Usable Security

Overview and Introduction

Outline

- The Problem Area
- The Course
- Course topics
  - Overview
  - Web privacy and security
    - Semantic web
  - Ubiquitous systems
  - Privacy and Trust
  - Design
- SecurePlace

Concern

"Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be left alone". … modern enterprise and invention have, through invasions upon his privacy, subject him to mental pain and distress, far greater than could be inflicted by mere bodily injury."

"The Right to Privacy"

Warren and Brandeis

Harvard Law Review.

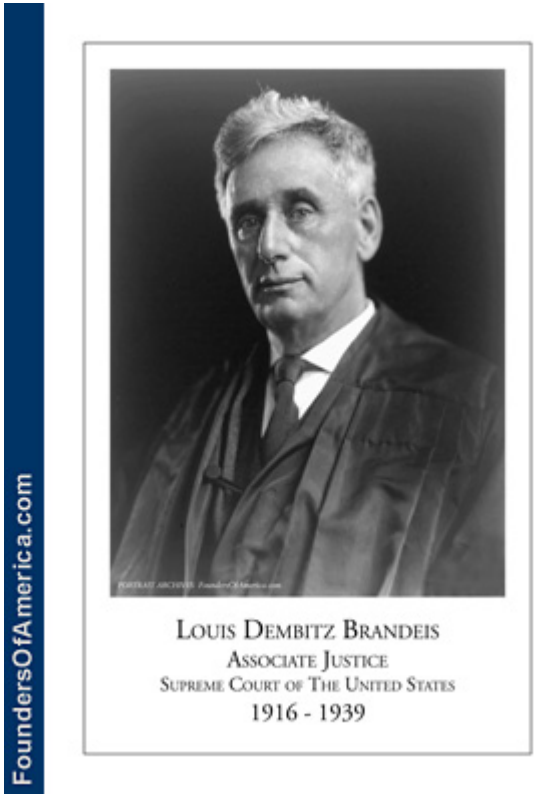
Concern

"The Right to Privacy"

Warren and Brandeis

Harvard Law Review.

Vol. IV December 15, 1890 No. 5



Promise and Peril

	Service	Threat
web	e-commerce email social networking news, entertainment search electronic medical records recommendations	identity theft spam pfishing unwanted correlation privacy incursion denial of service viruses, worms, …
ubiquitous systems	context awareness location awareness pervasive services smart objects	loss of privacy, anonymity electronic stalking invasive monitoring loss of control

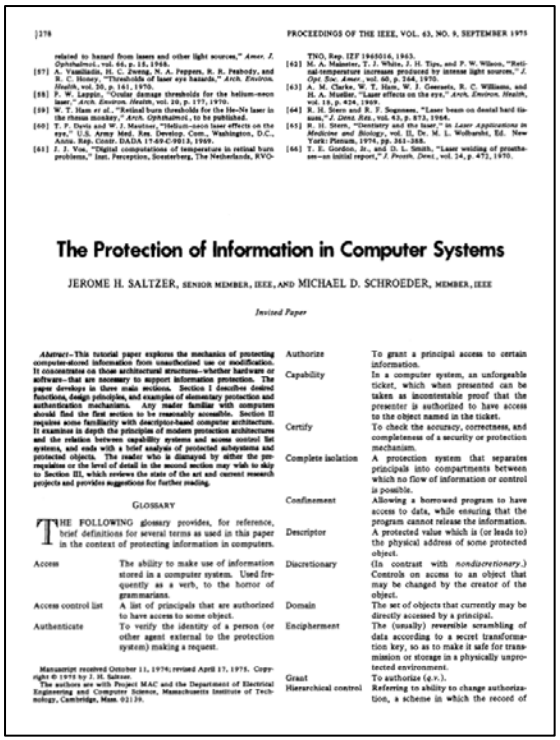
Grand Challenge

"For the dynamic, pervasive computing environments of the future, give computing end-users security they can understand and privacy they can control."

