Human Factors Engineering for IT Security

Peter Wolkerstorfer
Senior HCI Researcher
CURE – Center for Usability Research and Engineering

Agenda

- ***About CURE***
- Usability
- Mental Models
- User Experience (UX)
- HCISEC Challenges
- User Centred Design (UCD) Process
- Conclusions
- Contact

About CURE

- CURE – Center for Usability Research & Engineering
  - Non-profit research organisation
  - Spin-off from University of Vienna since 1998
  - Industrial consulting done by USECON
  - Team of over 25 researchers (multidisciplinary)
  - HCISEC Team (5 researchers)
  - Experienced in EC research (FP5,6&7)
    >20 int. projects,
    >300 nat. projects

UTRUSTIT

PICOS

PrimeLife

HERMES

uTRUSTit Project

uTRUSTit Facts

“Usable Trust in the Internet of Things (IoT)”

Project duration:	**3 years – Start: Sept. 2010**
Project funding:	**EU 7th Framework Programme ICT-2009.1.4**
Project coordinator:	**CURE – Center for Usability Research & Engineering**
Contact:	http://www.utrustit.eu utrustit@cure.at

SEARCH-LAB
SECURITY EVALUATION ANALYSIS AND RESEARCH LABORATORY

SWEDEN CONNECTIVITY

NR

CHEMNITZ UNIVERSITY OF TECHNOLOGY

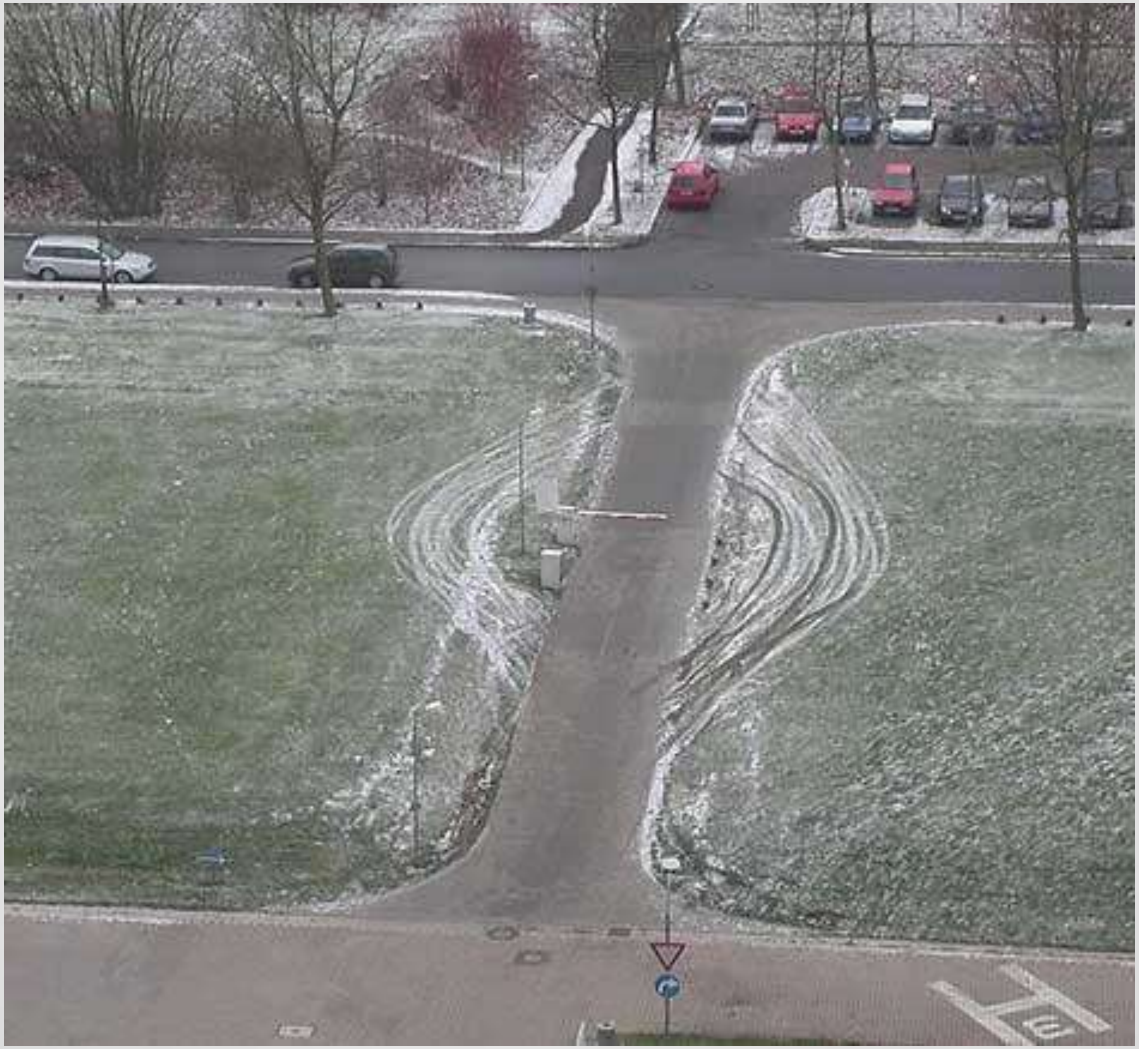
KATHOLIEKE UNIVERSITEIT LEUVEN

cure
center for usability research & engineering

Agenda

- About CURE
- ***Usability***
- Mental Models
- User Experience (UX)
- HCISEC Challenges
- User Centred Design (UCD) Process
- Conclusions
- Contact

Human Behaviour & Security



Source: blogs.oracle.com

Principle of Psychological Acceptance

“It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the user's mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized. If he must translate his image of his protection needs into a radically different specification language, he will make errors.”

