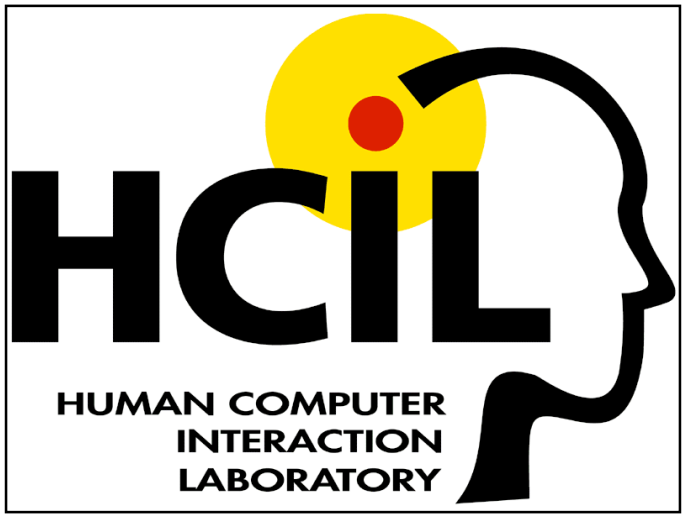
Human-Computer Interaction Opportunities for Improving Security/Privacy

Ben Shneiderman *ben@cs.umd.edu*

Founding Director (1983-2000), Human-Computer Interaction Lab
Professor, Department of Computer Science
Member, Institutes for Advanced Computer Studies &
Systems Research

UNIVERSITY OF MARYLAND

HCIL



Interdisciplinary research community

- Computer Science & Psychology
- Information Studies & Education

(www.cs.umd.edu/hcil)

HCIL

User Interface Design Goals

- **Cognitively comprehensible:**
  Consistent, predictable & controllable

- **Affectively acceptable:**
  Mastery, satisfaction & responsibility

NOT:

~~Adaptive~~, ~~autonomous~~ & ~~anthropomorphic~~

Scientific Approach (~~beyond user friendly~~)

- Specify users and tasks
- Predict and measure
  - time to learn
  - speed of performance
  - rate of human errors
  - human retention over time
- Assess subjective satisfaction

  (Questionnaire for User Interface Satisfaction)
- Accommodate individual differences
- Consider social, organizational & cultural context

HCIL

Design Issues

- Input devices & strategies
  - Keyboards, pointing devices, voice
  - Direct manipulation
  - Menus, forms, commands
- Output devices & formats
  - Screens, windows, color, sound
  - Text, tables, graphics
  - Instructions, messages, help
- Collaboration & communities
- Manuals, tutorials, training

www.awl.com/DTUI

HCIL

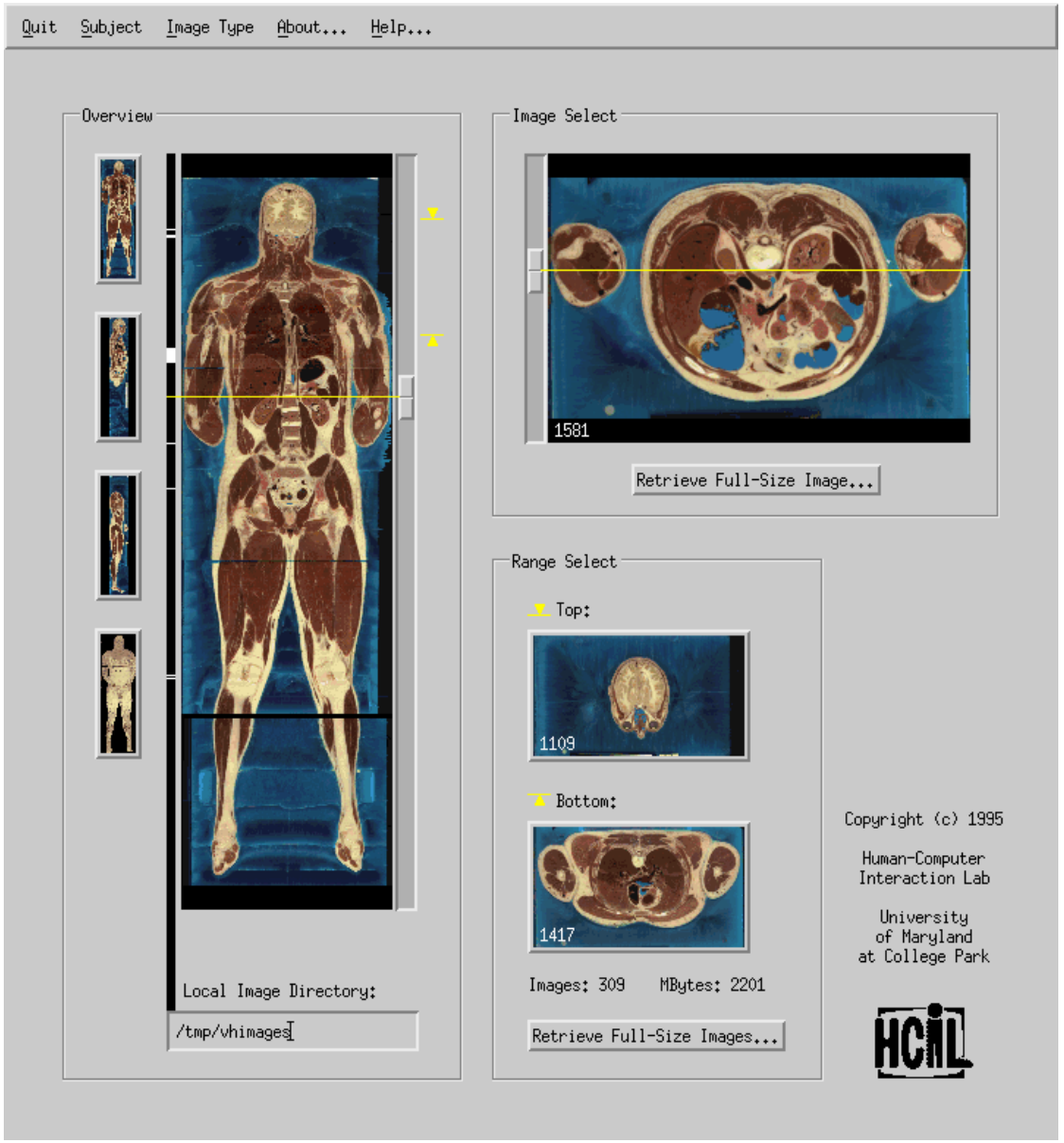
U.S. Library of Congress

- Scholars, Journalists, Citizens
- Teachers, Students

HCIL

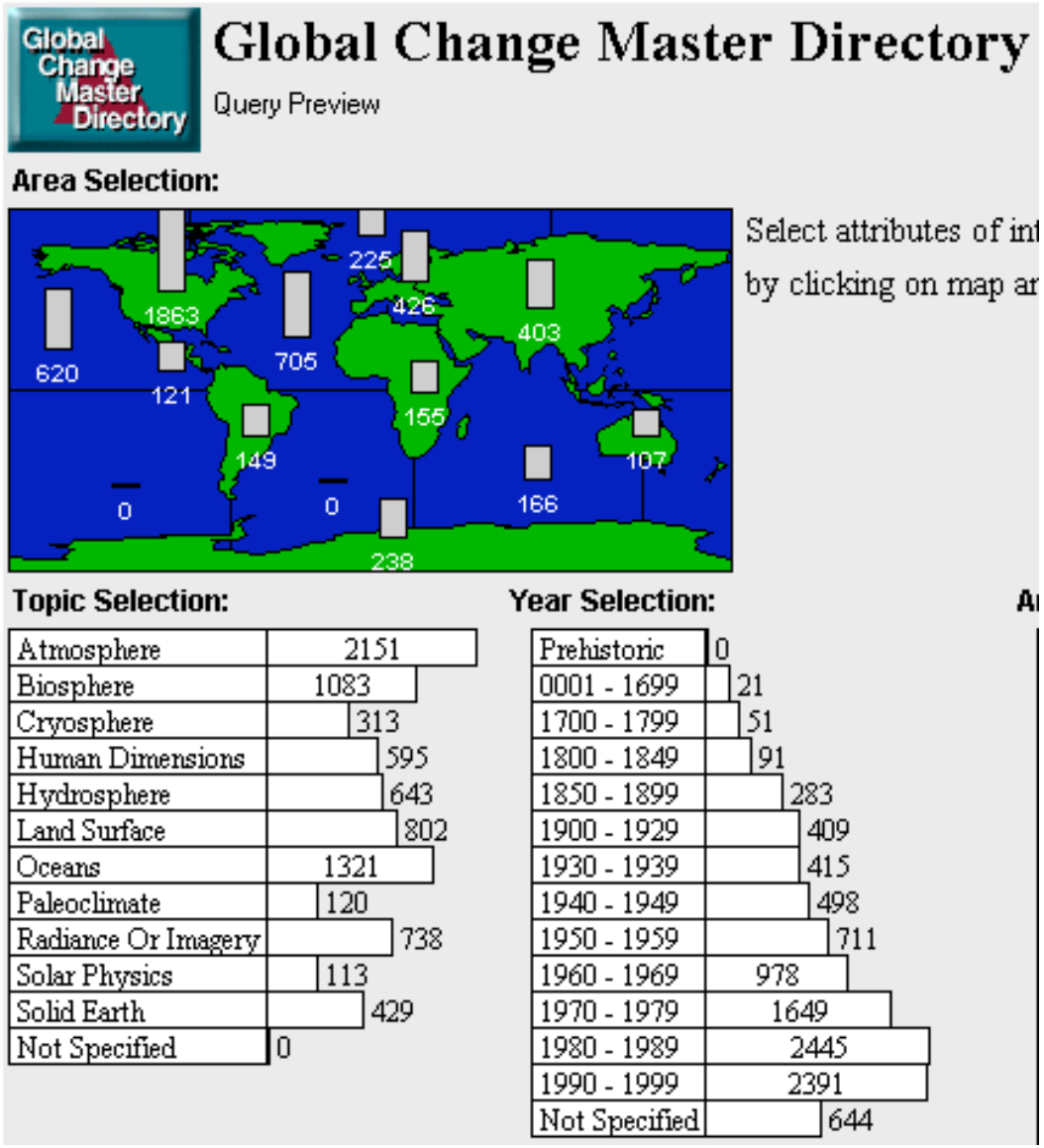
Visible Human Explorer (NLM)