Computer Research Association (CRA), 2003. Four Grand Challenges in Trustworthy Computing, CRA Conference on Grand Research Challenges in Information Security and Assurance, Airlie House, Warrenton, Virginia, November 16–19, 2003.

Not a new issue

“ h) Psychological acceptability: It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the user's mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized. If he must translate his image of his protection needs into a radically different specification language, he will make errors.”



PROCEEDINGS OF THE IEEE, VOL. 63, NO. 9, SEPTEMBER 1975

The Protection of Information in Computer Systems

JEROME H. SALTZER, SENIOR MEMBER, IEEE, AND MICHAEL D. SCHROEDER, MEMBER, IEEE

Invited Paper

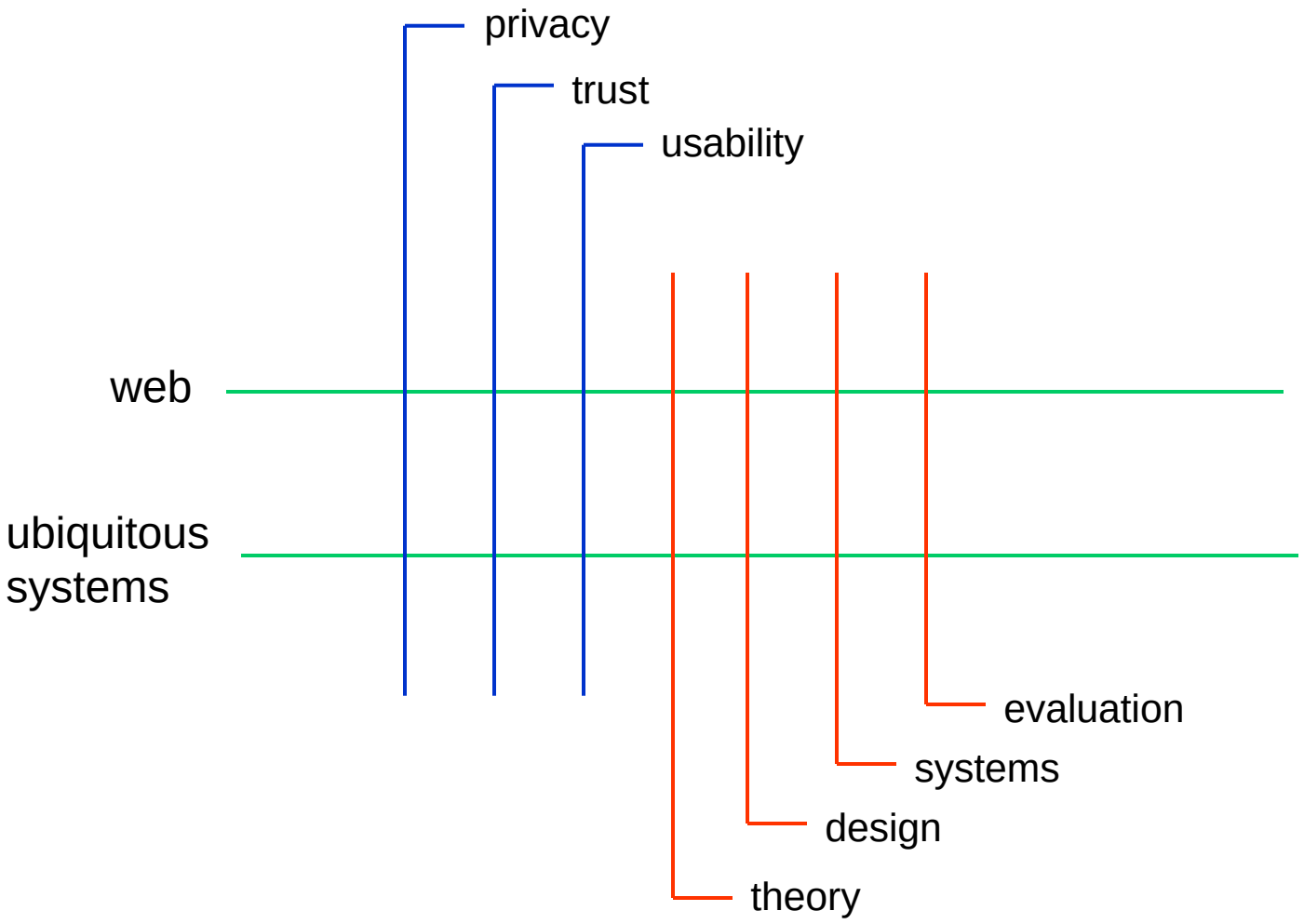
Jerome H. Saltzer and Michael D. Schroeder, The protection of information in computer systems, in *Proceedings of the IEEE*, Institute of Electrical and Electronics Engineers, Inc., 63(9), September 1975, pp.1278-1308.