Jerome Saltzer and Michael Schroeder: “The Protection of Information in Computer Systems”, Proceedings of the IEEE 63:9 (1975), 1278-1308.

Usability Definition

ISO 9241:

The effectiveness, efficiency and satisfaction with which specified users achieve specified goals in specified contexts.

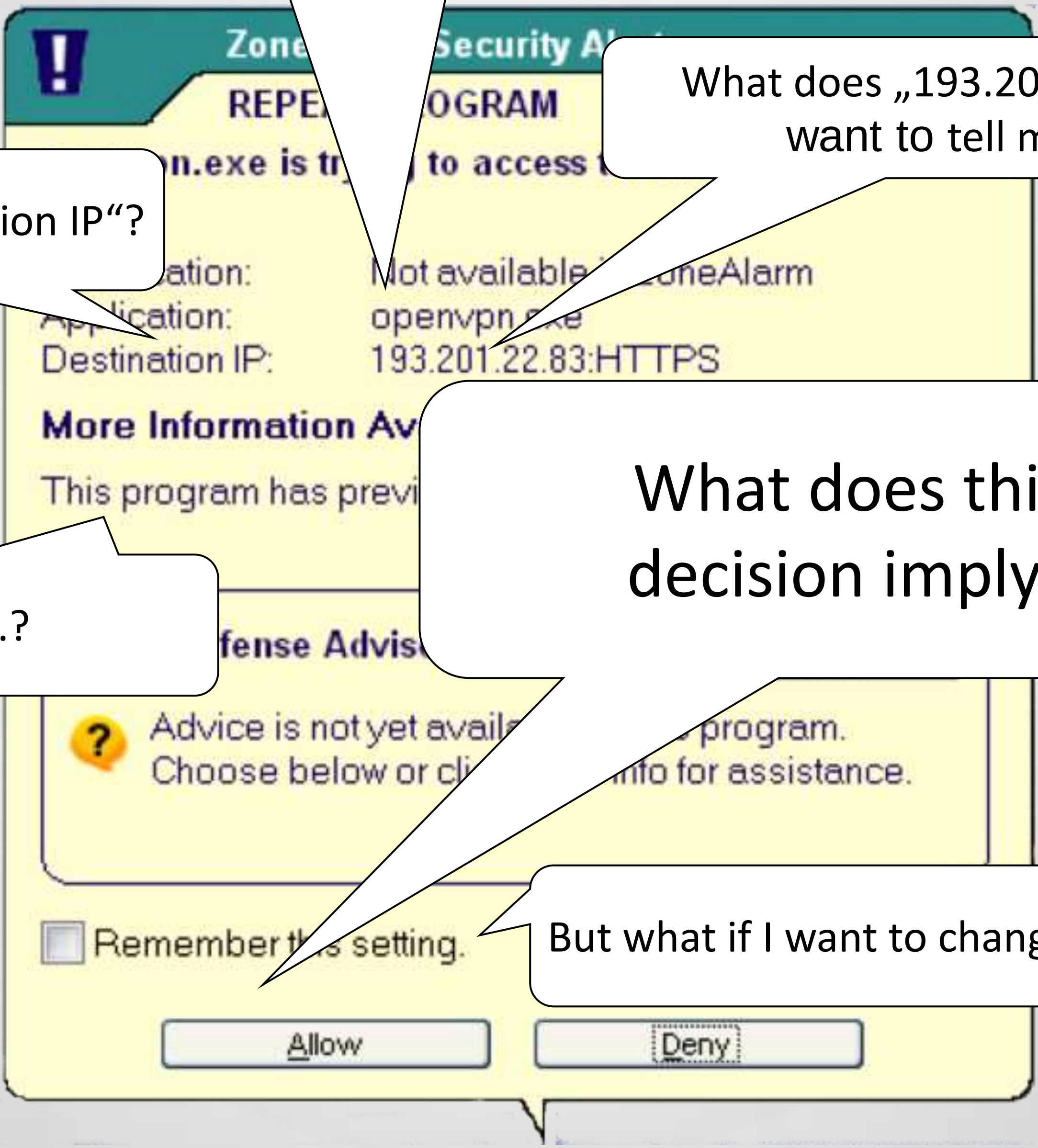
- How to not read it:
  - The effectiveness, efficiency and satisfaction with which specified users achieve specified goals in specified contexts.
- Hot to read it:
  - The effectiveness, efficiency and satisfaction with which specified users achieve specified goals in specified contexts.

