A New Paradigm for Individuals in the Information Age

David Chaum

Computer Science Department, University of California, Santa Barbara, CA 93106

ABSTRACT

Today, individuals provide substantially the same identifying information to each organization with which they have a relationship. In a new paradigm, individuals provide different "pseudonyms" or alternate names to each organization. A critical advantage of systems based on such pseudonyms is that the information associated with each pseudonym can be insufficient to allow data on an individual to be linked and collected together, and thus they can prevent the formation of a dossier society reminiscent of Orwell's "1984".

A system is proposed in which an individual's pseudonyms are created and stored in a computer held and trusted only by the individual. New cryptographic techniques allow an organization to securely exchange messages or payments with an individual known under a pseudonym--without the communication or payments systems providers being able to trace messages or payments. Other new techniques allow a digitally signed credential to be transformed by the individual, from the individual's pseudonym with the issuing organization, to the individual's pseudonym with a recipient organization. Credentials can be transformed only between pseudonyms of a single individual, and an individual can obtain at most one pseudonym with a particular organization, but even a conspiracy of all organizations can gain no information from the pseudonyms about their correspondence. The combination of these systems can prevent abuses by individuals, while averting the potential for a dossier society.

Introduction

As the use of computers becomes more pervasive, they are bound to have substantial influence on our relationships with organizations. Currency and paper checks as a way to pay for goods and services will largely be replaced by electronic means. Electronic mail will be the main way we send and receive messages. Our personal credentials will often be presented in electronic form. Below, two different paradigms for automation of the informational relationships between individuals and organizations will each be illustrated by an example scenario.

Current paradigm

The current paradigm is characterized by "identification" of the individual during every transaction. In an example scenario based on the logical extension of this paradigm, credit card sized computers held by individuals would provide an identifying account number to an organization receiving payment from the individual card holder. In a similar way, the card might provide the name and mailing address of its holder to an organization with a need to send messages to the individual, routinely (e.g. monthly statements) or only under exceptional circumstances (e.g. manufacturers recall or request for return of rented or borrowed things). An organization may require credentials (e.g. credit, professional license, citizenship, good tenant, education, or past employment) of the individual for establishing or maintaining a relationship with the individual. When credentials are required by an organization, the card would provide detailed identification and references to that organization which would allow the credentials to be checked with other organizations. Notice that in this paradigm identification is required presumably to allow detection and remedies against abuses and frauds perpetrated by individuals, such as default of payment, situations requiring legal notice, or the use of false credentials.

These identifying numbers, addresses, and references allow the various records and transaction details relating to a particular individual to be linked and collected together into a "dossier" or comprehensive file on the individual. While limited dossiers can be and are assembled today, the amount and nature of data which could automatically be captured in the scenario above would radically increase the significance

of the dossier. For example, if all payments transactions are captured, a great deal about a person's habits, entertainment, travel, organizational affiliations, information consumption, etc. would be included in the dossier. Similarly, in an electronic mail environment, a comprehensive history of the identity of all correspondents as well as the timing and length of correspondences could be very revealing. Finally, links to previous activities and details of past associations might be of great significance. If it is possible for dossiers to be compiled, but their compilation is officially denied, there may be concern that compilation is taking place secretly. Even if compilation does not occur, there should still be concern that dossiers could be constructed at a latter time based on current records; it is very difficult to be convinced that all copies of some obsolete information are destroyed. It is worth noting that advances in some areas of computer science, such as pattern recognition, make automated analysis of dossiers a possibility.

New Paradigm

In a new paradigm, instead of identifying information, individuals provide each organization with a different "pseudonym" or alternate name. Pseudonyms would be created and stored in the credit card sized computer held by the individual. The critical advantage of systems based on such pseudonyms is that the information they contain is insufficient to allow data on an individual to be linked together, and thus they can prevent the formation of a dossier society, reminiscent of Orwell's 1984.

There are three fundamental kinds of interactions required in the new paradigm:

(1) individuals need to communicate with organizations,

(2) individuals need to pay or be paid by organizations, and

(3) organizations need to exchange information about individuals.

