

Social Design for Information Security

Syun Tutiya
(Chiba University)

What are we?

- Group of people from
 - Philosophy
 - Psychology
 - Sociology
 - Social psychology
 - Law/jurisprudence/social and political philosophy
 - Anthropology
- Working on preliminary study of “social design for information security”, which I will briefly talk about

Outline

- What is social design, in particular wrt information technology?
- What is information security?
- Information security and social design
 - Maturing component technology
 - Immature concept of design social interaction
 - Need for a new field as integration
- What we are interested in
 - People's consciousness of "information security"
 - Trust, reliance, etc
 - Organizations' security policy
 - Proposals for full-fledged study

Social design

- Problem of arts vs science/technology
- Component oriented research dominant and mature
- Problem of “users”, people that use systems, but they are not just users
- Human interfaces are not enough, either, because human-to-machine relation is not 1:1
- Need for designing the multiple interaction of humans and artifacts

Embedding Technology in Social Contexts?

- Yes, in a sense
- But “social contexts” are given while social interaction must be designed for certain purposes
- Technology can not designed actually
 - Motivated independent of “social contexts”
 - Technological trends unpredictable
- In case of information technology, it is beyond control

Information technology

- For the second half of 20th century
- Big shift in 70s with
 - IC, LSI and further
 - Arpanet, NSFNet, Internet and further
- Namely
 - Personalization
 - Resource sharing
- These two not very consistent but converging in terms of
 - Communication, hence society

Attitudes towards ICT

- Welcoming
 - Better communication
 - New communication
 - More business
 - Better control
- Apprehensive
 - Unknown side effects
 - Too much communication
 - Unstable business
 - No control

In reality,

- Lots of new bad things:
 - Viruses
 - Internet worms
 - Unauthorized accesses
 - Cyberattacks
 - Wiretapping
 - Anonymity (really bad?)
 - New psychological problems
 - Unstable human relations
- Better system does not necessarily help

Safety and security

- Safety
 - Against probabilistic errors
 - Against “natural” hazards
 - Against unintentional actions
- Security
 - Against non-probabilistic errors
 - Against invasions, crimes, etc
 - Against human intentional deeds

Information security, conventional

- A la OECD
 - "availability" (of data, information and information systems)
 - being accessible and usable on a timely basis in the required manner;
 - "confidentiality"
 - being disclosed only to authorized persons, entities and processes at authorized times and in the authorized manner
 - "integrity"
 - being accurate and complete and the preservation of accuracy and completeness.

Information security, modern

- Accountability
 - To guarantee the traceability back to the agent and the agent alone from the agent's acts
- Authenticity
 - To guarantee the identity of user, system, information and resources being as alleged
- Reliability
 - To guarantee the consistency between action and its effects

Conventional security

- Realized by component technology
 - Availability by backup, fault-tolerant technology
 - Confidentiality by cryptography, digital signature etc
 - Integrity by error detection etc
- But only data, information and information systems are “secured”; it is not a bad thing but users are asked to behave for systems
- So users do not cooperate and do not use the technologies, say passwords.

Security of what?

- In case of information technology
 - Security of system is just about system
 - But it is the security of system-cum-humans
 - Or humans with systems
- Newer concepts must be more respected
- Research in this direction must be done
- But so far no discipline
 - Humanities
 - Social science
 - Technology

From syntax to pragmatics

- Assembling components into a system is not enough
- Needs for humans to use technology
 - Technology for information and communication
 - Technology for preventing dysfunctioning of thereof
- What must be presupposed is
 - Psychology?
 - Sociology?
 - What else?

What we are after

- Levels of system-cum-humans
 - Individuals
 - Corporate (part society)
 - Country/Nation
 - International society
- Things to protect
 - Bodies and properties
 - Intellectual properties
 - Rights
 - Feelings

Interests in humans with systems

- Trust generation
 - In face to face situation, “marginal properties” , like tone of voice, faces, demeanors, etc contribute
 - In internet situation, people or agents can be “anonymous”, hence no “marginal properties”
 - Why?
 - No backup channels?
 - Huge system behind?
 - ??

Must be based on facts

- Need for survey on facts
 - How people feel
 - How people think
 - In different countries
 - In different kinds of corporates
 - Presented tomorrow
- Need for experiments
 - Small scale more controllable
 - Psychological and social