Authentication Privacy Principles Working Group

Interest in authentication systems has increased dramatically over the last two years. But widespread adoption of the technologies will only occur if individuals trust that strong privacy and security protections have been built into authentication systems.

The recent release of Microsoft XP and its expanded use of Passport, along with the release of the Liberty Alliance 2.0 specification, have intensified the focus on authentication technologies and the questions they raise about privacy and security.

The development of e-government services has begun to focus partly on plans to develop authentication systems to enhance citizen-centered government. However, ongoing discussions about government use of authentication systems raise concerns about government use of personal information and the creation of a centralized identity system or card.

New technologies for authentication make possible greater realization of the Internet's potential by making online transactions more seamless, tying together information on multiple devices, enabling yet unimagined services and taking us a few steps closer to a pervasive computing society. However, many authentication systems will collect and share personally identifiable information, creating privacy and security risks. To mitigate these risks, it is essential that authentication systems be designed to support effective privacy practices and offer individuals greater control over their personal information.

Through a consultative process a working group comprised of companies and public interest groups has drafted basic privacy principles that should be considered in the design and implementation of authentication systems. These principles could be used by companies developing authentication systems for guidance in building privacy and security protections into authentication technologies to use in consumer initiated transactions and government services. The principles would also serve as a marketplace guide for individuals and companies deciding which authentication system to implement or adopt. This interim report from the Working Group serves as a first consensus document on this issue.

The principles are intended to apply only to authentication in consumer initiated transactions and government services. Separate documents describing how the principles apply to each of these two areas with explanatory scenarios are under development to be released as part of the final report. While not covered by this document, many privacy concerns are also raised in authorization and security applications that may utilize credentials created in the authentication process. A separate working group is currently developing privacy guidance for one subset of these applications -- data mining/pattern analysis.

Please send comments or question on the Working Group or Interim Report to Ari Schwartz (ari@cdt.org), Alan Davidson (abd@cdt.org), or Paula Bruening (pbruening@cdt.org), at the Center for Democracy and Technology (202) 637-9800).

Interim Report

Privacy Principles for Authentication Systems

Authentication systems, in order to build trust in consumer initiated transactions and government services and consistent with applicable law, should:

1) Provide User Control — *The informed consent of the individual should be obtained before information is used for enrollment, authentication and any subsequent uses.*

Consent controls are vital to building trust in authentication systems. Authentication systems should offer individuals meaningful control over disclosure of their information. Under this principle, individuals may choose to use a single form of authentication that always discloses the same information or credential for all interactions, or choose to employ a variety of authentication tools for different transactions. This principle is particularly important in systems designed to share attributes and/or also serve as authorization systems, which will likely be successful only if they balance added convenience with trust in the system. Individuals should not be forced to accept the sharing of information for secondary uses as a condition of utilizing the authentication or data transfer system.

2) Support a Diversity of Services — *Individuals should have a choice of authentication tools and providers in the marketplace. While convenient authentication mechanisms should be available, privacy is put at risk if individuals are forced to use one single identifier for various purposes.*

Concerns persist that one or a very few implementations will be used for multiple purposes, coercing individuals and diminishing the ability of authentication systems to enhance privacy. This need not be the case. Authentication systems should be designed to support development of a marketplace offering multiple services that deliver varying degrees and kinds of authentication. A marketplace with a diversity of services also helps to support the principle of user control. Rather than attempt to serve as the perfect single key, authentication services for individuals should function like keys on a key ring, allowing individuals to choose the appropriate key to satisfy a specific authentication need. Different government agencies, companies and organizations will likely need different types of authentication.

3) Use Individual Authentication Only When Appropriate —*Authentication systems should be designed to authenticate individuals by use of identity only when such information is needed to complete the transaction. Individual identity need not and should not be a part of all forms of authentication.*

Not all transactions need be tied to identity. In fact, different kinds of authentication happen all of the time. For example, a store may need only to verify that an individual can pay for a service without collecting personal information, as we do today with cash transactions. Or, in another example, a membership organization may need to verify that an individual is authorized to partake in an activity without gaining access to detailed personal information. Different types of transactions require different levels of confirmation.