Sometimes the communication or payments can be anonymous, such as with a simple purchase at a shop or an inquiry about an organization's policy or services. In other cases, authorizing messages must come from the holder of a particular pseudonym, or confidential messages must be sent by an organization in such a way that they can only be received by the holder of a particular pseudonym. Organizations also need to communicate amongst themselves about an individual; the term credentials will be used for this kind of communication. Sometimes credentials are positive, such as a diploma or certificate of good health issued to an individual. The individual can then supply the credential to organizations other than the issuer. In other cases, a credential may be negative in the sense that it is in the individual's interest not to provide the credential information, such as reporting income from an organization to the IRS or informing a credit agency about an additional debt incurred.

The following introduces and highlights some of the desired properties and considerations in the design of each of these three components of the new paradigm.

Communication

A communication system in which messages are routed through a number of nodes, any one of which is able to obscure the correspondence between messages in its input and those in its output, was described by the author [1981]. This system was based on public key cryptography. From the perspective of the new paradigm, its important properties might be described as follows:

Individual protected from system provider Even the system provider can not trace a message under normal conditions.

Organization protected from individual The individual can use a digital pseudonym to provide "third party authentication" (see section on cryptographic techniques) of a message sent to the organization under the pseudonym.

Society protected from individual Threats or other illegal messages are traceable to the point of origin, but consensus of a large number of parties who may not be mutually sympathetic is required for each message traced, and thus a trace is unlikely to be carried out covertly.

Individual protected from organization An individual may send messages to an organization, without the organization being able to determine the origin of the message. An individual may receive messages from an organization without the organization knowning the location of the recipient. Such messages are sent with an "untraceable return address," which the individual supplies to the organization. An individual can create as many untraceable return addresses as desired, but none of these addresses can be linked together or to the individual. Untraceable return addresses can each be used only to send a single message, and thus the individual can control to a large extent the quantity and origin of messages received. Messages sent with an untraceable return address can be read only by the individual who created the address.

Payments

A new kind of payments system was proposed by the author [1982]. The basis of the scheme is a new kind of cryptographic system called a "blind signature" cryptographic system (also discussed in the next section), which allows a signer to make a digital signature without knowing what is being signed. The way this is used in a payments system is that an individual forms a bank note and the bank signs it--only after taking from the individual's account the amount of money corresponding to the kind of signature made. Then the individual transforms the signed note so that the bank can not recognize it but still maintaining the digital signature property that allows anyone to determine that the note was actually signed by the bank. When the individual pays an organization with the transformed note, the organization sends it to the bank. The bank checks the signature on the note, and that the note has not already been deposited, and credits the organization's account for the value of the signature on the note. From the point of view of the new paradigm, this payments system has the following properties:

Individual protected from system provider The provider of the payments system, such as a bank, is unable to determine the correspondence between notes withdrawn and notes deposited. Of course the payments system provider knows the balance of each account, and also when each account balance is changed. But because funds are withdrawn and held in a bearer form, something like unmarked bills, before being deposited to another account, knowledge of timing of changes in account balance does not necessarily reveal the correspondence between a particular withdrawal and the ultimate deposit of the same funds. Also because transfers are accomplished using amounts represented as units of standard denomination, much like coins and banknotes, the amount of deposited does not necessarily reveal the account the funds were withdrawn from.

Organization protected from individual An organization is able to clear a payment received from the individual and know with certainty that it will be honored.

Society protected from individual Stolen media use can be stopped once reported, and use before a stop payment is in place is traceable, at least to the recipient. Any payer (e.g. a customer of a black market, a person making a payoff or bribe) can reveal the payee.

Individual protected from organization When an organization receives payment from an individual, the organization is not able to trace the payment to the account from which it originated. If an individual makes payment, but the organization latter denies receipt of the funds, then the individual can demonstrate to the system provider that payment was received by the organization.

Credentials

Credential schemes allow the individual to control the transfer of information about the individual between organizations. The essential idea of these schemes is that each organization knows an individual by a different pseudonym, and the individual can transform a digitally signed credential received from an organization in a way that preserves the digital signature but changes the pseudonym within the credential. Credential schemes do not require a separate system provider. From the point of view of the new paradigm, credential schemes may have the following properties:

Individual protected from organizations Even a conspiracy of all the organizations can not derive any information from the pseudonyms about which pseudonyms correspond to a particular individual, or even which correspond to the same individual. If pseudonyms are changed periodically, and records from old periods are passed forward only through credentials, then it is possible for individuals to be assured that certain information from previous periods can not be linked to current pseudonyms.

