New Ideas

Borrowing From Other Areas

Mary Ellen (Mez) Zurko
Open Group Research Institute

http://www.osf.org/~zurko/
zurko@osf.org
User Centered Intrusion Detection?

• Add usability testing
  – To ID test suites
  – To determine what to audit

• Enable users to use their knowledge to detect intrusion and misuse
  – The watchers watch the watchers
  – Minimize adversarial relationship
  – Distribute trust between technology and people
  Example: Misuse of CPU
User Centered Intrusion Detection?

- ID checks that policy is being properly enforced
  - Share authorization policy database
- Policy language work in both areas
  - Share syntax or semantics
- Use audit data for history-based authorization policies
User Centered Security

• Deep synthesis of security and usability

• Computer Human Interface (CHI)
  – Emphasis on understanding the end user
  – Users do things for a reason
  – Reliance on training is suspect
  – Iterative usability testing is the back bone
    • Early and often
Other Aspects of Security Management

• Trust management
  – Merges Authentication and Authorization
  – Policy Maker, SDSI

• Merge aspects of intrusion
  – Detection and authorization