Unique challenges of privacy/security

- Security is not the user's primary goal
- Must be usable by a wide range of individuals with differing skills sets
- Higher risk associated with failure of security applications than for other application types
- Need for updates to account for changes in law, organizational practices, or personal preferences.

Karat, C.-M., J. Karat, and C. Brodie, Editorial: why HCI research in privacy and security is critical now. International Journal of Human-Computer Studies, 2005. 63(1-2): p. 1-4.

Landscape of the Course



Course Information

http://courses.cs.vt.edu/cs6204/UsableSecurity

Section	Topics	Papers	Date(s)
Introduction	Course and Topic Overview	4	August 25
	Usability Studies	2	August 27
	Human factors and engineering principles	2	September 1
	Privacy in a ubiquitous world	2	September 3
Web Privacy and Security	Privacy preferences	2	September 8
	Policy authoring	2	September 10
	Privacy and Trust Frameworks/Systems	2	September 15
	Automatic Trust Negotiation	2	September 17
	Semantic Web: Foundations	3	September 22 September 24
	Semantic Web: Standards and policies	3	September 29 October 1
Ubiquitous Systems	Smart phones	4	October 6 October 8
	Medical applications	3	October 13
	Location disclosure	2	October 15
	Principles of context-aware systems	3	October 20
	Context-aware toolkits	2	October 22
Privacy and Trust	Multimedia communication	2	October 27
	Context and Place	5	October 29 November 3
	Social Factors	6	November 5 November 10
Design	Guidelines	4	November 12
	Spatial interfaces	2	November 17
	Visualization	3	November 19
Thanksgiving Break Week - No Classes			November 24
Project Presentations (final exam period also used if needed)			December 1,3,8

Semantic Web

- The Web
  - Designed for humans to read
  - Automated processing limited to simple tasks
    - rendering
    - following links
    - text-matching searches
- Semantic web
  - Designed for more machine processing
  - Based on
    - structured collections of information
    - inference rules for automated reasoning
  - A distributed knowledge representation system

