Visualization

Alex Endert
aendert@cs.vt.edu

Overview

- Presentation of Papers
  - **Reeder, R. W.,** Bauer, L., Cranor, L. F., Reiter, M. K., Bacon, K., How, K., and Strong, H. 2008 Expandable Grids for Visualizing and Authoring Computer Security Policies. In *Proceeding of the Twenty-Sixth Annual SIGCHI Conference on Human Factors in Computing Systems* (Florence, Italy, April 05 - 10, 2008). CHI '08. ACM, New York, NY, 1473-1482.
  - **de Paula, R**., Ding, X., Dourish, P., Nies, K., Pillet, B., Redmiles, D. F., Ren, J., Rode, J. A., and Filho, R. S. 2005. In the eye of the beholder: a visualization-based approach to information system security. *Int. J. Hum.-Comput. Stud.* 63, 1-2 (Jul. 2005), 5-24.
  - **Rode, J**., Johansson, C., DiGioia, P., Filho, R. S., Nies, K., Nguyen, D. H., Ren, J., Dourish, P., and Redmiles, D., Seeing further: extending visualization as a basis for usable security, in *Second Symposium on Usable Privacy and Security (SOUPS'06)*. 2006, ACM: Pittsburgh, Pennsylvania. p. 145-155.
- Critique / Discussion

EXPANDABLE GRIDS FOR VISUALIZING AND AUTHORING COMPUTER SECURITY POLICIES (2008)

Robert W. Reeder, Lujo Bauer, Lorrie Faith Cranor, Michael K. Reiter, Kelli Bacon, Keisha How, Heather Strong

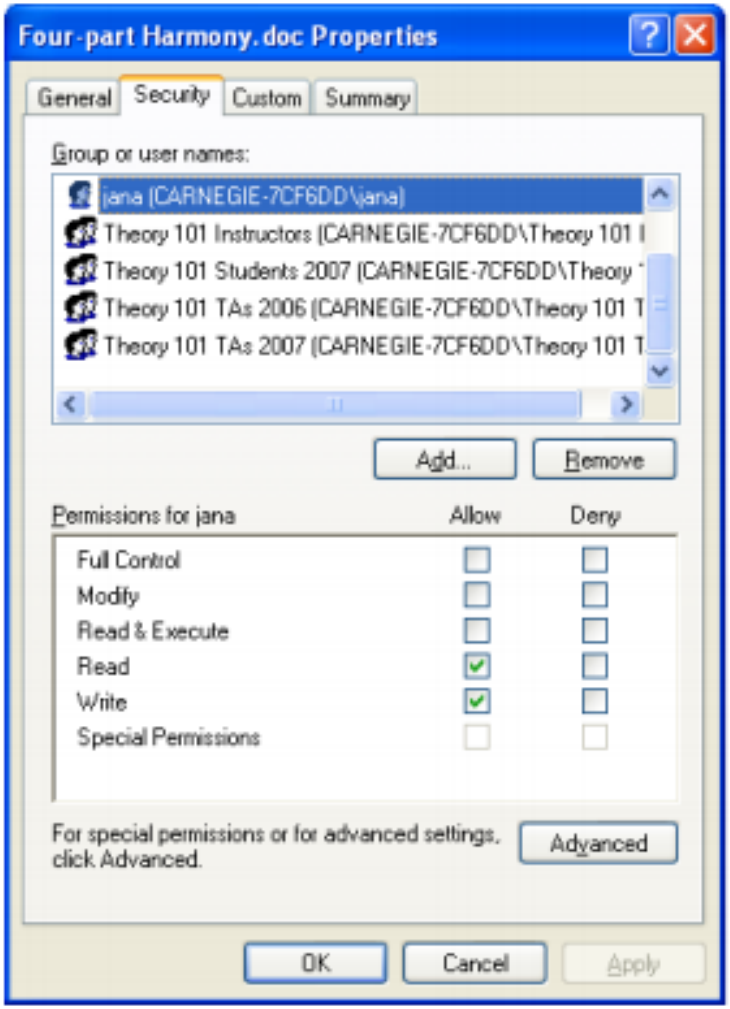
Background

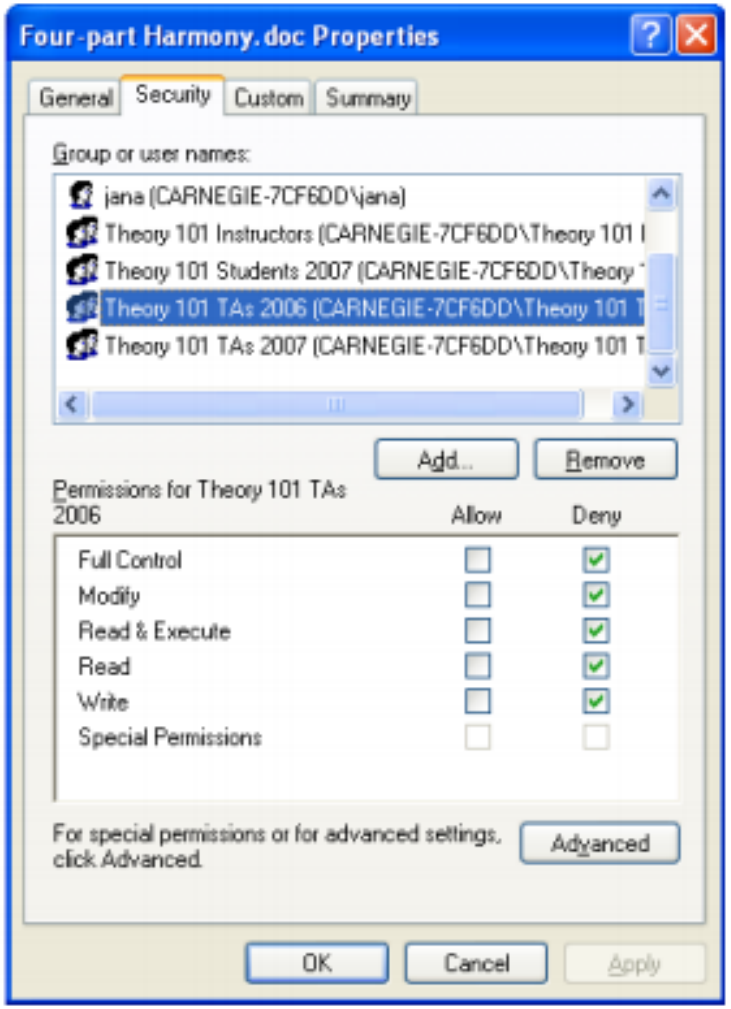
- Expandable Grid
  - Matrix-based visualization of a policy
- Windows XP policy management is not adequate. ("list-of-rules model")
  - Must give administrator overview (for context) of all rules.
  - Also on Linux, Mac OS X Server

Fundamental Operations of Policy-authoring Interfaces

1. Viewing Policy
2. Changing Policy
3. Viewing Composite Value Memberships
    1. “groups”
4. Detecting and Resolving Conflicts

List-of-Rules Model





Why does Jana not have access to Four-part Harmony.doc??