- Doctors
- Surgeons
- Researchers
- Students



NASA Environmental Data

- Scientists
- Farmers
- Land planners
- Students



Bureau of the Census

- Economists, Policy makers, Journalists
- Teachers, Students

American FactFinder™

NSF Digital Government Initiative

Census,

NCHS,

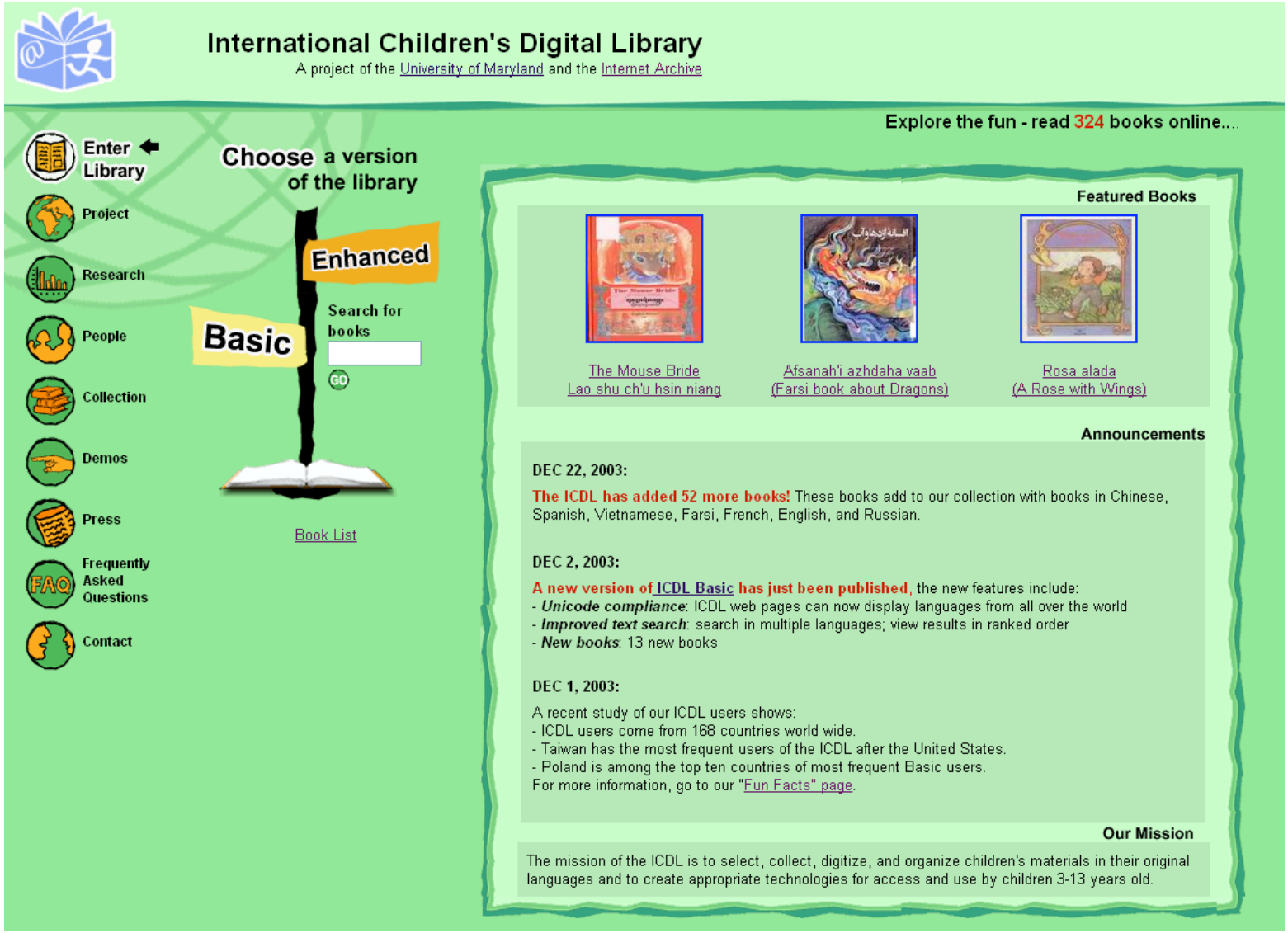
BLS, EIA,

NASS, SSA

- Find what you need
- Understand what you Find

www.ils.unc.edu/govstat/

International Children’s Digital Libary



www.icdlbooks.org

Piccolo: Toolkit for 2D zoomable objects

Structured canvas of graphical objects in a hierarchical scenegraph

- Zooming animation
- Cameras, layers

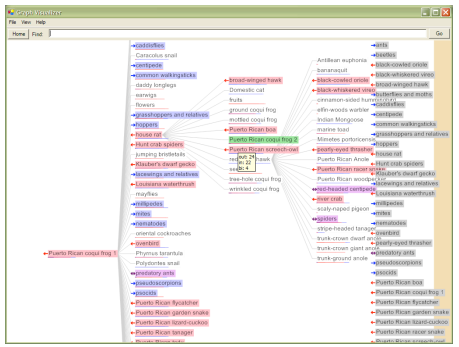
Open, Extensible & Efficient

Java, C#, PocketPC versions

www.cs.umd.edu/hcil/piccolo

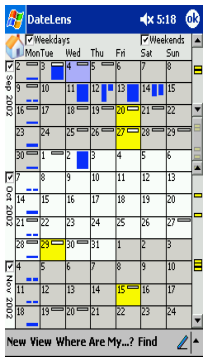
AppLens & Launch Tile

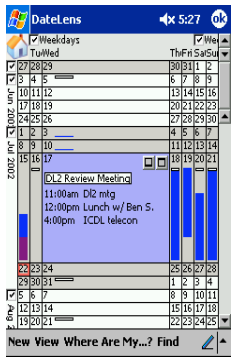
UMD, Microsoft Research



TreePlus

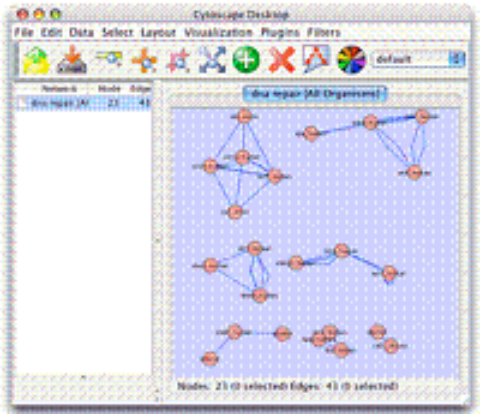
UMD





DateLens

Windsor Interfaces, Inc.



Cytoscape

Institute for Systems Biology

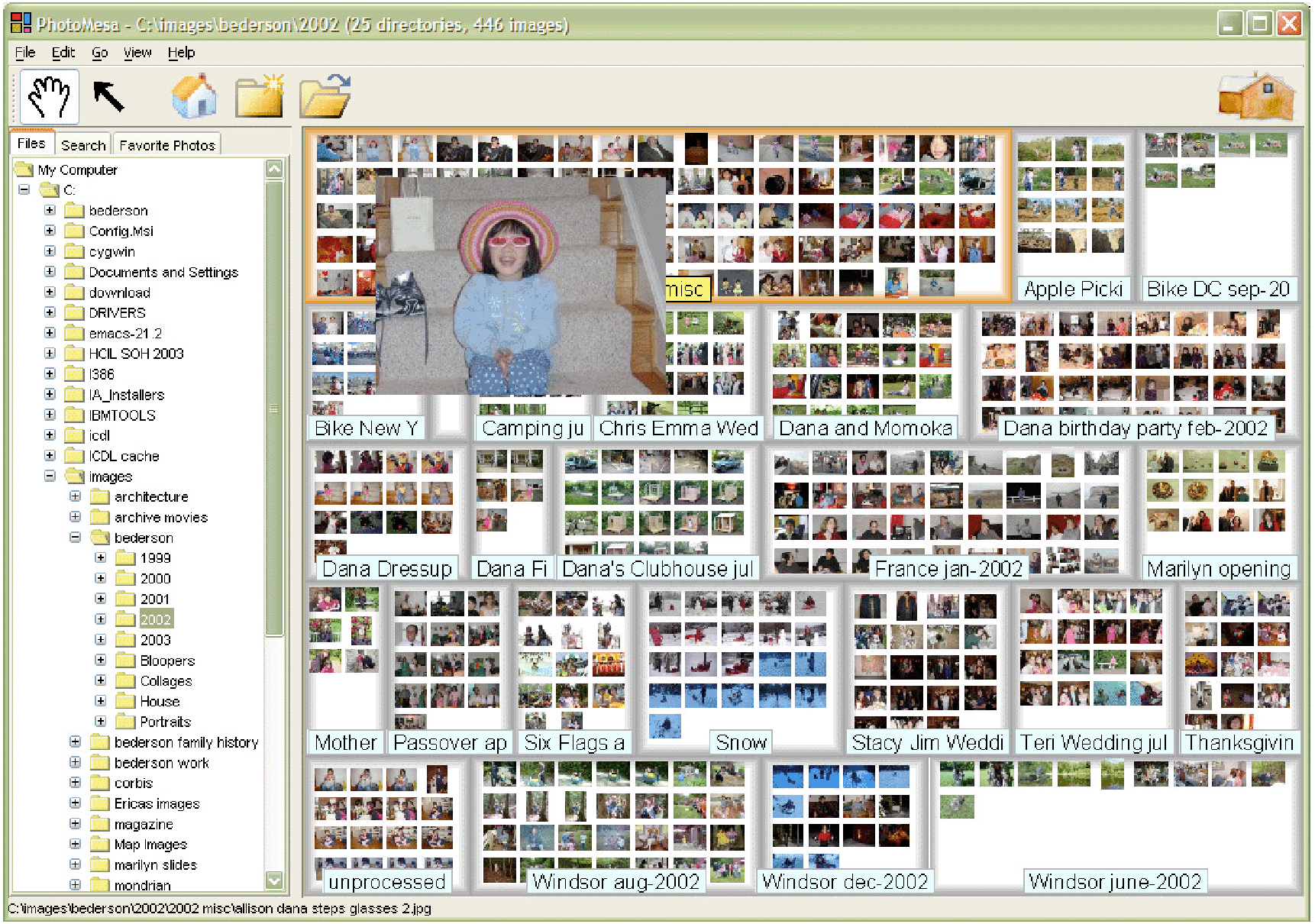
Memorial Sloan-Kettering

Institut Pasteur UCSD

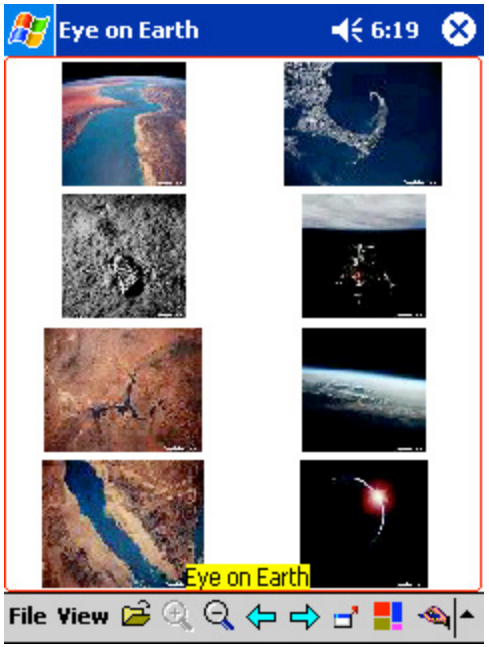
HCIL

PhotoMesa

www.cs.umd.edu/hcil/photomesa



Pocket PhotoMesa



CRA Grand Challenges, 2003

4) For the dynamic, pervasive computing environments of the future, give endusers:

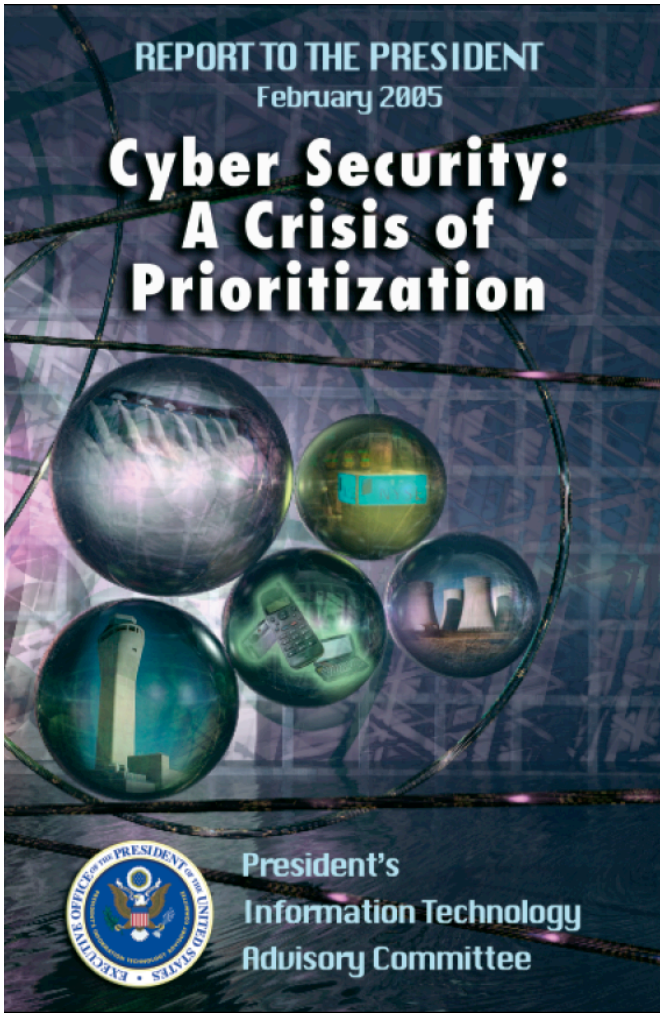
- security they can understand
- privacy they can control.

  - patient health record
  - electronic voting
  - law enforcement databases
  - financial management

http://www.cra.org/Activities/grand.challenges/security/

HCIL

PITAC Report, 2005 - Challenges



For end-users:

Incorrectly used software or hostile or confusing user interfaces can lead to user frustration and unauthorized workarounds that can compromise even the most robust security schemes.

For operators:

Usable presentation interfaces that allow operators to better understand incidents in progress.

http://www.nitrd.gov

HCIL

Profusion of Concepts for Security/Privacy

Personal computing was easier

- File protection vs sharing
- Passwords & Access Control

Networking adds complexity

- Firewalls & Virtual Private Networks
- Cookies: good or bad?
- Trusted sources & Digital signatures
- Certificates & Authentication
- Viruses & Worms

HCIL

Profusion of Concepts for Security/Privacy

Goals

- Availability: Accessible when needed
- Confidentiality: Crypto & limit access
- Data integrity: Prevent modifying your data
- Control: Access rights & physical security
- Audit: Logging, review & damage assessment

HCIL

Profusion of Concepts for Security/Privacy

Goals

- Availability: Accessible when needed
- Confidentiality: Crypto & limit access
- Data integrity: Prevent modifying your data
- Control: Access rights & physical security
- Audit: Logging, review & damage assessment

Most current systems present the user with an intricate interface for specifying his protection needs. The result is that the user has trouble figuring out how to make the specification and verifying that he requested the right thing. User interfaces that more closely match the mental models people have of information protection are needed.

HCIL

Profusion of Concepts for Security/Privacy

Goals

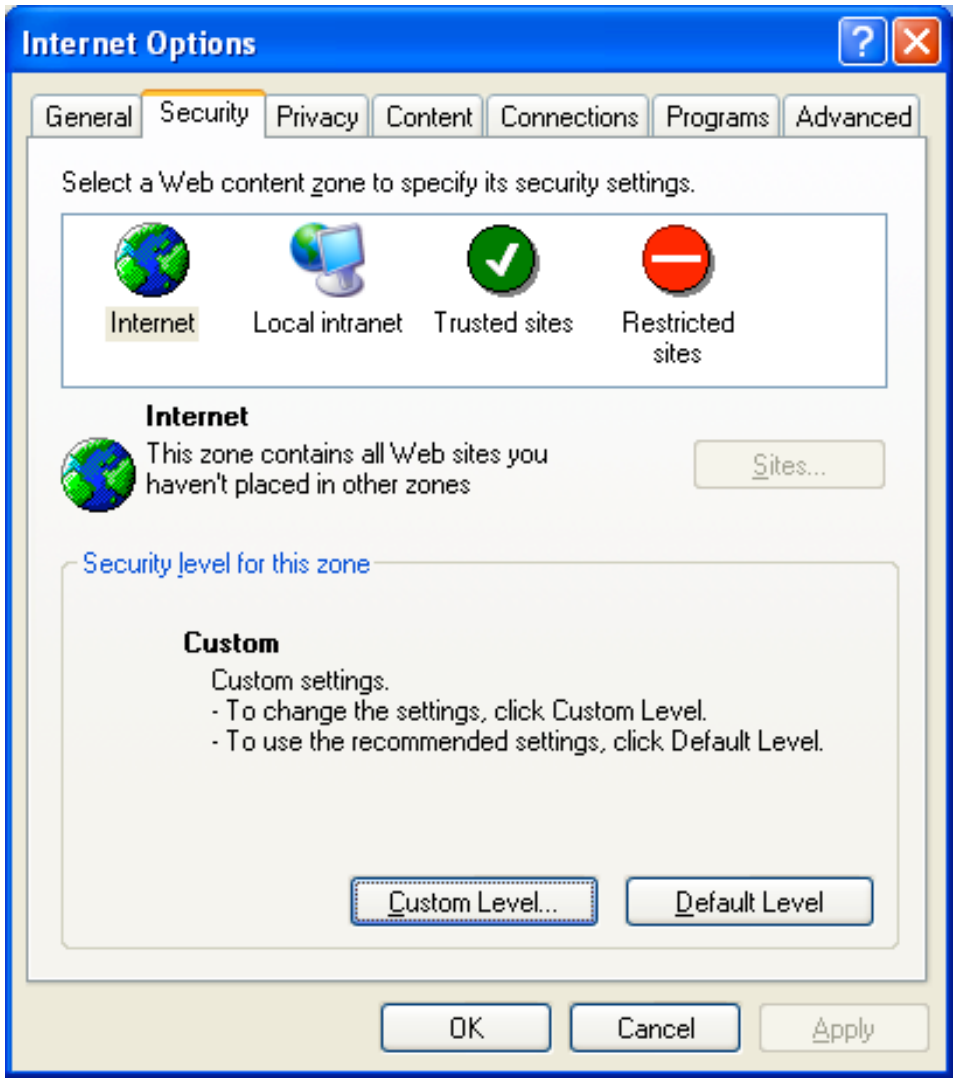
- Availability: Accessible when needed
- Confidentiality: Crypto & limit access
- Data integrity: Prevent modifying your data
- Control: Access rights & physical security
- Audit: Logging, review & damage assessment

