The Use of Communications Networks to Increase Personal Privacy

N. F. Maxemchuk

S. Low

AT&T Bell Laboratories
Murray Hill, New Jersey 07974

Abstract

Communications Networks can separate as well as join information. This ability can be used to increase personal privacy in an environment where advances in technology makes it possible to collect and correlate increasing amounts of information about individuals. The tools and principles necessary to increase personal privacy are demonstrated by creating an anonymous credit card, in which a person's identity and purchases are separated, and a national health insurance plan, in which treatment, payment and an individual's identity are separated. An analysis technique is developed to determine how well the information is separated.

1. Introduction

As computer memories have increased in size and decreased in cost, it has become reasonable to assemble vast amounts of information about individuals. As computer processors have become more powerful, it has become possible to correlate the information that is being assembled and to make inferences about individuals. As data networks have become ubiquitous and transmission rates have increased, it has become possible to combine the vast amounts of information that have been assembled in different locations, for different purposes.

Some of the uses of information can be annoying: Stores and credit card companies that sell information about an individual's purchases for directed advertising can significantly increase the mailings that we receive. Some of the uses of information have been made illegal: In January 1994 it was made illegal for video rental stores in New York State to sell lists of the movies that individuals rent. Some of the uses of information may change the way our society operates: In the Republican party rebuttal to the President's state of the Union message, in January 1994, one objection to a national health plan is the potential invasion of an individual's privacy.

Communications networks give us the ability to bring information together. They also give us the ability to separate and hide information. Some of the tools that make it possible to enhance privacy by communications are described in section 2. In section 2.1 a cryptographic protocol is described for communicating between two parties, and transferring trust between those parties, without either knowing the identity of the other. In section 2.2 an information analysis procedure is described that determines what information can be extracted when two or more parties collude. This analysis determines the effect when parties misbehave and also shows the worse that can happen when there are implementation errors.

Our objective is to control the access to information even though the information is needed and available in the network. The implementation of an anonymous credit card[1,2] is described in section 3. The information is separated and hidden so that a credit card company does not know its client's purchases or the stores that its client shops at, and a store does not know its customer's identity or the credit card company that has paid the bills. However, the company that extends credit knows its clients identity, the store knows what it has sold to a person, and there is a transfer of funds between the store and credit card company.

In the credit card system, anonymity is obtained while all of the capabilities of conventional credit cards, such as providing detailed billing and challenging purchases, are retained. It is also possible to issue the equivalent of an electronic subpoena to associate an individual's identity and purchases when there is reason to suspect illegal use of the payment mechanism. Currently, information about a person's purchases is available unless laws are passed to make that information private. With this mechanism, information about a person's purchases are private unless the law is used to make it available.

Three extensions of the basic anonymous credit card are digital cash, paying for network services, and increased privacy for electronic document distribution. When the mechanism is used for digital cash, section 3.3.1, there is no way to compromise a person's anonymity. However, this mechanism retains the protection against loss or theft of a credit card, and is more difficult to forge than conventional digital cash mechanisms. When paying for network services, section 3.3.2, this mechanism makes it possible for small venders, who aren't trusted to receive credit card numbers, to sell services. In electronic document distribution, section 3.3.3, the anonymous credit card is used to balance the interests of readers and publishers. Publishers cannot accumulate profiles on what a person reads, but can obtain the identities of people who illegally redistribute electronic documents.

An interesting extension of the anonymous credit card is to the the National Health Insurance Plan, in section 4. The straightforward application of the credit mechanism makes it possible to obtain anonymity when paying for services. In addition, it

— makes health records available anywhere, anytime, without disclosing a person's identity,
— makes it possible to conduct medical research on correlations between diseases and treatments without compromising the individuals involved, and
— allows an insurance company to monitor an individual's treatment without knowing who is being treated, unless they have illegally used the system.

As a result of considering the examples in this paper, the collusion analysis that was performed for the anonymous credit card has been related to the problem of finding paths in a graph, and generalized to take into account the difficulty or uncertainty in collusion. The generalized collusion analysis is described in section 5.

2. Tools

2.1 Double-Locked Box Protocol

The double-locked box provides communications between two users connected to different computers, or transfers funds between two accounts in two banks, without either computer, or bank, knowing the identity of the other. Only the bank that the account is located in knows the identity of the account, and only the computer that the user is connected to knows the identity of the user.