Expandable Grids

Principals

Jana has read, not write access

Resources

Change in WinXP Semantics:
Allow > Deny!!

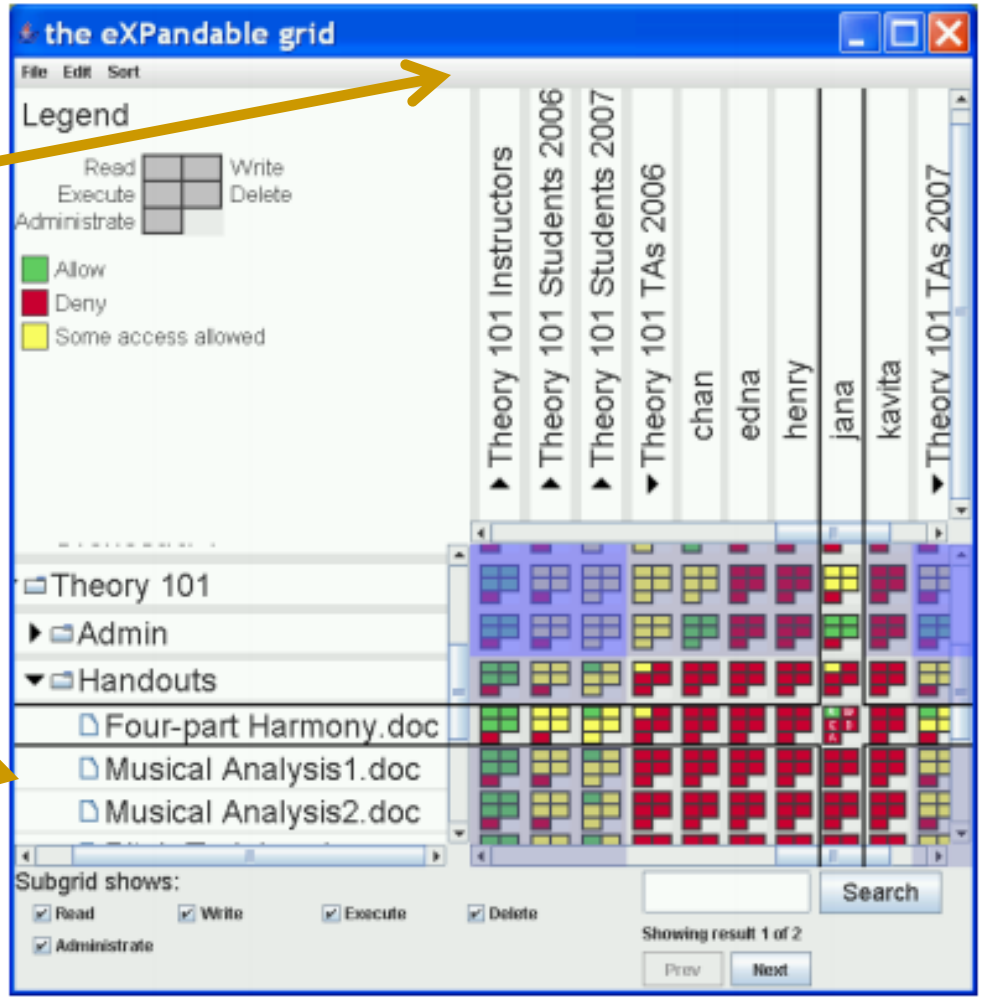


Figure 2. Screenshot of our Expandable Grid interface when the Jana task has been half-completed.

Expandable Grids

- Features:
  - Whole Policy
  - Effective Policy
  - Group Membership Info
  - Simple Changes
  - New Policy Semantics
  - Visual pop-out
  - *Highlighting*
  - *Search*

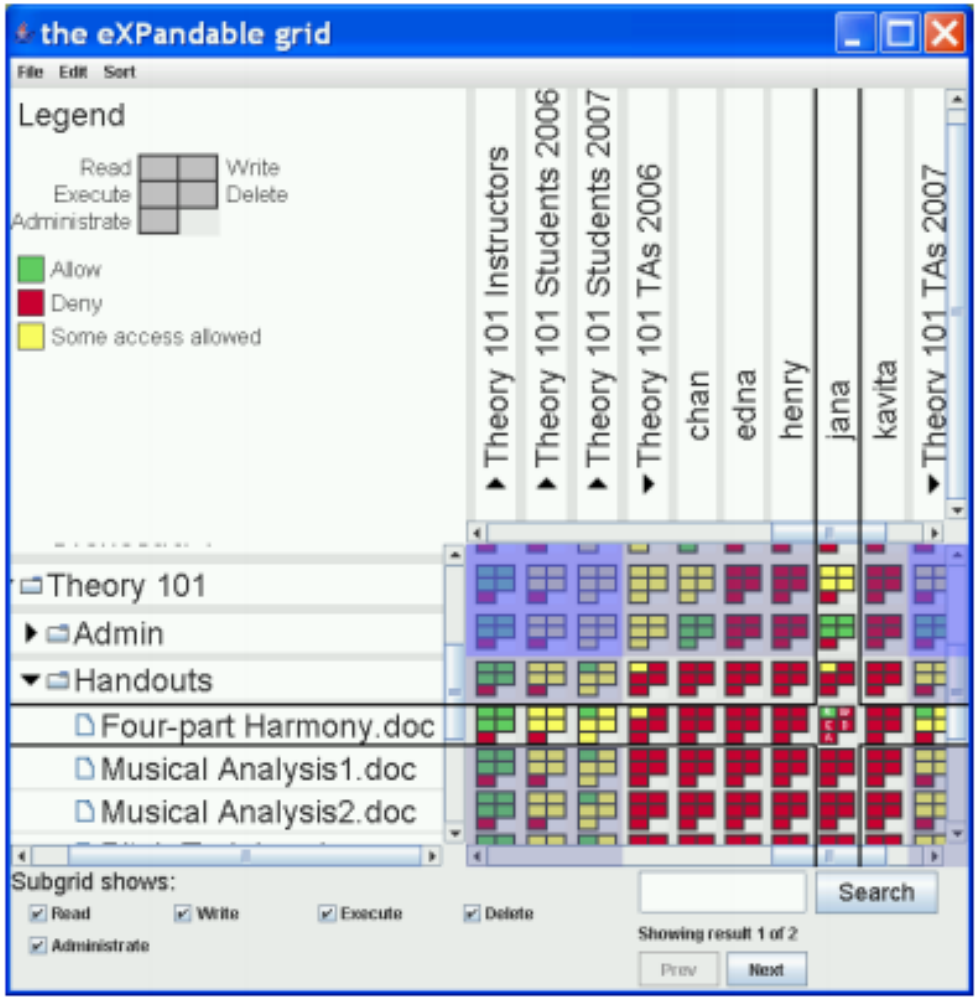


Figure 2. Screenshot of our Expandable Grid interface when the Jana task has been half-completed.