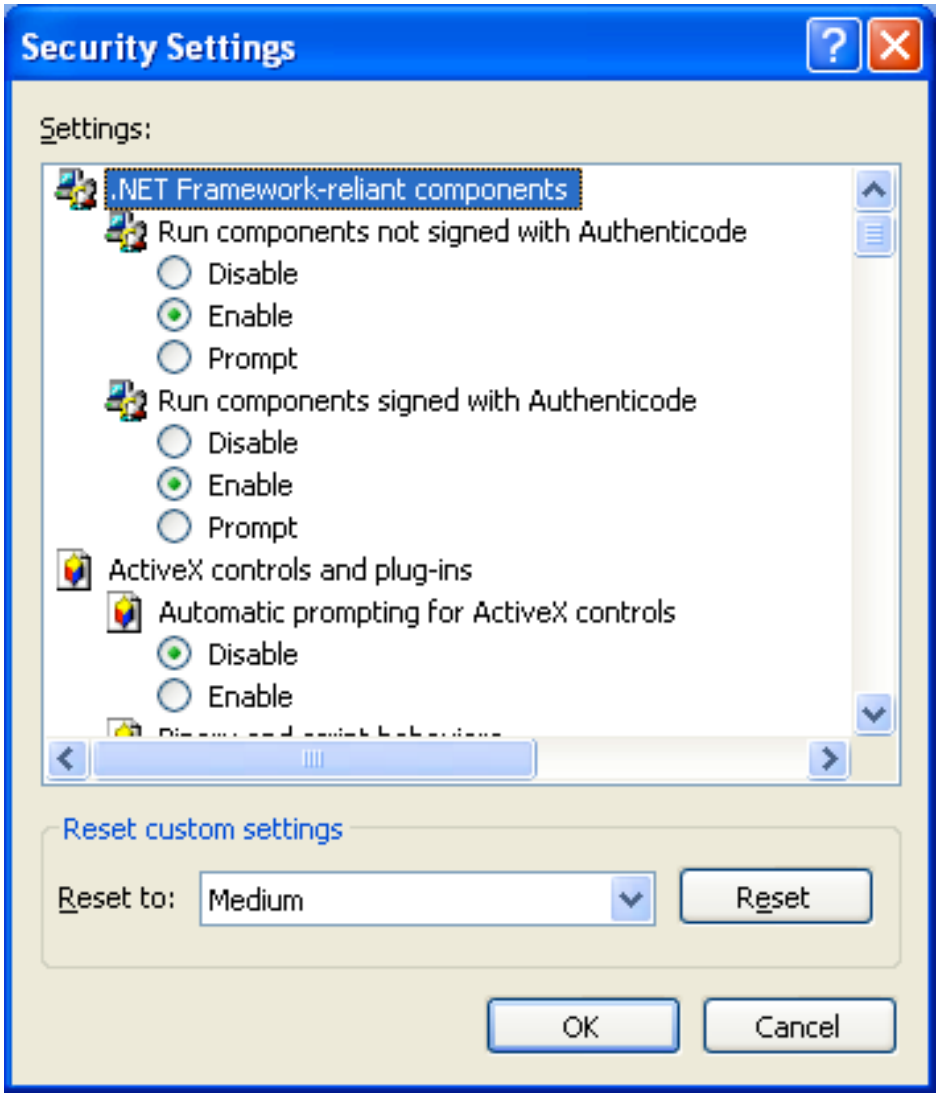
Most current systems present the user with an intricate interface for specifying his protection needs. The result is that the user has trouble figuring out how to make the specification and verifying that he requested the right thing. User interfaces that more closely match the mental models people have of information protection are needed.

