



T-110.5220 Information Security and Usability

Introduction to the course
and to the field

Contents at one glance



- ⌘ Introduction to the field of "Usable security"
 - ☒ Basic lectures: Trust-Privacy-User authentication-Usable security management-What's new
 - ☒ Guest lectures
- ⌘ 3 credits
 - = (lectures) + 3 small assignments + exam
- ⌘ "P" – good for graduate studies, too
- ⌘ T5 22.1.-7.5.2010 on most Fridays 12:15-13:45

Course schedule



⌘ Lectures on Fridays 22.1.-7.5.2010

⏏ No lecture on 5.3., 12.3. and 2.4.2010

⏏ Lectures are **voluntary**

⏏ Basic lectures by Kristiina Karvonen

⏏ <http://www.hiit.fi/~karvonen>

⏏ Introduction to the field & theoretical background

⏏ Guest lectures by visitors from companies

⏏ Ville Nore (F-Secure), Maria-Helena Markkula, F-Secure, Olli Immonen (Nokia), Andreas Heiner (Nokia), Laura Turkki (Nordea)

⏏ Practical information on real-life use cases and the real work behind the security UIs & chance to ask the makers of the services you might be using daily

⏏ The best part!!!

Lecture topics



22 Jan	Introduction to the course and to Usable Security
29 Jan	Usable security: The origins
05 Feb	What we mean when we talk about trust?
12 Feb	Privacy and publicity - a changing world
19 Feb	"U8kl%=)JJ" - user-friendly authentication
26 Feb	Usable security management - what is it and how to create it?
05 Mar	No lecture
12 Mar	No lecture (winter holidays)
19 Mar	Guest lecture: Ville Nore & Maria-Helena Markkula, F-Secure
26 Mar	Guest lecture Andreas Heiner, Nokia
02 Apr	No lecture (Easter)
09 Apr	Guest lecture: Laura Turkki, Nordea
16 Apr	Guest lecture: Olli Immonen, Nokia
23 Apr	Guest lecture Andreas Heiner, Nokia
30 Apr	Where do we go from here - the new topics in usable security
07 May	What have we learned – course summary + discussion

Course requirements



1. Exam on [course material & selected articles]
2. Three small home assignments
 - ☒ 2 analysis exercises and 1 design exercise
 - ☒ Based on material covered during the lectures
 - ☒ Lecture material will be available on course website
 - ☒ Graded "pass" or "good"
 - ☒ "pass" keeps you on the course; "good" aggregates to your total grade based on assignments and final exam

To get a good grade



- ⌘ *Applying* the knowledge gained during the course, making good use of the course materials and lectures
- ⌘ Assignments can help you raise your grade

Questions at this point?



⌘ Course website at Noppa

⌘ <https://noppa.tkk.fi/noppa/kurssi/t-110.5220/etusivu>

Usable security as a field



Short introduction to the basics

Introduction



- ⌘ Internet is not a safe place.
- ⌘ Computer systems are imperfect.
- ⌘ With security, no-one wants to be the guinea-pig

People don't feel secure. In a way, they shouldn't.

And yet they should, and would like to.

Allies.. or enemies?

⌘ Traditionally, usability and security are seen as opposites

- ☑ Easy-to-remember passwords are easy to crack

- ☑ Hard-to-remember passwords are forgotten or written on post-it

- ☑ Preventing errors poses restrictions on the user interaction.

-> use becomes cumbersome

⌘ Usability and Security as a field tries to fight this.



Being user-friendly means...

⌘...understanding the world user lives in

USER FRIENDLY by Illiad



Copyright (c) Illiad 1999



The Paradox



- ⌘ People tend to associate "difficult" with "security"
- ⌘ If interaction is easy, can it really be safe?
 - ☑ Too easy = not desirable
 - "Do they think I'm stupid or something?"
- ⌘ People also want to
 - ☑ Master difficult things
 - ☑ Appear more knowledgeable than they are

Goals vs. Needs



Needs and goals may not be entirely synonymous ... for example, users may need critical information but decide to do without it because their overriding goals are "finishing quickly" or "not looking stupid."

Goals will usually win over needs in user behaviour.

Security is not a goal, it is a need.