User Study Methodology

- 36 engineering undergrads (10 female, 26 male)
  - No sys admin experience (?)
- Windows XP
- Collected:
  - Video
  - Audio
  - Policies Created

User Study Tasks

- 20 (10 pairs) tasks, requiring:
  - Training
  - View-simple
  - View-complex
  - Change-simple
  - Change-complex
  - Compare-groups
  - Conflict-simple
  - Conflict-complex
  - Memogate
  - Precedence

Results

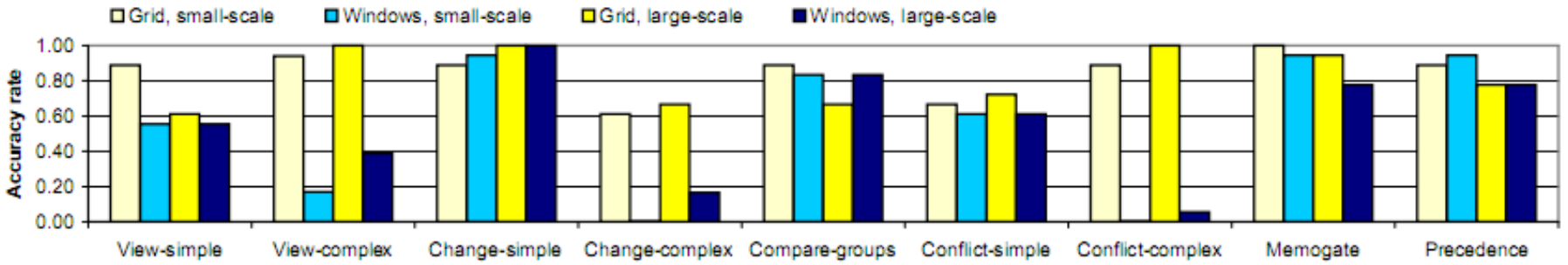
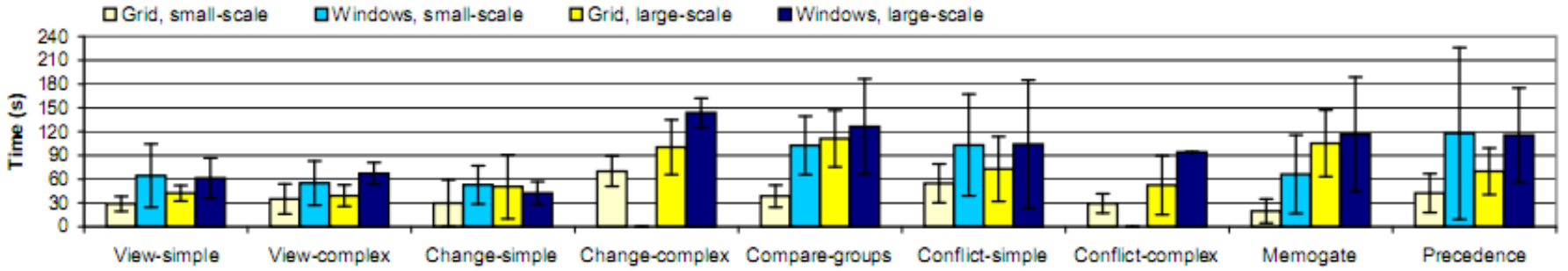


Figure 3. Accuracy results, showing proportion of participants correctly completing each task with Grid and Windows interfaces.



Results

Task pair	Small-scale			Large-scale		
	a_G	a_W	p-value	a_G	a_W	p-value
View-simple	0.89	0.56	$p = 0.03$	0.61	0.56	$p = 0.50$
View-complex	0.94	0.17	$\mathbf{p < 0.001}$	1.00	0.39	$\mathbf{p < 0.001}$
Change-simple	0.89	0.94	*No test*	1.00	1.00	*No test*
Change-complex	0.61	0.00	$\mathbf{p < 0.001}$	0.67	0.17	$\mathbf{p = 0.003}$
Compare-groups	0.89	0.83	*No test*	0.67	0.83	*No test*
Conflict-simple	0.67	0.61	$p = 0.5$	0.72	0.61	$p = 0.36$
Conflict-complex	0.89	0.00	$\mathbf{p < 0.001}$	1.00	0.06	$\mathbf{p < 0.001}$
Memogate	1.00	0.94	$p = 0.5$	0.94	0.78	$p = 0.17$
Precedence	0.89	0.94	$p = 0.5$	0.78	0.78	$p = 0.65$

- Bottom line: Expandable Grid allows authors to complete tasks more accurately and faster (significantly!)

IN THE EYE OF THE BEHOLDER: A VISUALIZATION-BASED APPROACH TO INFORMATION SYSTEM SECURITY (2005)

Rogerio de Paula, Xianghua Ding, Paul Dourish, Kari Nies, Ben Pillet, David F. Redmiles, Jie Ren, Jennifer A. Rode, Roberto Silva Filho

View on Security

- Focus on “whether a system is secure enough for [the user’s] immediate needs”
  - Effective Security < Theoretical Security
  - Control over Security

- 3 major elements:
  - Empirical investigation into everyday security practices
  - “systems approach”: vis & event based architectures
  - Initial prototype of P2P file sharing (face-to-face)

Usable Security!!

through information systems (as the examples here show). Researchers in the HCI community have long argued that "usability" cannot be an afterthought in information system design; a system cannot be made usable merely by the addition of a graphical user interface, however pretty. Security researchers have made a similar argument about the design of secure systems; insecure systems cannot be turned into secure ones merely by the addition of a layer of encryption. Both of these argue, then, that security and usability need to be understood as a holistic design problem. A lick of "usability paint" will not cure the difficulty of making use of, say,

Empirical Investigation Results (Users)

- Optimization
  - Security is not the point of their work, their task is
- Contingent Assessment
  - Balance of immediate needs and overall security
- Delegation
  - Rely on trusted “agents” (i.e. encryption agents, pre-configured “security” system).
- Embeddedness
  - Defining boundaries of “information systems” is difficult

Empirical Investigation Results (Security)

for their immediate needs. Security is evaluated and managed in a range of contexts—physical, personal, organizational, interactional, and more.