Saltzer & Schroeder, 1975

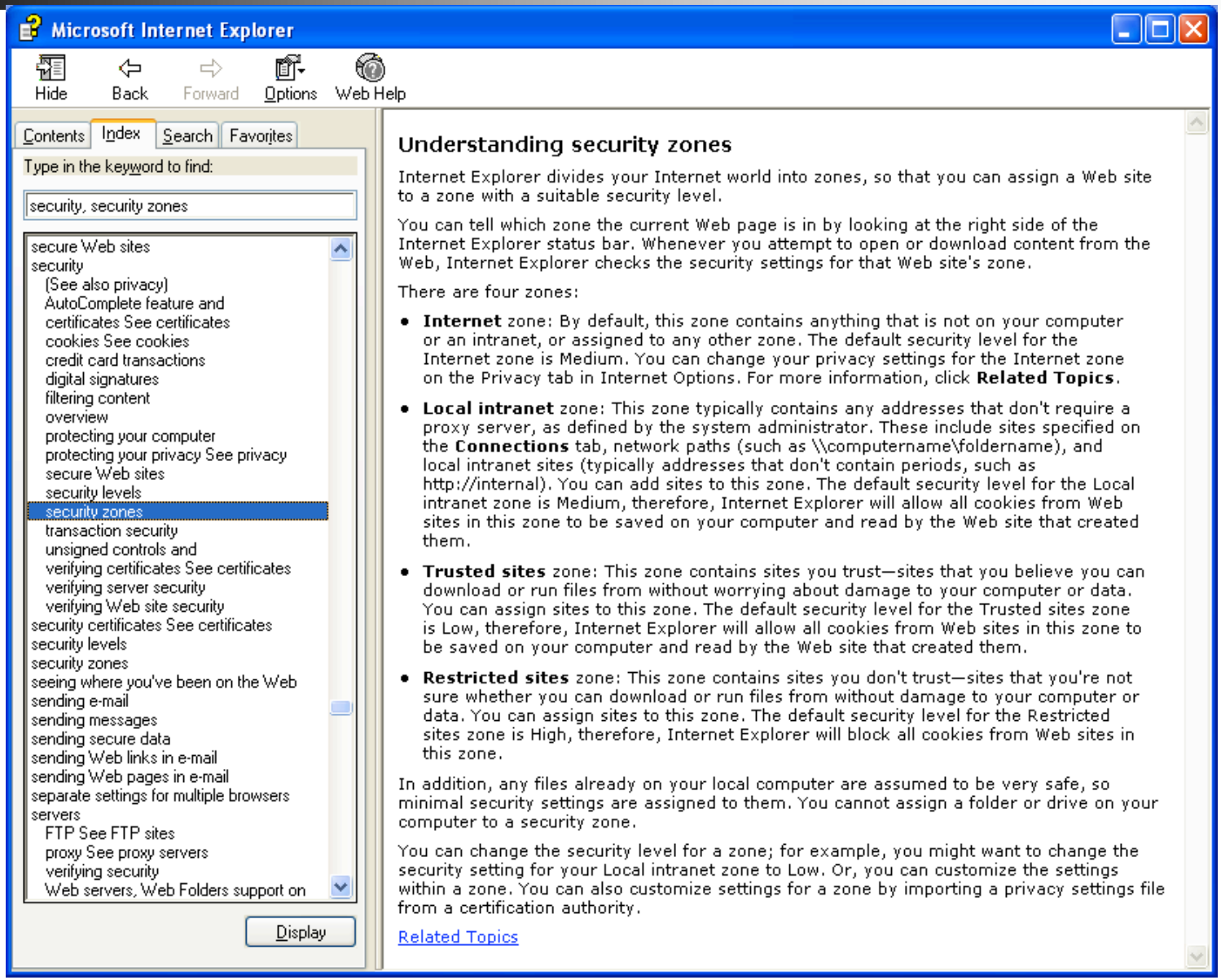
HCIL

Security setting - IE

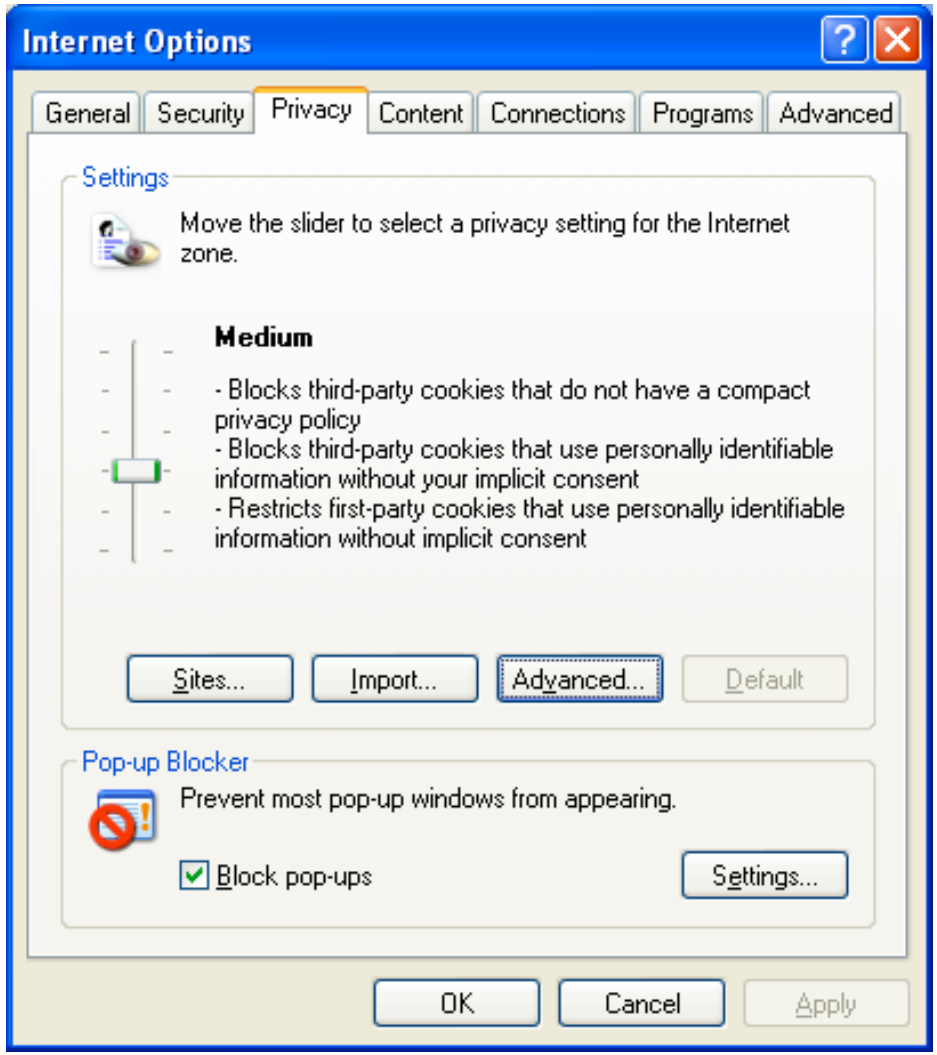


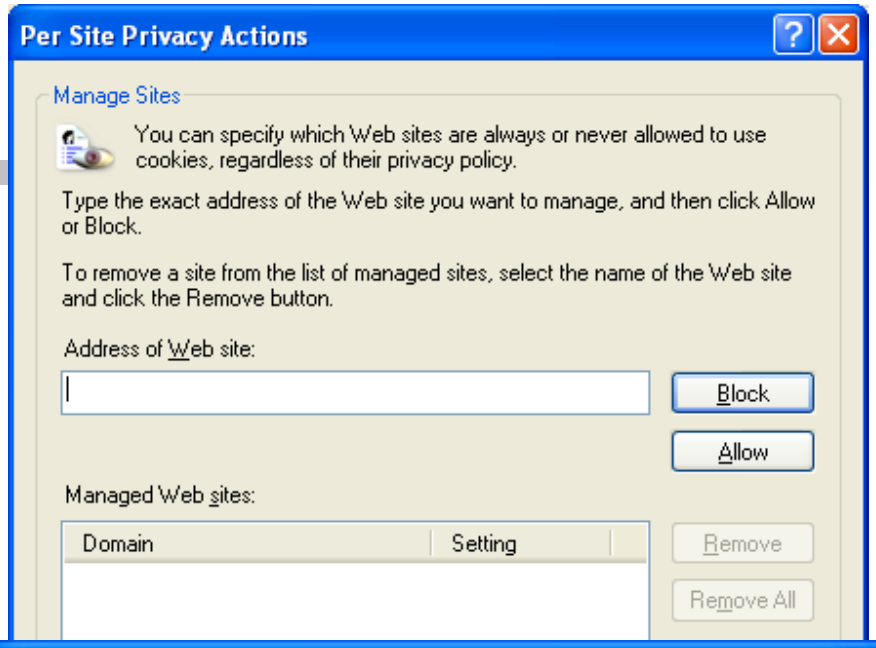


Security zones – Online Help

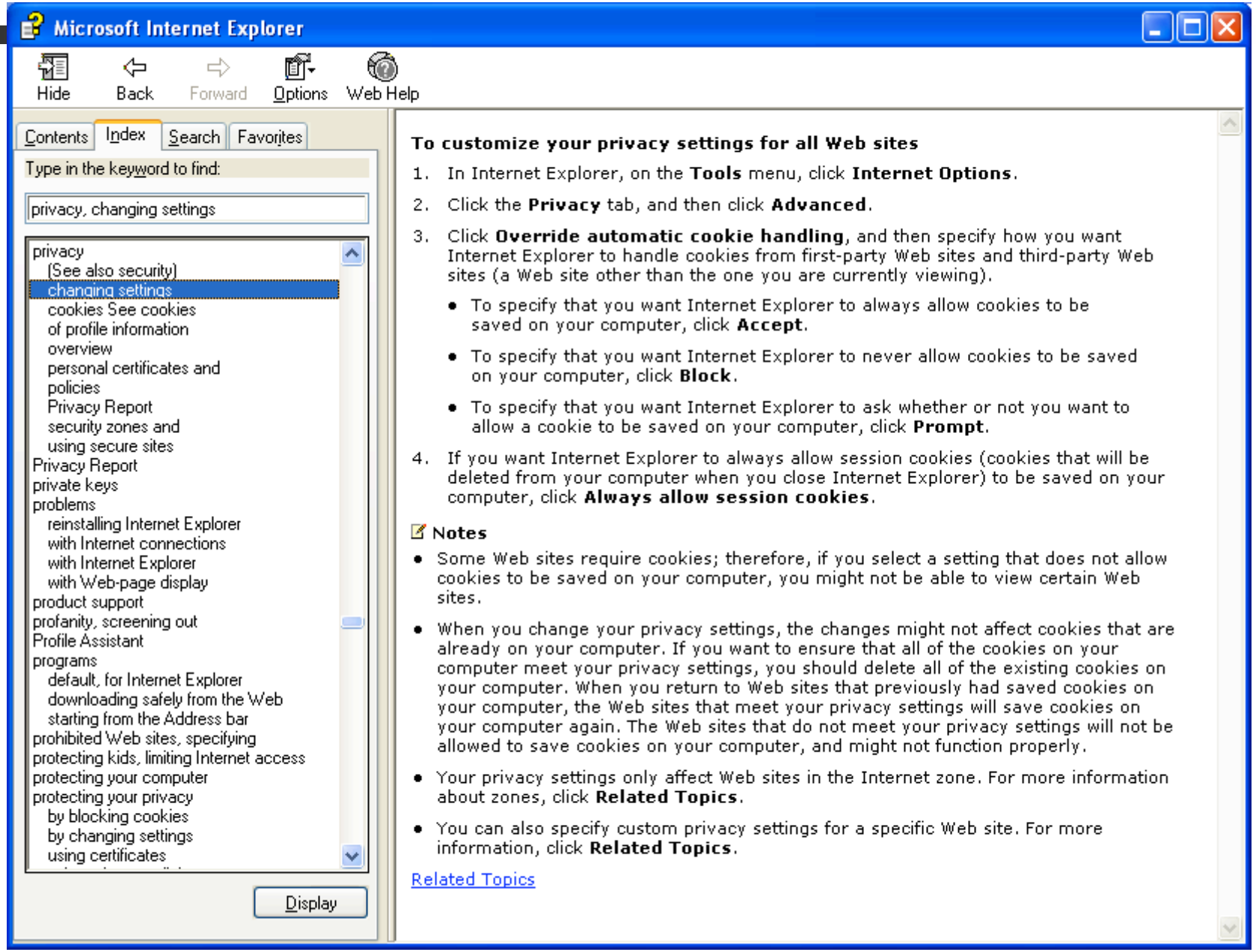


Privacy setting

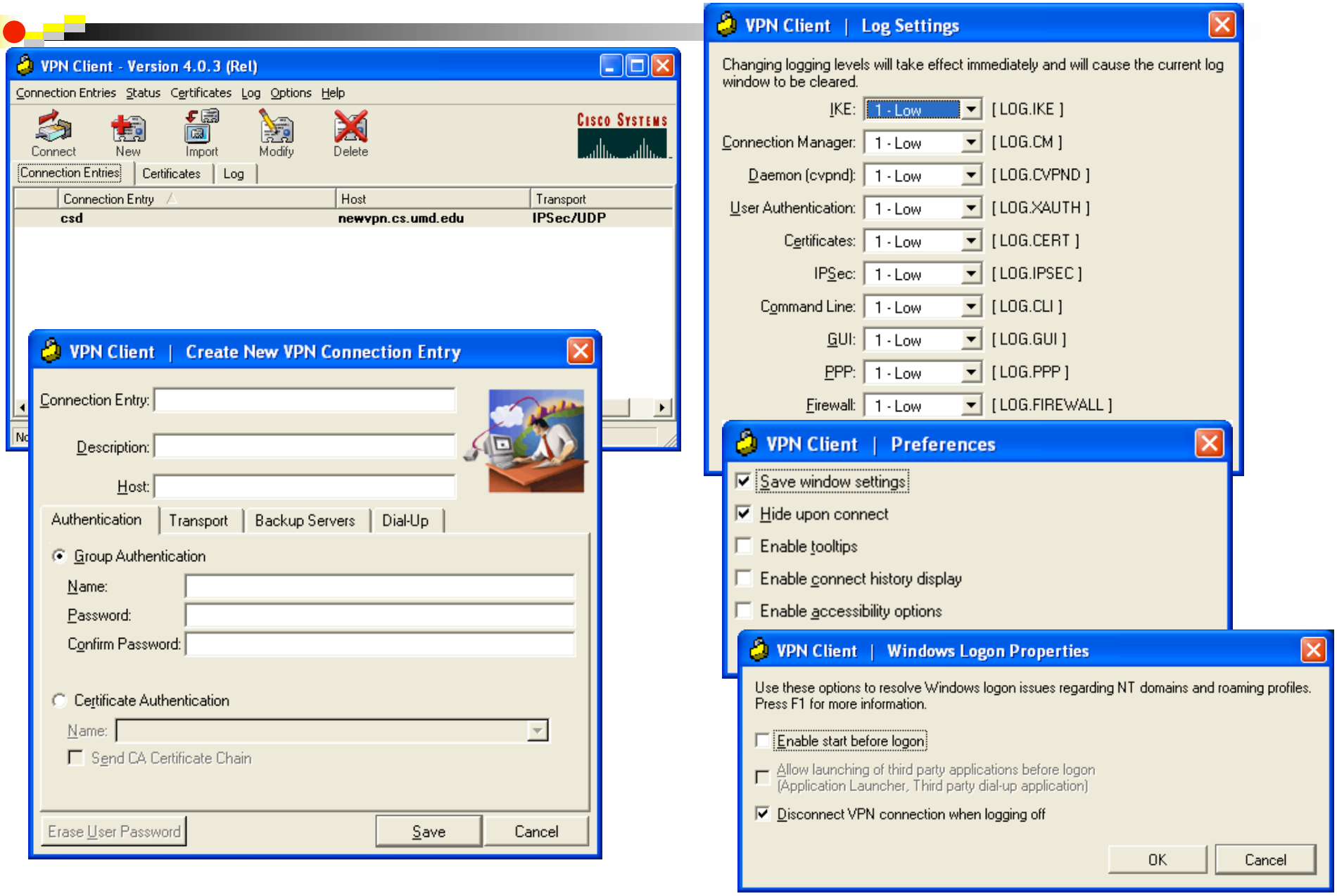




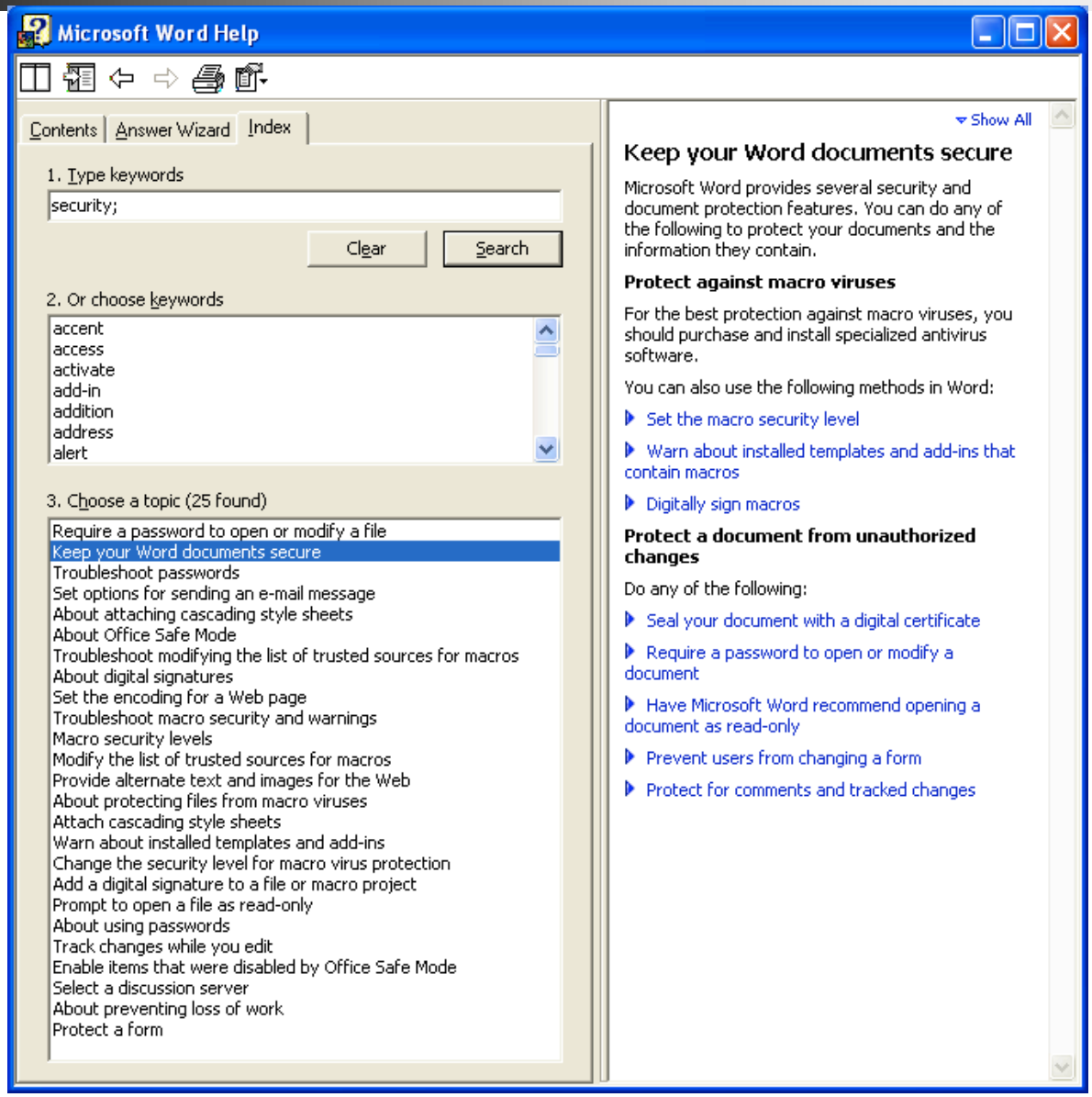
Privacy setting – Online Help



VPN Virtual Private Network



MS Word Security



Emerging Research

- Saltzer & Schroeder, IEEE, 1975
- Adams & Sasse, *CACM*, 1999
- Whitten & Tygar, USENIX, 1999
  "Why Johnny Can't Encrypt"
- Gene Spafford, Purdue Univ
  Center for Education and Research Information and Assurance and Security
- Ka-Ping Yee, UC-Berkeley, 2002

HCIL

Guidelines

Match the most comfortable way to do tasks
with the least granting of authority

Grant authority to others in accordance
with user actions indicating consent

Offer the user ways to reduce others' authority
to access the user's resources

Maintain accurate awareness
- of others' authority as relevant to user decisions
- the user's own authority to access resources

K-P Yee, http://www.sims.berkeley.edu/~ping/sid/

HCIL

Guidelines

Protect the user's channels to agents that manipulate authority on the user's behalf

Enable the user to express safe security policies in terms that fit the user's task

Draw distinctions among objects and actions along boundaries relevant to the task

Present objects and actions using distinguishable, truthful appearances

Indicate clearly the consequences of decisions that the user is expected to make

K-P Yee, http://www.sims.berkeley.edu/~ping/sid/

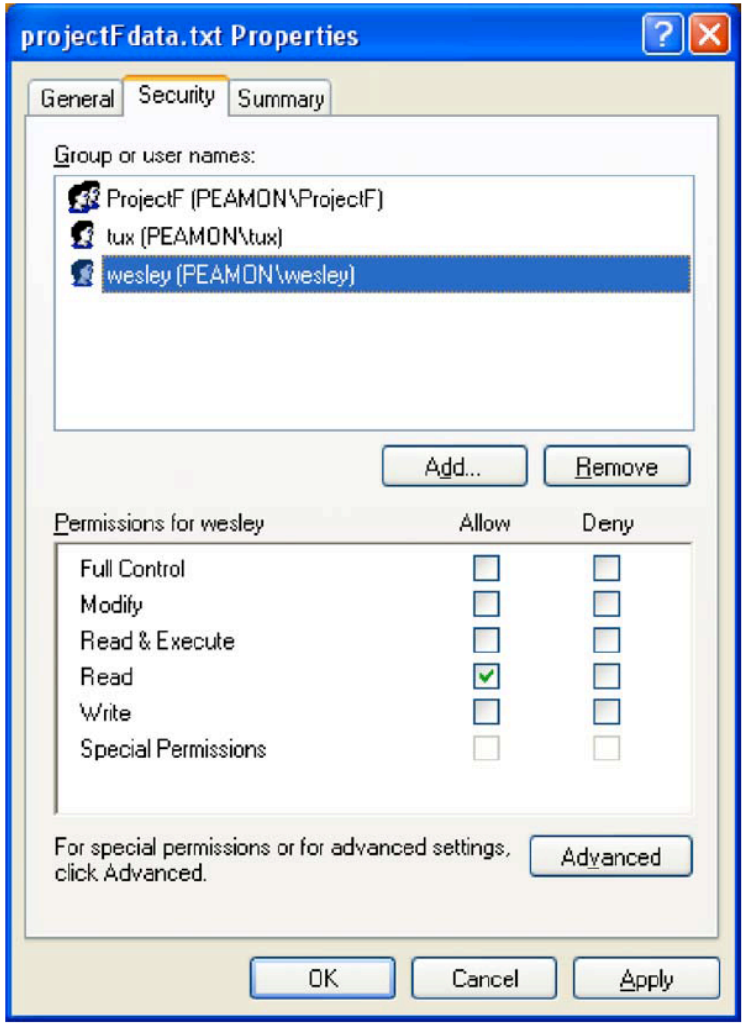
HCIL

Emerging Research

- Good & Krekelberg, CHI 2003, Kazaa
- Simson Garfinkel, MIT, 2004 (David Clark, Rob Miller)
- Lorrie Cranor, CMU
  - Center for Usable Privacy and Security (CUPS)
  - Symposium on Usable Privacy and Security (SOUPS 2005)
- Karat, Karat & Brodie, IJHCS 2005 Special Issue: HCI Privacy & Security