Communications passes through an intermediary, as was proposed by Chaum for untraceable electronic mail[3]. The message sender presents the computer he is connected to with a box that can only be opened by the intermediary. Inside the box is the identity of the destination computer and a second box that only that computer can open. Inside the second box is the identity of the message recipient.

When funds are transferred from an account in one bank to an account in a second bank, the intermediary operates as the federal reserve and trust is transferred as well as information. A funds transfer between account i in bank 1 to account j in bank 2 is demonstrated in figure 1. When bank 1 transfers amount M to an account specified by a double-locked box that the customer has provided, it signs the message so that the federal reserve can verify that it is from a trusted bank. The federal reserve sends a signed message to bank 2 to deposit amount M in the account in the locked box. The federal reserve is responsible for settling the accounts between banks.

In a funds transfer environment it is particularly important to prevent messages from being replayed. For instance, if the destination account intercepted the message ordering the second bank to deposit funds, it might be tempted to have the deposit repeated. Two standard techniques to prevent replay attacks are sequence numbers and challenge response protocols. Either public keys or secret keys can be used to construct the funds transfer protocol, as described in references 1 and 2 respectively.

2.2 Collusion Analysis

Pieces of information about an individual are placed at different nodes in a network in order to make it difficult to associate the information. For instance, in the anonymous credit card we separate an individual's identity and purchases. Collusion analysis is used to determine how well the information is separated.

The players, such as the banks and intermediaries, associate information and messages. For instance, in figure 1, when funds are transferred from account i to account j

— bank 1 associates message A with all of the information in account i,
— the federal reserve associates bank 1, bank 2, message A, and message B, and
— bank 2 associates message B with all of the information in account j.

Messages A and B are unique. If bank 1 and the federal reserve collude they can combine all of the information each associated with message A. The source account becomes associated with bank 2 and message B. If the combination of bank 1 and the federal reserve then collude with bank B, they can combine all of the information each associates with message B. The source account and destination account become associated.

Collusion is dependent upon unique information. If two players have the same unique piece of information, and collude, then they can combine information. For instance, if there are a large number of accounts in each bank, banks 1 and 2 collude without the intermediary, and there is no unique information that is common accounts i and j, then there is no reason to associate the information in two of the accounts. However, if the two accounts have the same social security number associated with them, then the accounts can be associated.