Usability methods will reveal needs - to a careful observer.


Creating usability

⌘ What is usability?

- ☑ "getting there" - successful and effective interaction
- ☑ "feeling good" - perceived easiness of use
- ☑ "getting it right" - understanding the system

⌘ different things for different users

What is a usability problem?



- ⌘ aspects of a user interface that make the system difficult, inefficient and frustrating to learn and to use.
- ⌘ Nielsen (1994): if a change would improve the system, it is a usability problem.
- ⌘ In different contexts, problems carry different weights.

What about "usability of security"?



- ⌘ introducing usability methods to new area
- ⌘ making a complex thing simple with usability tools
- ⌘ making security understandable
- ⌘ creating security features that people want and need
- ⌘ dealing with a need, not a goal.

What is "security" from a user point of view?



- ⌘ feeling something that is hard to put into words
- ⌘ preserving your privacy and being willing to do things that require trust
- ⌘ being in control

What are the threats?



- ⌘ Viruses
- ⌘ Intrusions
- ⌘ Identity theft
- ⌘ Losing money
- ⌘ Losing face
- ⌘ Losing fame
- ⌘ ...

Technical threat may be different from the threat user is seeing or believing to be there:

Both need to be covered.

Trust?



⌘ Hard to capture

- ☒ A combination of an emotional and rational response

⌘ Hard to express

- ☒ Who would you give your house keys to?

⌘ Hard to gain

- ☒ "Trust me, I know what I'm doing"

⌘ Hard to explain

- ☒ Based on decision-making, conscious or subconscious

Privacy?



⌘ a different thing for different users

- ☑ People vary in the level of privacy they need
- ☑ Cultural differences

⌘ a different thing in different situations

- ☑ In control of information about oneself
- ☑ Anonymity. Knowing who knows.
- ☑ Multiple identities. Chosen identity.

Control?



⏏ Knowing what's going on

⏏ Being able to

⏏ decide

⏏ cancel

⏏ verify

⏏ re-do

⏏ remember

⏏ recognize

⏏ get information

Data security instructions in a nutshell

Netbank's security practice in brief
General data security on the Internet
Viruses and other harmful programs
Protection against harmful programs
Control and hindrance of traffic between your computer and the net
Protection of privacy
Minimising the damage
When using a computer that is not yours

There is a technical as well as a human side to data security. Users can actively contribute to maintaining data security in their operational environment.

Technological security solutions may prove insufficient if the users are not aware of the risks involved, or if they are careless, for example by leaving their passwords available to outsiders. Data security is not merely a technological question but consists of many factors.

However, ordinary users need not know every detail. It suffices well to know what the worst threats are and how to protect oneself against them. An overall picture of the situation and preparedness against threats are sufficient protective measures.

These instructions have been divided into two sections: summary of Netbank's security practice and general data security on the Internet. These general instructions are meant for all computer users and especially Internet users.

The instructions mainly focus on technological threats and protection against them. The purpose of these instructions is to make things understandable even to an inexperienced user. Therefore, the used terms and instructions may not be entirely fitting from the viewpoint of a data security expert. These instructions were written with the Windows operating system in mind, but they are applicable to other systems as well.

▲Netbank's security practice in brief

Protection of sessions

The SSL security protocol is an encryption technology supported by browsers. When SSL encryption is activated in Netscape and Explorer browsers, a lock icon is shown on the display. By clicking the **Lock** icon (once in Netscape and twice in Explorer) you can view the bank's security certificate, for example in Netbank. A secure connection begins with the letters **https://** in the address field of the Internet service. If the Internet address begins with **http://**, the connection is **not** secured.

The connection to Netbank is protected with the SSL security protocol and Solo codes. The SSL protocol encrypts the data communications, and with the Solo codes the customer is identified by the bank. In addition, cookies are used to control the session.

...not like this!

⌘ Too much information

- ☒ "...instructions in a nutshell"
- ☒ "must be a huge nut. Huge!"

⌘ Speak the user's language

- ☒ "The SSL security protocol is an encryption protocol supported by browsers".
- ☒ Too technical. Way too technical.

⌘ Don't appear condescending

- ☒ "...ordinary users need not know every detail."
- ☒ Everyone likes to be described as "ordinary", right?
- ☒ "But I'd like to know!"