Usability Principles

- Consistency
- Feedback
- Efficiency
- Flexibility
- Clearly marked exits
- Wording in users‘ language
- Task orientation
- Control
- Recovery and forgiveness
- Minimize memory load
- Transparency
- Aesthetics and emotional effect

These principles enable learnability, efficiency, effectiveness, reduced error-rate, memorability, and subjective satisfaction.

Example: Personal Firewall



Zone Security Al

REPE OGRAM

n.exe is tr to access t

ation: Not available ZoneAlarm

Application: openvpn.exe

Destination IP: 193.201.22.83:HTTPS

More Information Av

This program has previ

fense Advis

Advice is not yet avail program.
Choose below or cl info for assistance.

□ Remember th setting.

What is „openvpn.exe“?
I clicked on „VPN-Connection“...

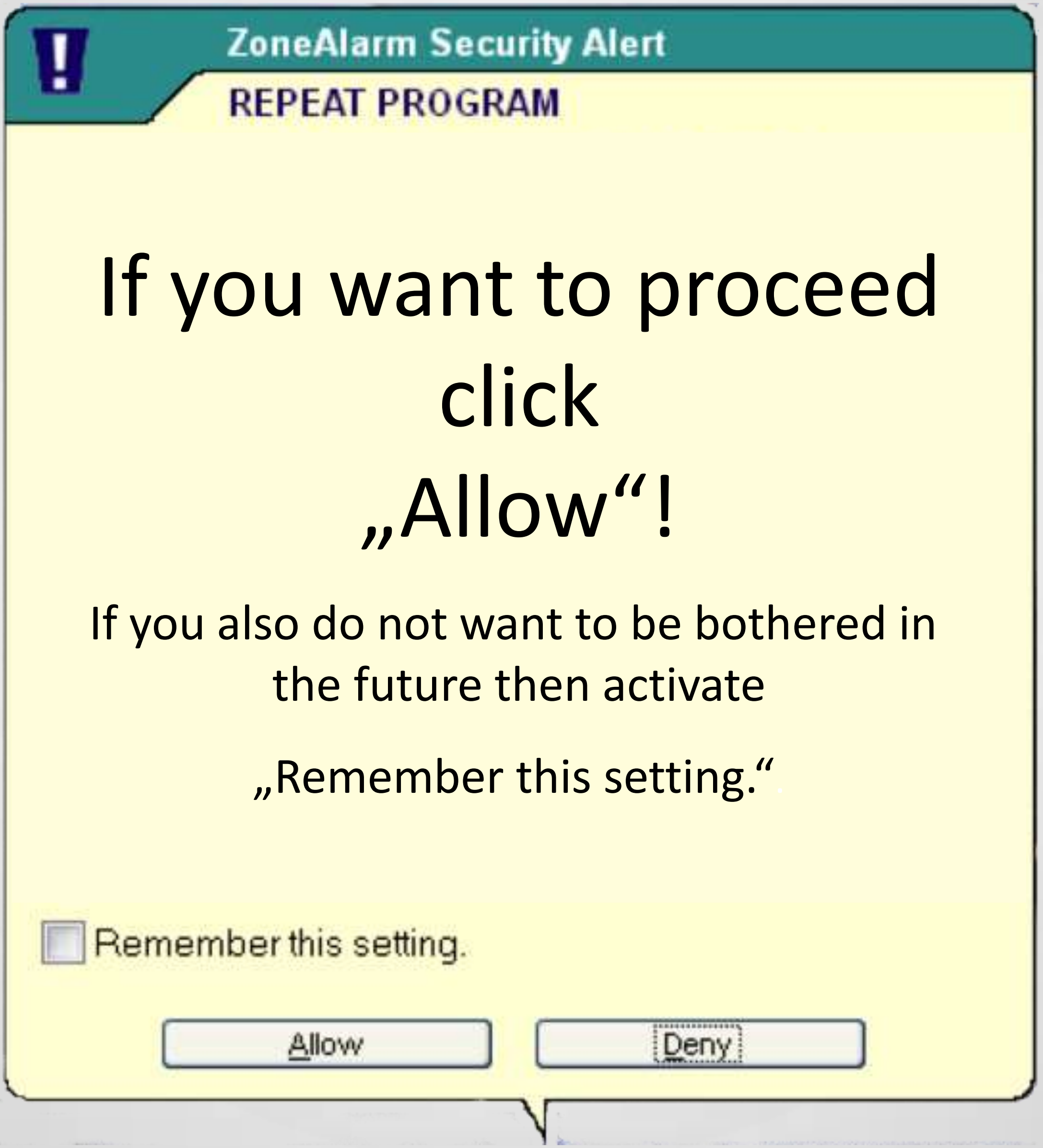
What does „193.201.22.83“
want to tell me?

What is a „Destination IP“?

What does this
decision imply?

Yes - and...?

But what if I want to change it in the future?