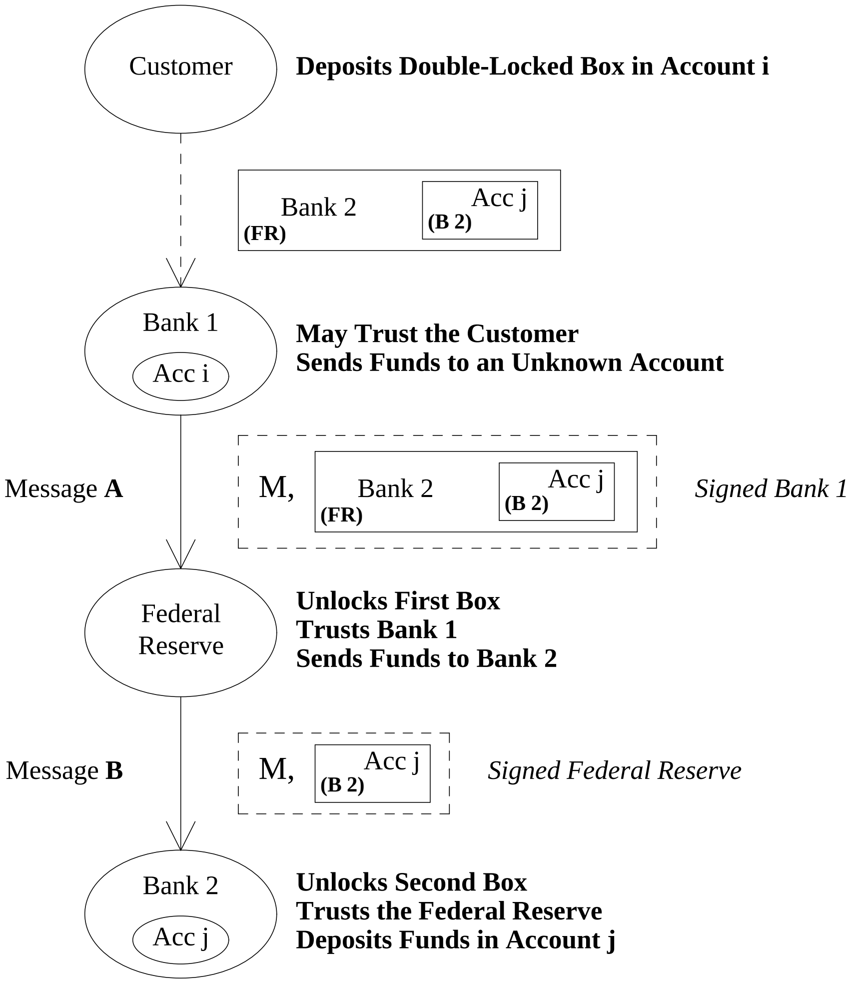

Figure 1. The Double-Locked Box Protocol

In a real system there is a large amount of information and a large number of messages. The amount of information that must be considered for collusion analysis can be reduced by combining similar information. When two pieces of information always appear jointly, there is no reason to consider them separately when performing collusion analysis. When several messages follow the same path, for the same purpose, then the ability to collude, in many instances, isn't improved by considering more than one. Even after combining information into common sets, the amount of information to be considered for collusion analysis may be large. In reference 2, collusion analysis is reduced to row reductions and multiplications on binary matrices. Automating this process makes it possible to consider more complex systems.

When performing collusion analysis, careful consideration must be given to what constitutes identifiable information. Suppose a bank logs a charge of $4.11 at 10:15 AM on 6/14/94, and a store logs a sale of the same amount, within a minute of the same time. Can this information be used to combine the information at the two locations? Depending upon what information is considered unique, different results are obtained from a collusion analysis.

3. Anonymous Credit Card

The anonymous credit card is implemented by constructing the electronic equivalent of a credit card company, a Swiss bank with anonymous accounts, a communication exchange, a federal reserve, and banks for stores, as shown in figure 2. The credit card company trusts an individual to repay a debt, and knows his identity. The store knows the merchandise that is purchased. The objective is to distribute the information so that a number of players must collude in order to associate an individual's purchases and identity. The detailed protocols, including the message formats that are transmitted, are described in reference 1. A higher level description of the protocol is presented here.

Credit is extended to the individual by the credit card company. The credit card company places credits in the individual's anonymous account using a double-locked box that the individual has placed in his credit card account. The bank with the anonymous account does not extend credit to the individual. This bank trusts the federal reserve, which trusts the credit card company. Therefore, the bank with the anonymous credit account does not need to know the individual's identity. At the end of the month, or when the credits are all used, the bank with the anonymous account presents a bill to the credit card company, using a double-locked box that the individual has deposited in his account. The credit card company presents the individual with a bill, and when it is paid, the credit card company deposits additional credits in the anonymous account.

An individual makes purchases in two phases, first he convinces the bank with the anonymous account that he is authorized to draw on that account, then he instructs that bank to transfer funds to the store's bank. Mechanisms that an individual can use to identify himself in the first phase, are described in references 1 and 2. In the second phase, funds are transferred from the bank with the anonymous account to the store's bank, using a double-locked box that the store gives to the customer with the bill. Once the funds transfer is complete, the store's bank notifies the store that it as been paid. Since the store does not trust the individual to pay a bill, the store does not need to know the individual's identity. The encryption and identification techniques required for the anonymous credit card have been implemented on a smart card.

Banks and credit card companies expect to make a profit when credit is extended. Either the store or customer must expect to pay for the use of the funds, and the service provided by the communication exchange. As funds flow through this system, each party can skim off a percentage or a fixed amount, depending upon what agreements have been reached.

3.1 Additional Services

The basic function performed by credit cards is to extend credit, pay the vendor for purchases, then to bill credit card holder. In the previous section we have described how this function is performed. However, we also expect to be able to:

— cancel lost cards,
— detect unusual spending patterns,
— receive itemized bills,
— return purchases, and
— challenge purchases that are charged to us.

Cancelling a lost cards is straightforward. We report the loss to our credit card company, which reduces the credit extended to our anonymous account to zero.

Two mechanisms are used to detect or prevent unusual use of the credit mechanism;

— the amount of credit transferred from the credit card company to the anonymous account is the maximum that can be spent, and
— rules can be placed in the anonymous account to limit the rate at which charges are made, or the maximum for a single charge.