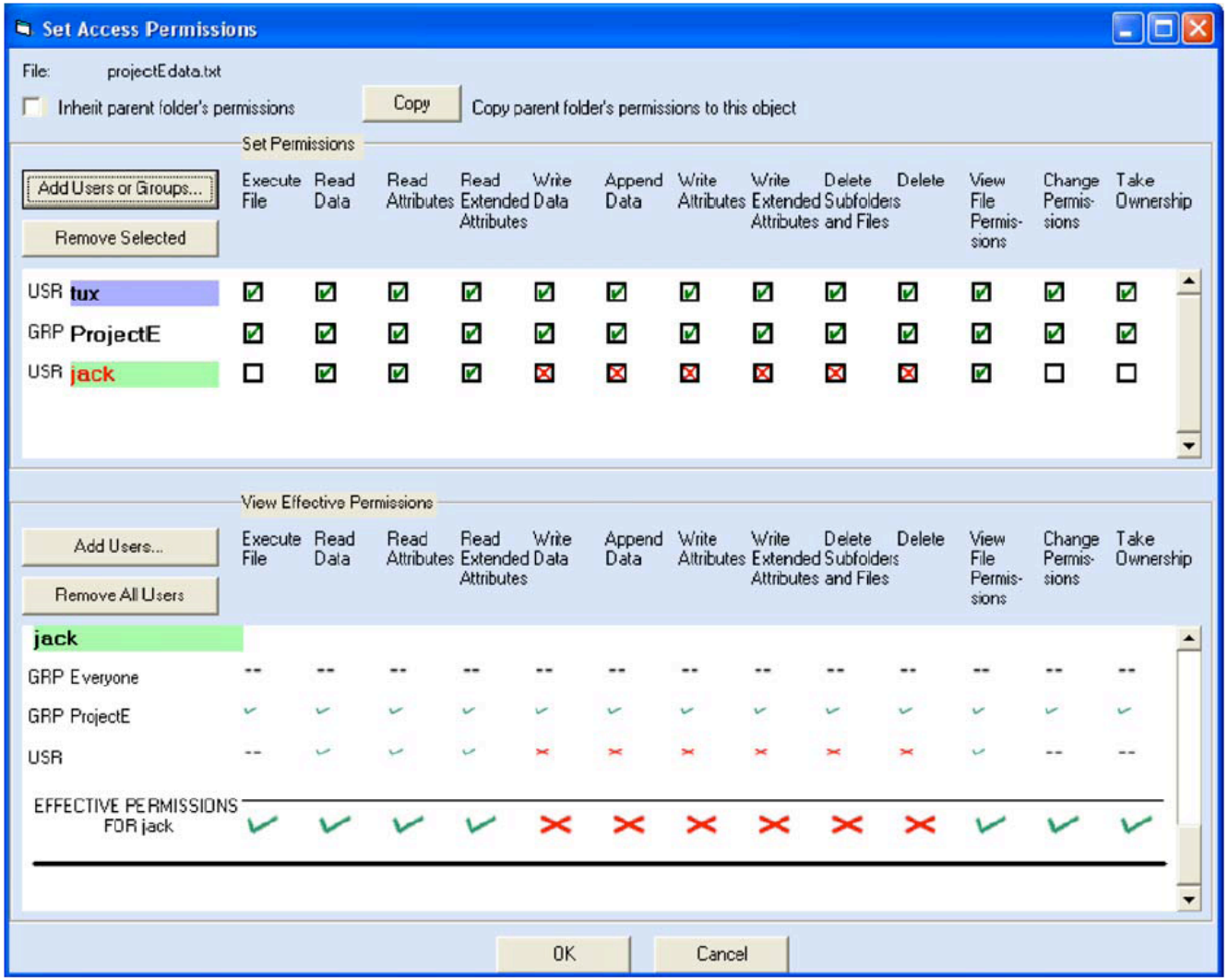
HCIL

Controlled Experiment: XPFP



(Maxion & Reeder, IJHCS Special Issue, 2005)

Controlled Experiment: Salmon



(Maxion & Reeder, IJHCS Special Issue, 2005)

Controlled Experiments

- 12 subjects for each interface

Tasks	% done	
	XPFP	Salmon
W	58	83
J	25	100
T	75	100

Errors	
XPFP	Salmon
9	4
16	6
3	0

- Successful users: XPFP=178s Salmon=61s

(Maxion & Reeder, IJHCS Special Issue, 2005)

HCIL

Possible Strategies

- Multi-layer interface that:
  - Ties increasing complexity to increasing control
  - Permits evolutionary learning as needed
- Cleaner cognitive model
  - Fewer objects & actions
  - Clearer feedback about decisions
- Show consequences of decisions
- Show dynamics of activity with viewable log

HCIL

Commercial Practice - Usability Engineering

- User-centered design processes
  - Contextual Design - Beyer and Holtzblatt
  - Participatory Design
- Guidelines documents and processes
- User interface building tools
- Expert reviews and usability testing

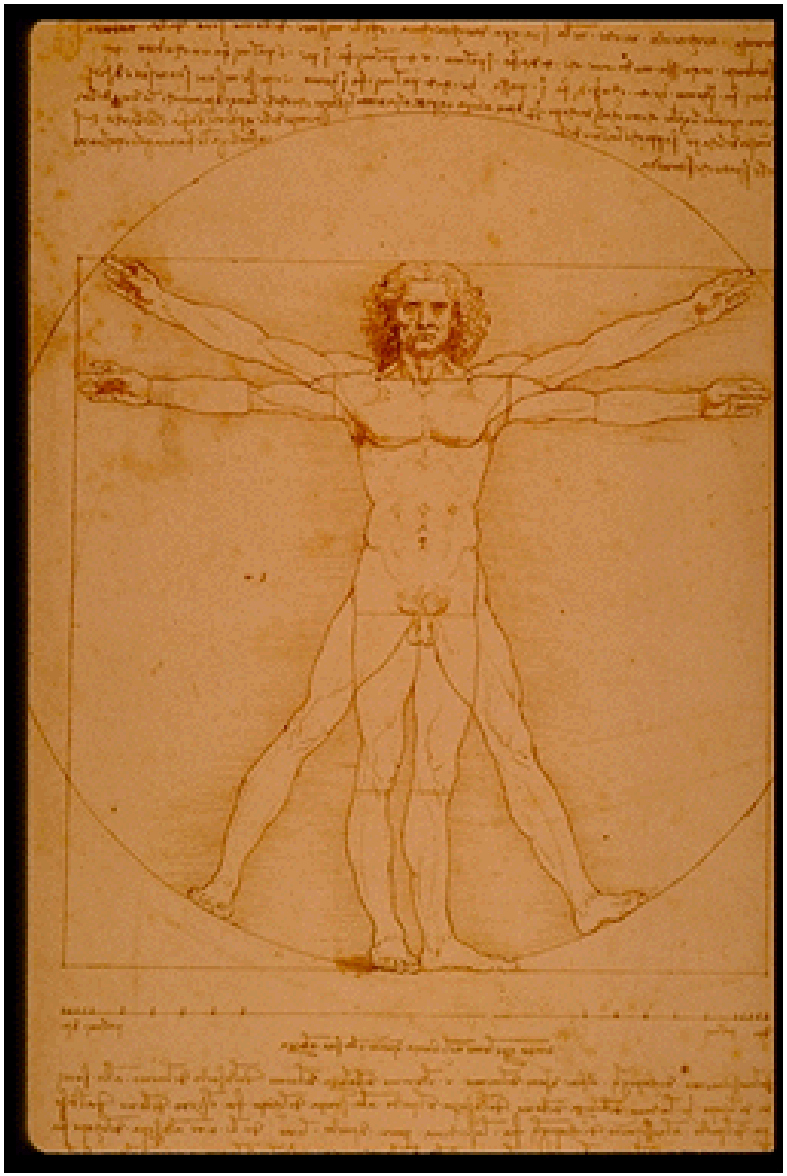
Usability Testing

- Physical place and permanent staff vs. discount usability testing
- Focuses attention on user interface design
- Encourages iterative testing
  - Pilot test of paper design
  - Online prototype evaluation
  - Refinement of versions
  - Testing of manuals, online help, etc.
  - Rigorous acceptance test
- Must participate from early stages
- Must be partners, not "the enemy”

(Dumas & Redish, 1999; Nielsen, 1993)

HCIL

Information Visualization- SysAdmin



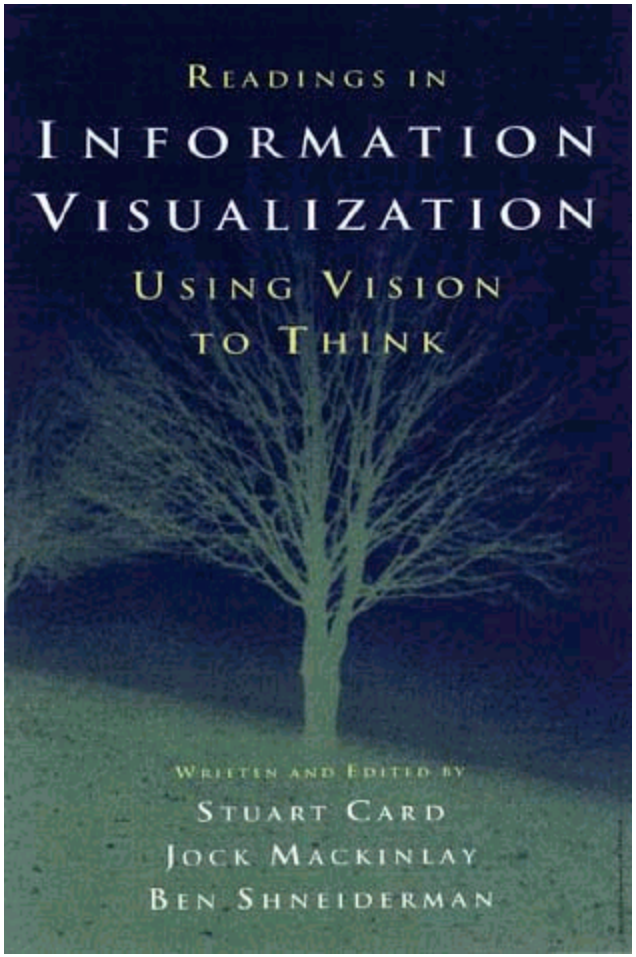
The eye…
the window of the soul,
is the principal means
by which the central sense
can most completely and
abundantly appreciate
the infinite works of nature.

Leonardo da Vinci
(1452 - 1519)

HCIL

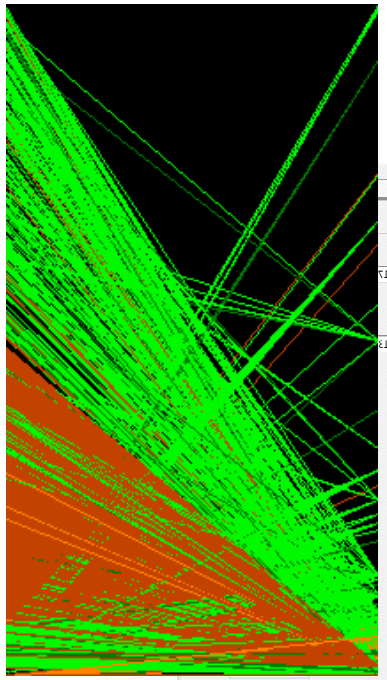
Using Vision to Think

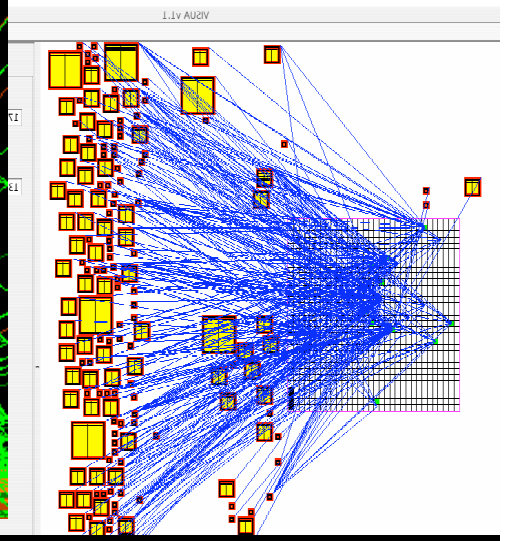
- **Visual bandwidth is enormous**
  - Human perceptual skills are remarkable
    - Trend, cluster, gap, outlier...
    - Color, size, shape, proximity...
  - Human image storage is fast and vast
- **Opportunities**
  - Spatial layouts & coordination
  - Information visualization
  - Scientific visualization & simulation
  - Telepresence & augmented reality
  - Virtual environments