⌘ Give them the means to act

- ☒ " It suffices well to know what the worst threats are and how to protect oneself against them".
- ☒ "Yes, and exactly how will I do that? "
- ☒ "Why can't *you* protect me??"

⌘ Give them the information

- ☒ "By clicking the **Lock** icon (once in Netscape and twice in Explorer), you can view the bank's certificate, for example in Netbank."
- ☒ "What lock icon? What does it look like? Where exactly is it?"
- ☒ "Why would I want to look at a certificate? What is it?"



When trying to make security
usable..

Always apply the basic usability rules..



- ⌘ Simple and natural dialogue
- ⌘ Speak the user's language
- ⌘ Minimise the user's memory load
- ⌘ Consistency
- ⌘ Feedback
- ⌘ Clearly marked exits
- ⌘ Shortcuts
- ⌘ Precise and constructive error messages
- ⌘ Prevent errors
- ⌘ Help and documentation

Be multi-disciplinary...



⌘ making use of

- ☑ human psychology
- ☑ sociology
- ☑ aesthetics
- ☑ consumer studies
- ☑ fashion trends!
- ☑ ...just to name a few

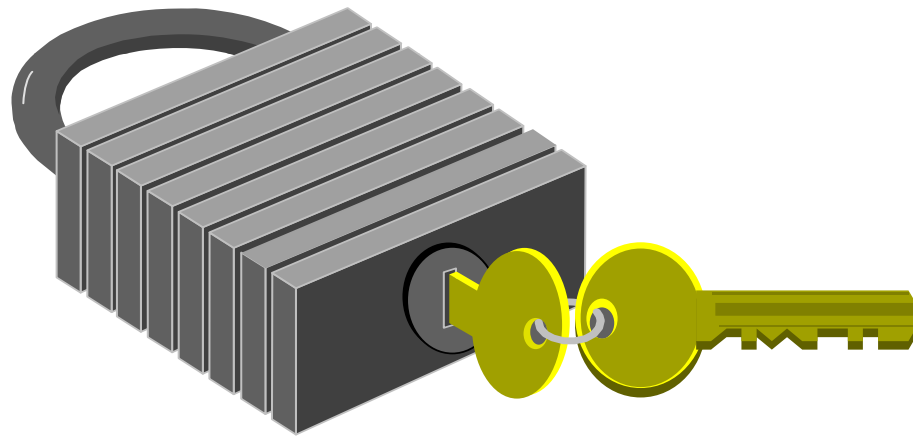
⌘ gives best results

Do the difficult things, too



- ⏏ Will they hate it?
 - ⏏ trade-offs between usable and secure
- ⏏ Do they get it?
 - ⏏ the accuracy of the mental model of the user
- ⏏ What's good and what's not?
 - ⏏ finding out about user preferences
- ⏏ Do they like it?
 - ⏏ the overall satisfaction with the product
 - ⏏ the acceptability of the interface
- ⏏ Will they use it?
 - ⏏ Find out if users really want to use the product and really feel secure
- ⏏ ..capture the *user experience of feeling secure*

Secure or insecure?



Visualising security - how?



- ⌘ Simple statements of security?
- ⌘ Detailed technical descriptions?
- ⌘ Intuitive interface metaphors?
- ⌘ Standards and conventional notations?

- ⌘ One of these? All? More?

Designing for security is hard.



- ⌘ People do not know how security looks like.
- ⌘ In fact, no-one knows.
- ⌘ Security visual indicators (padlocks etc.) are hard to detect and to interpret.
- ⌘and people are looking somewhere else, anyway.

Next week



⌘ The Origins: Three "classic" articles

☐ Users are not the enemy

Adams, A and Sasse, M.A, in Communications of the ACM, Vol. 42, No. 12, December 1999, pp. 41-46

☐ Usability and privacy: a study of KaZaA P2P file-sharing

Good, N.S. and Kreckelberg, A, in Proceedings of CHI 2003, April 5-10, 2003, Ft. Lauderdale, Florida USA. ACM Press

☐ Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0

Whitten, A, Tygar, J.D, in Proceedings of the 8th USENIX Security Symposium, August 1999.