Authentication systems that use identity create greater privacy concerns as they can become ripe for abuse and targets for identity fraud and theft. Identity based authentication should only be used when necessary. To enable user control, support a diversity of services and protect privacy, it will be important to use both identity authentication systems relying on pseudonymous identifiers and attribute authentication relying on anonymous attributes whenever possible.

Credentials created in individual authentication systems are particularly sensitive information. Secondary use and sharing of these credentials for purposes such as authorization or marketing often compromise privacy and security. In particular, entities should be aware that Identification numbers become open to greater privacy misuses if they are often used for secondary purposes. Therefore, multiple uses of these numbers should be discouraged.

4) Provide Notice —*Individuals should be provided with a clear statement about the collection and use of information upon which to make informed decisions.*

Notice should be given in a manner consistent with the technology and be provided before information is used for enrollment, authentication and any subsequent use. Notice should not occur several links removed from the enrollment and authentication processes. The notice should in no way be a burden to read or understand.

5) Minimize Collection and Storage— *Institutions deploying or using authentication systems should collect only the information necessary to complete the intended authentication function.*

Authentication systems can collect and share information in several ways. They may collect sensitive information for enrollment, vetting and verification of an individual; they may use a subset of a user profile as the primary purpose of any intended authentication; and they may facilitate the onward transfer of information for secondary purposes. It may be necessary to store some information to provide ongoing services. Information on retention practices should be available. In every instance, the information collected and stored should be limited to the minimum necessary to provide the intended authentication and service.

6) Provide Accountability - *Authentication providers should be able to verify that they are complying with applicable privacy practices.*

Privacy practices must be the cornerstone to building a trust relationship in authentication.[1] Training and regular audits are necessary to ensure that reasonable technical, administrative and physical privacy and security safeguards are in place. New privacy technologies can aid in tracking data flows for these purposes. Individuals, with appropriate authentication, should be able to access their own information used in the ordinary course of business and correct inaccurate information.

[1] All organizations collecting, maintaining or using personally identifiable information should develop internal practices that address applicable regulatory and self-regulatory guidelines, such as, the OECD Guidelines on the Protection of Privacy, the EU Directive on Data Protection, the Online Privacy Alliance guidelines, the US Financial Services Modernization Act, the US Health Information Portability and Accountability Act, as appropriate.

Glossary

(Italicized definitions are from Computer Science and Telecommunications Board, National Research Council, Who Goes There?: Authentication Through the Lens of Privacy (Washington, DC) National Academy Press, 2003.)

Attribute Authentication. Attribute authentication is the process of establishing an understood level of confidence that an attribute applies to a specific individual.

Attribute. An attribute describes a property associated with an individual.

Authentication. Authentication is the process of establishing confidence in the truth of some claim.

Authenticator. An authenticator is evidence that is presented to support the authentication of a claim. It increases confidence in the truth of the claim.

Authorization. Authorization is the process of deciding what an individual ought to be allowed to do.

Biometrics. Biometrics is the automatic identification or identity verification of individuals on the basis of behavioral or physiological characteristics.

Credential. Credentials are objects that are verified when presented to the verifier in an authentication transaction. Credentials may be bound in some way to the individual to who they were issued, or they may be bearer credentials. The former are necessary for identification, while the latter may be acceptable for some forms of authorization.

Enrollment. Enrollment is the process by which an individual person, corporation or device is issued a credential for an authentication system.

Identification. Identification is the process of using claimed or observed attributes of an individual to infer who the individual is.

Identifier. An identifier points to an individual. An identifier could be a name, a serial number, or some other pointer to the entity being identified.

Identity Authenticiation. Identity authentication is the process of establishing an understood level of confidence that an identifier refers to an identity. It may or may not be possible to link the authenticated identity to an individual.

Identity. The identity of X is the set of information about an individual X, which is associated with that individual in a particular identity system Y. However, Y is not always named explicitly.

