Effort for Sensitive Data Protection to Users

Jonas Flodin Konstantinos Koukos Carl Leonardsson
Aleksandar Zeljic Johannes Åman Pohjola

Ethics Course, 7:th November 2013

Adobe Hacked 2013

- Information of 38 million active accounts stolen
  - User names
  - Encrypted passwords
  - Encrypted credit card numbers
- Flaws in security of information storage

Sony Hacked 2011

- Information of 77 million accounts stolen
- Sony fined £250 000 for lacking security
  - Out-of-date security software

- Responsibility towards Users' Data Security

Small Organizations

- Small companies
- Non-profit organizations
- Organizers of academic conference
- Your local board game club

The problem: what security responsibility does a small organization with limited resources have?

Small Organizations and Responsibility

Example: Organizing academic conference

- Hire a security expert?
- Implement it yourself?
  - Spend an evening?
  - A week?
  - A month full-time?

Data Criticality

Base security demands on type of data.

- Mail?
- Bank account / credit card number?
- Passwords?
- User name (membership in particular organization)?

Difficult to limit criticality

- Ex: Password reuse

What data is critical to each user?

Approaches

1. State of the art security
   - Impossible with limited resources?
2. No security
   - Your users may not like that...
3. Options for users of what information to store
   - Difficult for the user
   - May prevent use of service entirely
4. Security as allowed by available resources
   - Subjective
   - Judgement

Trade-off: Responsibility vs Resources

How to Ensure that the Approach is Ethical?

- Openness to user about security approach
- Openness about breaches.
- Openness to scrutiny
  - Use of open security protocols