ZoneAlarm Security Alert

REPEAT PROGRAM

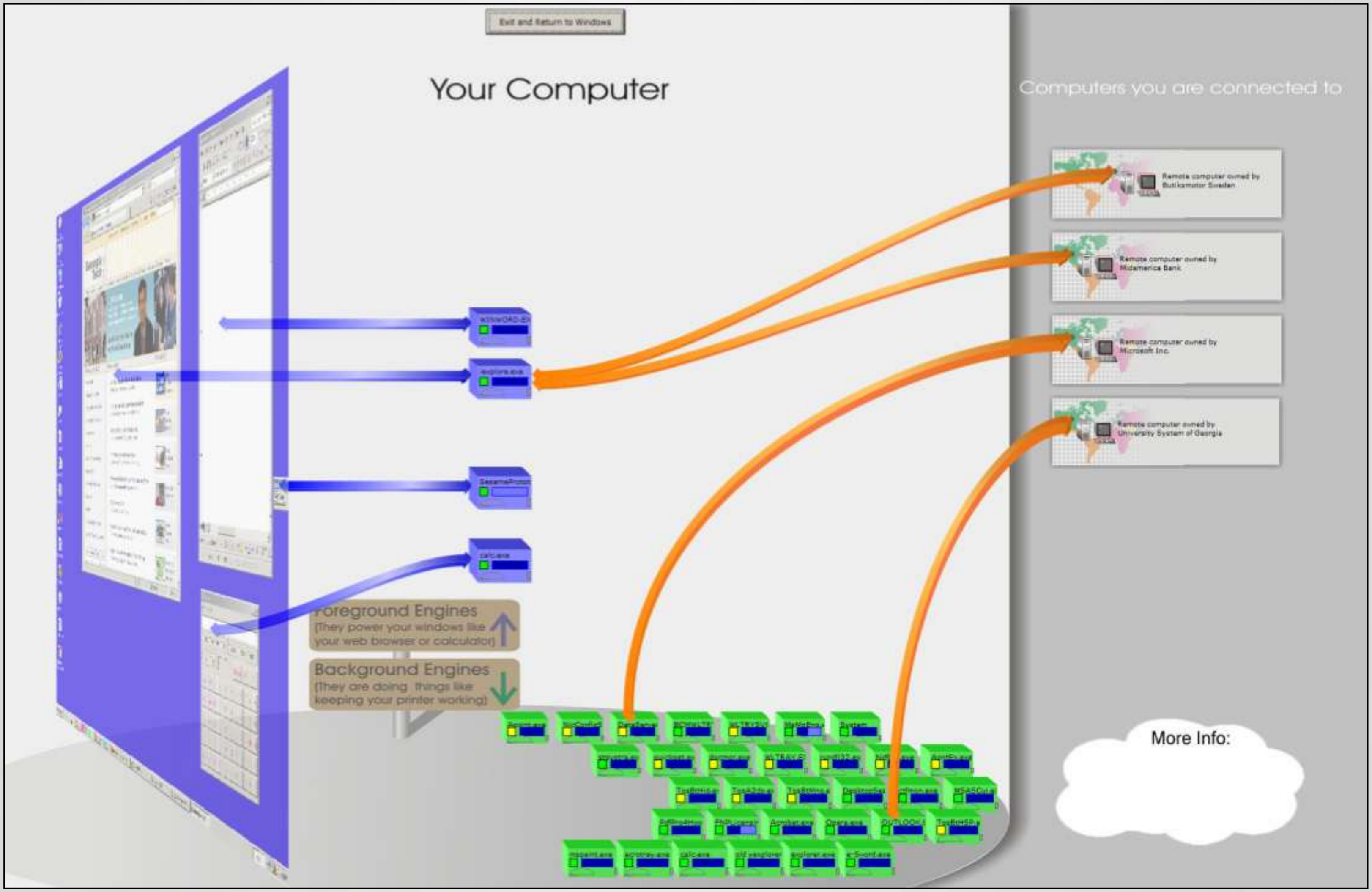
If you want to proceed click „Allow“!

If you also do not want to be bothered in the future then activate

„Remember this setting.“

□ Remember this setting.

