T-110.5220 Information Security and Usability P (3 cr)

- This course is a basic introduction to the field of usable security.
- In the course, key areas of usable security as a field are introduced.
- Through examples, it is also shown how to apply usability and user-centred methods to security.
- the latest developments in the field are looked into through recent work in this area

Course prerequisites

- T-110.4206 **Information Security Technology (3 cr)** and T-121.2100 **Introduction to User-Centred Design** or equivalent skills

= Basic knowledge of usability and user-centred design is expected from the student

= Basic knowledge on information security is expected from the student

- No formal requirements – you just have to work harder if you miss this background!

Learning outcomes

After finishing this course, the student is (hopefully) able to

- name the key areas of usable security
- name the classic articles of usable security and explain why these articles are so important
- list the specific requirements of usable security compared to “general usability”
- apply various usability methods to testing usable security and to improve usable security through user-centred design
- evaluate the level of usability of security on security applications,
- name new areas of research in usable security
- name some main articles, researchers and research forums of usable security, and
- present arguments for the importance of usability for creating security.

Course practicalities

- Spans periods III & IV
- Consists of
  - 3 introductory lectures and
  - Essay writing period with two deadlines
  - Short presentation of the essay to others
  - Optional: participation in course blog (may improve your grade)
  - **NO EXAM!**
- Essay graded with 1-5

Essay

- Students are required to **write an essay** on a selected topic in the course's area. The essay will be graded from 1-5.
- The students can **select a topic** from the list or suggest their own topics by March 2, 2012 via email to the lecturer.
- Length of the essay should be **about 8 pages with given template.** We will use the ACM CHI 2012 template for Work-in-progress papers.
- There are **two deadlines** for returning the essay:
  - first draft DL **April 13, 2012** - a scheme of intended essay contents + some references
  - final version DL **May 4, 2012.**
- Return your essay as a pdf file to **kristiina.karvonen@hiit.fi** by each deadline.
- Consultation via course blog and email
- The students are expedted to **give a presentation on their essay May 11, 2012** 14:00-16:00 (15 minutes each).

Essay topics

1) ”Definition for Usable security”. Whitten and Tygar aimed at a definition for usable security in their paper Why Johnny Can’t Encrypt. Make a literature survey on more recent related work to compare, abandon or extend their original definition.

2) ”Why is privacy management so hard?” With so many new social media tools, such as Facebook and Google Buzz, just to name two examples, we have seen that maintaining one’s privacy online can indeed be tricky. On basis of recent work in this area, discuss these challenges and the current aims to tackle them.

3) ”Better privacy management” – on basis of related work and your own analysis, redesign the privacy management for an online service you know well. First present the service and issues related to its current privacy management, then proceed with the redesign.

4) ”Trust online”. Learning who to trust online and who not to trust can be tricky business, as the usual cues for trustworthiness tend to be missing in the online world. On basis of previous work in the area of trust formation in the online environment, discuss issues related to users and online trust from a selected viewpoint (e.g. how to design for trustworthiness; how online trust is formed; how usability and trust formation are related; or similar) .

5) ”Usable security and social networking”. Users are involved more and more intensely in interactions online through social networking tools. Discuss the challenges and novel demands to creating usable security due to the emergence of social networking tools.

6) ”Usable security – a case study”. Select a service or product that somehow involves security and analyse its usability against course material and other related work as you see fit. You can also make a case study or run a small user study on a security product/service.

7) ”Identity online”. Identity theft has become a major problem in the Intenet. Discuss the different issues related and present an overview of interesting work in this area.

8) ”Why we fall for Phishing”. Users are susceptible to online scams where they end up losing private information and/or money. Why do users fall for these scams? Discuss the issue on basis of relevant work in the area.

9) ”New ways to authenticate”. Users tend to do badly when it comes to remembering good passwords. Why? Here you can either 1) discuss the human side, why users are bad at passwords and cite relevant work in the area or b) present work that aims at developing new ways to authenticate users that go beyond traditional passwords (e.g. graphical passmeans).

10) ”How to study usable security?”. Present how usable security has been studied since the classics through a selection of papers that you consider good (or bad). What is missing? What could be improved?

11) = your own topic. You can suggest something completely different or for example combine two topics from above.

Each topic will be introduced in course blog before March 2, 2012

Examples from last year modified essay topics

“Designing Better Privacy Management for Facebook “ “Privacy management in Twitter”

"Identity & authentication online”

“New ways to authenticate – beyond traditional text passwords”

"New ways to authenticate. What we have today and how to make them more user-friendly.”

“Privacy and Identity Online”

“Usable Security and Online Social Networks for the Health Application Domain“

Writing a good essay

- Choose a topic that really interests you
  - Can also be related to your other course work or thesis work, or similar
    - E.g. an alternative view to a topic you are already involved in
- Emphasis on usability and user-centredness, **not** on the technology!
- Combination of good background work (= good amount of references to earlier work) and own ideas & observations brings best results
- Essay can be written in English, Finnish, Swedish or German – but presentation May 11, 2012 has to be in English

Individual work vs. working in pairs/ groups

- It is possible to work on the essay also in pairs or as a group
  - Makes sense especially if you wish to conduct a small user study, as this is difficult on your own
  - Clearly defined areas of responsibility needed
  - Groups members will be asked to give feedback on each others' performance
  - Same grade to all group members (unless there are problems with the groupwork)
  - Get in touch with me to agree on working as a pair or as a group.