Organizations/society protected from individual Individuals can not create or alter credentials; they may only transform them from one pseudonym to another. Credentials can not be transformed between pseudonyms of different individuals, even if many individuals conspire before the credential system is established. An organization can ensure that it receives at most one pseudonym from any individual. An individual can provide substantiation, which is capable of third party authentication, that some negative credential information was transmitted to an organization responsive to a particular request made by a second organization. The expectation of a positive or negative credential can be established for all clients of an organization, or on an individual bassis, such that if no credential is supplied then the negative one is assumed.

Background

Two major literatures are related to the present work: one largely to its impact on society, and the other to the predecessors of the fundamental cryptographic techniques which are the precursors of the mechanisms discussed above.

The Policy Debate

The computers and privacy debate is the subject government reports of many countries, tens of books, hundreds of scholarly articles in a variety of disciplines, and thousands of articles addressed at a broader audience. It is far beyond the scope of the present work to survey this vast literature (but see, e.g., the bibliographies of Harrison [1969] Latin [1976] and Stone & Stone [1979]). It is clear from this literature, however, that there is substantial public concern about the continuing emergence of an unprecedented collection of information by organizations about individuals.

There have been five major studies of actual systems and practices in English [DCDJC 1972; PPSC 1977; Rule 1973; Westin 1972; Younger 1972]. These have suggested three major policy alternatives: (1) freeze or dismantle the record collection systems planned or in place; (2) provide individuals with a right to inspect and challenge the accuracy of records about themselves, expect that only pertinent data will be collected, and expect that personal data will only be used for the purposes intended; (3) restructure the major systems using detailed personal information, such as taxation, credit, welfare, and employment, in such a way that they require less detailed information. The first alternative is of course not a credible option. The second alternative, in various forms, has been recommended by many, and has found its way into law. Proponents of the third approach maintain that the second does not actually address the privacy problem or the danger of a massive surveillance capability, and that a real solution requires some restructuring of the rules of major institutions.

Mention of the subtleties of the interelation between policy and mechanism appears conspicuously absent from these studies. Theorists, most notably Mumford [1934], have argued extensively that societal forces, such as policy, significantly influence development and adoption of new technologies. (Also see Kuhn [1962] for discussion of the power of societal forces within a scientific community.) In the other direction, the policy alternative(s) raised by the present work have not been considered in the policy literature, and thus they are an example of new mechanisms providing unanticipated policy alternatives. It appears from the literature that those scholars involved in the computer privacy debate and those scientists concerned with the mechanisms of information technology have drifted apart after only brief initial inquiries and a few defections from one camp to the other. It is hoped that the present work will re-open interaction between the two camps and spawn new contributions from each.

Cryptographic Techniques

The literature on cryptology is also rather broad, but much of it is concerned with classical cryptologic techniques, and is of little relevance here. In the last several years, there have been several major open meetings devoted to modern cryptology, and several new textbooks on the topic have appeared. Efforts in the field seem to be dividing up into a number of separate areas, such as protocols; verification of protocols; cryptanalysis of modern systems; development of new algorithms which implement standard types of modern systems; complexity analysis aimed at formalizing and ultimately proving cryptographic strength; and the whole spectrum of more applied concerns, from actual engineering, to applications of standard types of systems. The present work, however, is primarily concerned with development and application of new types of cryptographic techniques, and so only a summary of the various fundamental types of cryptographic systems proposed in the literature will be presented.