Itemized bills are created, without disclosing the purchases, by allowing an individual to store a sales slip and personal note, encrypted with a key that only he can decrypt, along with the charges. The encrypted list is transferred form the anonymous account, to the credit card company, and then to the individual, along with the bill. When the digital sales slip is signed by the store, it provides a proof of purchase that the customer can use to return an item.

All of the messages that transfer funds are signed and are unique. These messages are saved for a period of time, as is currently required of funds transfer messages to banks. If a customer believes that a charge is erroneous, he can challenge it through the bank with the anonymous account. This bank has a signed message from the communications exchange authorizing the funds transfer. The bank presents this message to the communications exchange with an order from the customer to challenge the purchase. In order to prevent a bank from initiating a trace on its own, a separate organization issues these orders. The communications exchange keeps a log associating the message that it sent to the bank with the message that it received from the customer, that was signed by the customer's card. If an erroneous charge has been made, the bank with the anonymous account can trace the message that it sent to the store's bank to recover the funds.

A real concern with an anonymous payment mechanism is the ability to use it for illegitimate purposes. In this system, the linkages between customers and stores can be traced. If the equivalent of an electronic subpoena is issued against an individual, the billing messages can locate the anonymous accounts and the charging messages can locate the stores. Similarly, a subpoena against a store can force the store's bank to trace the messages transferring funds into the store's account back to the customers' anonymous accounts and from there back to the individuals. This is a secure tracking method, since the individuals cannot erase

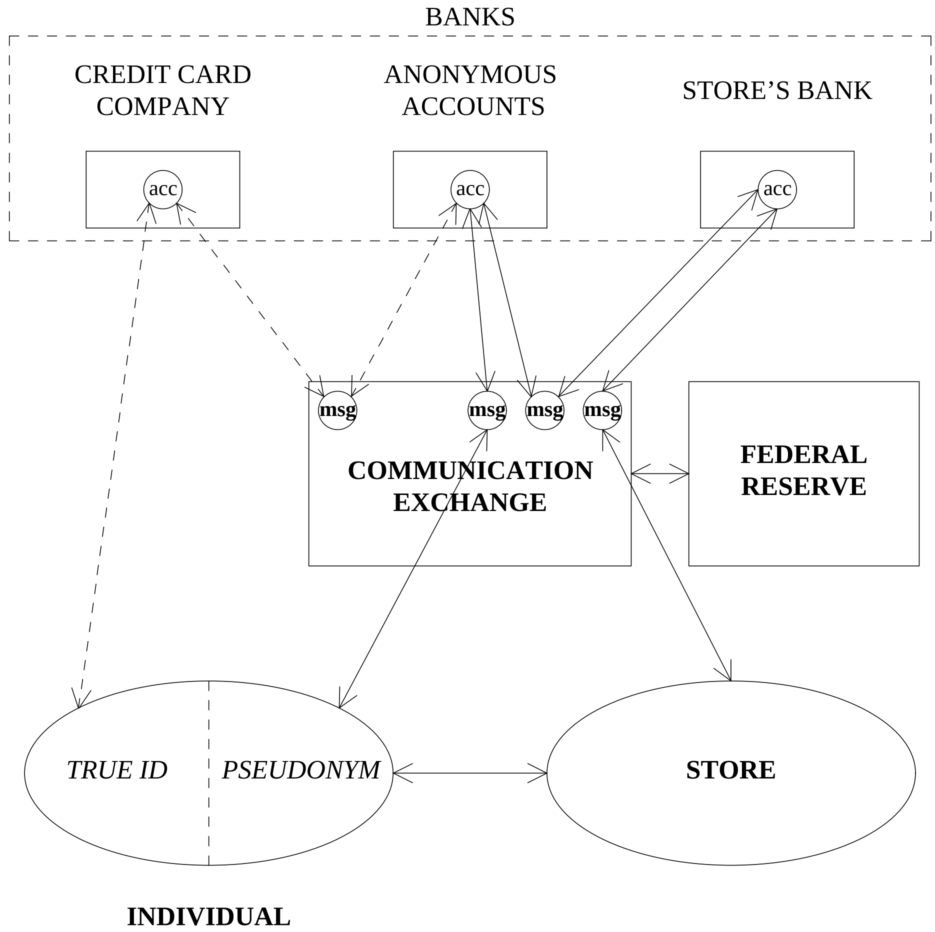

Figure 2. The Participants in an Anonymous Credit Card

messages in the trusted banks or the communications exchange.