Example Solution

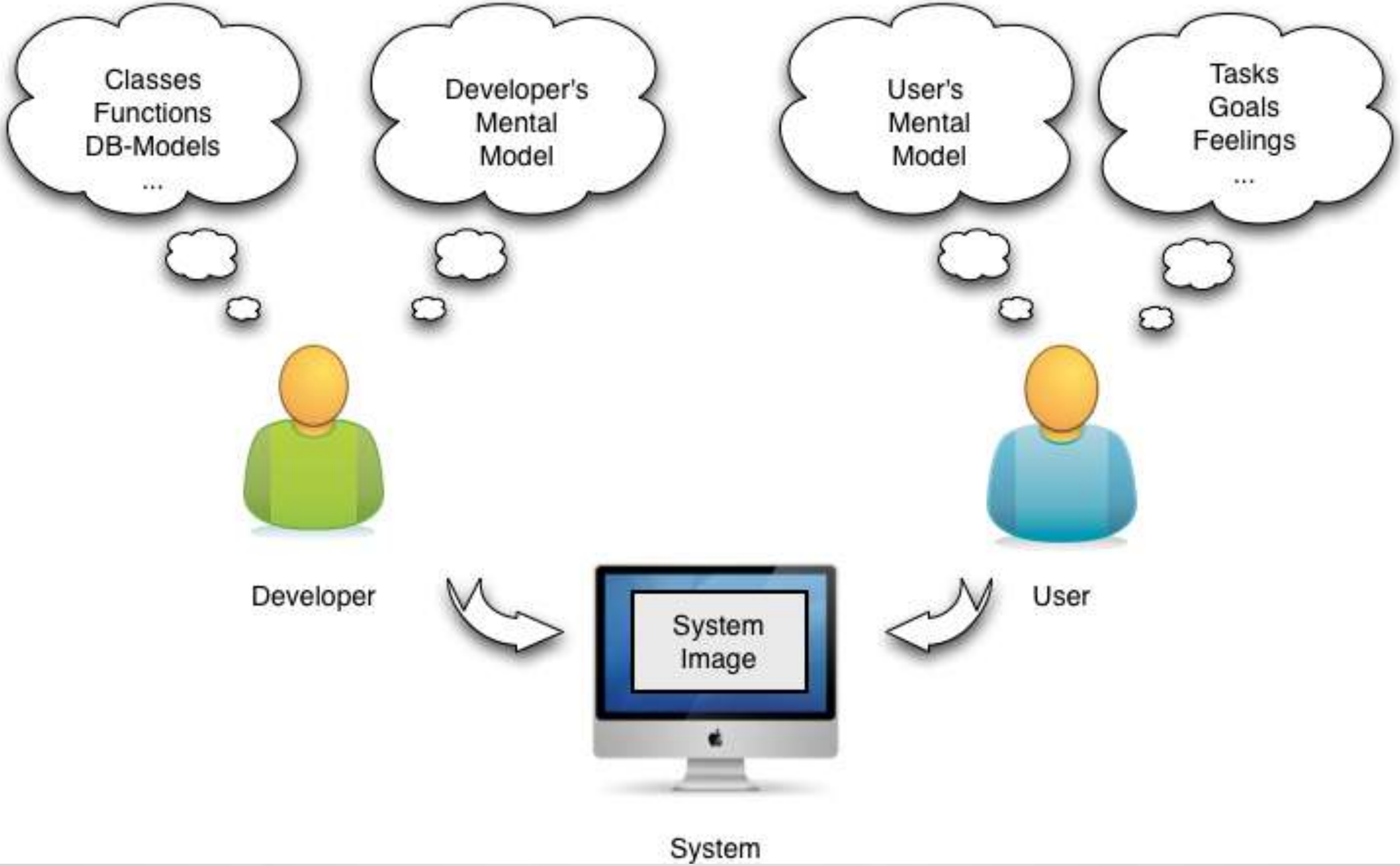

Exit and Return to Windows
Your Computer
Computers you are connected to
WINWORD.EX
iexplore.exe
SesameProto
calc.exe
Foreground Engines
(They power your windows like your web browser or calculator)
Background Engines
(They are doing things like keeping your printer working)
Remote computer owned by Butikamotor Sweden
Remote computer owned by Midamerica Bank
Remote computer owned by Microsoft Inc.
Remote computer owned by University System of Georgia
More Info:

Source: Stoll et. Al. Sesame: Informing User Security Decisions with System Visualization

Agenda

- About CURE
- Usability
- ***Mental Models***
- User Experience (UX)
- HCISEC Challenges
- User Centred Design (UCD) Process
- Conclusions
- Contact

