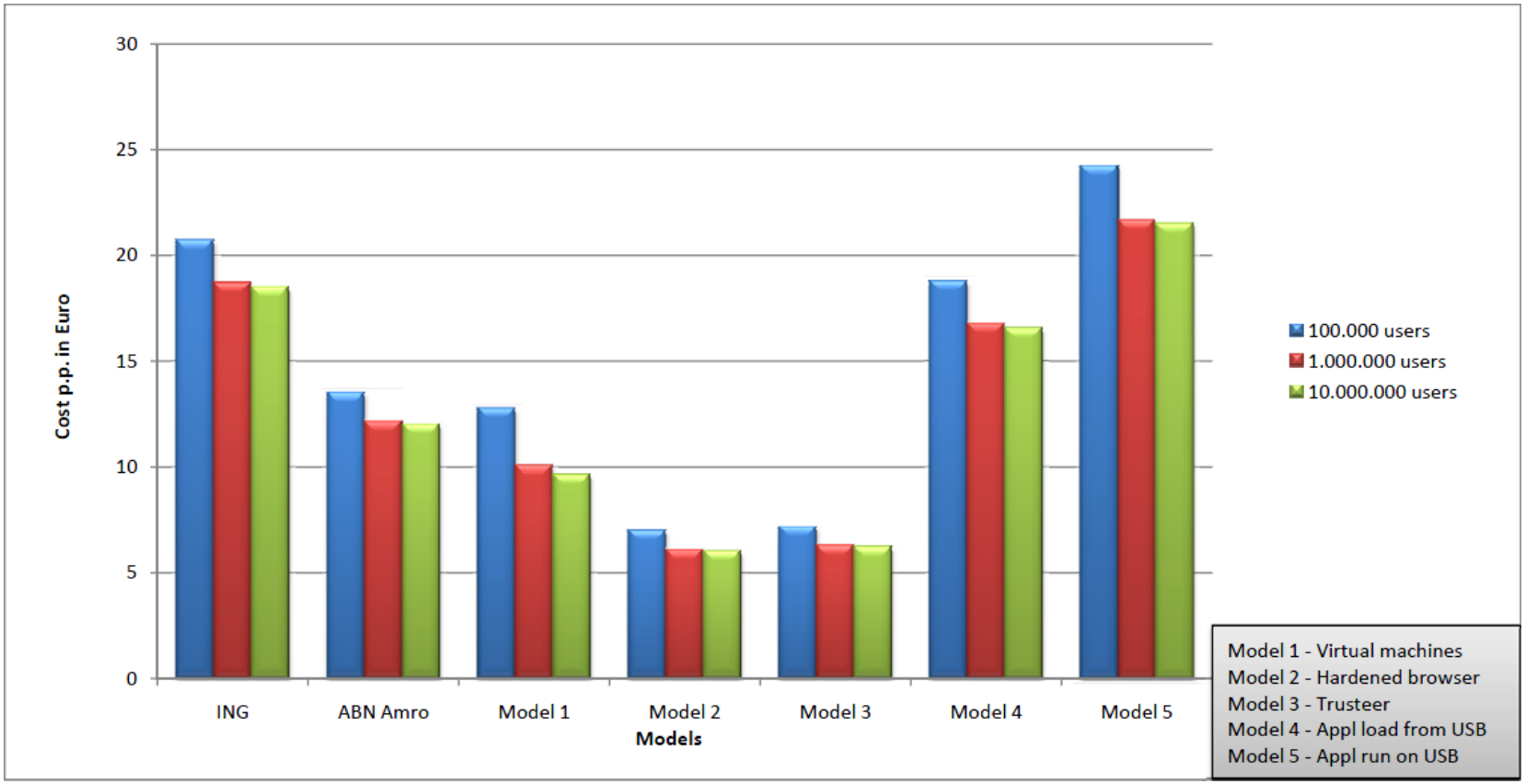
- Model 1: Thin server-side virtual machine
  - Username
  - Challenge-response token
  - Secure environment

The most balanced model

Compare models using the following:

