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”
  - Trust-Privacy-User authentication-Security experience-Hot topics in usable security
  - Some lectured by guest lecturers
- 3 credits

= (lectures) + individual work + exam. Lectures are voluntary. Exam in May.

- ”P” – good for graduate studies, too
- T2 18.1.-3.5.2010 on most Tuesdays 14:15-15:45
  - For exceptions see schedule at Noppa

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

Usable security as a field

Short introduction to the basics

Introduction

Stating the obvious:

- 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.

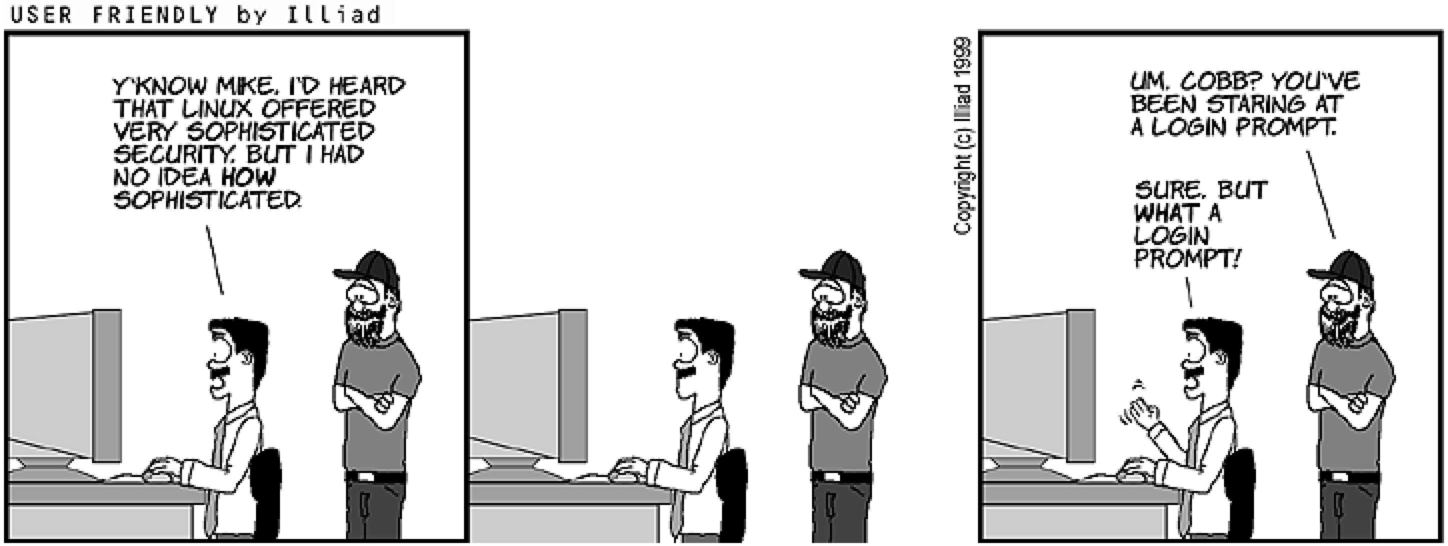
Allies.. or enemies?

- 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
Y'KNOW MIKE, I'D HEARD THAT LINUX OFFERED VERY SOPHISTICATED SECURITY. BUT I HAD NO IDEA HOW SOPHISTICATED.
Copyright (c) Illiad 1999
UM, COBB? YOU'VE BEEN STARING AT A LOGIN PROMPT.
SURE, BUT WHAT A LOGIN PROMPT!

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

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

Whitten & Tygar

Definition: Security software is usable if the people who are expected to use it:

1. are reliably made aware of the security tasks they need to perform;
2. are able to figure out how to successfully perform those tasks;
3. don’t make dangerous errors; and
4. are sufficiently comfortable with the interface to continue using it.

Ka-Ping yee suggested

…10 principles for secure interaction design:

1. Path of Least Resistance Match the most comfortable way to do tasks with the least granting of authority. **2. Active Authorization** Grant authority to others in accordance with user actions indicating consent. **3. Revocability** Offer the user ways to reduce others‘ authority to access the user's resources. **4. Visibility** Maintain accurate awareness of others' authority as relevant to user decisions. **5. Self-Awareness** Maintain accurate awareness of the user's own authority to access resources. **6. Trusted Path** Protect the user's channels to agents that manipulate authority on the user's behalf. **7. Expressiveness** Enable the user to express safe security policies in terms that fit the user's task. **8. Relevant Boundaries** Draw distinctions among objects and actions along boundaries relevant to the task. **9. Identifiability** Present objects and actions using distinguishable, truthful appearances. **10. Foresight** Indicate clearly the consequences of decisions that the user is expected to make.