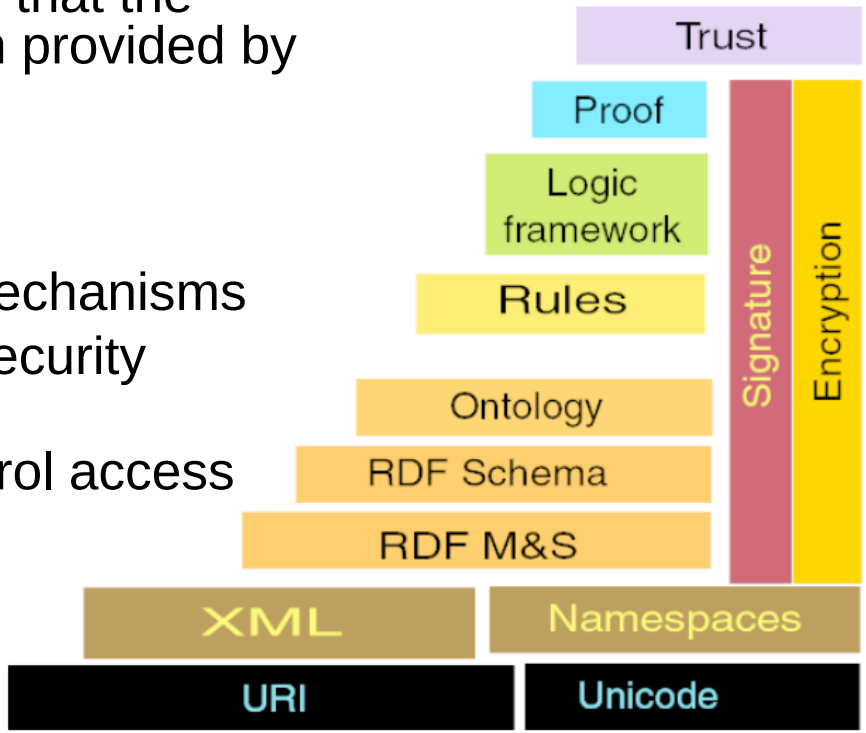
> The Semantic Web will enable machines to COMPREHEND semantic documents and data, not human speech and writings.

Semantic Web

- Technologies
  - XML – defines structure of information
  - RDF (Resource Description Framework)
    - written in XML
    - Encodes relationships as a triple (subject, relationship, object), each expressed as a URI
  - Ontologies
    - Contains
      - Taxonomy (relations among classes of items)
      - Inference rules
    - Based on Description Logics

Relationship to Security

- Semantic web relies on:
  - "…digital signatures…to verify that the attached information has been provided by a specific trusted source."
  - "*trusted* service"
- Uses for security
  - ontologies used by security mechanisms
  - policy languages to express security concepts
  - embedded information to control access



Weitzner, D.J.,Hendler, J., Berners-Lee, T., Connolly, D., "Creating the Policy-Aware Web: Discretionary, Rules-based Access for the World Wide Web", in Web and Information Security, E. Ferrari and B. Thuraisingham, Editors. 2005

Ubiquitity

- Philosophy: “The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it. …only when things disappear in this way are we freed to use them without thinking and so to focus beyond them on new goals.” (Useful also to think about security as a technology that needs to disappear.)
- Important factors
  - location
    - allows adaptation of behavior to setting
    - allows interaction with other co-located devices
  - scale (badges to large scale displays)
  - network connectivity (“The real power of the concept comes not from any one of these devices – it emerges from the interaction of all of them.”)

Weiser, M., The Computer for the 21st Century. Scientific American, 1991. 265(3): p. 94-104.

Ubiquity and security/privacy

- Creates privacy concerns:
  - "…this scenario points up some of the social issues that embodied virtuality will engender. Perhaps key among them is privacy."
  - "a single rogue tab in a room could potentially record everything that happened there."
  - "Not only corporate superiors or underlings but also overzealous government officials and even marketing firms could make unpleasant use of the same information that makes invisible computers so convenient."
- …and offers possible solution
  - "If designed into systems from the outset, [cryptographic] techniques can ensure that private data do not become public. A well-implemented version of ubiquitous computing could even afford better privacy protection than exists today."

Weiser, M., The Computer for the 21st Century. Scientific American, 1991. 265(3): p. 94-104.

Context-awareness

- "…context-aware software adapts according to the location of use, the collection of nearby people, hosts, and accessible devices, as well as to changes to such things over time."

	manual	automatic
information	proximate selection & contextual information	automatic contextual reconfiguration
command	contextual commands	context-triggered actions