Mental Models 1/2

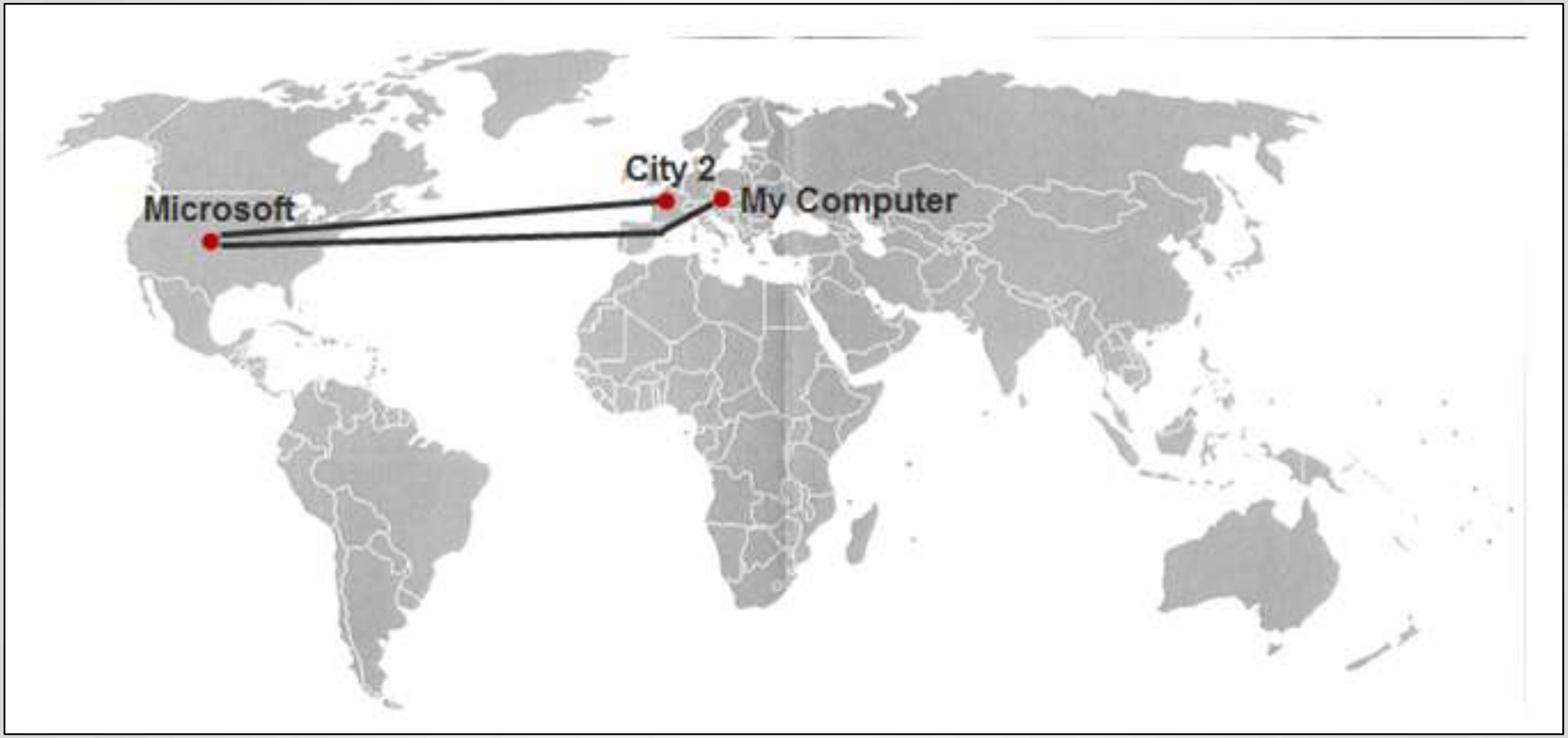


Mental Models 2/2

A mental model is an explanation of a thought process about how something works in the real world. It is an explanation on a person’s perception about their own acts and consequences in the world.

Source: Young, I. 2008. Mental Models: Aligning Design Strategy with human behavior. Rosenfeld Media, New York.

Mental-Models Research Example



Agenda

- About CURE
- Usability
- Mental Models
- ***User Experience (UX)***
- HCISEC Challenges
- User Centred Design (UCD) Process
- Conclusions
- Contact

User Experience (UX)

