Electronic Security and Privacy: Expectations, Practice and Prevention

Electronic Security and Privacy: Technological, Human, Enterprise, and Legal Considerations

Perspectives
- Technology
- Human Factors & Behavior
- Public Policy and Law
- Enterprise & Business Issues
- Healthcare Information

IGERT-ESP Philosophy:

Values
- Promote privacy rights and safe information sharing, prevent from harm

Norms
- Informational, product, and service norms

Outcomes
- Principles, Frameworks, Tools, Policies, usable solutions

Current Focus Areas
- Expectations of privacy, online healthcare sharing practices, data theft prevention

Current Focus Areas

PROBLEM STATEMENT

Privacy Expectations Fail Online
- Unexpected **audiences**
- Change in social **interaction norms**
- Viral videos: e.g. Dog Poop Girl (South Korea), Star Wars Kid
- Target sent pregnancy coupons based on consumers' behavior

RESEARCH GOALS

Propose models for using mass media as educators.
- Foster **privacy literacy** and solve ambiguity
- Suggest the role of **ethical self-regulation** for protection
- Transmit and reinforce **social consensus**, **social norms**, or encourage **social change**

APPROACH

Multi-method
- Delineate evolution of privacy discourse in the media in the last century through **content analysis** and **discourse analysis**
- Exploration of **media functions** in spreading privacy literacy

I share to connect with others but I expect the network to respect my privacy

what happens to personal information posted online?

could mass media spread privacy literacy and encourage ethical self-regulation online?

EVALUATION

Measurement of frames activation and media functions
- **Descriptive statistics** and **ANOVA** to compare frame activation and media functions across time
- Multiple coders for content analysis (**intercoder reliability** will be measured for 15% of articles coded)

PUBLICATIONS & CONFERENCES

- Fornaciari, F. (forthcoming). *The language of technoself: storytelling, symbolic interactionism, and online identity*. In R. Luppicini (Ed.), Handbook of Research on Technoself: Identity in a Technological Society. IGI Global.
- Fornaciari, F. Cultural backgrounds and privacy concerns in the Web 2.0 era. Google buzz in Europe and in the United Statess. IAMCR, Cities, Creativity, Connectivity (Istanbul, Turkey, 2011).

PROBLEM STATEMENT

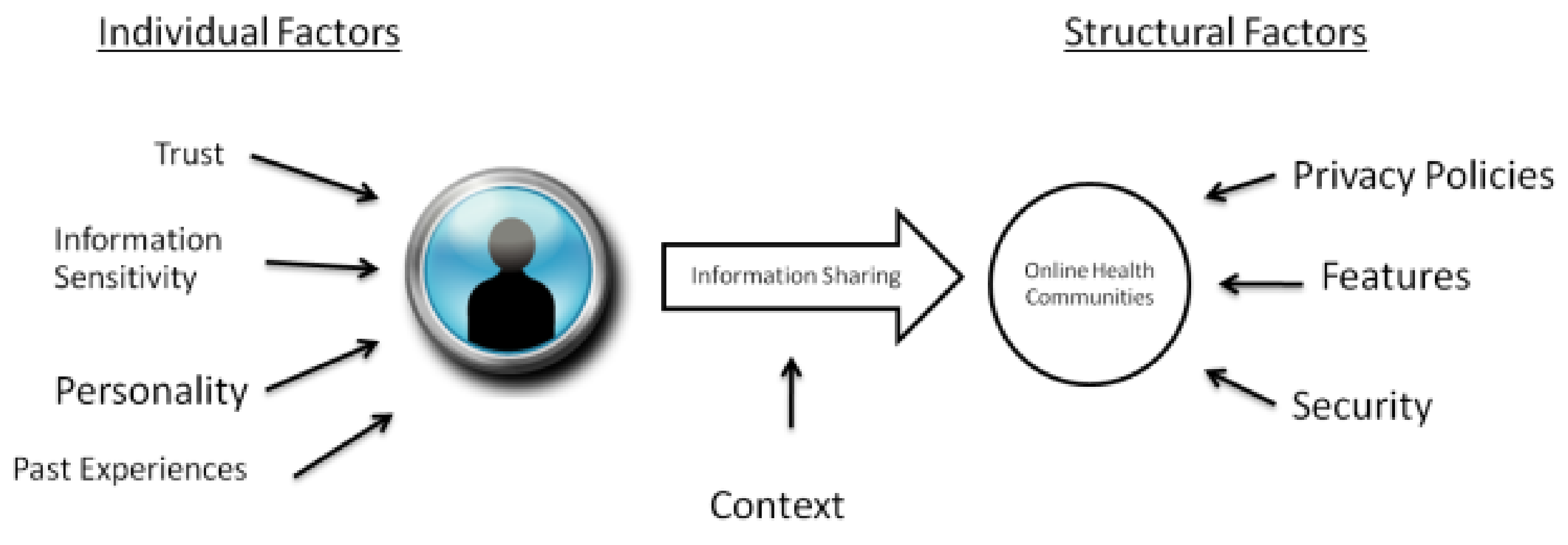
Online Health Information Privacy Paradox
- People willingly sharing private health information
- PatientsLikeMe.com (690,000 visitors/month)
- MedHelp.org (2,600,000 visitors/month)