3.2 Collusion

In the anonymous credit card, since the messages in the system are unique, it is always possible to collude along the message path linking two pieces of information. For instance, the store knows the purchases and the credit card company knows the customer's identity. If a store does not eavesdrop on the messages from its customers, the message path linking the store to the credit card company, as shown in figure 2, includes the store, the store's bank, the bank with the anonymous account, the credit card company, and the communications exchange. Depending upon whether or not the same communications exchange is used for all transactions, either five, six, or seven parties must collude to associate a customer's identity and purchases. If the store listens to the customer's messages, the number of parties that must collude is reduced to four or five, the store, the bank with the anonymous account, the credit card company, and one or two communications exchanges.

The collusion path can be reduced if two parties share a unique piece of information. For instance, if the credit card system is small so that the time and amount of a purchase is unique, then the store and bank with the anonymous account, which both know this amount, can collude. The additional parties that must collude to learn the customer's identity are the communications exchange and the credit card company, so that the number of parties that must collude is reduced to four. When there are several banks with anonymous accounts, this is a weaker attack than following the message path because the store cannot be certain that it is colluding with the correct bank.

3.3 Related Applications

3.3.1 Digital Cash The electronic funds transfer mechanisms developed for the anonymous credit card can be used as a replacement for digital cash. To construct a digital cash system from the anonymous credit card a user physically deposits funds in an anonymous account. Since credit is not extended to the individual, there is no need to know his identity. As a result, there is no way to associate a person's purchases and identity.

In most digital cash mechanisms[4,5,6,7,8,9] a user obtains sequences of bits that represent cash. Communications, processing and bookkeeping are required to make certain that a user does not duplicate the bits and spend them more than once. In addition, cryptographic techniques are relied upon to prevent a user from forging sequences of bits that are mistaken for cash.

When digital cash is implemented with the funds transfer mechanisms used in the anonymous credit card, the bits representing cash remain in trusted banks rather than being in a person's possession. The person cannot lose the bits. The bits cannot be stolen. And, the person cannot forge new bits.

The main disadvantage of the funds transfer mechanism is that it requires communications to make purchases. The more advanced digital cash mechanisms enable a user to "spend" the bits without communicating with a checking agency while the bits are being spent. At a later time the bits are sent to a central processing agency. If the bits are "spent" once, the spender is anonymous. If the bits are "spent" more than once, the spender's identity is revealed.

3.3.2 Paying for Network Services In a commercial network environment, such as that being established on the Internet, electronic payment mechanisms are needed to make it possible for small businesses to start up.[10,11,12] It is not adequate to provide secure mechanisms to transfer credit card numbers. An individual may trust a large company, like Sear's, not to misuse a credit card number, but has no reason to trust an unknown individual. In addition, it is not always possible for new buisnesses to obtain mercantile accounts with credit card companies. In order to make it easier to start new businesses, electronic cash or credit mechanisms should be used to transfer funds.

Anonymity in a network environment is more difficult to obtain than when a person enters a store. When a person enters a store and carries his purchases out, there is no reason for the store owner to know the person's identity. However, if the individual wants the goods delivered, then he must disclose where he lives. Unfortunately, a network is like the second case rather than the first. In order to become anonymous, the recipients network address must be obscured. Conventional ways to hide addresses on a network are to:

1. communicate through an intermediary that forwards messages from a source to a destination,
2. post information, encrypted with the recipients secret key, in a public place or broadcast it, or
3. place calls through a telephone company that is trusted not to provide "Caller ID."

It is possible to use the anonymous credit card without hiding network addresses. However, complete anonymity may be useful when there are a large number of small transactions between two parties. Instead of transferring funds for each transaction, a customer can transfer funds at the beginning of a session and trust the vendor to return the unused funds. If the user is anonymous, there is more reason for the vendor to be honest since the recipient may be a network checker.

3.3.3 Electronic Document Distribution It has been noted that a major impediment to electronic document distribution is the relative ease with which electronic documents can be copied and redistributed. In order to protect a publisher's revenues, it has been proposed that each copy of an electronic document that a publisher distributes be made unique and registered to the individual who ordered it.[13,14] When illicit copies of a document are located, a publisher can use the unique characteristics to determine the original recipient.

