Principles for Privacy Protection Software

Harry Hochheiser
Human-Computer Interaction Laboratory
Department of Computer Science, University of Maryland
hsh@cs.umd.edu

1. Introduction

The privacy impact of computer systems is clearly a hot topic in the mainstream press [10] and the research world [1]. Experience with systems that protect privacy and others that violate it provides an opportunity to evaluate issues raised by current tools and proposed designs. Study of the strengths and shortcomings of existing tools can help clarify needs for the next generation of tools. This paper will use an analysis of some of these systems as input for definition of a set of principles for privacy-protection systems.

2. A Mini-Taxonomy

Privacy protection systems can cover a wide range of functionality, from network protocols to end-user applications. An informal (and incomplete) categorization of privacy tools will help frame our discussion.

2.1 Network Privacy

Protocols like SSL, Crowds [9], and onion-routing [3] use a combination of encryption and/or request re-routing to provide data privacy and some anonymity. At a higher level, PGP uses encryption to protect the content of SMTP transactions, with the cost of a complicated user interface.

These systems have several limitations. Installation, configuration, and use of these tools can be complicated. Systems requiring modification of network protocols or access to proxy servers may be inaccessible to users who are behind firewalls or are users of custom Internet access software, such as clients used by AOL. Furthermore, these systems do not address the question of which data is disseminated.

2.2 Personal Information Privacy

The Lucent Personal Web Assistant (LPWA) [2], the Platform for Privacy Preferences (P3P) [8] and related tools offer increased privacy through mechanisms that control the release of personally

identifying information. LPWA provides a pseudonym proxy for logging in to web sites, giving user consistent access to registration based systems without revealing potentially sensitive personal data. P3P is a protocol for release of personal information according to a negotiation exchange between a website's practices and individual preferences.

LPWA and P3P address a crucial issue: protection of the contents of information disseminated, and the conditions under which that dissemination occurs. LPWA's use of pseudonyms is a potentially significant privacy innovation, but LPWA's utility is potentially limited by its proxy-based design, which may limit performance and decrease reliability.

P3P appears to have the appeal of putting users in the position of making informed decisions about the use of personal data. However, the vocabulary used to convey information practice disclosures is quite complex, opening the door to misinterpretation and confusion. Contract negotiations place users in a position of weakness: the negotiation process starts with a proposal from the server, followed by a response from the user. Revising the protocol to start with statements of the user positions might provide more effective privacy protection.

2.3 Preference Privacy

Systems that track items related to individual tastes and habits have been a focus of privacy controversy. Championed by some as necessary tools for provision of customized services, these systems pose significant privacy concerns, as illustrated vividly by the recent controversy over the RealNetworks RealJukebox player [10], which monitored playlists and sent them back to the software publisher.

CollabClio's privacy interface [4] is an example of one possible approach to user-controlled sharing of preferences. CollabClio provides shared, searchable web histories for an implicitly local community of users. Privacy concerns regarding this sharing of information are addressed by an intensional, rule-based restrictions on information that will be released. The result is support for specification of rules for withholding of information in the context of a tool designed for collaborative sharing of information. This is just one possible approach for negotiating a balance between privacy and constructive sharing of information. RealJukebox revealed information to a for-profit corporation without the user's knowledge or control. CollabClio provides information to co-workers and colleagues, while using an interface that supports user-controlled withholding of information. These questions of which information is released and to whom is it released are likely to be crucial determinants in the success or failure of privacy protection systems.

3.0 Implementation Issues

Experience in cryptography and security have illustrated the difficulty of building reliable systems. Designs that attempt to protect privacy have not been immune to compromising flaws. Recent efforts have identified privacy holes in LPWA, onion-routing, the anonymizer [5][12], and PGP addins to popular mailers[7].

4.0 Principles

Based on these observations, we can define several necessary (but still perhaps insufficient) principles for privacy protection systems:

4.1 Simplicity

Privacy systems must be as simple as possible, but no simpler. Avoidance of complexity in design, implementation and user interfaces will reduce the risk of failure, and user error.

