Users' Conceptions of Web Security: A Comparative Study

Batya Friedman[1], David Hurley[1], Daniel C. Howe[1], Edward Felten[2], Helen Nissenbaum[3]

[1]The Information School
University of Washington
Seattle, WA 98195-2840 USA
+1 206 616 2548
batya@u.washington.edu
hurley@u.washington.edu
dchowe@u.washington.edu

[2]Dept. of Computer Science
Princeton University
35 Olden Way
Princeton, NJ 08544 USA
+1 609 258 5906
felten@cs.princeton.edu

[3]Center for Human Values
Princeton University
5 Ivy Lane
Princeton, NJ 08544 USA
helen@phoenix.princeton.edu

ABSTRACT

This study characterizes users' conceptions of web security. Seventy-two individuals, 24 each from a rural community in Maine, a suburban professional community in New Jersey, and a high-technology community in California, participated in an extensive (2-hour) semi-structured interview (including a drawing task) about Web security. The results show that many users across the three diverse communities mistakenly evaluated whether a connection is secure or not secure. Empirically-derived typologies are provided for (1) conceptions of security based on users' verbal reasoning, (2) the types of evidence users depend upon in evaluating whether a connection is secure, and (3) conceptions of security as portrayed in users' drawings. Design implications are discussed.

Keywords

Security, user conceptions, user differences, user models, value-sensitive design, Web models, Web security, WWW

INTRODUCTION

Since "9/11," even greater international emphasis has been placed on the importance of Web security. This study contributes to the user-centered security literature [2] by focusing on how users across diverse communities conceptualize Web security.

METHODS

Seventy-two individuals, 24 each from a rural community in Maine, a suburban professional community in New Jersey, and a high-technology community in California, participated in an extensive (2-hour) semi-structured interview concerning users' conceptions, views, and values about Web security. Equal numbers of men and women participated from each community (mean, 42 years; median, 40; standard deviation, 14.8; range, 19 – 75).

CHI 2002, April 20-25, 2002, Minneapolis, Minnesota, USA.
ACM 1-58113-454-1/02/0004.

We report here on one section of the interview that focused on users' conceptions of Web security. Participants were first asked to define a secure connection. Then participants were shown actual screen shots of a browser connecting to a Web site and asked to recognize a secure connection. For each of four screen shots, participants were asked to state if the Web connection was secure or not secure as well as to provide the rationale for their evaluation. Finally, to elicit participants' non-verbal knowledge about Web security, participants were asked to revise a drawing of the Web that they had made earlier in the interview to reflect a secure connection. Thus, both non-verbal and verbal understandings were assessed.

RESULTS

Definition of a Secure Connection

When asked to define a secure connection, participants (76%) primarily provided one of three definitions. *Transit* (36%) refers to protecting the confidentiality of information while it moves between machines on the Web. *Encryption* (29%) refers to the specific mechanism of encoding and decoding information. *Remote Site* (11%) refers to protecting information once it has arrived at its destination on the Web. High-technology participants (83%) provided correct definitions of a secure connection (e.g., transit, encryption, and secure protocol) more frequently than rural (52%) ($p < .05$) but not suburban participants (68%).

Recognition of a Connection as Secure or Not-Secure

Across communities, roughly half of the participants correctly recognized a secure connection when shown actual screen shots of a browser connecting to a Web site (rural, 50%; suburban, 46%; high-technology, 67%). In contrast, high-technology participants (92%) correctly recognized a non-secure connection more frequently than either rural (59%) or suburban (50%) participants ($p < .05$).

Table 1 shows the types of evidence participants used to evaluate a connection as secure or not secure when they viewed actual screen shots. As shown, participants depended upon primarily six types of evidence: 1. *HTTPS*

Table 1. Percentage of Types of Evidence Participants Used to Evaluate a Connection as Secure or Not Secure

Type of Evidence	Correct Eval.		Incorrect Eval.	
	Not Secure	Secure	Not Secure	Secure
1. HTTPS Protocol	16	20	0	9
2. Icon (Lock or Key)	45	53	45	18
3. Point in Transaction	11	2	0	9
4. Type of Information	2	18	27	27
5. Type of Web Site	2	0	27	0
6. General Distrust	5	0	0	18
7. Blue Line	3	4	0	0
8. Amount/Presence of Info.	1	0	0	0
9. Accessibility of Site	2	0	0	9
10. Text From Web Site	6	0	0	9
11. Alerts on Screen	2	2	0	0
12. Security Conventions	1	0	0	0
13. Transaction Completed	1	2	0	0
14. Unspecified	3	0	0	0
15. Uncodeable	2	0	0	0

Note: Some participants provided multiple types of evidence. All types of evidence were coded for each participant.

