Ames GRANT
7N-61-CR
280689

p.12

Baffling Big Brother

Peter J. Denning

July 16, 1987
(Revised July 31, 1987)

RIACS Technical Report TR-87.19

NASA Cooperative Agreement Number NCC 2-387

(NASA-CR-181401) BAFFLING BIG BROTHER (Research Inst. for Advanced Computer Science) 13 p

N91-70343

Unclas
00/61 0280689

Research Institute for Advanced Computer Science

Baffling Big Brother

Peter J. Denning

Research Institute for Advanced Computer Science
NASA Ames Research Center

RIACS Technical Report TR-87.19
July 16, 1987
(Revised July 31, 1987)

Smart cards and cryptography enable a new system of business transactions that balances the power of individuals to control how information about them is linked and disseminated against the need of organizations to be certain that credentials and payments are valid. Each person uses a different name (pseudonym) with each organization and a personal card computer manages all the names and cryptographic protocols. The most difficult protocols are for credentials and payments. Even though we complain about a world in which our transactions are too easily traced, would we want a world in which none of our transactions could be traced?

This is a preprint of the column *The Science of Computing* for *American Scientist 75*, No 5 (September-October 1987).

Work reported herein was supported in part by Cooperative Agreement NCC 2-387 between the National Aeronautics and Space Administration (NASA) and the Universities Space Research Association (USRA).

Baffling Big Brother

Peter J. Denning

Research Institute for Advanced Computer Science

July 31, 1987

Who hasn't asked whether large organizations will one day be able to use computers to monitor every detail of people's lives? Who doesn't occasionally wonder whether our high-tech society is moving inexorably toward dossiers, surveillance, scrutiny of private lives, and complete distrust of individuals? Who hasn't asked whether anything can be done about these trends?

Commercial transactions began to be computerized in the 1950s. Today, most businesses entrust valuable information assets to electronic media, using them to store records, compute accounts, transfer funds, and generate receipts.

Two trends have accompanied this widening use of computers. The rate of computer abuse has risen in direct proportion to the value of information assets and the expertise of users, and the existence of databases has created incentives to link the data they contain. To protect against abuse, organizations demand

PRECEDING PAGE BLANK NOT FILMED

personal information from customers for checking credentials; they keep confidential files on customer activities, payments, and credit histories, frequently making it difficult for customers and employees to review or correct information in those files. On the other hand, they often sell or distribute information about their clients to other organizations. Government agencies have begun to link information in their own and some private databases in their efforts to detect persons who are violating the law. What emerges is a one-sided arrangement: most of the power to control information lies in the hands of organizations and agencies. As a result, calls for legislation to protect individuals from abuse or mistakes are increasingly heard.

Technology has been blamed for the gradual weakening of the individual's power; but can technology strengthen the individual? The answer is yes. Card computers – the so-called smart cards – and public-key cryptography can be used to construct a system of business transactions in which organizations have absolute assurance that all credentials and payment orders are valid and individuals have absolute assurance that no group of organizations can compile dossiers about them by linking databases.

David Chaum of the Centre for Mathematics and Computer Science in Amsterdam has proposed a system of transactions that allows ordinary communications, payments, and credentials to be exchanged electronically (*1,2*). In Chaum's system, it impossible for the records of various organizations to be linked or traced to a specific individual; individuals retain control over how infor-

mation about them is used. The system also protects the organizations against abuse -- perhaps even better than current systems.

Chaum's starting point is the possibility that a person can create a different name -- a pseudonym -- for use with each organization. This is analogous to supplying each bank, store, service establishment, or other organization with a different name, postal address, and identification number. A card computer is needed to assist the person to make transactions and keep track of which name is used with which organization. To guarantee that they cannot be linked between organization, names are actually long random numbers generated by the card computer. Public key cryptosystems are used for communications and digital signatures.

Let me digress for a brief review of public key cryptosystems, which I described more fully in the January-February issue (*9*). Associated with a name (or pseudonym) A are two complementary keys chosen by A. The public key PA is used to encipher messages intended for A, and the secret key SA is used by A to decipher messages. The secret key cannot be deduced from the public key. To insure their security, the keys must contain about 200 digits (approximately 665 bits). The encipherment of an item Z under a key K is denoted $[Z]^K$. A public key is sealed in a key certificate

$$K(A) = [A, PA, D]^{SN},$$

where SN is the secret key of a trusted notary and D is the date and time of

the notary's signature. Anyone receiving $K(A)$ can unseal it by computing $[K(A)]^{PN}$, because the public and private keys cancel; that recipient can have confidence that PA is A's public key because only the notary could have sealed the certificate. A message M from A to B is encoded as

$$[M, K(A)]^{PB}.$$

Only B can decipher this message; B can reply to A by using the key enclosed with the message. A block of the form $[\text{checksum}(M)]^{SA}$ can be attached to the message to serve as a digital signature of the sender.