4.2 Privacy must be the default

Current privacy solutions require significant active effort from each individual user. Since even experienced users often find systems too difficult to customize [6], tools that place significant burdens on users are unlikely to be used effectively. Designs that make privacy the default, require explicit assent, and use "opt-in" policies will provide the best protection.

4.3 No penalties for privacy

Designs that impose a penalty for privacy present an implicit tradeoff that may discourage users from protecting their privacy. Systems should minimize the performance, utility, and usability penalties might might be required for protecting privacy.

4.4 Users must be fully, accurately, and fairly informed

Negotiations implicit in systems such as P3P are meaningless without appropriate information. Systems that might affect privacy must provide accurate and complete information regarding the impact of user actions. Using the model of Social Impact Statements [11], Privacy Impact Statements might provide standardized formats for disclosure of privacy policies. Such disclosures must be unbiased, leaving determination of "utility" or "value" to the individual.

4.5 Services built on trust must be accountable

Tools like LPWA depend upon trust between service providers and users. This trust will be meaningless without appropriate enforcement of accountability based on an appropriate combination of legislation, industry self-regulation, and public oversight.

4.6 Privacy is security, and must be treated as such.

As privacy is information security for individuals privacy systems should be subject to the techniques of review and analysis used in computer security and cryptography communities to verify the security of proposed systems.

5. Conclusions

Although some problems - such as the retraction or revision of information once disseminated - may prove to be difficult, the barriers to effective privacy protection are social, not technical. As long as collectors and disseminators of data fail to make meaningful and binding commitments to protect privacy, software solutions for protect privacy will be fundamentally limited.

REFERENCES

1. Cranor, L., ed. Communications of the ACM, Special Issue on Internet Privacy, February 1999.

2. Gabber, E., Gibbons, P., Kristol, D., Mataias, Y. & Mayer, A. Consistent, Yet Anonymous, Web Access with LPWA. Communications of the ACM 42(2), February 1999. pg. 42-47.

3. Goldschlag, D., Reed, M., & Syverson, P. Onion Routing for Anonymous and Private Internet Connections. Communications of the ACM 42(2), February 1999. pg. 39-41.

4. Lau T., Etzioni, O. & Weld, D. Privacy Interfaces for Information Management. Communications of the ACM 42(10), October 1999. pg. 89-94.

5. Lewis, P. Peekaboo! Anonymity Is Not Always Secure. The New York Times, April 15, 1999. http://www.nytimes.com/library/tech/99/04/circuits/articles/15pete.htm

6.Mackay, Wendy. Triggers and Barriers to Customizing Software. Proceedings of CHI'91 Conference (New Orleans, LA April-May 1991). ACM Press, p. 153-160

7. Neumann, P., ed. Exchange/Outlook plug-in for PGP bypasses crypto. The Risks Digest, 19(81). June 16, 1998. http://catless.ncl.ac.uk/Risks/19.81.html#subj4.1

8. Reagle, J. & Cranor, L. The Platform for Privacy Preferences. Communications of the ACM 42(2), February 1999. pg. 39-41.

9. Reiter, M. & Rubin, A. Anonymous Web Transactions with Crowds. Communications of the ACM 42(2), February 1999. pg. 32-38.

10. Robinson, S."CD Software Is Said to Monitor Users' Listening Habits" New York Times, November 1,1999. http://www.nytimes.com/library/tech/99/11/biztech/articles/01real.html

11. Shneiderman, B. & Rose, A. Social Impact Statements: Engaging Public Participation inn Information Technology Design. In Human Values and the Design of Computer Technology, ed B. Friedman. CSLI Publications, Stanford CA, 1997.

12. Smith, Richard. Problems with Web Anonymizing Services: http://www.tiac.net/users/smiths/anon/anonprob.htm.