- "security in practice is not an all-or-nothing matter"
- "secure" and "insecure" is not absolute
- Security mechanism visible to user
- Security is "end-to-end" – all components play role

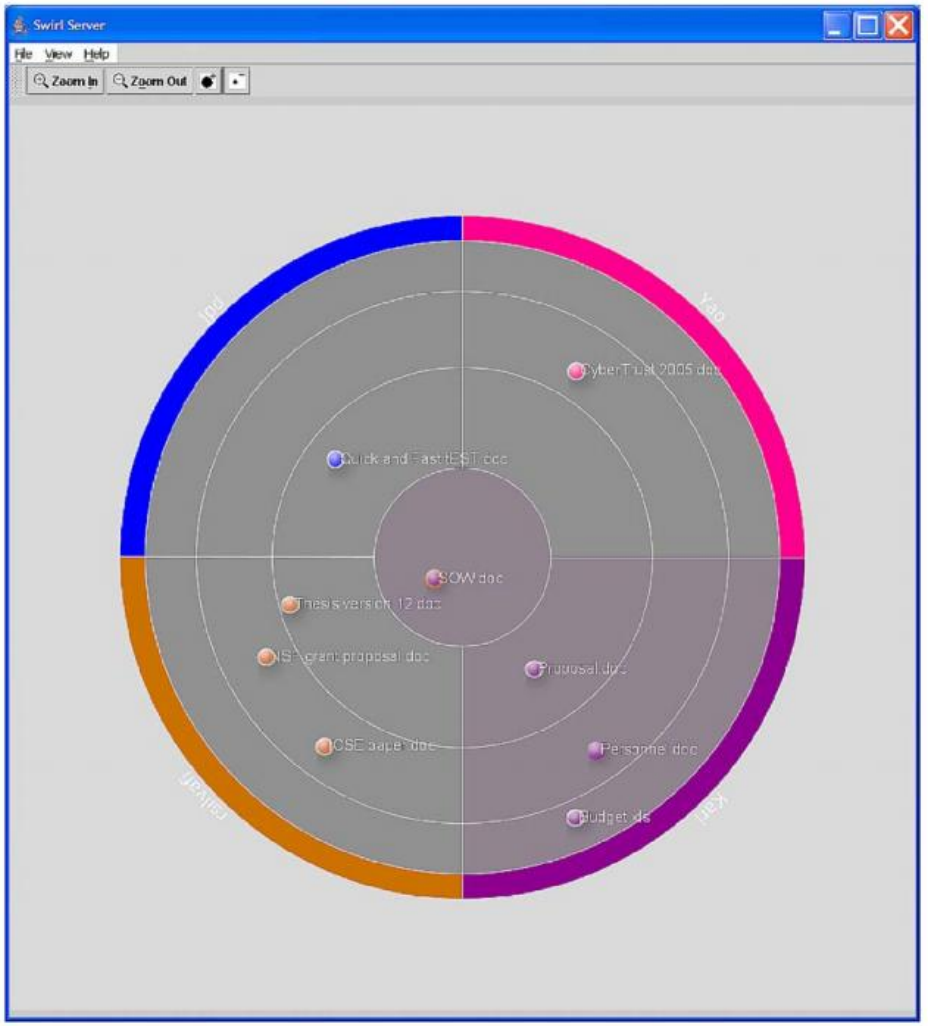
Design Guidelines for Effective Security

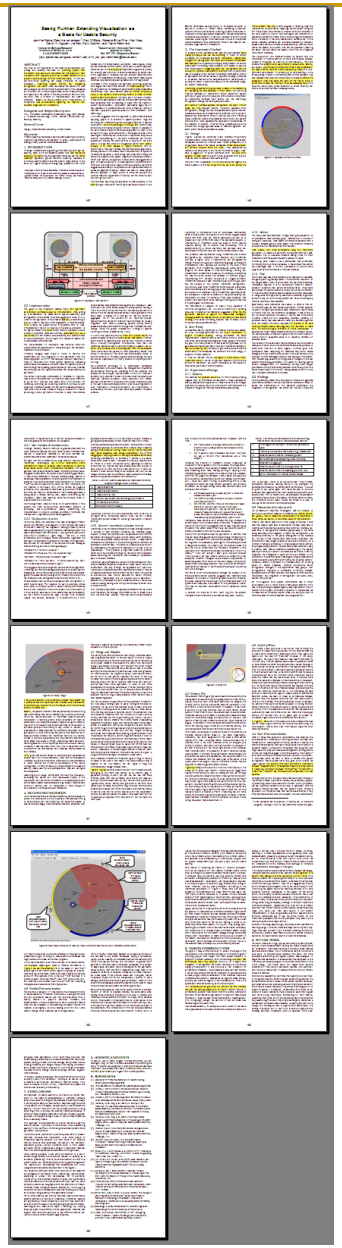
In particular, our approach in Swirl is based on supporting informed decision-making. The central problem of security, for end-users, is two-fold: it involves understanding the system's configuration and state, and understanding their consequences for user action. People act through information technology, and so our goal is to help them understand how an information system might mediate their actions. This turns our attention away from traditional considerations of expression

- In other words, their focus is on:
  - Visualizing system activity
  - Integrating configuration and action

Testbed: "Impromptu"

- Collaborative, face-to-face P2P file sharing system
  - "evaluation exercise is ongoing"
  - (more detail in later paper)





SEEING FURTHER: EXTENDING VISUALIZATION AS A BASIS FOR USABLE SECURITY (2006)

Jennifer Rode, Carolina Johansson, Paul DiGioia, Roberto Silva Filho, Kari Nies, David H. Nguyen, Jie Ren, Paul Dourish, and David Redmiles

Focus

- File Sharing Visualization (Impromptu) that:
  - Shows system activity
  - Integrates configuration and user action
  - Shows temporal and structural information
  - Allows collaboration