Protocol (e.g., "Usually, it says http for non-secure or standard and https for, the s meaning secure."); 2. *Icon* (e.g., "[The site is secure] just because the key is there."); 3. *Point in Transaction* (e.g., "It looks like one of the main pages on the site and usually main pages are non-secured connections."); 4. *Type of Information* (e.g., "That at least has the indication of a secure connection; I mean, it's obviously asking for a social security number and a password."); 5. *Type of Web Site* (e.g., "I can't imagine a bank would be online and not have security measures in there."); and 6. *General Distrust* (e.g., "I'm wary of the computer itself…I basically don't think any of the sites are secure.").

Visual Portrayal of a Secure Connection

When asked to draw and explain a secure connection in the context of their earlier drawings of the Web, participants (89%) sketched primarily five different representations: *Screen Shot* (12%) refers to users' conceptions of a secure connection in terms of a symbol on the screen, such as the key icon. *Direct Connection* (12%) refers to a direct line between the user's computer and the target Web site. *Secure Boundary* (14%) refers to a barrier, such as a firewall, that surrounds or protects the user's computer, a server, or the target Web site. *Encryption* (40%) refers to scrambling the information while it is in transit, and in sophisticated drawings, includes both an encoding and decoding of the message. *No Difference* (11%) refers to drawings that remained unchanged from the participant's initial drawing.

Participants' drawings were then analyzed in terms of whether they represented an understanding of a secure connection as something that applies to information while it is in transit from one machine to another, a correct understanding (see Figure 1a), or as something that applies to a specific "place" on the Web, an incorrect understanding (see Figure 1b). High-technology participants (74%) provided transit (i.e., correct) representations more frequently than either rural (33%) or suburban (46%) participants ($p < .05$).

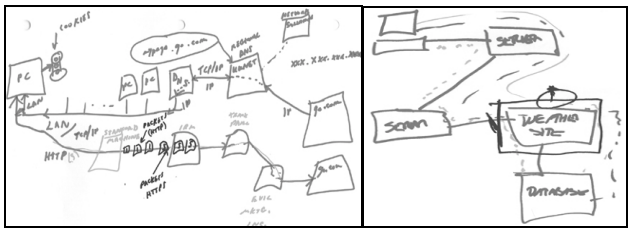

Figure 1a. **Figure 1b.**

Figure 1 The drawing on the left (Figure 1a) shows a conception of a secure connection in terms of encryption while the information is in "transit". Dark gray lines represent the secure connection. The drawing on the right (Figure 1b) shows a conception of a secure connection in terms of a secure boundary around a specific "place" on the Web. Dark gray lines represent the secure connection.

DISCUSSION

This study provides empirically-derived typologies of users' conceptions of Web security. In addition, the quantitative results suggest that many users across diverse communities inaccurately evaluate a connection as secure when it is not, and vice versa. In addition, users who correctly recognized connections as secure or not secure sometimes did so for incorrect reasons. One of the surprising findings was that the high-technology participants did not always have more accurate or sophisticated conceptions of Web security than did their rural and suburban counterparts.

Through Web browser design, we need to help users construct more accurate understandings of the meaning of a secure connection. Such design work can profit from this study's typologies. For example, the most frequently used icons to represent the security status of a connection – the key or padlock – convey the idea of a "place" that can be made secure. Such a conception runs counter to the more accurate meaning of a secure connection that refers to the security of the information in transit. We are currently building on the above typologies to guide our design work on implementations with the Mozilla Browser to support informed consent online [1].

ACKNOWLEDGMENTS

B. Bly, L. Hasler, P. H. Kahn, Jr., S. Olveda, T. J. Roderick, and D. Tatar contributed to this research. Colby College and Stanford University graciously provided the use of facilities for data collection. This research was funded by NSF Awards SES-0096131 and SBR-9729447.

REFERENCES

1. Friedman, B., Howe, D. C., and Felten, E. Informed consent in the Mozilla browser: Implementing value-sensitive design. *Proceedings of HICSS-35* (2002), IEEE Computer Society, Abstract p. 247, CD-ROM OSPE101.
2. Zurko, M. E., and Simon, R. T. User-centered security. *1996 ACM New Security Paradigm Workshop*, Lake Arrowhead, CA, (1997), 27-33.