Course blog

- http://blogs.aalto.fi/usablesecurity/
- Course blog to support you during your essay writing
  - During the course, I will create an entry on each topic before the topic selection deadline (March 2, 2012) to introduce the topics, including some references
- Participation voluntary
  - Active participation improves course grade
  - All course attendees can create blog entries and comment on others' entries
  - Write on problems, interesting topics you run into, recent news related to usable security…the choice is yours
  - When commenting others, please be constructive!
  - Language: English so that everybody can participate
- Will add you as users with your Aalto user account
  - Follow the confirmation link in your Aalto email to be able to participate

Questions?

- …then we'll start with the introduction to usable security as a field.

Usability and security – an oxymoron?

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 and can make usage cumbersome.

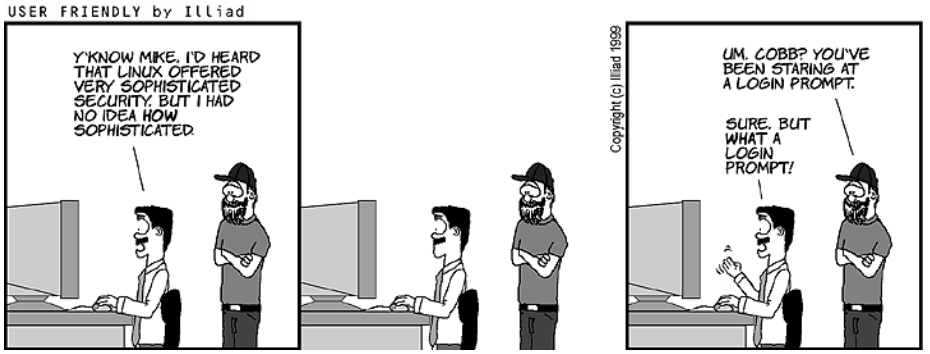
Usable cannot be secure?

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

Usable security – why?

- Introducing usability and user-centred design methods to “new” area

= Making a complex thing (security) simple by applying usability tools & usability thinking

= Making security understandable

= Creating security features that people want and need

= Supporting users in managing security

= making security seem like an asset, not a threat

Usable security – a “new” field

- First mention usually understood to be Saltzer & Schroeders mention of “psychological acceptability” in 1975 as one eight principles that need to be taken into account when creating security systems
- In late 1990s, articles where usability and security were combined started to emerge
  - The so-called classics (topic of next lecture)
- Own workshops, symposium, a thematic topic in generic human-computer interaction conferences
- Idea of double expertise – researchers experts in both security and usability (hasn’t really happened; work based on working as multi-disciplinary teams)
- First doctoral programme in usable security started in 2009 at Carnegie Mellon University - http://cups.cs.cmu.edu/igert/

Usable security vs. “General usability”

Let’s observe one standard definition for usable security:

“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.”

Whitten & Tygar, 1999

Let’s now look at each to see what is different (if any)

…are reliably made aware of the security tasks they need to perform;

- Security tasks are usually not first priority for the user
- Security mechanisms are unfamiliar to most users
- Users tend not to be aware of security taking place nor what it relates to
- Security seen as a burden

…are able to figure out how to successfully perform those tasks;

- Users tend to be afraid of security
- Users do not feel competent to manage security
- Not first priority to users
- Strange and unfamiliar terminology
- No mental model on security → no understanding on how own behaviour and choices affect overall security

…don’t make dangerous errors

- In security, one error may be enough to jeopardize security “for good”
- Trial-and-error method will not do to learn to manage security (as e.g. when learning to use Word”)
- Preventing dangerous user errors may make usage cumbersome or boring – user may feel at the mercy of the system

…are sufficiently comfortable with the interface to continue using it.

- usage can become cumbersome or boring ("why do I need to press "OK"??")
  - Can lead to habitual clicks which compromise security
  - Also depends on jurisdiction "user agreement needed to escape liability" (end user agreements, privacy statements, and similar are unusable because of this)
- Security should be seen as asset, not a burden
- Again, not first priority to most users.

Conclusion

- Yes? There seem to be some differences, most notably
  - Not first priority
  - Security is a need, not a goal
  - Security imposed on the user instead of user as an active and potent actor
  - Lagging behind in basic usability: strange and unfamiliar terminology, cumbersome usage, user kept “in the dark”
- No? Why would “general usability” not be enough
  - All usability subfields have their own specific requirements, yet are not considered as separate fields
    - E.g. mobile human-computer interaction
- No final answer exists, future will show if the field remains as “separate” or if it merges into the “general HCI”.

Next time (Feb 3, 2012)

- Next time we'll go in detail through the so-called classics
  - These articles formed the field and its sub-fields (trust, privacy, usability of security software)
  - Still mostly valid
  - The out-dated parts reveal how the field has developed
  - You need to be familiar with this work if you work in usable security!
- Blog access will be sent to all via email
- Blog entries on the first essay topics will appear in the course blog before next time