

Research Statement

Robert W. Reeder

My primary research interests are at the intersection of human-computer interaction (HCI), computer security, and online privacy, in an area known as HCISEC. I seek to understand computer users' needs for security and privacy in their computing and to develop user interface designs that allow users to better manage the security and privacy of their data. I believe this work is increasingly important as we share more data – especially personal data – in a networked world.

Thesis work

In my thesis work, I have created an information visualization technique, called Expandable Grids, for creating, viewing, and editing – in a word, *authoring* – security and privacy policies, such as file system access control policies and website privacy policies.

Expandable Grids are a solution to problems with the inadequate but dominant paradigm for policy-authoring interfaces, the "list-of-rules" paradigm.

List-of-rules interfaces are centered around a list of a policy's rules, which state what users have what access to what data. For example, a rule may state that a user "jsmith" can "execute" the "calc.exe" program. Users and data may be grouped, and a rule may apply to a whole group; for example, a rule might state that the group "Employees" cannot "read" the

"salaries.xls" file. In list-of-rules interfaces, rules may be selected one-at-a-time from the list for viewing and editing. The list-of-rules model has at least two major drawbacks. First, group membership information is not displayed in context with the rules. Second, rules may interact with each other, and even conflict with each other. List-of-rules interfaces do not give any indication of these rule interactions; instead it is left to the policy author to figure out how rules will interact.

In contrast to list-of-rules interfaces, Expandable Grids show group membership and show *effective policy*; that is, they show precisely what a policy allows or does not allow, rather than merely showing the rules from which effective policy is derived. Expandable Grids consist of a matrix with hierarchical axes that can be expanded or contracted to show more or less

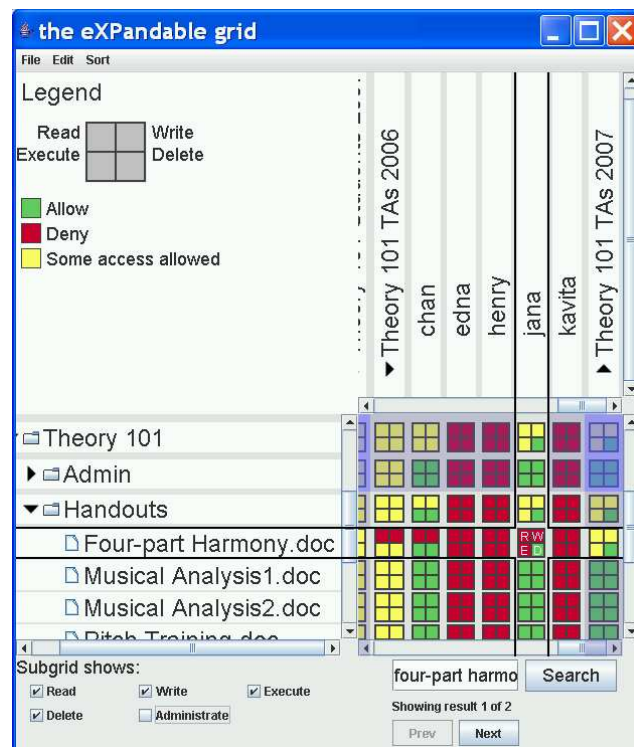


Figure 1. A user interface I built for setting Windows XP file permissions based on the Expandable Grids concept. The interface shows files and folders in the tree on the left, users and groups in the tree on top, and effective policy in the colored squares within the grid.

policy detail. Because they show effective policy directly, Expandable Grids do not require policy authors to determine subtle interactions amongst rules.

With collaborators, I have implemented three user interfaces that use the Expandable Grids idea, including one for setting file permissions in a Windows file system (shown in Figure 1), one for viewing website P3P privacy policies, and one for managing physical access control policies in an office building. I have conducted user studies testing the first two of these interfaces. In one study comparing the Expandable Grids interface for setting file permissions with the native Windows file permissions interface, users performed vastly more accurately and faster on a broad range of file-permissions tasks using the Expandable Grids interface. I published this work at CHI 2008, the top ACM conference in human-computer interaction [2].

Other past work

Access control needs analysis

As part of the Grey project at Carnegie Mellon University, I contributed to an effort to understand people's needs for access control to their offices and laboratories in our building. Grey is a distributed access-control system that allows users to unlock doors with smartphones and allows those users who control resources, such as their offices, to create access-control policy anytime and from anywhere on their smartphones. As part of an effort to design better user interfaces for managing Grey access-control policies, we conducted interviews with Grey users over the course of a year of Grey usage to elicit their ideal policies and the policies they actually implemented with Grey and with physical keys. We created a new methodology for evaluating access control systems by comparing ideal policies with implemented policies. With our new methodology, we were able to identify several areas in which Grey is an improvement over physical keys as well as several potential areas for improvement in the Grey user interface. We recently published a paper on this effort at CHI 2008 [1].

