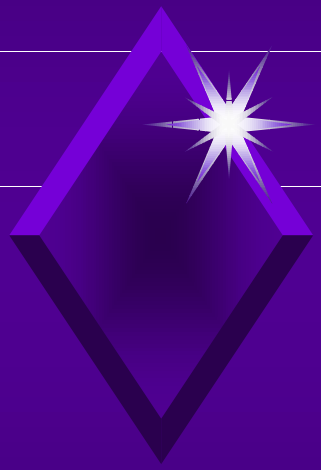
User-Centered Security

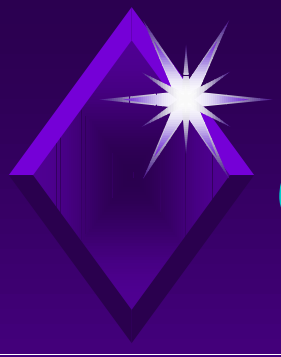


Oxymoron or Inevitability?

Mary Ellen Zurko

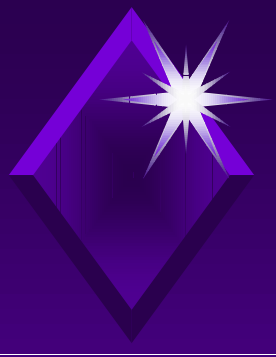
Iris Associates

mzurko@iris.com



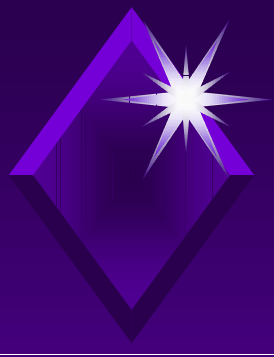
Overview

- Cultural conflict
  - The user-centered view
  - The traditional information security view
- Cultural agreement
- Problem areas
- Areas for synthesis



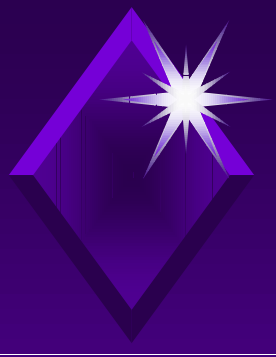
The User's Bill of Rights, Clare-Marie Karat

- The user is always right. If there is a problem with the use of the system, the system is the problem, not the user.
- The user has the right to be in control of the system [...].
- The user has the right to a system that provides clear, understandable, and accurate information regarding the task it is performing and the progress toward completion.



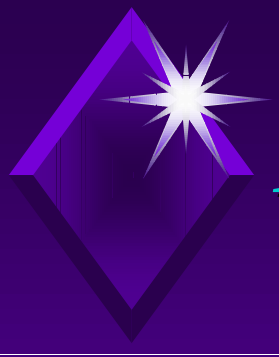
Security Survival, The Open Group

- The main purpose of information security is to [...] protect and preserve the organization's information and computing assets in a cost-efficient manner.
- [Information security] requires the cooperation of the administrator, programmers and users.
- Technology alone cannot compensate for inadequate administration [or] user error, so the procedural aspects [...] will be just as important [...].



User-Centered Security Overlap

- The user has the right to a system that performs exactly as promised.
- 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.
- The set of supported measures offers added value to users, enhancing rather than restricting the set of capabilities available to users.



Problem Areas

- Who is the user?
  - Person with information to protect or convey
  - Person wanting to see information
  - Institution[s], if any
- Smart engineer syndrome vs. actual user data
- Easier to "fail safe" and force the user to adapt
- Process and results of design of security standards explicitly ignores user issues
- Least privilege

Areas for Synthesis

- Usability techniques (particularly testing) for security software
- Security and privacy for applications with a clear user model (CSCW)
- Explicitly including the user in the model of the secure system
- User-centered design of functions of secure systems (e.g. scenario based design)