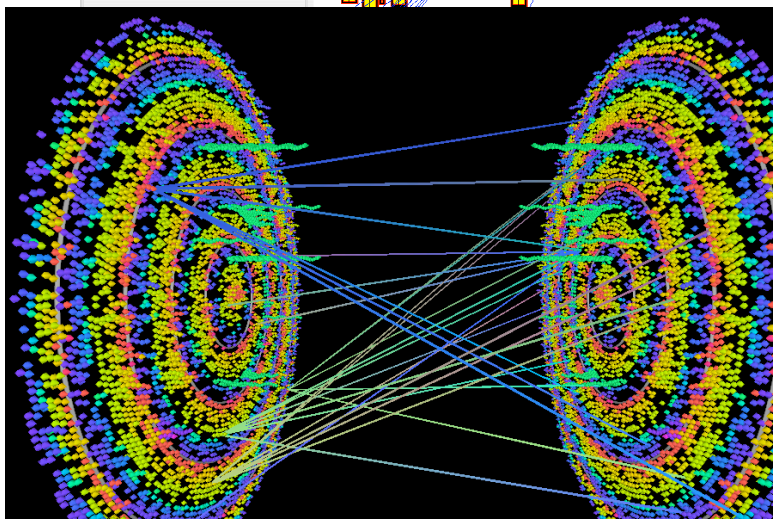


Information Visualization for Security

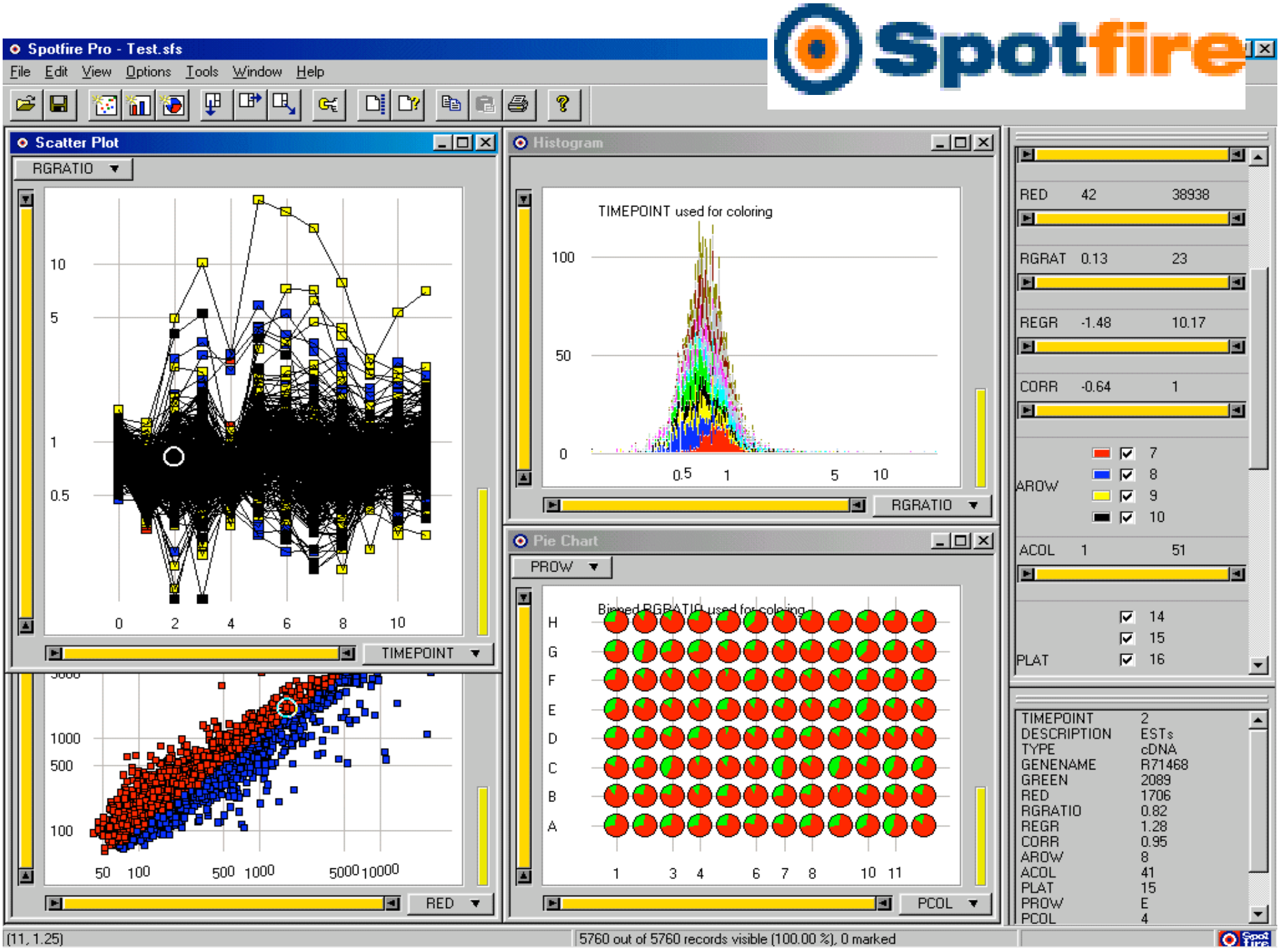
- Detecting intrusions
- Anomaly detection
- Network Traffic classification
- Hostile event
- Link Relationships
- Security Situation Awareness
- Fingerprint network attacks
- Attack Graph complexity
- Profiling users & traffic
- Malicious insider detection



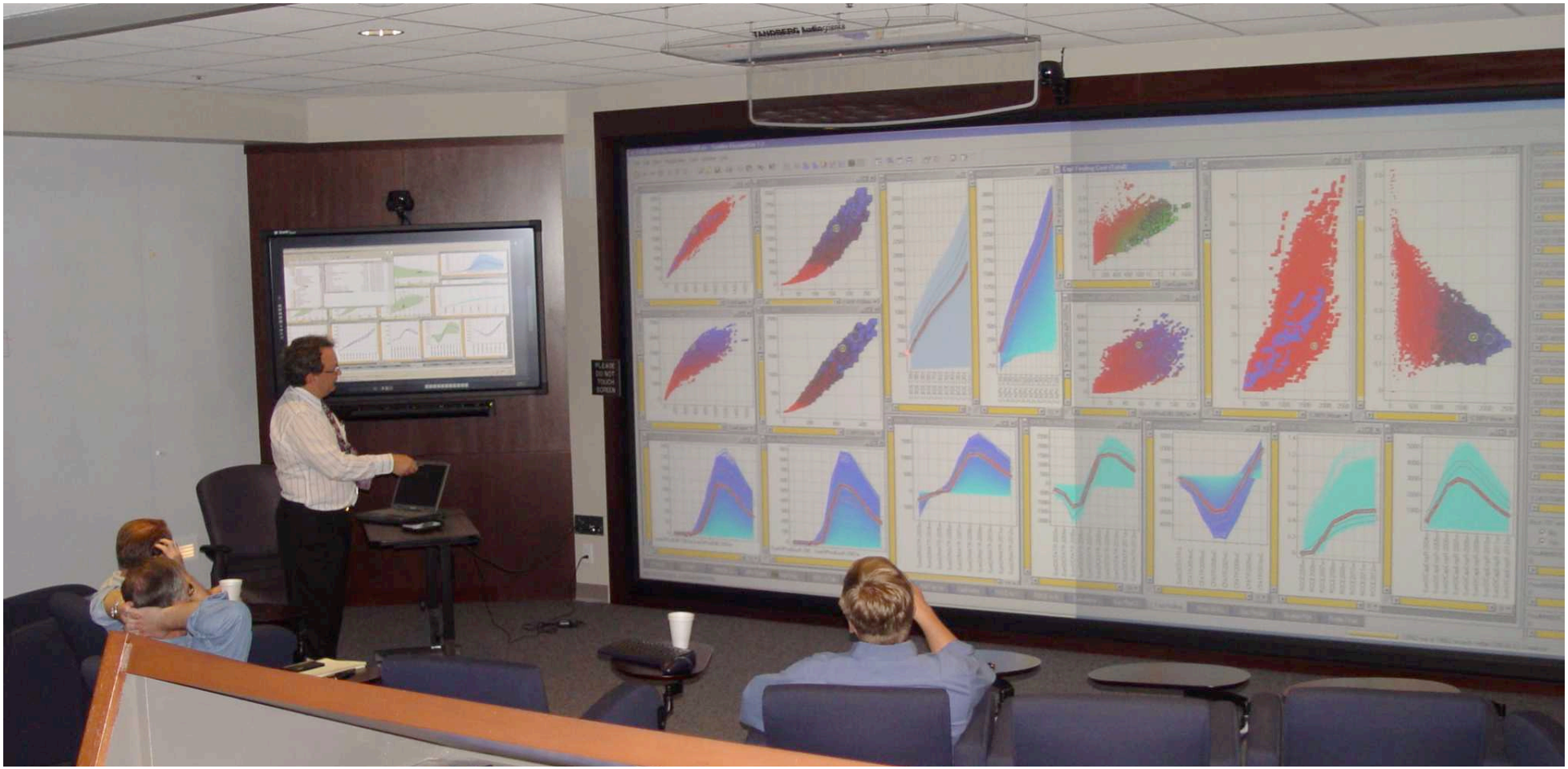




VIZSEC 2004


Spotfire Pro - Test.sfs
File Edit View Options Tools Window Help
Scatter Plot
RGRATIO
10
5
1
0.5
0 2 4 6 8 10
TIMEPOINT
1000
500
100
50 100 500 1000 5000 10000
RED
Histogram
TIMEPOINT used for coloring
100
50
0
0.5 1 5 10
RGRATIO
Pie Chart
PROW
Binned RGRATIO used for coloring
H
G
F
E
D
C
B
A
1 3 4 6 7 8 10 11
PCOL
RED 42 38938
RGRAT 0.13 23
REGR -1.48 10.17
CORR -0.64 1
AROW
7
8
9
10
ACOL 1 51
14
15
PLAT
16
TIMEPOINT 2
DESCRIPTION ESTs
TYPE cDNA
GENENAME R71468
GREEN 2089
RED 1706
RGRATIO 0.82
REGR 1.28
CORR 0.95
AROW 8
ACOL 41
PLAT 15
PROW E
PCOL 4
(11, 1.25)
5760 out of 5760 records visible (100.00 %), 0 marked