With cryptography, I can prevent organizations from linking records about me. I simply generate a separate random number for each organization with which I deal and use the numbers as pseudonyms in transactions with those organizations. It is impossible for the organizations to link my assumed names because the connection between the names is known only to me. Of course, if I reveal personal information in my messages, organizations may be able to link message files under different pseudonyms by comparing their contents. The assignment of separate pseudonyms guarantees only that messages cannot be linked by using information in their headers and address fields.

Many business transactions depend on credentials, special tamperproof certifications that a specific person is authorized or qualified to do something. Examples are driver's licenses, passports, and traveler's checks. A credential issued by X can be represented electronically by a cryptogram

$$[A \text{ authorized for } T]^{SX} .$$

Anyone can check that A has authorization for the specific transaction T by unsealing the credential with the issuer's public key. (A receiver of the above credential may demand proof that its bearer is in fact A ; the important authentication protocols that accomplish this are not covered here.)

Credentials of this sort do not work with a multiple pseudonym system. The problem is that the pseudonym by which the person is known to the issuer is sealed inside the credential. Thus, if I obtain a credential from a bank under name A certifying me for $1000 in credit, a store knowing me as B will not honor that credential. What is needed is a way to transform a credential issued under one pseudonym into a valid credential under a different pseudonym, without restricting my choice of pseudonyms.

Chaum has devised a method of accomplishing this seemingly impossible task. The idea is that a name has a special form, consisting of a fixed part uniquely associated with the person multiplied by a variable part that depends on the particular organization with which that name is used. The unique part can be obtained from a special registrar that associates a unique identifier with a standard item of personal information such as a thumbprint; a person need give no other information than this to the registrar. Because a person's unique identifier is a hidden, multiplicative component of a name, no one else can learn it; in particular, the registrar will not be able to link the information it has – unique identifiers plus thumbprints – with any information held by another

organization.

Within this scheme a challenge protocol is needed to permit a third party to determine unequivocally that two pseudonyms belong to the same person. If some organization challenges my claim that the pseudonyms A and B are both mine, both the claim and the challenge can be submitted to an arbiter who can verify that the claim is true or false without revealing my unique identifier. Protocols for doing this are beyond the discussion here. I'll assume that the notary can serve this function.

To illustrate Chaum's method, suppose that I want to request a credential of issuer X under pseudonym A and present it to credential user Y under pseudonym B. Associated with a credential of type T are secret and public keys, ST and PT, the secret key being known only to the credential issuer X. Let U denote my unique identifier, and let V and W denote random numbers I generate. From these numbers I create two special pseudonyms for this transaction,

$$a = U[V]^{PT}$$
$$b = U[W]^{PT}$$

and have them signed by the notary, who returns them in the key certificates $K(a)$ and $K(b)$. My request to X for a credential takes the form

$$[\text{“Request } T\text{”}, K(a), K(A)]^{PX}.$$

On receipt, X can check that as A I am authorized for T and return the

credential in the form

$$[[a]^{ST}, K(T)]^{PA}.$$

I can check that the credential comes from X and agrees with my request by unsealing it with PT and checking that the result is a. To generate the credential for my pseudonym B, all I need to do is divide the credential by V and multiply by W. This works because $[a]^{ST} = [U[V]^{PT}]^{ST} = [U]^{ST} V$, and similarly $[b]^{ST} = [U]^{ST} W$. I pass the result to Y in the form

$$[\text{“Claim } T\text{”}, [b]^{ST}, K(b), K(T), K(B)]^{PY}.$$

Y can check the claim by unsealing the credential with PT and checking that the result is b. Organization X can ask the notary to certify that the pair $K(a)$ and $K(A)$ are both mine and Y can do the same for $K(b)$ and $K(B)$. Thus the challenge protocol can be used by the organizations to assure themselves that I am not submitting special pseudonyms and credentials belonging to another person.

Can this scheme be used for payments? The obvious approach is to extend credentials into electronic bank checks: I obtain from my bank a credential that says "A is good for $\$T$"; then I transform it as above to a credential that says "B is good for $\$T$", which I pass to Y in payment of a bill. Unfortunately, an electronic bank check is susceptible to tracing. Suppose I request a check for an unusual sum, say $385, and a short time later Y deposits the same sum; by

matching withdrawals and deposits, the bank can to link my pseudonyms A and B.