A straightforward implementation of document marking requires publishers to create a reading profile for an individual. This invades an individual's privacy and, if the reading is work related, will concern employers. The anonymous credit card provides a means of balancing the interests of both the individuals and the publishers.

If articles are payed for with the anonymous credit card, the publisher doesn't need to know the purchaser's identity to discourage redistribution. The publisher can associate the message that verified that funds were transferred with the copy of the article. If multiple copies are located, a subpoena can be obtained to force the collusion needed to disclose the purchaser's identity.

4. National Health Insurance

The national health insurance plan presents an interesting application where an individual's right to privacy and society's need to control spending conflict. Most individuals feel that any medical or psychiatric treatment that they receive is between them and their physicians. Society has a responsibility to monitor any programs that it pays for, so that the programs are not abused. These apparently conflicting goals can be resolved by the privacy mechanisms that have been described.

The system can be set up as shown in figure 3. An individual has a personal account in a bank that knows his identity, an anonymous account with a health insurance company, and an anonymous account in a database of medical histories, as well as an anonymous credit card.

A person's complete medical history is stored in the anonymous account in the medical history database. Since the database is connected to the communications network, the medical history is available anywhere, anytime.

An employer, the government, or the individual deposits funds to pay insurance premiums into the personal account. Payments are made to the insurance company using the double-locked box protocol. The insurance company does not know the individual's identity, but has a double-locked box to the medical history account that is used to determine premiums and pay for medical services. It also has a double-locked box for the personal account, to present bills to the individual.

When a person acesses this database to make the information available to a health care provider, he uses a smart card and proves his identity the same way he does before making a purchase with the anonymous credit card. After treatment, the health care provider sends the information needed for insurance coverage and future treatment to the person's medical history account, using a double-locked box that it received with the patient information. Although funds are not transferred in this operation, trust is. The message from the health care provider is signed. The communications exchange verifies that the message is from a registered health care provider, and sends a message that it signs to the medical history database. The medical history database trusts the communications exchange to have checked the credentials of the health care provider, and enters the information into the account.

The entry that the health care provider makes in the medical history database also contains a double-locked box for his own bank account so that the insurance company will be able to pay his bill. After an individual receives medical treatment, he instructs his insurance company to pay for the service. The insurance company uses the double-locked box that accesses the individual's medical history file to obtain the bill and the double-locked box for the medical provider's account. The bill is certified by the communications exchange as being from an authorized health care provider. The insurance company pays for the covered services and the individual is made aware of any expenses that were not covered. Presumably the remaining charges will be paid with the anonymous credit card, to maintain the patient's anonymity.

There is no direct link between a person's medical history and his identity. Insurance companies can audit medical history accounts on a regular basis without compromising an individual's right to privacy. If the insurance company suspects that an individual has misused his insurance policy, he must present the evidence to an agency that can authorize parties to collude in order to determine the individual's identity. The medical history database can also be used for medical research on correlations between diseases and treatments without compromising individual privacy.

The message path from an individual's medical history and his identity has four or five parties, the medical history database, the insurance company, the agency that maintains personal accounts, and one or two communications exchanges. The message path from an entry in a medical history to the health care provider has only the medical history database and the communication exchange. It is more difficult in this system to compromise an individual's privacy than that of a health care provider.

A model where an individual goes to a health care provider and proves his identity to obtain information stored in a medical history database is reasonable for many health care situations. It is not adequate for emergency situations when a person is unable to use, or does not have, his identification card. One means to obtain information in an emergency is to establish a server that associates biometric identifiers for individuals and double-locked boxes for medical history accounts. In an emergency the health care provider sends a signed message with the biometric identifier through a communications exchange to the emergency server. The communications exchange verifies that the health care provider is legitimate. The emergency server uses the double-locked box to request the medical history and forwards it to the health care provider.

5. Generalization of Collusion Analysis

As we have gone through the examples in this paper, it should be evident that collusion analysis is equivalent to finding the paths in a graph. The accounts in banks and the transactions in the intermediaries are nodes in the graph. Whenever there is information in two nodes that can be identified as belonging to the same individual, then a link exists between the nodes. The minimum number of parties that must collude to associate the two pieces of information is one plus the shortest path between the nodes with the information.