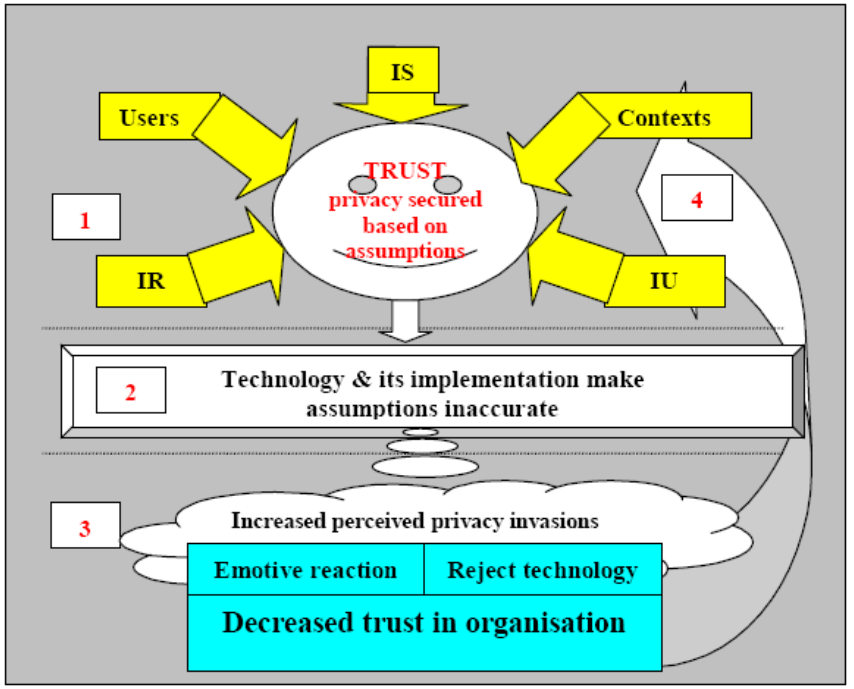
Table 1: Context-Aware Software Dimensions

Schilit, B.N., N.I. Adams, and R. Want, Context-aware Computing Applications, in Workshop on Mobile Computing Systems and Applications. 1994, IEEE Computer Society: Santa Cruz, CA, USA. p. 85-90.