To avoid this kind of tracing, Chaum proposes instead to use electronic currency. When I make a withdrawal, the bank will return a set of certificates of standard denominations; thus my payment of \$385 might consist of three \$100 certificates, eight \$10 certificates, and five \$1 certificates. Unlike paper certificates, electronic ones are easy to copy, so it is necessary to include a method that permits the bank to recognize the first copy of a currency certificate. The obvious method, allowing the bank to attach a note number to the original certificate, will not work because the note number would permit the bank to link my pseudonyms A and B. What is needed instead is a way that I can provide a note number that the bank cannot associate with me, and seal that note number in the credential.

One way to accomplish this is the following. Suppose k binary bits are allocated for names. I will exploit the fact that if I string two copies of the k-bit name n together, I create a binary string of $2k$ bits, representing the number $n\,2^k + n$. To initiate a payment of denomination T, I choose a random note number N and hide it in the name $M = (N\,2^k + N)[V]^{PT}$. My request to the bank takes the form

$$[\text{“Request denomination } T\text{”}, M, K(A)]^{PX}.$$

after deducting \$$T$ from my account, the bank returns the certificate

$$[[M]^{ST}, K(T)]^{PA} .$$

When I divide the certificate by V, I transform it automatically to $[N 2^k + N]^{ST}$. I can submit the transformed certificate to the store, which can unseal it with PT and verify from its two-copy structure that it is worth $\$T$. In turn the store can submit the certificate to the bank, which can extract the note number and deposit $\$T$ in the store's account if that note number has not been seen before.

Chaum's system of transactions is different from current systems in three principal ways. First, a person can use a different pseudonym, a random number, for each organization. Current systems are based on universal identifiers. Second, a person can use a card computer to manage interactions with organizations under each pseudonym, to generate random numbers for use in names, and to carry out the cryptographic protocols. A card computer need have no secrets from its owner. Current systems rely on organizations giving customers cards that contain secret patterns known to the organization but not to the card holders. Third, individuals get to control how information about them is distributed and linked. Current systems are one-sided, giving organizations most of the power to protect themselves from abusive customers while giving customers little power to protect themselves from abusive organizations.

So a system of untraceable business transactions is technically feasible. But is such a system politically feasible? Even though we complain about a world in which our transactions are too easily traced, would we want a world in which

none of our transactions could be traced?

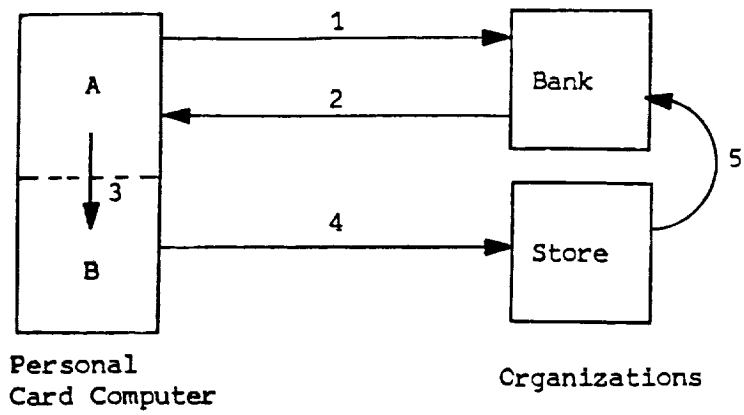
References

1. D. Chaum. 1985. "Security without identification: Transaction systems to make Big Brother obsolete." ACM *Communications 28*, 10, October. 1030-1044.

2. D. Chaum. 1987. "A secure and privacy-protecting protocol for transmitting personal information between organizations." *Proc. CRYPTO 86* (A. Odlyzko, Ed.). Lecture Notes in Computer Science. Springer-Verlag.

3. P. Denning. 1987. "Security of data in networks." *American Scientist 75*, 1. 12-14.

HOW SMART CARDS CAN HELP



Smart cards and cryptography make possible a new system of business transactions that balances the interests of individuals and organizations. Individuals can control how information about them is linked and disseminated, and organizations can be certain that credentials and payments are valid. Each person uses a different name – a pseudonym – with each organization and a personal card computer manages all the names and cryptographic protocols. The diagram shows the interactions needed in a payment transaction. Under pseudonym A , the user requests a payment credential of denomination $\$T$ from the bank (1), which deducts the money from A 's account and issues the credential (2). The credential is a cryptogram enciphered with the denomination's secret key; anyone can read it by deciphering with the denomination's public key. Using a simple transformation, the card computer converts the credential to be valid for pseudonym B without altering the declaration that the bank is willing to pay the holder $\$T$ (3). The result is forwarded to a store (4) in payment of a bill, and the store can in turn forward the payment to the bank for deposit to its account (5). Pseudonyms consist of a unique identifier multiplied by a random number chosen by the person; the conversion at step 3 is simply a replacement of the random number corresponding to the bank with the random number corresponding to the store. A note number must be included in the credential so that the bank can recognize duplicates (and not pay them).