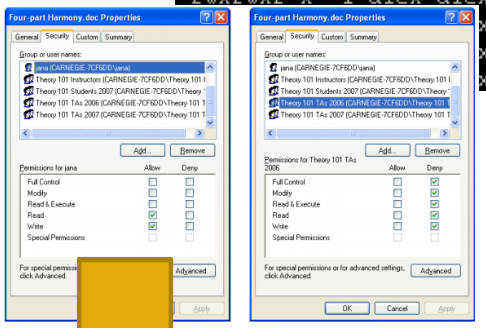
Views on Security

- "Strict Usability"
  - Traditional methods for security measures used regularly
    - E.g. passwords, encryptions, VPNs, etc.
- "Everyday Use"
  - "privacy and security cannot be held to absolute measures…need to be negotiated [per situation]"
  - "people must make informed decisions"

Impromptu Concept

- Design Principles:
  - Visualization Mechanisms
  - Integration of Configuration and Action
  - Use of event-based architectures
- “integrating action and configuration and the concept of dynamic visualization of activity”

```
drwxr-xr-x  3 alex alex    4096 Nov  2 15:37 Desktop
-rw-rw-r--  1 alex alex   12331 Sep 22 17:57 outputfile_Subject1.txt
drwxrwxr-x 29 alex alex    4096 Oct 26 17:08 simple
drwxr-xr-x  6 root root    4096 Oct 26 16:38 storyboard_pda
drwxrwxr-x  2 alex alex    4096 Oct  7 10:50 temp
-rwxrwxr-x  1 alex alex 7479585 Nov 11 12:14 Trial015.csv
-rwxrwxr-x  1 alex alex 3796708 Nov 18 14:18 Trial016.csv
-rwxrwxr-x  1 alex alex 3233927 Nov 20 11:43 Trial017.csv
-rwxrwxr-x  1 alex alex 3954649 Sep 22 18:27 User1_vicon.csv
-rwxrwxr-x  1 alex alex 5481865 Sep 23 13:40 User2_vicon.csv
-rwxrwxr-x  1 alex alex 3875073 Sep 23 15:22 User3_vicon.csv
-rwxrwxr-x  1 alex alex 4727169 Sep 25 11:53 User4_vicon.csv
-rwxrwxr-x  1 alex alex 3901497 Sep 29 14:54 User5_vicon.csv
x 4586942 Oct  7 13:24 User6_vicon.csv
x 3296042 Nov  4 14:19 User8_vicon.csv
x 4103940 Nov  9 16:20 User9_Vicon.csv
```



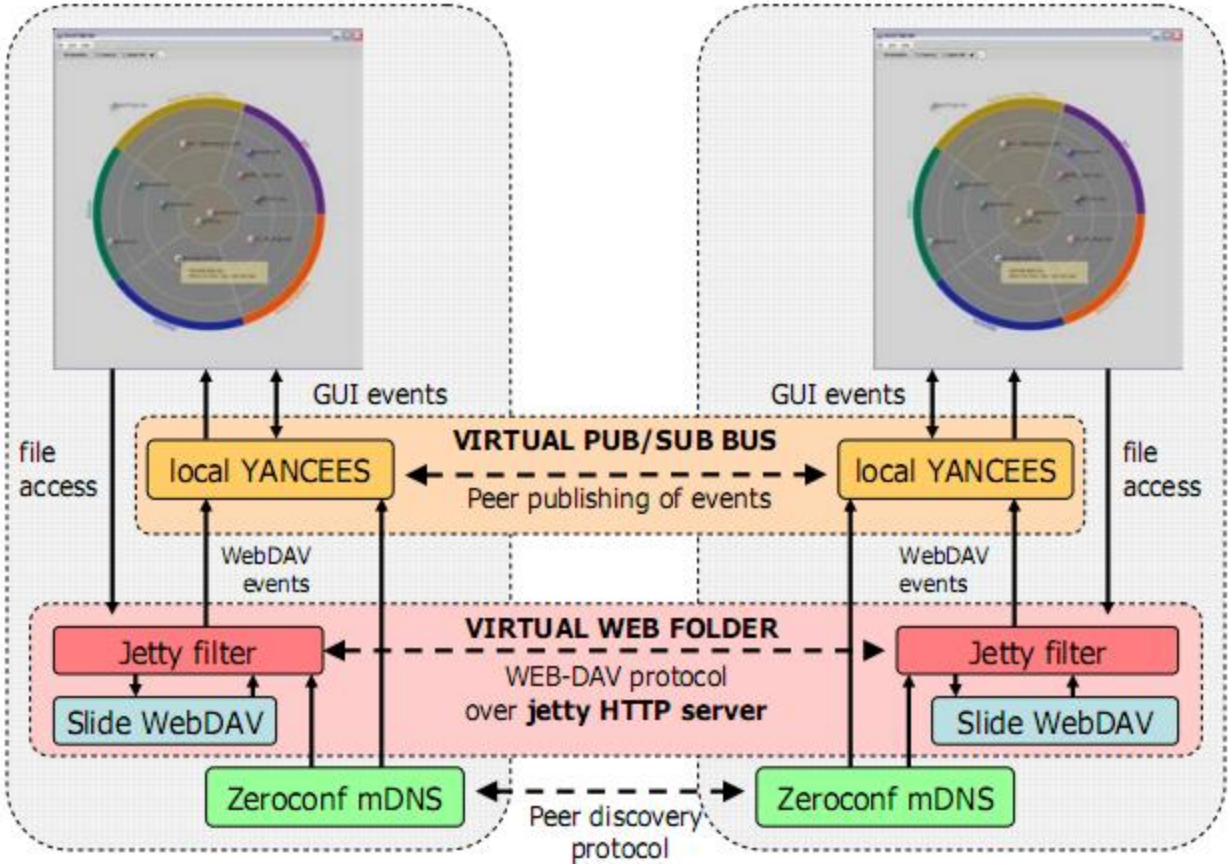
Impromptu Design

- Colors = Users
- Closer to center, “more shared”
  - Center = “persistent file”
- Dots = files
  - Color of dots = last user accessing file

Impromptu Design

- Degrees of sharing
  1. Not shared, local only
  2. Visible, local only
  3. Readable
  4. Readable & Writable
  5. Persistent

Impromptu Architecture



- No central server, all P2P
- User leaves, file leaves (unless persistent)
- “strict security is *not* a requirement”

User Study

- 24 graduate students
- 8 sessions (3 users each)
- Used Impromptu, Excel, and Word

- Did not tell users to focus on security, but rather their task

- “not a usability trial … designed an open-ended, semi-naturalistic study”

Findings

- User Feedback

Table 2. List of 20 positive comments volunteered during debrief about the ability to visualize system activity:

5	The rings and blink around file icons indicate what is open
5	Permits you to see what others are doing, "awareness"
4	Clear indication of which files belong to who
2	Concentric spheres representing levels of privacy
1	Clear who is logging in
1	Clear indication of who is looking at what file
1	Clear indication of who is accessing your own files
1	Good visualization of different levels of access

Findings

- Try:
  - Which user (color) most recently accessed the file?