Individual Authentication. Individual authentication is the process of establishing an understood level of confidence that an identifier refers to a specific individual.

Informed Consent. Informed Consent is an agreement made by an individual with the legal capacity to do so; who is so situated as to be able to exercise free power of choice, without the intervention of any element of force, fraud, deceit, duress, over-reaching, or other form of constraint or coercion; and given sufficient information of the subject matter and the elements of the transaction involved as to enable him or her to make an informed and enlightened decision. (See “Provide Notice” Principle).

Information Privacy. Information privacy protects the individual’s interest in controlling the flow of information about the self to others.

Pseudonymous Identifiers. A pseudonymous identifier is an identifier that cannot, in the normal course of events, be associated with a particular individual.

Vetting. Vetting is any process of examining and evaluating information or data provided for the purposes of the issuance of credentials.

Verification. Verification is any procedure in which a set of authentication credentials are validated using internal standards or third party confirmation.

The following companies and organizations[2] encourage the consideration of the Authentication Privacy Principles in the development, procurement and use of authentication technologies:

Center for Democracy and Technology
Consumer Action[3]
Corporate Privacy Group
eBay
Hewlett-Packard
Intel
Liberty Alliance[4]
Microsoft
NeuStar
TRUSTe[5]
VeriSign

[2] Several individuals are members of the working group and were instrumental in the development of the principles especially Deirdre Mulligan, Peter Swire, and Michael Willett.

[3] Consumer Action is a non-profit, membership-based organization that was founded in San Francisco in 1971. Since then, Consumer Action has continued to serve consumers nationwide by advancing consumer and privacy rights, referring consumers to complaint-handling agencies through its free multilingual hotlines, distributing educational materials in Chinese, English, Korean, Spanish, Vietnamese through its national network of 6,500 community based organizations, advocating for consumers in the media and before lawmakers, and comparing prices on credit cards, bank accounts, and long distance services.

[4] The Liberty Alliance Project was formed in September 2001 to establish an open standard for federated network identity. The Alliance has stated this will be accomplished by developing technical specifications that support a broad range of identity-based products and network devices. It is a consortium of more than 150 technology and consumer organizations working together towards this common goal. Sponsors of the Liberty Alliance include: America Online, Inc., American Express Travel Related Services, Bank of America Corporation, Communicator, Inc., Deloitte & Touche LLP, Electronic Data Systems, Inc., Entrust, Ericsson, Fidelity Investments, France Telecom, Gemplus , General Motors, Hewlett-Packard Company, Intuit, Inc., MasterCard International, NEC Corporation, Netegrity, Inc,, Neustar, Inc., Nextel Communications, Nippon Telegraph and Telephone Company, Nokia Corporation, Novell, Inc., NTT DoCoMo, Inc., Phaos Technology, Ping Identity Corporation, RegistryPro, Inc., Royal Mail Group plc, RSA Security Inc., SAP AG, SchlumbergerSema, Sony Corporation, Sun Microsystems, VeriSign, Inc., Visa International, and Vodafone Group Plc.

[5] TRUSTe is an independent, nonprofit organization dedicated to enabling individuals and organizations to establish trusting relationships based on respect for personal identity and information in the evolving networked world. Founded in 1997, TRUSTe runs an award-winning global privacy certification and seal program. Our seal programs are considered Safe Harbors for the Children's Online Privacy Protection Act (COPPA) and the EU Safe Harbor Framework. The TRUSTe seal is currently displayed on all of the Internet's portal sites and has been rated as the most trust-invoking seal online and the most visible symbol on the Internet. Today, TRUSTe maintains the largest privacy seal program with more than 1,500 companies' Web sites certified throughout the world. The TRUSTe coalition of sponsoring companies includes AOL Time Warner, AT&T Wireless, Intuit, the Japan Engineers Federation and Microsoft Corporation. TRUSTe boasts a large network of online and brick-and-mortar member companies, including BMW, Walt Disney Group, and The New York Times. TRUSTe is based in San Francisco and has an office in Washington, DC. Descriptions of TRUSTe's programs are available at http://www.truste.org.