Privacy and Trust

- Multimedia communications
- Context and place
- Social factors

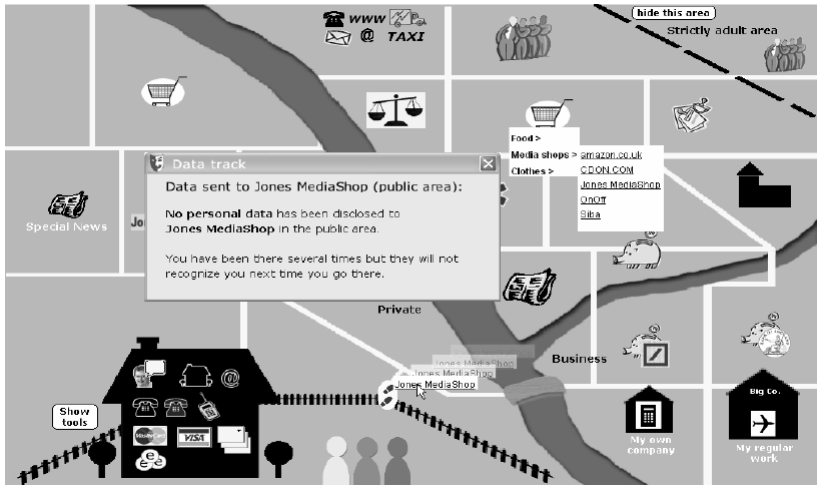
Privacy invasion cycle



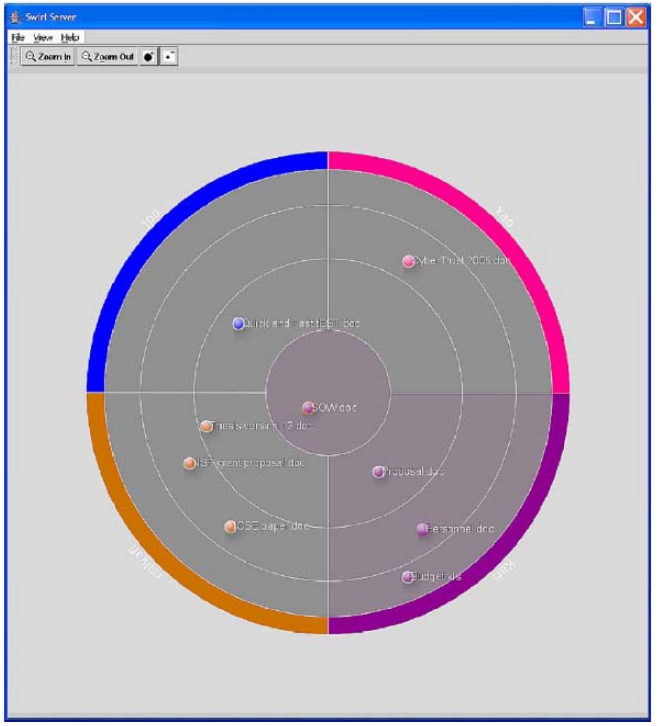
Adams, A. and A. Sasse, Privacy in Multimedia Communications: Protecting Users, Not Just Data.

Design

- Design guidelines
- Spatial interfaces
- Visualization



Bergmann, M., M. Rost, and J.S. Pettersson, Exploring the Feasibility of a Spatial User Interface Paradigm for Privacy-Enhancing Technology



de Paula, R., Ding, X., Dourish, P., Nies, K., Pillet, B., Redmiles, D. F., Ren, J., Rode, J. A., and Filho, R. S., In the eye of the beholder: a visualization-based approach to information system security.

SecurePlace

Team: Dennis Kafura, Francis Quek, Steve Harrision, Denis Gracanin

Goal: the development of an integrated set of devices, interfaces, services, and protocols which together create a usable means for ordinary individuals to have effective control of the disclosure of personal information.

Environment: socio-technical contexts, that is, technology-rich environments in which people are in direct face-to-face contact with each other but which extend beyond that place and time.

Mechanism: a system that interacts with an individual, the local ***sensed environment***, and networked information resources.

Theoretical Foundations:

- ***Place***: the spatial/physical context and its role/effect in making and realizing security decisions
- ***Embodiment***: the individual's senses and observations in making security decisions.

Scenario

Medical license

Medical records

Information disclosure

The Sensed Environment

- Attestations (e.g., medical licenses) can be
  - Authoritatively, digitally signed
  - Place specific (embedded GPC coordinates)
  - Accessed via RFID or similar technologies
- User's device
  - Access requires biometric signature (person-specific)
  - Communicates using RFID, Near Field, wireless
  - Is location aware (GPS or similar technologies)
  - Stores/generates keys to enables access to back-end servers
- Disclosure
  - Limits set by user
  - Visible to user (displayed by categories/type)
  - May require additional approval if out-of-bounds requests detected.

Key Ideas

- Tangible authorization
  - Related to mobile device
  - Physical actions of the user in the spatial context implies the desired authorization and/or disclosure
  - Based on embodiment notion of “material carrier”
- Reciprocity
  - Access to information requires identity disclosure equivalent to the subject identity acquired
  - Different levels of identity disclosure (anonymous, temporal, role, affiliation, unique identifier, full identity)
  - Allows review by subject and creates social backpressure

Systems Issues

- Mobile device
  - Platform (iPhone, Android)
  - Environment sensing
  - Interoperability
- Systems architecture
  - Semantic content of information
    - Semantic web and trust negotiation
  - Relationship to access control mechanisms
    - Part of semantic web
    - Separate from semantic web

Application Domain

- Personal Health Informatics
  - Compelling application domain
    - extreme concerns for privacy/security
    - Strong and conflicting requirements (privacy vs. accessibility to health care professionals)
  - Current focus in health-care industry
    - Stimulus funding for Electronic Medical Records
    - Growing feasibility/desire for Personal Medical Records