One-way functions (i.e. functions that are publically known, but whose inverse is supposed to be difficult for anyone to compute) were proposed first in the literature by Purdy [1974]. Lamport suggested a technique for providing "third party authentication," (a technique mentioned elsewhere in the present work, sometimes called a "digital signature" technique, in which, after an initial agreed on set-up, anyone can check a signed message and know that it could have only been formed by the holder of a particular secret key) based on one way functions [Diffie and Hellman 1976b]. Diffie and Hellman proposed the existence of commutative one way functions, offered an example algorithm, and showed how they could be used to build a "public key distribution system" (i.e. a way for two parties to develop the same secret key while only using a channel that provides authentication but no secrecy). So called "conventional" cryptographic techniques (a cryptosystem in which a function and its inverse can be derived from a secret key) appear to have been in use for thousands of years [Kahn 1967]. The possibility of commutative conventional cryptosystems was suggested and illustrated by an actual algorithm by Shamir, Rivest and Adleman [1981] in a solution to Floyd's mental poker problem. The existence of true public key schemes (cryptosystems in which the creator of a public one way function retains the exclusive ability to compute its inverse) was first proposed by Diffie and Hellman

[1976a], and a potentially viable algorithm was first suggested by Rivest, Shamir and Adleman [1978]. The possibility of publically generated invertible functions which commute with the functions of a public key system was suggested by Chaum [1983], and forms the basis of the blind signature payments system discussed in the present work. Actual algorithms have been developed which appear to meet the requirements for a blind signature system [chaum 1984a]. Parameterized blind signatures have also been suggested and actual algorithms proposed [chaum 1984b], that allow a greater flexibility in the payments and credentials mechanisms described.

Summary

A new paradigm, in which identification of individuals is replaced by use of cryptographic pseudonyms, can provide secure informational relationships while averting the potential for a dossier society.

References

(1) Chaum, D., "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, February 1981.

(2) Chaum, D., "Blind Signatures for Untraceable Payments", proceedings of CRYPTO 82, Plenum Press, 1983.

(3) Chaum, D., "New Secret Codes Can Prevent a Computerized Big Brother", Communications of the ACM, to appear.

(4) Chaum, D., "Parameterized Signatures", in preparation.

(5) Department of Communications/ Department of Justice, Canada, Privacy and Computers, Information Canada, Ottawa, 1972.

(6) Diffie, W. and Hellman, M.E., "Mulltiuser Cryptographic Techniques," NCC 1976a, pp.109-112.

(7) Diffie, W. and Hellman, M.E., "New Directions in Cryptography," IEEE Trans. Info. Theory, vol IT-22, pp. 644-654, November 1976b.

(8) Harrison, A. The Problem of Privacy in the Computer Age: An Annotated Bibliography, (2 volumes) Rand Report: RM-5495/1-PR/RC, Rand Corporation, Santa Monica CA, December 1969.

(9) Stone, E., and Stone, D., Information Privacy: A Bibliography With Key Word and Author Indices, Information Privacy Research Center Working Paper No. 6, Purdue University, Laffeyete IN, May 1979.

(10) Kahn, D., The Codebreakers: The Story of Secret Writing, Macmillan Co., N.Y., 1967.

(11) Kuhn, T.S. The Structure of Scientific Revolutions, University of Chicago Press, Chicago, 1962.

(12) Latin, H.A., Privacy: A Selected Bibliography and Topical Index of Social Science Materials, Fred B. Rothman & Co., South Hackensack, NJ, 1976.

(13) Mumford, L. Technics and Civilization, Harcourt, Brace and Co., N.Y., 1934.

(14) Privacy Protection Study Commission, Personal Privacy in an Information Society, U.S. Government Printing Office, Washington D.C., July 1977.

(15) Purdy, G.B., "A High Security Log-in Procedure," Communications of the ACM, vol. 17, no. 8, August 1974, p.442.

(16) Rivest, R., Shamir, A. and Adleman, L., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, vol. 21, no. 2, February 1978.

(17) Rule, James, Private Lives and Public Surveillance, Allen Lane, London 1973.

(18) Shamir, A., Rivest, R., Adleman, L., "Mental Poker," in The Mathematical Gardner, Klarner, D. (Ed.), Prindle, Weber & Schmidt, Boston, 1981, pp. 37-43.

(19) Westin, A. and Baker, M., Databanks in a Free Society: Computers, Record-Keeping, and Privacy, Quadrangle Books, N.Y., 1972.

(20) Younger, K., Report of the Committee on Privacy, Cmnd. 5012, Her Majesty's Stationery Office, London 1972.