Spotfire



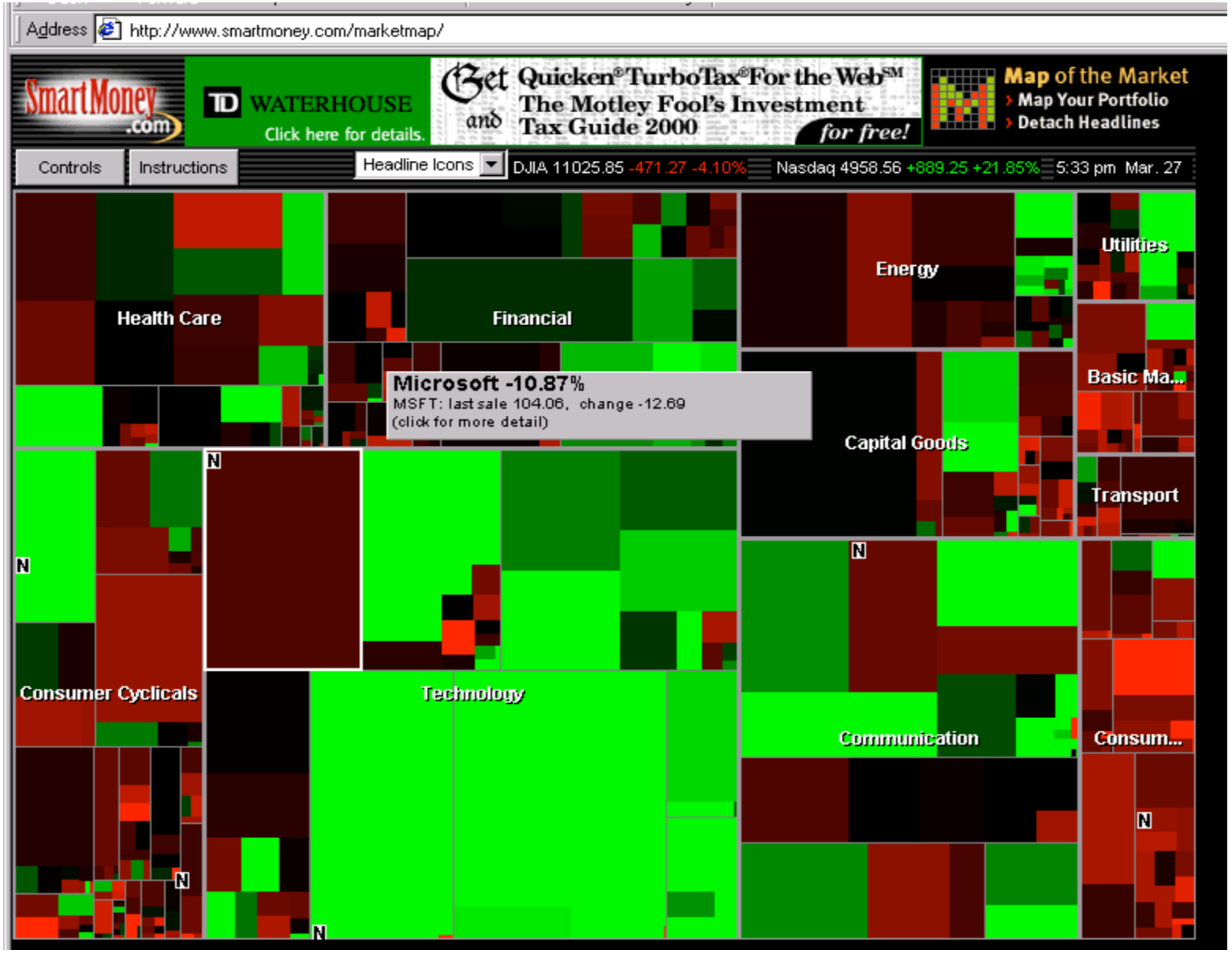
HCIL

Information Visualization: Mantra

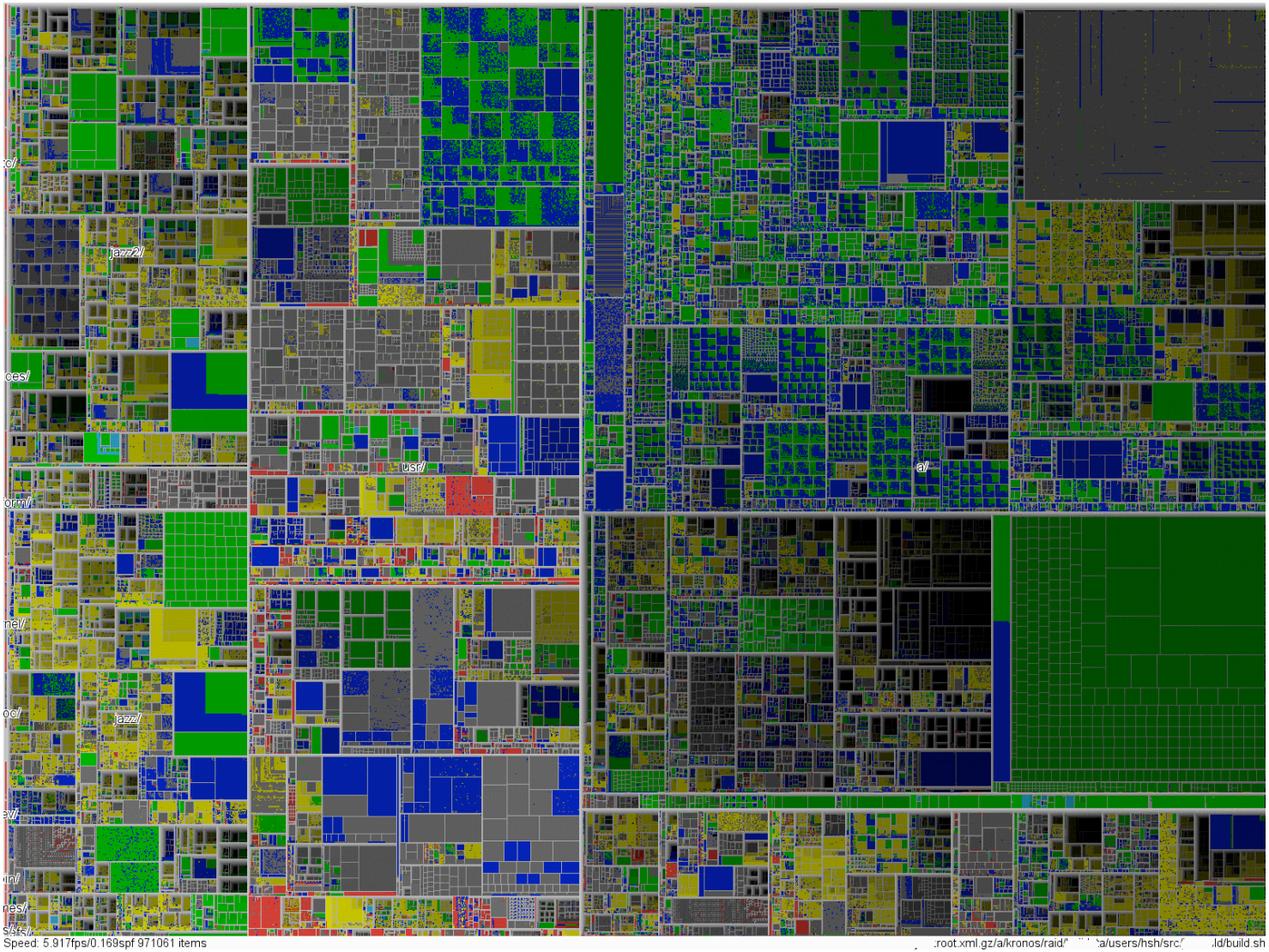
- Overview, zoom & filter, details-on-demand
- Overview, zoom & filter, details-on-demand
- Overview, zoom & filter, details-on-demand
- Overview, zoom & filter, details-on-demand
- Overview, zoom & filter, details-on-demand
- Overview, zoom & filter, details-on-demand
- Overview, zoom & filter, details-on-demand
- Overview, zoom & filter, details-on-demand
- Overview, zoom & filter, details-on-demand
- Overview, zoom & filter, details-on-demand

HCIL

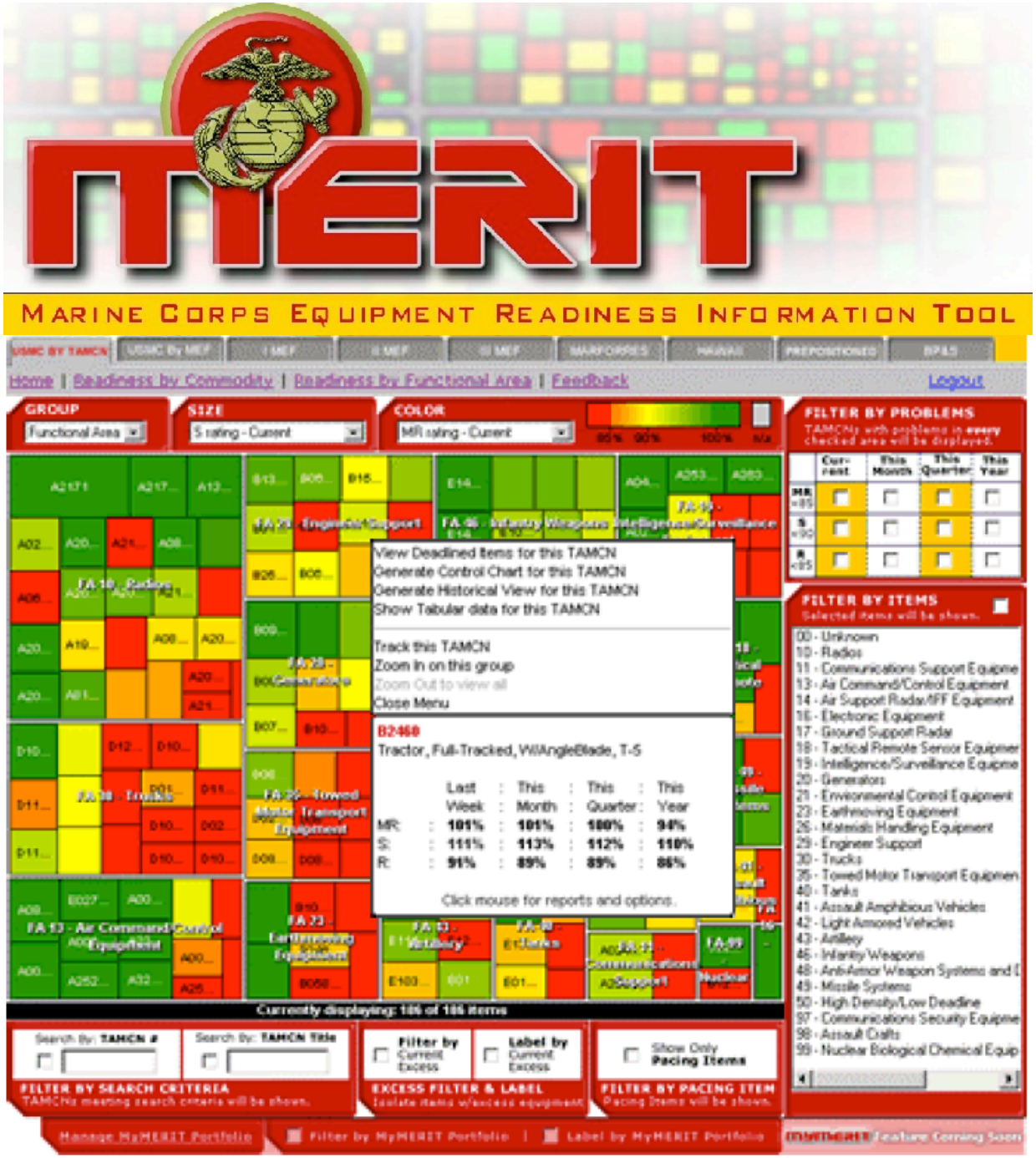
Treemap: Stock market, clustered by industry



Treemap: Million files



www.cs.umd.edu/hcil/millionvis/

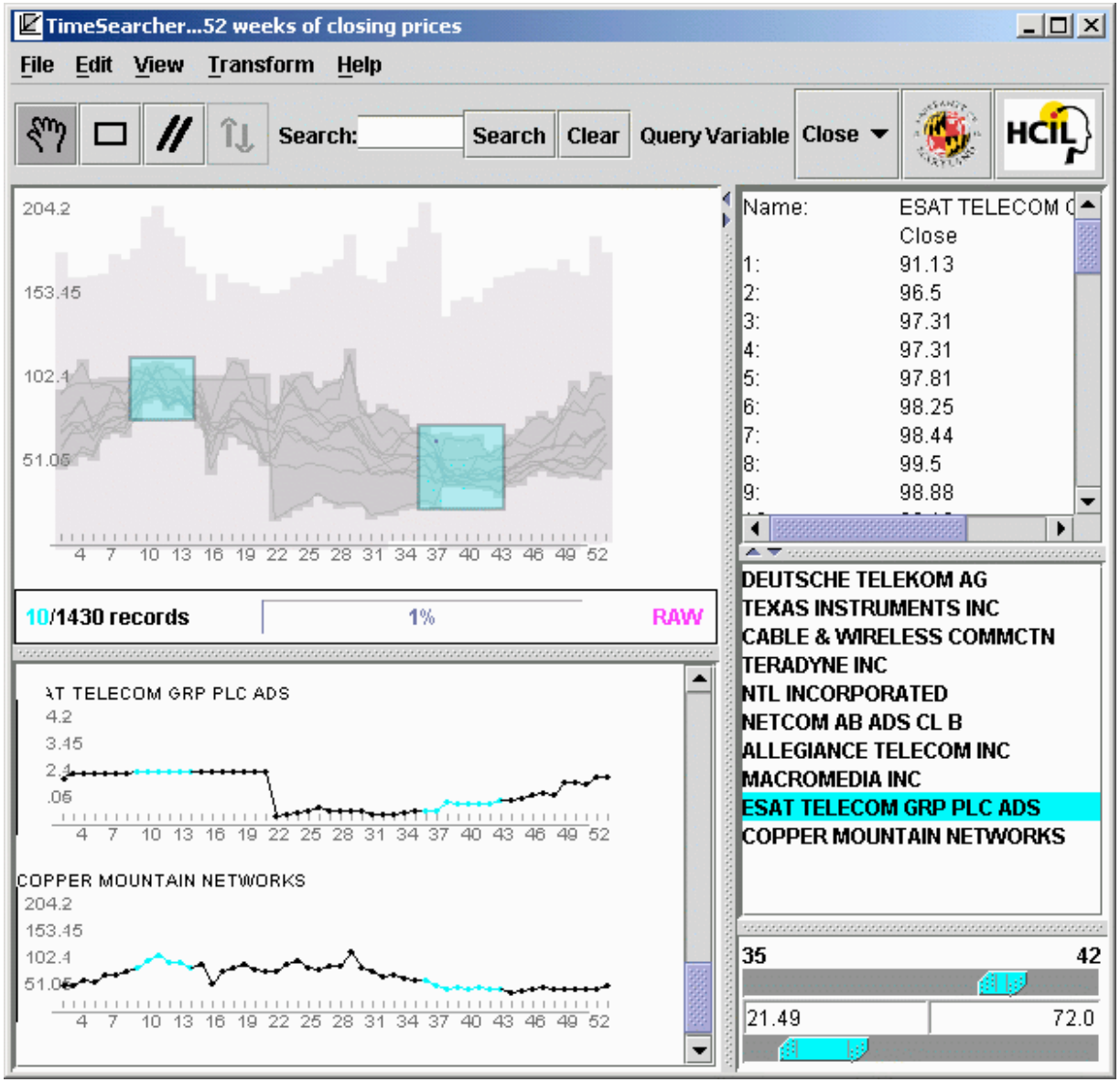

MERIT
MARINE CORPS EQUIPMENT READINESS INFORMATION TOOL
Home | Readiness by Commodity | Readiness by Functional Area | Feedback
Logout
GROUP
Functional Area
SIZE
S rating - Current
COLOR
MR rating - Current
FILTER BY PROBLEMS
TAMCNs with problems in every checked area will be displayed.
FILTER BY ITEMS
Selected items will be shown.
View Deadlined Items for this TAMCN
Generate Control Chart for this TAMCN
Generate Historical View for this TAMCN
Show Tabular data for this TAMCN
Track this TAMCN
Zoom in on this group
Zoom Out to view all
Close Menu
B2460
Tractor, Full-Tracked, W/AngleBlade, T-5
Last Week
This Month
This Quarter
This Year
MR: 101% 101% 100% 94%
S: 111% 113% 112% 110%
R: 91% 89% 89% 86%
Click mouse for reports and options.
Currently displaying: 186 of 186 items
FILTER BY SEARCH CRITERIA
EXCESS FILTER & LABEL
FILTER BY PACING ITEM
Manage MyMERIT Portfolio
Filter by MyMERIT Portfolio
Label by MyMERIT Portfolio

UNITED STATES MARINE CORPS
SEMPER FIDELIS

MARINE CORPS EQUIPMENT READINESS INFORMATION TOOL
254
MERIT
AWARDS:
AFEI EXCELLENCE IN INTEGRATION
GOVERNMENT COMPUTER NEWS
NAVY EGOV
DOD CIO
DNE WATCH