(ok, ok, ok – no good definition
nor design principles for
usable security exist as yet)

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
- A need, not a goal

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.

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.

Usable security ”subfields”

- Trust
- Privacy
- (often also: usability of authentication)

- Field evolving and changing
  - This division into subareas may be vanishing

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
- Easier to lose
  - When gone, hard to retain

Separate lecture later in the spring.

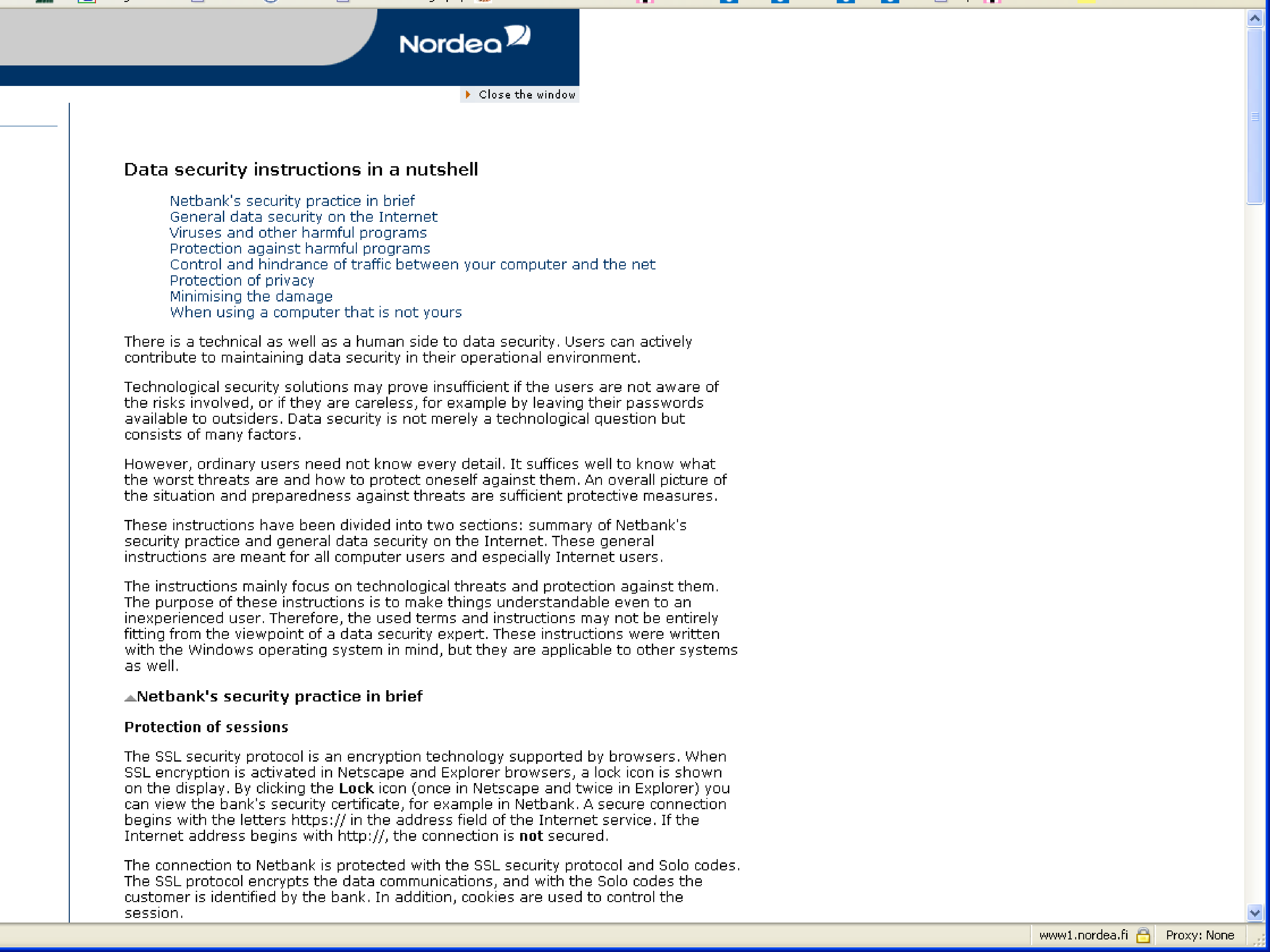
Privacy?

- 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.

Separate lecture later in the spring.

Control?

- Knowing what’s going on
- Being able to
  - decide
  - cancel
  - verify
  - re-do
  - remember
  - recognize
  - get information



Data security instructions in a nutshell

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!”

Does not speak the user’s language

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

May seem condescending

- ”…ordinary users need not know every detail.”
  - Everyone likes to be described as ”ordinary”, right?
  - ”But I’d like to know!”

How to act on this information?

- ” 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??”

Where *is* 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..