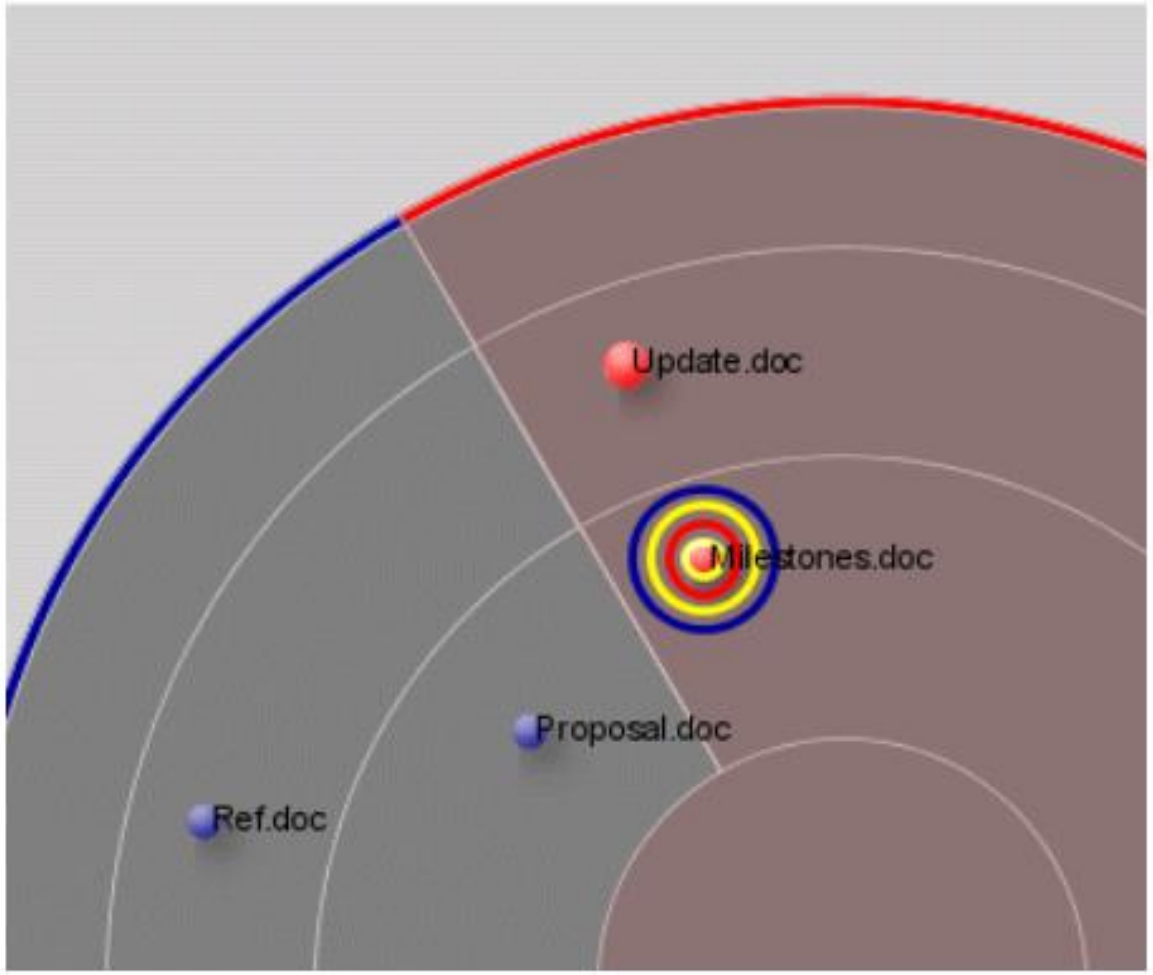


Figure 3: History Rings

Findings

- History
  - Owner = red
  - Usage history:
    - Yellow (most recent)
    - Red
    - Yellow
    - Blue

  *more recent, closer to middle (?)