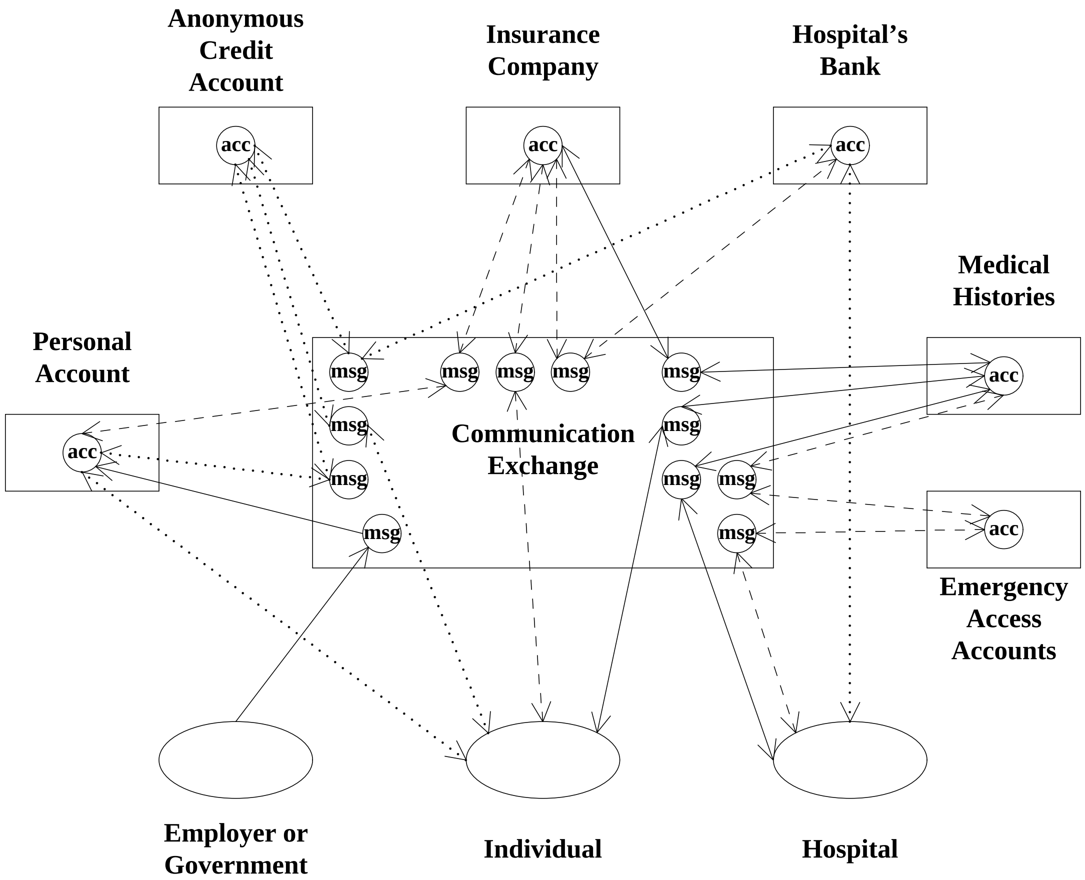

Figure 3. The Participants in the National Health Insurance

Certain messages in the applications must be unique. A graph with links corresponding to the unique messages determines the maximum number of parties that must collude. In order to achieve this upper bound, the rest of the information at the nodes is distributed so that no shorter paths are created. In the anonymous credit card and national health insurance applications, the upper bound can be realized.

The shortest path analysis is a first step toward performing collusion analysis, but does not provide the complete answer. The next step should take into account how difficult or how likely it is that unique, identifiable pieces of information can be used for collusion. In the message passing case, nodes are able to determine the other nodes that share the unique information. There are also instances in which multiple sites share a unique piece of information, but don't know the location of the other site, and instances in which the information isn't completely unique.

There are different degrees of difficulty in associating a message source and destination in communications networks. The funds transfer messages in the anonymous credit card are unique and identify the source and destination to the application. In the Internet, packets are addressed so that the source must know the destination address. When an acknowledgement is expected, the destination must also know the source address. Information about the source and destination is available at the network layer, rather than in the application, and can be made less accessible to the user. When communications occurs in a switched network, such as the telephone network, the source and destination need not have access to each other's identity, but the network that established the circuit must. Collusion is more difficult because it involves another party.

When two sites have common information that can be used to collude, but the sites do not know each other's identity, collusion is more difficult. For instance, assume that a person has credit cards in two out of one hundred credit card companys, and each credit card company knows his social security number. If some of the credit card companies collude, the probability that the two companies with the common social security number are colluding is less than one. More parties must collude, on the average, to combine information than when the source and destination can identify each other.