Policy-authoring user study

While a summer intern at IBM's T.J. Watson Research Center in 2006, I worked with SPARCLE, a Web application for authoring enterprise privacy policies, the kind of policies a company might write to govern how their employees are allowed to handle customers' personal data. I ran a user study in which I analyzed the errors users made in the policies they created with SPARCLE. This work led to a paper [3] identifying several policy-authoring usability challenges, such as resolving rule conflicts and finding group membership information. Working with SPARCLE also led me to the idea for Expandable Grids, which address several of the policy-authoring usability challenges. During the summer, I also filed a patent application covering the Expandable Grids idea.

Planned future directions

In future work, I plan to apply my expertise to applications that are likely to have high social value and impact. In particular, my expertise is in user needs analysis, data collection, functional interface design, experimental design, and information visualization. I hope to apply this expertise to the human aspects of computer security and privacy. In the short term, I have two areas in which I plan to expand my work: usable access control and configuration.

Usable access control

Numerous interesting research questions remain in the area of usable access control. The Expandable Grids idea, the focus of my thesis work, is a user interface technique for allowing for accurate authoring of fine-grained, large policies by novice policy authors. It does not necessarily address authoring of small policies (e.g., policies involving a handful of friends, rather than hundreds or thousands of system users), authoring of coarse-grained policies (e.g., policies in which access is either allowed or denied to all resources or all users, rather than being given out resource-by-resource or user-by-user), or authoring by experts (e.g., system administrators). Moreover, we do not even know whether these contexts are important for usability researchers to address. Important research questions include:

1. In what contexts are small and coarse-grained policies useful and sufficient?
2. In these contexts, are simple text-based or list-of-rules interfaces sufficient for supporting accurate policy authoring? Or are more advanced visual interfaces needed even for small and coarse-grained policy authoring?
3. Do Expandable Grids interfaces help policy-authoring experts, or do experts perform best with text-based or scripting-language interfaces? If the latter, can we combine visualization with text-based or scripting-language approaches to improve expert performance?

I would like to study novice users' needs for policy authoring in a variety of domains through interviews and by capturing their actual policies. I particularly wish to study new domains in which user privacy concerns and behavior are still not fully understood, such as online social networks, instant messaging, and shared calendars. Once I have established a better understanding of user needs for policy authoring in different contexts, I would develop interface techniques to address them. I would also like to adapt my ideas in policy visualization to interfaces for experts, if I can identify a group of experts to work with.

Usable configuration

In a second line of future research, I plan to find the common causes behind configuration errors and develop user-interface solutions to address them. I see policy authoring, an application on which my thesis is centered, as an example of the larger set of configuration tasks. Configuration tasks involve setting parameters of system operation. Examples of difficulty with configuration abound; probably every computer user has encountered difficulty configuring a printer, setting up an email client, or installing a new software application. In the security realm, recent studies have revealed vulnerabilities or inefficiencies in configurations for home wireless networks, BGP routers, DNS servers, firewalls, and operating systems. Configuration problems are especially difficult for users because they are encountered infrequently (thus, users may never develop expertise at solving them) and are usually secondary to a user's primary computing task (e.g., setting up the printer is a secondary goal to printing a document).

There are usually common patterns to usability failures and I suspect that there are a few common causes to configuration errors, e.g., in many cases users do not know where to start when they have a configuration problem, or they find configuration terminology confusing. I plan to find these common causes by collecting a large set of configuration problems from the research literature and from Web forums and categorizing the problems by cause. Once I understand the primary causes of configuration errors, I will develop solutions. Likely

products of this research include a taxonomy of the causes of configuration errors, a list of design principles for mitigating these errors, and specific interface designs and/or visualizations that help with configuration tasks.

Additional research interests

While I have some specific directions in which I hope to go next, I also maintain flexibility in defining my future work. My interests range from the specific field of usable security and privacy to the broader field of human-computer interaction, including information visualization, interface evaluation techniques, cognitive modeling, and intelligent user interfaces. I hope to work in a collaborative environment in which my colleagues' ideas and directions help shape my own. At CMU, I have had fruitful collaborations with researchers in the theoretical and systems aspects of security and privacy, as well as researchers in HCI. I hope to continue my career in an environment in which such collaboration is expected and encouraged.

References

* For a complete list of publications, please see my C.V.

1. Bauer, L., Cranor, L.F., Reeder, R.W., Reiter, M.K., and Vania, K. A User Study of Policy Creation in a Flexible Access-Control System. Conference paper accepted to *ACM SIGCHI Conference on Human Factors in Computing Systems (CHI '08)*. 2008.
2. Reeder, R.W., Bauer, L., Cranor, L.F., Reiter, M.K., Bacon, K., How, K., and Strong, H. Expandable Grids for Visualizing and Authoring Computer Security Policies. Conference paper accepted to *ACM SIGCHI Conference on Human Factors in Computing Systems (CHI '08)*. 2008.
3. Reeder, R.W., Karat, C.-M., Karat, J., and Brodie, C. Usability Challenges in Security and Privacy Policy-Authoring Interfaces. Conference paper presented at *INTERACT 2007*. Published in Springer *Lecture Notes in Computer Science (LNCS 4663, Part II, pp. 141-155)*. 2007.