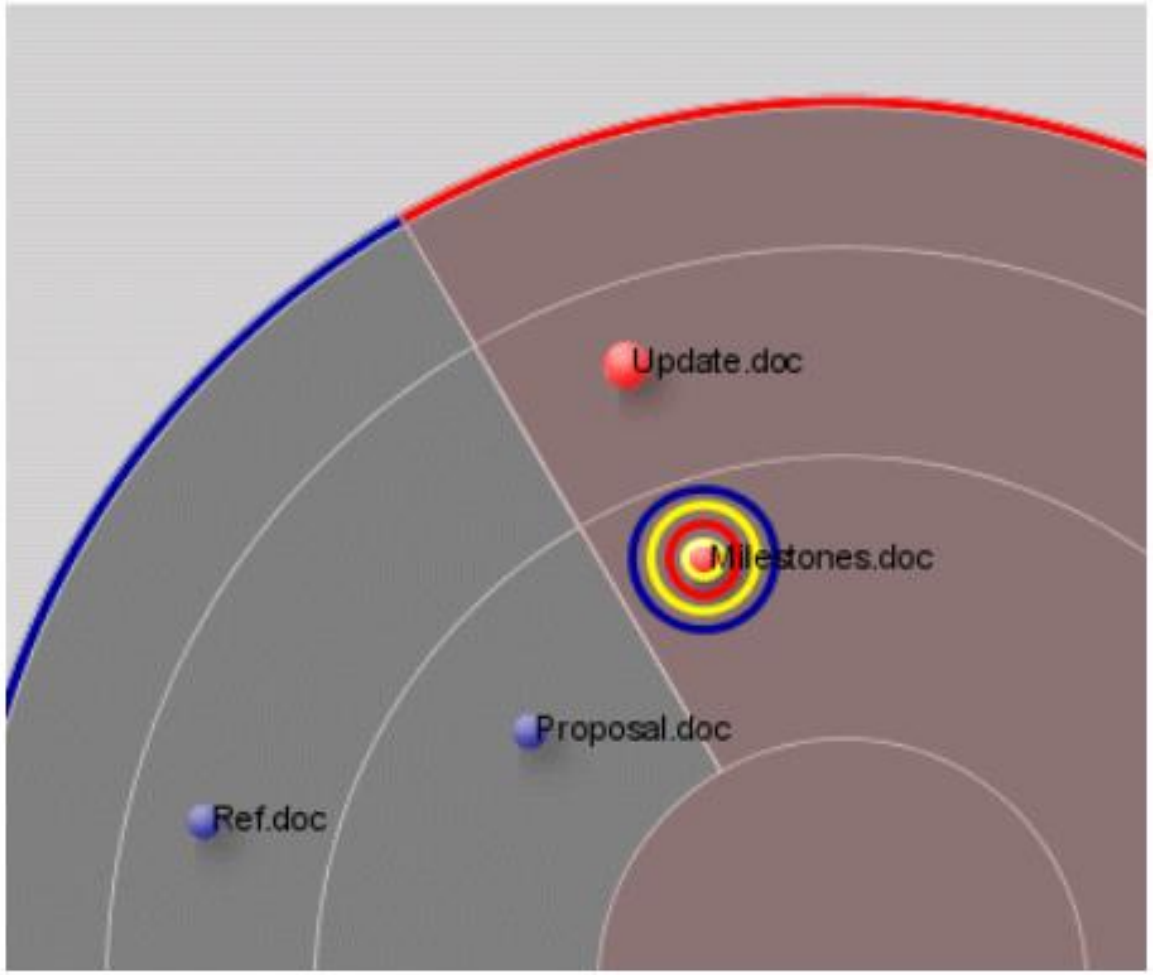


Figure 3: History Rings

Findings

- History
  - Owner: blue
  - Most Recent:
    - Blue
    - Yellow
    - Red (?)

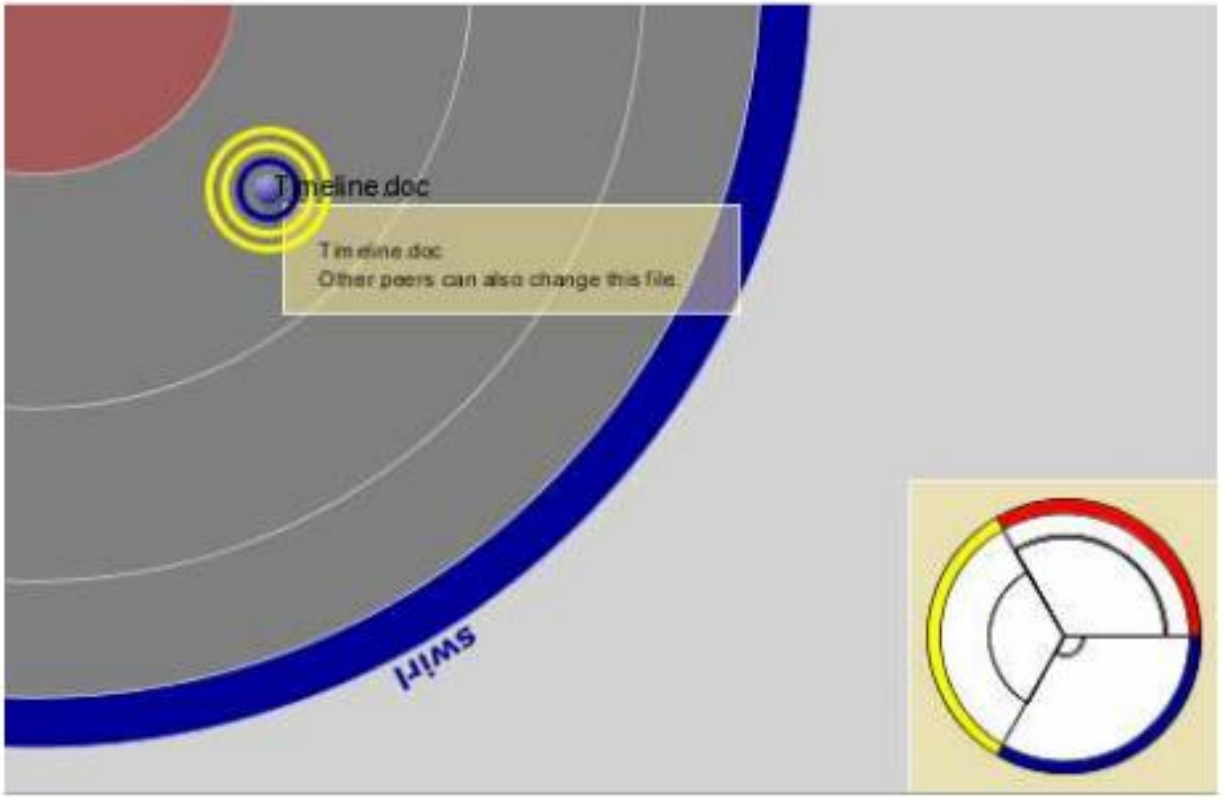
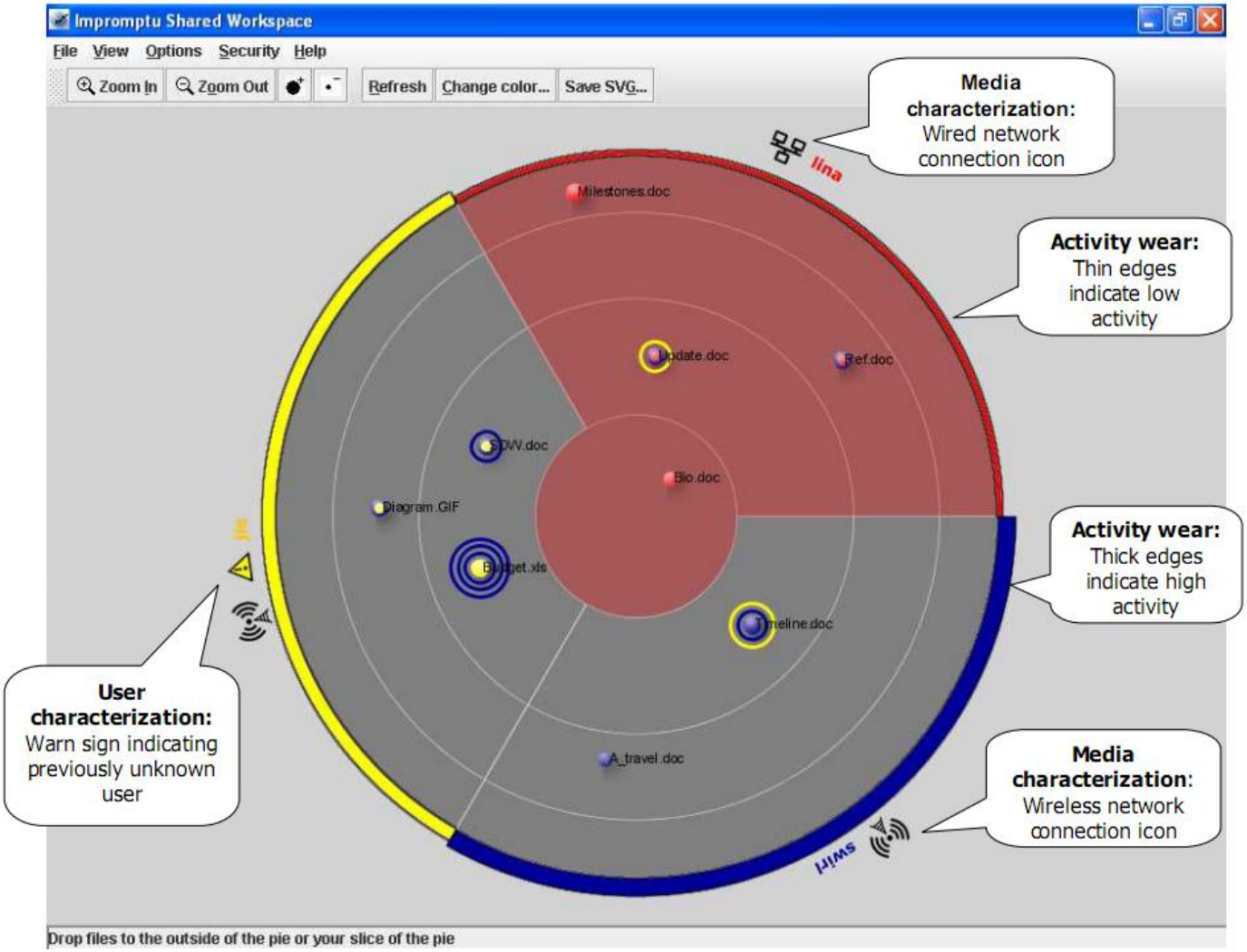


