Design Principles and Patterns for Computer Systems That Are Simultaneously Secure and Usable

by

Simson L. Garfinkel

S.B., Massachusetts Institute of Technology (1987)
S.B., Massachusetts Institute of Technology (1987)
S.B., Massachusetts Institute of Technology (1987)
M.S., Columbia University (1988)

Submitted to the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy in Computer Science and Engineering

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

May 2005

Author . . . .
Department of Electrical Engineering and Computer Science
May 16, 2005

Certified by . . . .
David D. Clark
Senior Research Scientist
Thesis Supervisor

Certified by . . . .
Robert C. Miller
Assistant Professor
Thesis Supervisor

Accepted by . . . .
A. C. Smith
Professor
Chair, Committee on Graduate Students

Design Principles and Patterns for Computer Systems That Are Simultaneously Secure and Usable

by

Simson L. Garfinkel

Submitted to the Department of Electrical Engineering and Computer Science
on May 16, 2005, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy in Computer Science and Engineering

Abstract

It is widely believed that security and usability are two antagonistic goals in system design. This thesis argues that there are many instances in which security and usability can be synergistically improved by revising the way that specific functionality is implemented in many of today's operating systems and applications.

Specific design principles and patterns are presented that can accomplish this goal.

Patterns are presented that minimize the release of confidential information through remnant and remanent data left on hard drives, in web browsers, and in documents. These patterns are based on a study involving the purchase of 236 hard drives on the secondary market, interviews conducted with organizations whose drives had been acquired, and through a detailed examination of modern web browsers and reports of information leakage in documents.

Patterns are presented that enable secure messaging through the adoption of new key management techniques. These patterns are supported through an analysis of S/MIME handling in modern email clients, a survey of 469 Amazon.com merchants, and a user study of 43 individuals.

Patterns are presented for promoting secure operation and for reducing the danger of covert monitoring. These patterns are supported by the literature review and an analysis of current systems.

In every case considered, it is shown that the perceived antagonism of security and usability can be scaled back or eliminated by revising the underlying designs on which modern systems are conceived. In many cases these designs can be implemented without significant user interface changes.

The patterns described in this thesis can be directly applied by today's software developers and used for educating the next generation of programmers so that longstanding usability problems in computer security can at last be addressed. It is very likely that additional patterns can be identified in other related areas.

Thesis Supervisor: David D. Clark
Title: Senior Research Scientist

Thesis Supervisor: Robert C. Miller
Title: Assistant Professor

Acknowledgments

While a dissertation is meant to represent the work of a single person, every dissertation is necessarily the result of numerous interactions between the author, the author's advisors, peers, colleagues, friends, and family. This one is no different.

Thesis advisors and readers

Foremost, my thanks are with my thesis advisors, David Clark and Rob Miller. Both of them have worked with me for years to create not only this document and the research behind it, but to help me make the transition from journalist to scientist. They have shared with me their time, their resources, and their judgment. They have helped me to correct numerous errors with this document—not merely typographical errors, but deep errors in thinking, purpose and presentation. All of the errors that remain are mine alone; I am far better for my association with them.

I would also like to thank my thesis readers, Ron Rivest and Danny Weitzner. Both of them offered me numerous comments in writing and during my defense which made this document much better than it would have otherwise been.

Hard drive study

Mig Hofmann, Peter Wayner, and several employees at Microsoft graciously told me of good places to obtain used hard drives and, in some cases, even accompanied me on my collection trips.

Amy Bruckman at Georgia Tech suggested that I read the *Ethical Principles and Guidelines for the Protection of Human Subjects*, generally known as the "Belmont Report." This information proved very important for me to ensure that this work proceeded with the highest ethical standards.

At MIT Abhi Shelat and Ben Gelb both worked with me to make sense of the 112 gigabytes of data that I acquired. Abhi's credit card recognizer was instrumental in helping us to find the data that ultimately brought the study so much attention in the general media—a vital element to having this work make an impact on computer users everywhere. Ben's email histogram tool proved invaluable in tracking down the names and identities of people whose information we had recovered.

Browser sanitization study

Marc Rotenberg suggested comparing the "clear history" and "reset" features in Internet Explorer and Apple Safari. Marc is always a source of good ideas; my only regret is that we were not able to co-author a paper together on this topic, as we had originally planned.

Regulatory approaches

The idea of using icons to denote functions in programs appears to have originated with Cranor, Resnick and Gallo.[CRG97] The icons presented with the "Pure Software Act of 2006" were created by TechnologyReview.com senior graphic designer Matthew Bouchard. Jonathan Zittrain at Harvard Law School offered many helpful comments on the proposal, as did Steven Bauer at MIT. Likewise, the "RFID Bill of Rights" was first published in *Technology Review*. My editor Herb Brody was instrumental in giving me the editorial freedom to pursue both ideas, and then on forcing me to make the article as good as it possibly could have been. Overall, some of the best technology writing that I have ever done was under Herb's supervision. I miss writing for him.

Laura Ruby at Microsoft very graciously discussed accessibility issues with me and provided me with copies of her writings. Carolyn Hodge and Fran Maier at TRUSTe reviewed the section on their organization and offered useful corrections.

S/MIME survey

The idea for the S/MIME survey was originally suggested by Jean Camp when she was at Harvard's Kennedy School. Sean Smith at Dartmouth College and John Linn at RSA Security provided useful comments on the survey design and questions, as did David Clark, Karen Sollins and Min Wu at MIT.