When a piece of information at two sites is not unique, but has a probability of belonging to the same individual, then a degree of collusion becomes possible. The ability to collude increases as the probability that the information belongs to the same individual increases. For instance, if an individual receives a credit card bill for a specific amount and an anonymous account issues a bill for the same amount, then there is a probability that they both apply to the same individual. If two successive bills that the anonymous account issues and the individual receives are the same, then the likelihood that the bills apply to the same individual increases. As the sequence of identical bills increases, so does the likelihood that they belong to the same individual. It is possible to collude at any point, but the confidence in the result of the collusion becomes higher as the probability increases.

Collusion analysis can be generalized to take into account the difficulty in obtaining information, the likelihood that useful sites will collaborate, or the uncertainty in information, by associating weights with the paths in the graphs. The generalized analysis indicates that collusion is easier when two parties that have unique information know each other's identity, than when they do not. Therefore, it is worth hiding the identities.

The techniques described in section 3.3.2, to hide the source and destination when transmitting information in a network, can be used to increase the difficulty of collusion. For instance, the broadcast mechanism can be used in a sysyem that requires acknowledgements if

— The source transmits to an unknown destination by encrypting a message with a key supplied by the user. The message is broadcast to all destinations, but only the destination with the decryption key can receive it.
— If the source supplies its own key in the message, then the destination can use the broadcast channel to acknowledge the message without knowing the source.

6. Conclusion

The tools presented in this work provide the means to design a range of applications that balance the rights of an individual to preserve his privacy, and the rights of society to protect the interests of the group. The proper balance between an individual's rights and society's needs are not addressed.

REFERENCES

[1] S. Low, N. F. Maxemchuk, S. Paul, "Anonymous Credit Cards," Proceedings of 2nd ACM Conference on Computer-Communications Security, Fairfax, Va. Nov. 2-4, 1994.

[2] S. Low, N. F. Maxemchuk, S. Paul, "The Anonymous Credit Card and Its Collusion Analysis," Submitted to IEEE Trans. on Networking.

[3] D. L. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Proceedings of Communications of the ACM, Vol. 24, No. 2, February 1981, pp. 84-88.

[4] D. Chaum "Security without Identification: Transaction Systems to make Big Brother Obsolete" Communications of the ACM, October 1985, Vol. 28, No. 10, pp. 1030-1044.

[5] D. Chaum, "Privacy Protected Payments: Unconditional Payer and/or Payee Untraceability," Proceedings of Smart Card 2000, D. Chaum & I. Schaumuller-Bichl eds., North Holland, 1989, pp. 69-93.

[6] R. J. Anderson, "UEPS - A Second Generation Electronic Wallet," Proceedings of Computer Security - ESORICS 92, November 1992, pp.411-418.

[7] T. Okamoto, K. Ohta, "Universal Electronic Cash," Crypto '91, Santa Barbara, CA 11.-15., August 1991, Abstracts, 8.7-8.13, pp. 324-337.

[8] S. D'Amiano, G. Di Crescenzo, "Methodology for Digital Money Based on General Cryptographic Tools," Proceedings of Eurocrypt'94, pp. 151-162.

[9] T. Eng, T. Okamoto, "Single-Term Divisible Electronic Coins," Proceedings of Eurocrypt'94, pp. 311-323.

[10] S. Dukach, "SNPP: A Simple Network Payment Protocol," Proceedings of Computer Security Applications Conference, November 1992, pp. 173-179.

[11] G. Medvinsky, B. C. Neuman, "NetCash: A Design for Practical Electronic Currency on the Internet," Proceedings of the First ACM Conference on Computer and Communications Security, November 1993.

[12] M. A. Sirbu, "Internet Billing Server Prototype Scope Document," Carnegie Mellon University, Information Network Institute, INI Technical Report 1993-1, October 14, 1993.

[13] J. T. Brassil, S. Low, N. F. Maxemchuk, L. O'Gorman, "Electronic Marking and Identification Techniques to Discourage Document Copying," IEEE Infocom '94, June 14-16, 1994, Toronto, Canada, pg. 1278-87.

[14] N. F. Maxemchuk, "Electronic Document Distribution," ATT Technical Journal, Sept. 1994, pg 73-80.