Figure 4: History Pie

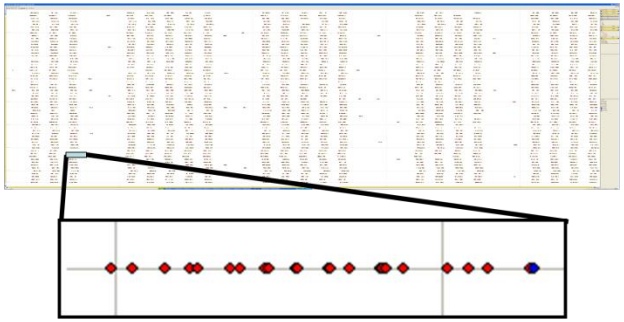
Future Work

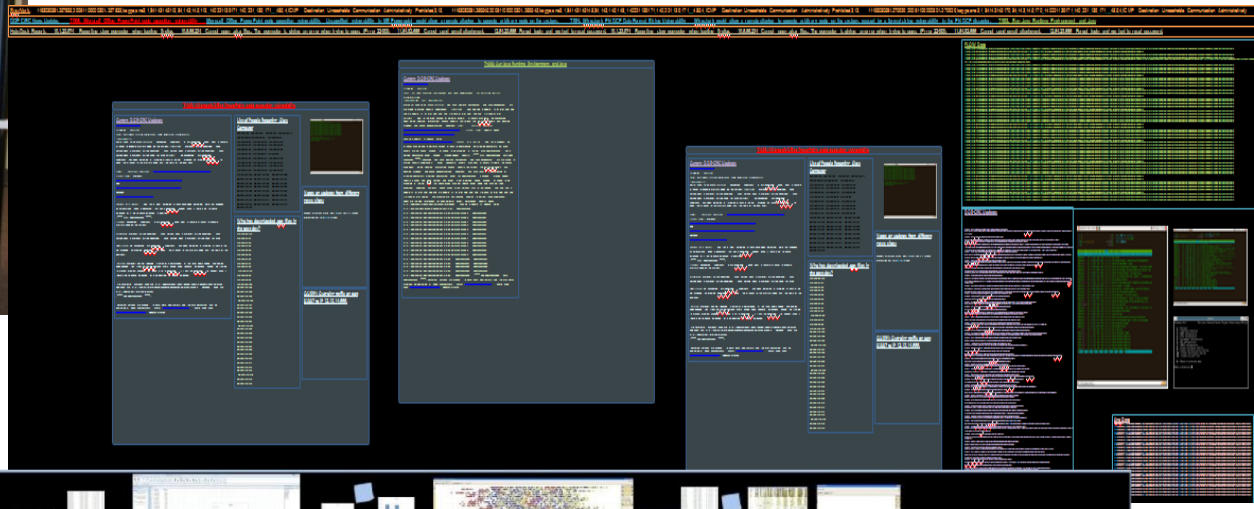

Impromptu Shared Workspace
File View Options Security Help
Zoom In
Zoom Out
Refresh
Change color...
Save SVG...
Media characterization: Wired network connection icon
Activity wear: Thin edges indicate low activity
Activity wear: Thick edges indicate high activity
User characterization: Warn sign indicating previously unknown user
Media characterization: Wireless network connection icon
Milestones.doc
Update.doc
Ref.doc
Bio.doc
Diagram.GIF
Timeline.doc
A_travel.doc
lina
swin
Drop files to the outside of the pie or your slice of the pie

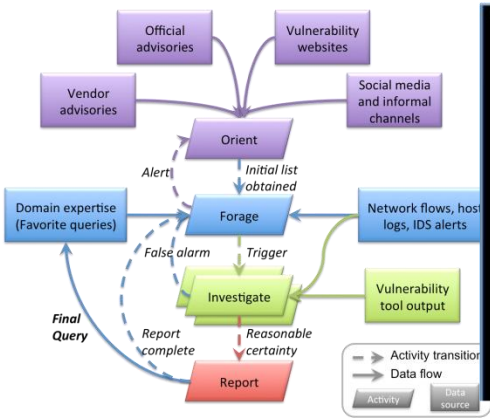
Critique

- Expandable Grid
  - Pros
    - Good design
  - Cons
    - User study participants (no experience in sys admin)
- Impromptu
  - Pros
    - Good initial visualization concept
  - Cons
    - Scalability

Next week…






Official advisories
Vulnerability websites
Vendor advisories
Social media and informal channels
Orient
Alert
Initial list obtained
Domain expertise (Favorite queries)
Forage
Network flows, host logs, IDS alerts
False alarm
Trigger
Investigate
Vulnerability tool output
Final Query
Report complete
Reasonable certainty
Report
Activity transition
Data flow
Activity
Data source