= Jacob Nielsen’s heuristics

- 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

What kind of usability methods to use?

Interviewing or observing a variety of users to gain an understanding of the users' world

…and to gather basic criteria for UI design

UI design on basis of the analysis of the material gathered

…iterative user testing of the UIs developed

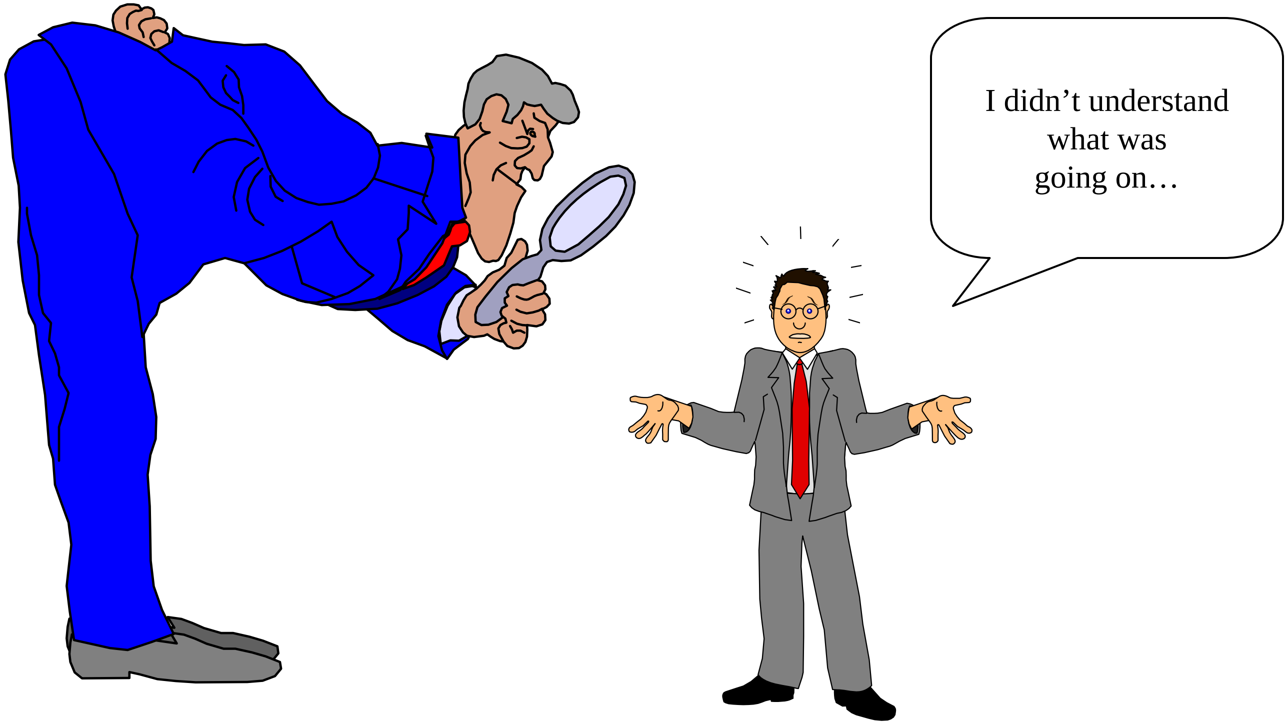
…analysing the results into generic design principles