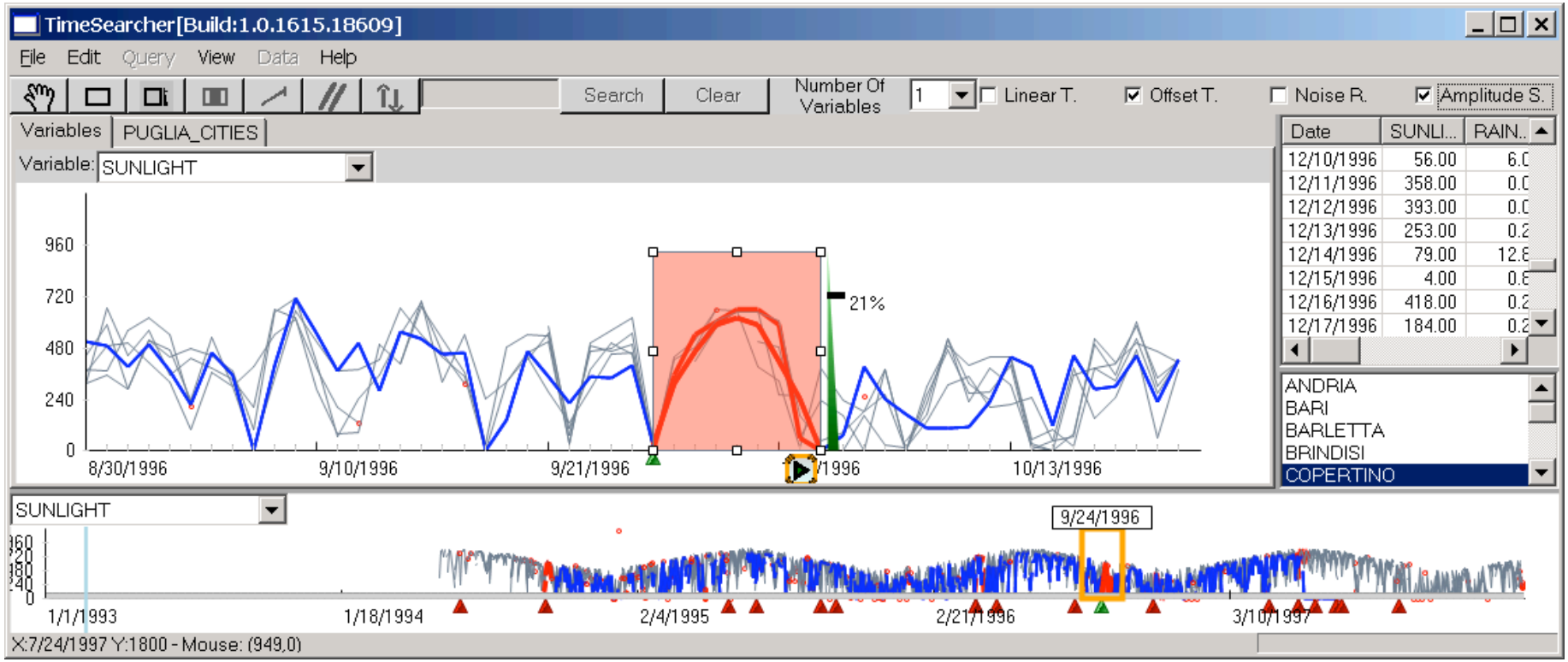
Temporal Data: TimeSearcher 1.3

- Time series
  - Stocks
  - Weather
  - Genes
- User-specified patterns
- Rapid search

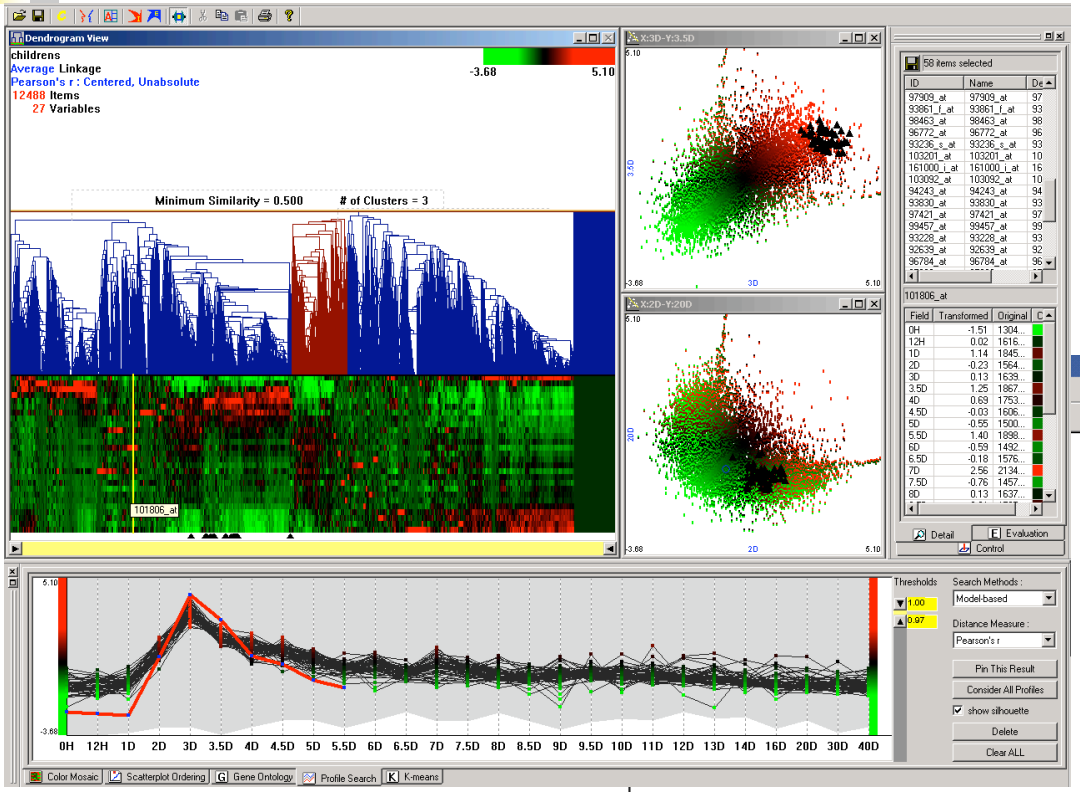


Temporal Data: TimeSearcher 2.0

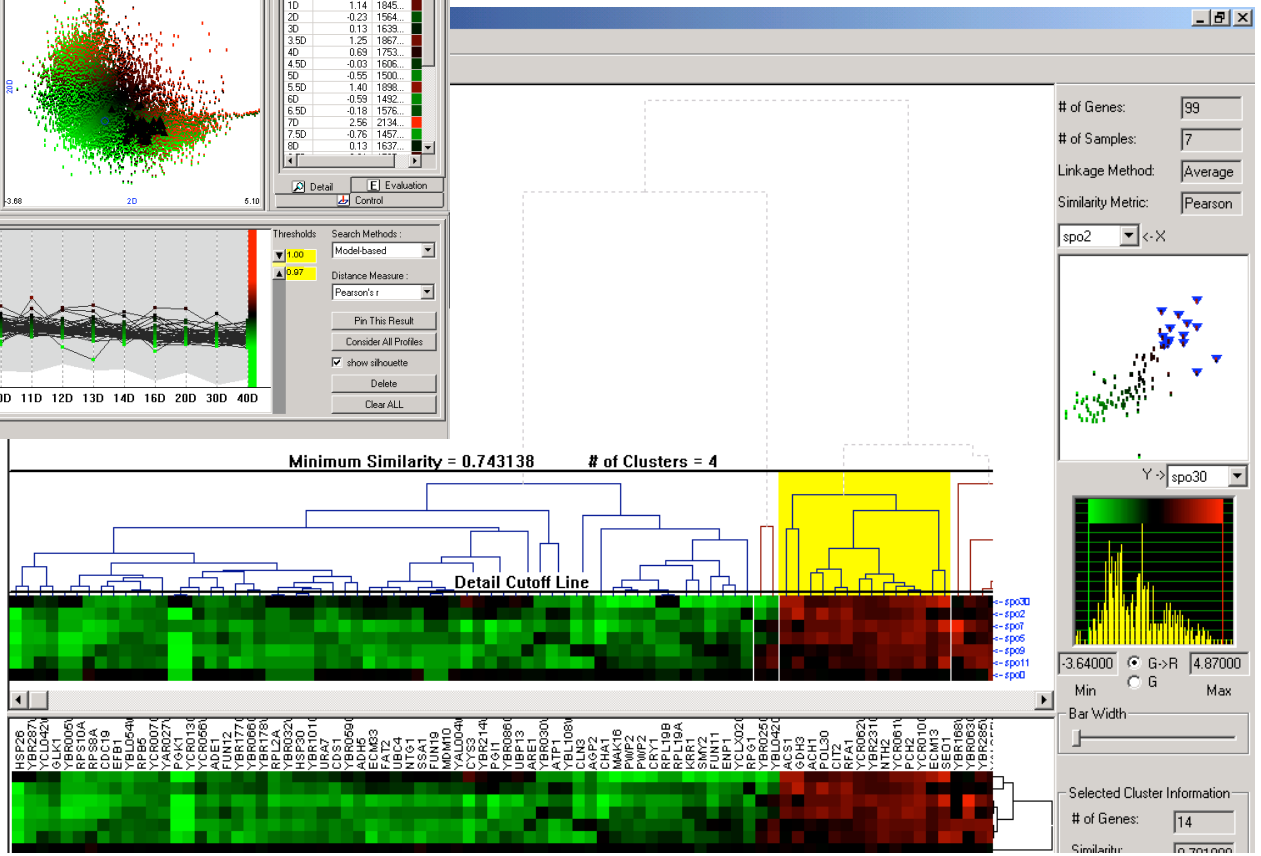
- Long Time series (>10,000 time points)
- Multiple variables
- Controlled precision in match
  (Linear, offset, noise, amplitude)



Multi-V: Hierarchical Clustering Explorer



www.cs.umd.edu/hcil/hce/

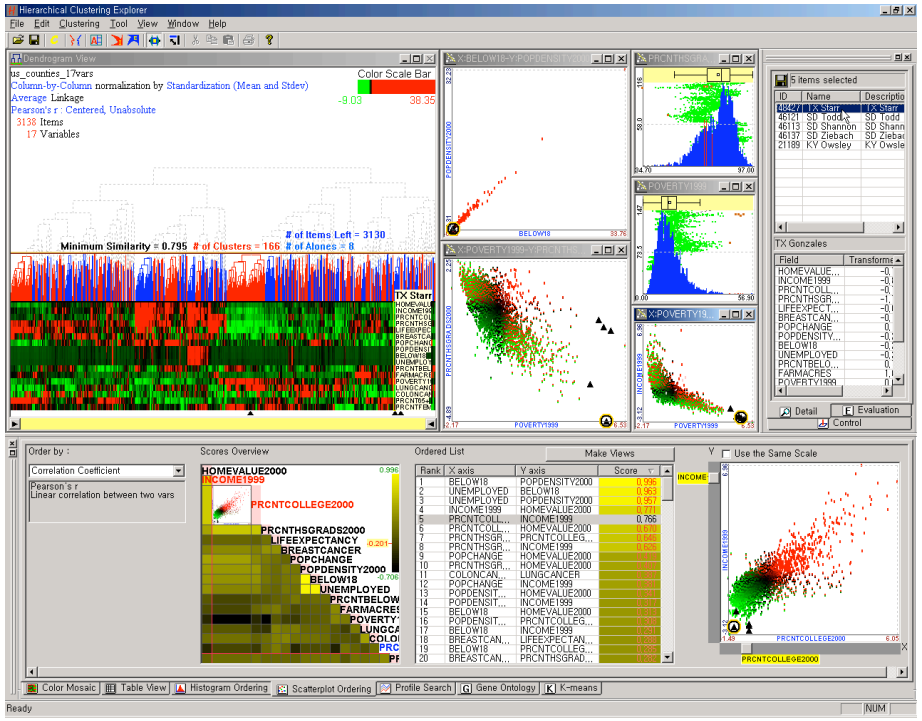


"HCE enabled us to find important clusters that we didn't know about."
- a user

HCE Status

- In collaboration and sponsored by Eric Hoffman: Children's National Medical Center
- Categorical Variables: 4.0 beta, May 2005
- 60K lines of C++ codes, 58 Classes
- 2,000+ downloads since April 2002

- www.cs.umd.edu/hcil/hce



www.cs.umd.edu/hcil

For More Information

- Visit the HCIL website for 350 papers & info on videos
  www.cs.umd.edu/hcil
- Conferences & resources: **www.infovis.org**
- See Chapter 14 on Info Visualization
  Shneiderman, B. and Plaisant, C., *Designing the User Interface: Strategies for Effective Human-Computer Interaction: Fourth Edition* (April 2004) **www.awl.com/DTUI**
- Edited Collections:
  Card, S., Mackinlay, J., and Shneiderman, B. (1999)
  Readings in Information Visualization: Using Vision to Think
  Bederson, B. and Shneiderman, B. (2003)
  The Craft of Information Visualization: Readings and Reflections

HCIL

For More Information

- Treemaps
  - HiveGroup: `www.hivegroup.com`
  - Smartmoney: `www.smartmoney.com/marketmap`
  - HCIL Treemap 4.0: `www.cs.umd.edu/hcil/treemap`
- Spotfire: `www.spotfire.com`
- TimeSearcher： `www.cs.umd.edu/hcil/treemap`
- Hierarchical Clustering Explorer:

  `www.cs.umd.edu/hcil/hce`

HCIL

Logical User Centered Interaction Design

- **Design Methodology**
  - Management strategy to highlight usability engineering
  - Processes, Deliverables, and Reviews
- **Stages for LUCID**

  1: Envision

  2: Discovery

  3: Design Foundation

  4: Design Detail

  5: Build

  6: Release

(Cognetics Corp, www.cognetics.com)

Guidelines Document and Processes

- Social process for developers
- Records decisions for all parties to see
- Promotes consistency and completeness
- Facilitates automation of design
- Should contain philosophy and examples of:
  title screens, menus, forms, buttons, graphics, icons, fonts, colors, instructions, help, tutorials, error messages, …
- Multiple levels are desirable:
  standards, practices, guidelines
- **E**ducation, **E**nforcement, **E**xemption & **E**nhancement

HCIL

Expert Reviews and Usability Testing

- Improved product quality
- Shorter development time
- More predictable development lifecycle
- Reduced costs
  - Speed development
  - Simplify documentation
  - Facilitate training
  - Lower support
  - Fewer updates
- Improved organizational reputation
- Higher morale: staff and management

HCIL

Expert Reviews

- **Experienced reviewers**
  - Review every screen, menu, dialog box
  - Spot inconsistencies and anomalies
  - Suggest additions
- **Disciplined approaches**
  - Heuristic evaluation: check if goals are being met
  - Guidelines review: verify adherence
  - Consistency inspection: terms, layout, color, sequencing
  - Cognitive walkthrough: pretend to be a user following scenario
  - Formal inspection: public presentation and discussion

HCIL