RESEARCH GOALS

Identify driving factors behind information sharing
- To examine the role that **electronic security and privacy** play in an individuals decision making process when **sharing health information** in an online context
- To explore how the design of online health communities influence perception of **security and privacy** within the community

APPROACH

Multi-method
- Surveys to capture users degree of **trust and information sensitivity**, as well as **personality** and **perceived levels of security** within the community
- Data mining to capture actual user information sharing behavior



EVALUATION

Statistical Analysis
- **Factor Analysis, ANOVA, PLS**

Data Mining

•**Text Mining** , Posting Behavior Analysis

PUBLICATIONS & CONFERENCES

- Kuo, Benjamin; Ranganathan, Chandrasekaran, "Knowledge Contribution in Online Patient to Patient Health Care Communities" (2012). *AMCIS 2012 Proceedings (to appear)*.

PROBLEM STATEMENT

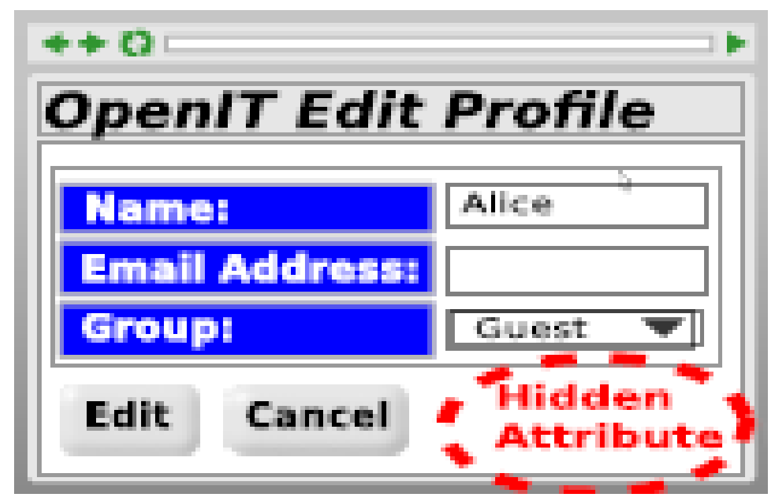
Prevention of Data Theft
- Data is **vulnerable to theft** due to inherent **security weaknesses** on the web
- Attackers can bypass security to launch attacks and steal data due to insufficient validation of user inputs (the number one cause of threats on the web according to OWASP)

RESEARCH GOALS

Identify validation weaknesses automatically
- Automated penetration testing
- Automated patching and secure code generation

APPROACH

Automatically understand application logic
- Compare client-side and server-side validation constraints
- Find mismatches in client-side and server-side validation



OpenIT Edit Profile

Name: Alice

Email Address:

Group: Guest

Example of input validation
- Client-side constraint: hidden value of *userid* refers to current user
- **Server does not validate** updates profile matching the provided *userid*
- Attacker can modify userid

EVALUATION

Working prototype
- Discovered **severe vulnerabilities** in numerous web applications used in blogs, forums, galleries, support, content management, shopping, real estate, and banking
- Aided organizations to **patch weaknesses** before hackers exploit them

PUBLICATIONS & CONFERENCES

- Skrupsky N., Monshizadeh, M., Bisht P., Hinrichs, T., Venkatakrishnan V., Zuck L. Don't Repeat Yourself: Automatically Synthesizing Client-side Validation. In the 3rd USENIX Conference on Web Application Development (To appear).
- Bisht, P., Hinrichs, T., Skrupsky, N., and Venkatakrishnan, V. WAPTEC: Whitebox Analysis of Web Applications for Parameter Tampering Exploit Construction (CCS'11). ACM Conference on Computer and Communications Security.

UIC UNIVERSITY OF ILLINOIS AT CHICAGO

This work has been funded with support from NSF under the IGERT Grant Number 1069311