Should not mention study is about security not to cause user bias

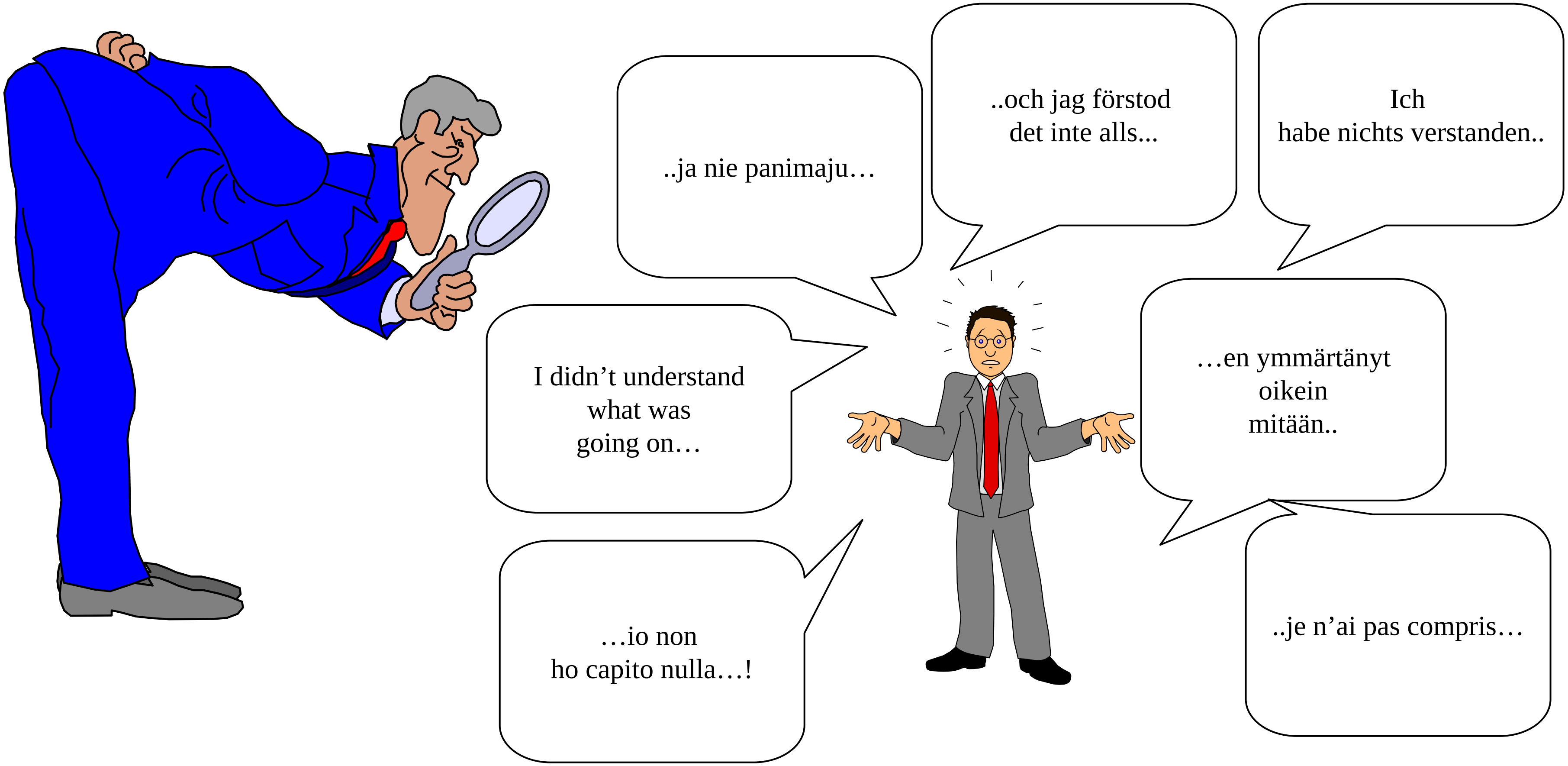
Be ethical: can’t really jeopardize users’ security!!

Getting to know the users' world(s)

- Interviewing users



Taking cultural effects into account


..ja nie panimaju…
..och jag förstod det inte alls...
Ich habe nichts verstanden..
I didn’t understand what was going on…
…en ymmärtänyt oikein mitään..
…io non ho capito nulla…!
..je n’ai pas compris…

Security experience?

- Traditional usability not enough for usable security
- Utilise user experience research, methods, and toolboxes
  - E.g. www.allaboutux.org presents many possibilities on how to conduct your research

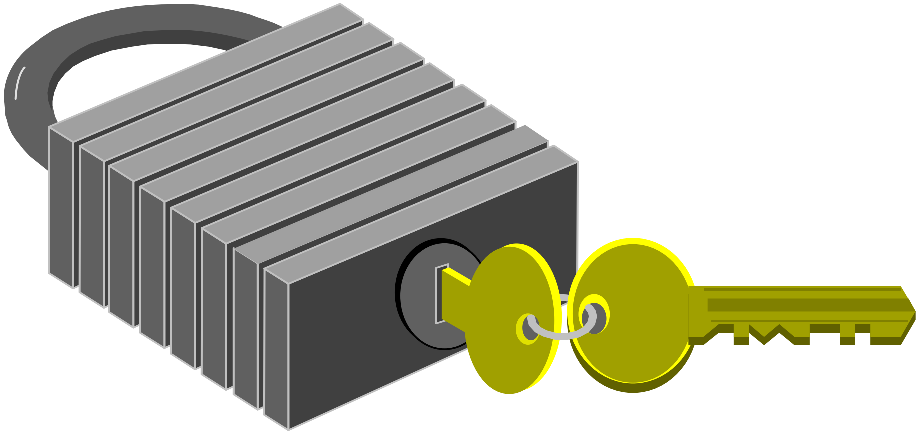
Covering the security experience

- 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

Separate lecture later in the spring.

Btw, how does security look like?

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.

Conclusions

- usability of computer security
  - has various ingredients: technical, legal, social, psycohological etc.
  - claims to be a field in its own right
  - cornerstones: privacy and trust
  - an area where even one mistake may be too much
    - Trial-and-error method will not do.
    - Get it right the first time, every time.

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.