- Cost overview
- User convenience & Security

Estimated cost overview



Convenience & Security overview

Security questions

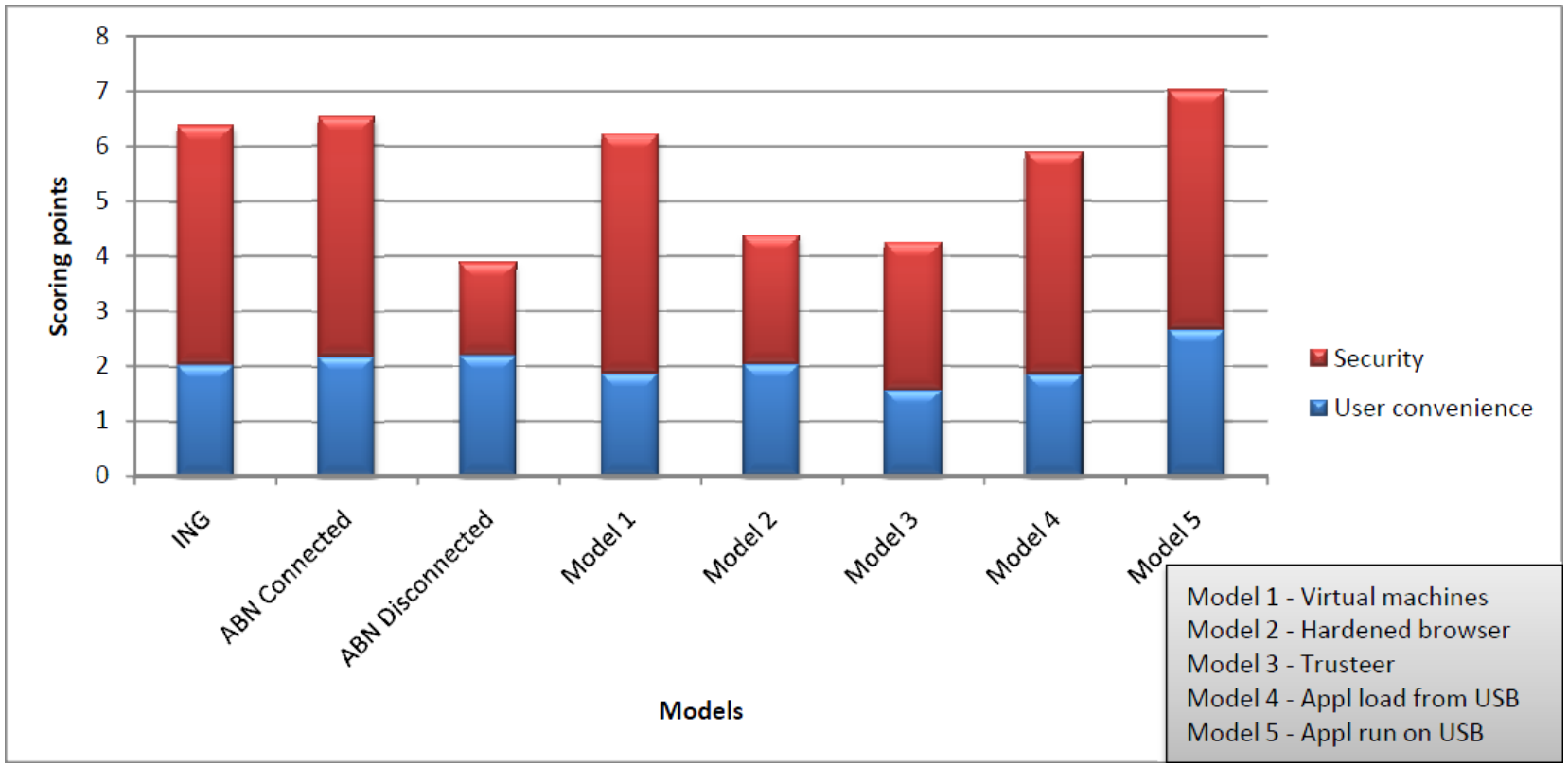
- The number of attacks it does not counter
- Degree of difficulty to perform possible attacks
- User skill-level/awareness dependence
- Maturity

Convenience & Security overview

Some of the user convenience questions

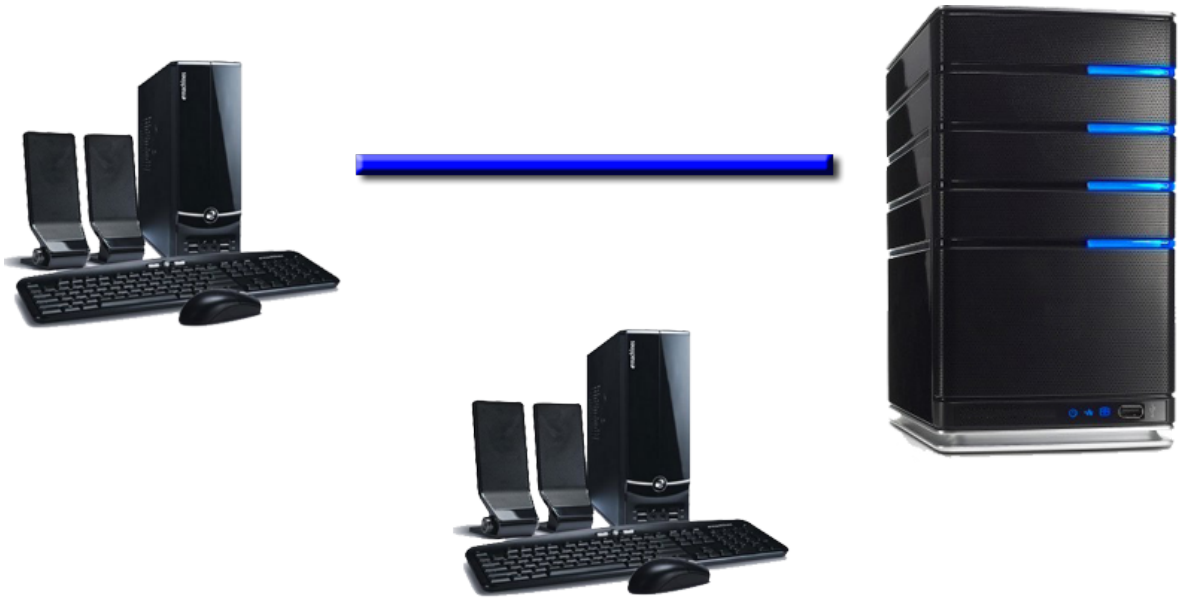
- The number of steps / operations for the customer
- The time needed to login and make a transaction
- The number of physical items to keep
- The familiarity with the solutions (by other sites / banks)
- Is the solution "perceived" to be secure

Convenience & Security overview



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?

Conclusion

- Most of the current models not protected against Man-in-the-Browser
- Thin server-side virtual machine : Our most balanced model