The work on the S/MIME survey was done in conjunction with David Margrave at Amazon.com, Jeffrey I. Schiller at MIT Information Systems, Erik Nordlander at CSAIL, and Robert C. Miller. This work was previously published in part as [GSN$^+$05] and [GNM$^+$05]. I am grateful to my co-authors for their permission to incorporate that work into this thesis.

Apart from allowing its employees to participate in the study, Amazon.com did not contribute monetarily to the S/MIME survey and does not necessarily endorse the conclusions and recommendations that appear in this dissertation.

PKI

My most sincerest thanks are due to Peter Gutmann and Carl Ellison for teaching me to be critical of PKI. Thanks are also due to Loren Kohnfelder for reading key sections of my thesis and offering his commentary.

Thanks also to Mary Ellen Zurko at IBM, to the engineers at Groove, to Jan R. Brands at Philips, and to all of the members of the hcisec mailing list on Yahoo! Groups for engaging in interesting discussions about PKI philosophy and practice.

Johnny 2

The Johnny 2 study never would have taken place had not Alma Whitten blazed the trail with her original paper *Why Johnny Can't Encrypt*. Thanks are due to her for sparking much of the interest in the field of HCI-SEC which continues to this day, and for answering my numerous questions regarding her study.

Peter Gutmann suggested the phrase "key continuity management" and provided me with many examples of PKI's failure, helping me to realize that I wasn't the only person in the room who thought that PKI was an unworkable solution.

Microsoft's security team, especially David Ladd and Scott Culp, offered insight, suggestions, and answered many questions regarding this project at various times over the past year.

Design principles and patterns

Chris Noessel at Microsoft Research graciously reviewed my chapter on design patterns. He provided a lot of good suggestions and recommendations on ways that I could tighten up the text; the chapter benefited immensely from his input.

The inclusion of the "Principle of Least Surprise" is a result of an email exchange that I had with Jerome Saltzer, who told me that he was now using this language instead of his 30-year-old principle of "Psychological Acceptability." Although Saltzer said that he doubts the term (or the concept) originated with the paper he wrote with Michael Schroeder [SS75], I have been unable to find any prevous references that described this design principle with such clarity.

The application of design principles to the field of HCI-SEC was pioneered by the work of Whitten and Tygar [WT98], and by Yee [Yee02]. I am indeed fortunate that I can stand on their shoulders.

MIT

Since arriving at MIT I have had been a member of the Advanced Network Architecture Group and have truly enjoyed my associations there. It has been a wonderful place to work, made all the better by the researchers, staff, and student members. I'd especially like to express thanks to Becky Shepardson for making sure that things in the group run so smoothly.

I have also benefited tremendously through my associations with the Cryptography and Information Security research group, and especially with Ron Rivest, Silvio Micali, Ben Ardita, Susan Hohenberger, Abhi Shelat, Stephen Weis, and Be Blackburn, all of whom have provided both intellectual stimulation, friendship, and emotional support.

And a special thanks to Paula Michevich and Maria Sensale at the CSAIL reading room. While working on this thesis, I have been helped by their skills in procuring both journal articles and chocolates. I shall miss them—and their yummies–very much.

A personal note

At the start of 2001, I decided to return to graduate school and pursue a degree in computer science. I received significant encouragement from Eric Grimson, who had been my recitation instructor for an introductory computer course in the fall of 1984. Professor Grimson's encouragement convinced me that I really had a chance of being accepted into the program.

Frans Kaashoek sent me an email message in the spring of 2002 telling me that I had indeed been accepted; this was followed by a letter from the department informing me that I had been awarded an MIT Presidential Fellowship. It was this award that cemented my decision to attend MIT: I am indebetted to Provost Robert Brown for being the program's champion.

During the fall of 2002 I spoke with many MIT professors and researchers in an attempt to identify a suitable research problem for me to work on. Discussions that I had during that time with Jerry Saltzer, Frank Field and Joel Moses were all helped me to decide on a thesis that would explore the apparent conflict between usability and security.

Professor Ron Rivest allowed me to be his Teaching Assistant during the fall of 2003 for his course *6.857: Cryptography and Computer Security*. The following Spring, I had the good luck to be a Teaching Assistant for Jerry Saltzer and David Karger in the course *6.033: Computer System Engineering*. Some of the ideas presented in this thesis—especially the system's approach to usability engineering—are a direct result of my close contact with those three professors.

Other ideas presented in this thesis are the result of discussions with attendees of the 2003 CRA Conference on Grand Research Challenges in Information Security & Assurance[CRA03] and the 2004 DIMACS Workshop on Usable Privacy. [CAM$^+$04] I am indebetted to Gene Spafford for inviting me to attend the CRA conference and to Lorrie Faith Cranor for inviting me to both attend and present at DIMACS. I am also indebetted to Gene for agreeing in February 1990 to be my co-author on the book *Practical Unix Security*. [GS91] Gene and I have been collaborators and friends for the past 15 years; it has been both a productive and pleasurable relationship.

It had been one of my most sincerest hopes to show this completed thesis to Jef Raskin, who I met in 1996 and who taught me about many things—not only about usability and computers, but also about model aircraft, child rearing, and the gentle art of leading a humane life. Sadly, this was not to be, as Jef passed away on February 26, 2005, after a brief and intense battle with cancer.

Finally, I need to express my thanks, appreciation and gratitude to my wife Beth Rosenberg and my three children, Sonia, Jared, and Draken, all of whom have sustained me on this massive project and have been tolerant of the stress that it has caused in our home.

Belmont, Massachusetts
April 2005