Comfort

Aesthetics

Findability

Privacy

Attractivity

Accessibility

Trust

Benefit

Desire

Fun

UX

Identity

Stimulation

Usability

Security

Usefulness

Credibility

Convenience

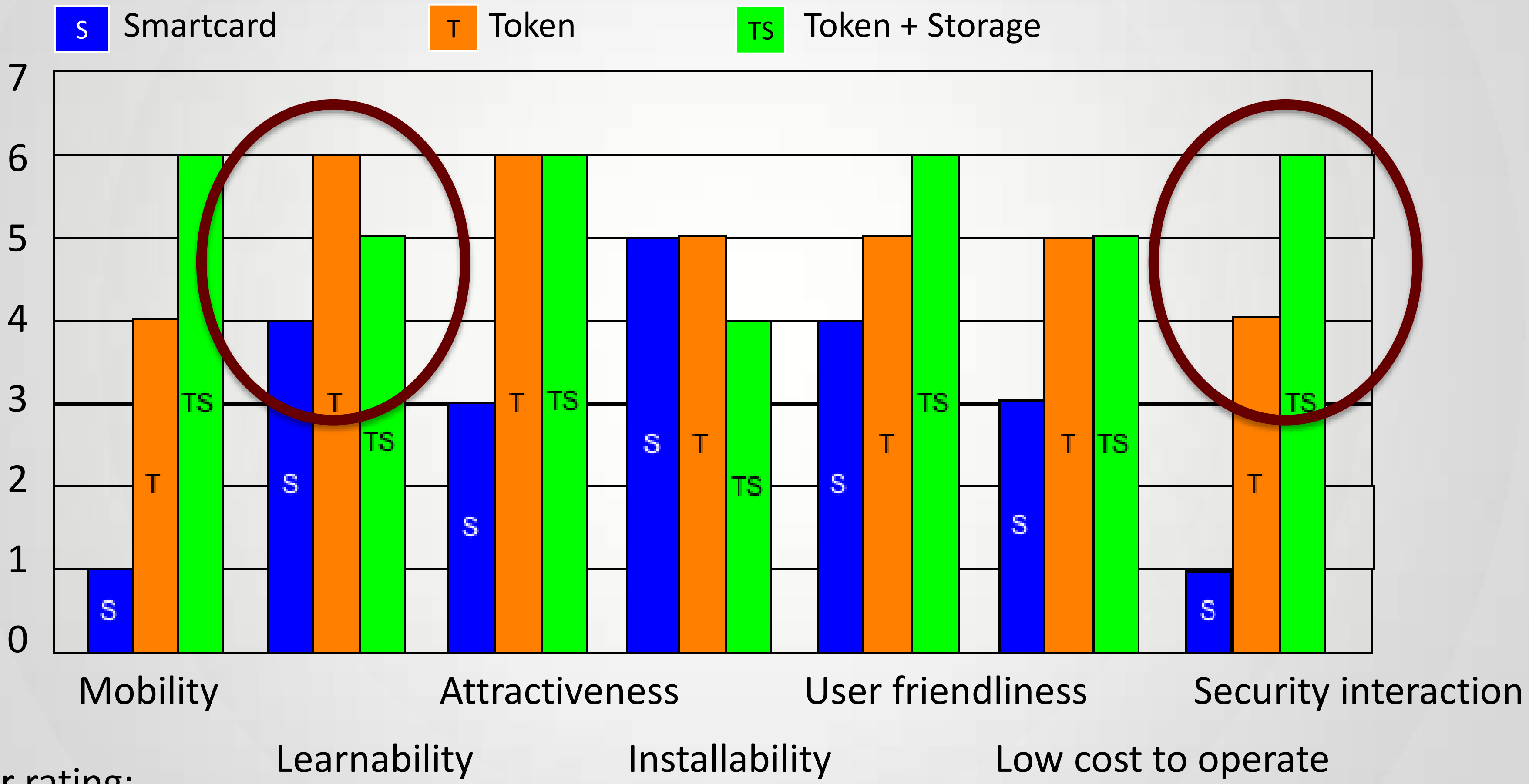
Performance

Playfulness

Pleasure

Enjoyment

Example 1: Authentication UX



User rating:
1 = poor
7= excellent

Source: Piazzalunga et al. The Usability of Security Devices

Example 2: „Road Apple Attack“

Source: http://hack5.org

Source: http://hack5.org

UHU
stic
SAMSUNG

Agenda

- About CURE
- Usability
- Mental Models
- User Experience (UX)
- ***HCISEC Challenges***
- User Centred Design (UCD) Process
- Conclusions
- Contact

HCISEC Challenges 1/2

- Security is a secondary task
  - Users focus on primary task
- Concepts are hard to communicate
- "Informed decision" hard to undertake
  - Users lack a working mental model
  - GUIs often support wrong mental models
  - GUI elements and interaction processes are hard to interpret

HCISEC Challenges 2/2

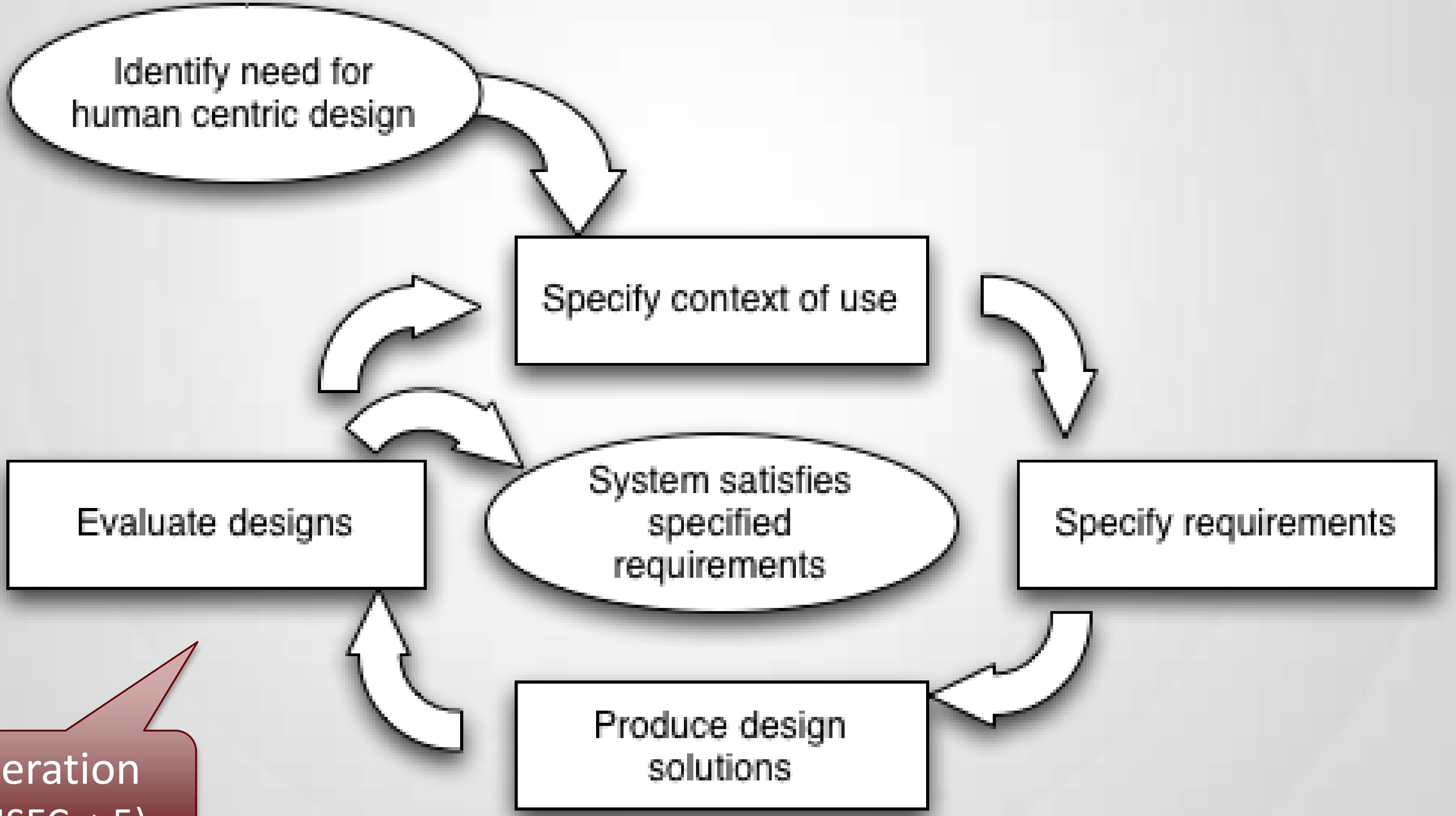
- Technical origins shine through
  - "Technical language" hard to understand
- Users' Trust Perception
  - Lack of transparency of underlying security properties
- Lack of awareness of possible consequences
- Heuristic risk analysis not appropriate online

