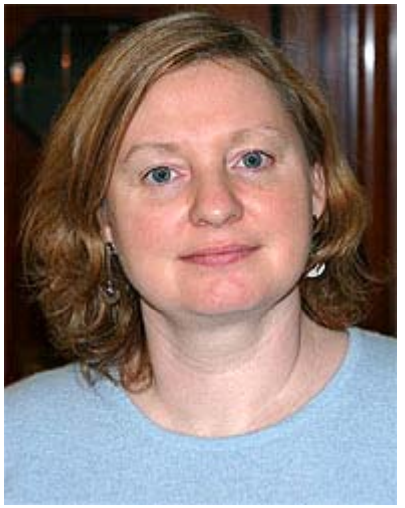
# Usable Security: The Origins

T-110.5220 Information Security and Usability

# Three "classic" papers in usable security

- Adams A and Sasse A: Users are not the enemy (CACM) 1999
- Whitten A and Tygar D: Why Johnny can't encrypt (USENIX) 1999
- Good, N. S. and Krekelberg, A. 2003. Usability and privacy: a study of Kazaa P2P file-sharing (CHI)

# Users are not the enemy



- Angela Sasse
  - Professor at UCL
  - Head of Information Security Research
- Anne Adams, Dr.
  - Former student
  - University of Nottingham

# Users are not the enemy

- Organizational study on how security procedures are followed in different organizations
- Background in password security and its problems
- Main claim: users can cooperate when it comes to security
- Against earlier ideas on how users are unwilling to cooperate

# Users are not the enemy

- Users lack security knowledge
- Security nees user-centred design
- Motivating users
- Users and password behaviour

→ Security policies should reflect work practices and organizational procedures + be usable, to be followed.

# Usability and privacy: a study of Kazaa P2P file-sharing

- Nathan Good
  - grad student at Berkeley
  - Formely at PARC
- Aaron Krekelberg
  - University of Minnesota

# Usability and privacy: a study of Kazaa P2P file-sharing

- Main claim: users do not understand what they share
- Bad usability of KaZaa leads to terrible privacy violations
- Privacy awareness often starts only with loss of privacy, which is not good.

# Why Johnny can't encrypt

- Alma Whitten
  - Graduate from Berkeley
  - Now at Google
- Doug Tygar
  - Professor at Berkeley iSchool

# Why Johnny can't encrypt

- A usability evaluation of PGP 5.0
- Main claim: the promoted ”nice and user-friendly graphical UI” was not usable at all
- A definition for usable security
- Nice showcase of how to build a credible user study
  - Believable scenarios
  - Role playing
- Main lessons:
  - UI solution should not follow the technical implementation unnecessarily
  - Speak the users’ language!

# Why Johnny can't encrypt

- 5 problems with security
  - The unmotivated user
  - Abstraction
  - Lack of feedback
  - Barn door property
  - Weakest link

# Visualisation of what?