Agenda

- About CURE
- Usability
- Mental Models
- User Experience (UX)
- HCISEC Challenges
- ***User Centred Design (UCD) Process***
- Conclusions
- Contact

User Centred Design Process

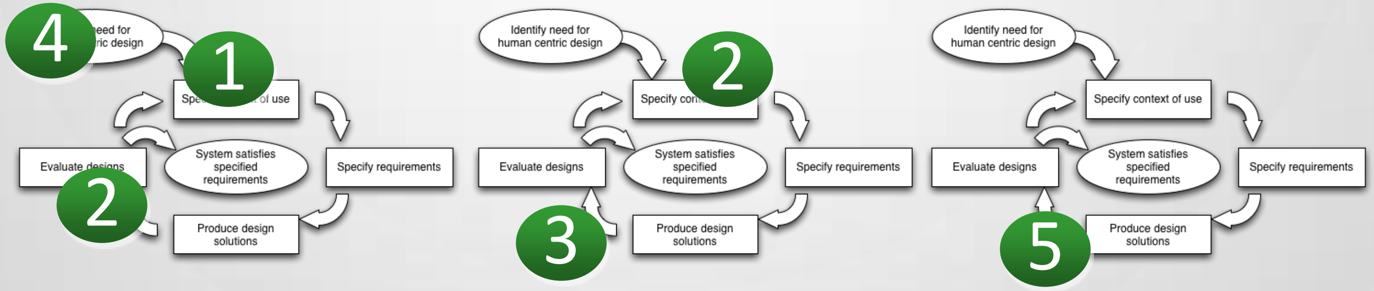
ISO/TR 16982



1 Iteration
(HCISEC: >5)

HCISEC Design Process

- User centred Design Process (extended HCI methodology)
  1. Personas
  2. Mental model research
  3. Evaluation beyond task-times and error rates (additional questionnaires)
  4. Pre-studies (e.g. wording…)
  5. Retrospective testing



Example: The uTRUSTit Approach

- Personas
- Scenarios
- User-studies
  - Laboratory evaluations
  - Mental model research
- VR-Evaluations
- Design guidelines
  - Accumulate results from studies
  - Iterated three times
- End-user trials

Example Persona: Fredrik Clasen

- Has dyslexia
- Uses assistive technologies
- Technophile
- Supports his family in technical matters
- Tries to avoid reading
- Always online

Agenda

- About CURE
- Usability
- Mental Models
- User Experience (UX)
- HCISEC Challenges
- User Centred Design (UCD) Process
- ***Conclusions***
- Contact

Conclusions

- Why?
  - Maintain holistic security
  - Avoid damage & threats (customer/client/organisation)
  - Effective application & usage of security technology
- Who?
  - Real end-users
  - Specified users (Not "the user"; e.g. use Personas)
- How?
  - End-user studies
  - Mental model research
  - Iterative end-user testing & re-engineering
- Users are not the enemy!

Thank you for your attention!

UTRUSTIT

Agenda

- About CURE
- Usability
- Mental Models
- User Experience (UX)
- HCISEC Challenges
- User Centred Design (UCD) Process
- Conclusions
- ***Contact***

Contact

Peter Wolkerstorfer

Senior HCI Researcher

CURE - Center for Usability Research & Engineering

[Mail] wolkerstorfer at cure dot at

[Web] http://www.cure.at