NETWORKS WITHOUT USER OBSERVABILITY -- DESIGN OPTIONS

Andreas Pfitzmann, Michael Waidner
Institut für Informatik IV, Universität Karlsruhe, Postfach 6380,
D 7500 Karlsruhe 1, West Germany

ABSTRACT

In usual communication networks, the network operator or an intruder could easily observe when, how much and with whom the users communicate (traffic analysis), even if the users employ end-to-end encryption. When ISDNs are used for almost everything, this becomes a severe threat. Therefore, we summarize basic concepts to keep the recipient and sender or at least their relationship unobservable, consider some possible implementations and necessary hierarchical extensions, and propose some suitable performance and reliability enhancements.

0 Motivation

Public and private networks have a growing importance for our daily life. We use them for telephony, telegraphy, television, videotex, radio and in the near future we will use them for video telephony, electronic mail, ordering and receiving of newspapers, home banking, etc.
All these services will be integrated in a so called Integrated Services Digital Network (ISDN). If such a network is built as planned e.g. by the german PTT and operated on a "transmission on demand basis" even for the classical broadcast services TV and radio, great parts of the life of any user could easily be observed by the PTT or by an intruder.
Eavesdropping can be foiled by link-by-link encryption [Bara_64], but this does not foil attackers at the stations (e.g. via Trojan Horses).
There are some well known measures how the users themselves can decrease their observability. The content of a message can be sufficiently hidden by end-to-end encryption. However, an attacker can still see who sends how many messages to whom and at what time (traffic analysis). To hide this information, too, they can use public network stations (e.g. telephone boxes) instead of private ones. This will prevent observation but is very uncomfortable for the users (e.g. who would watch TV in a video telephone box?). If they use private network stations, they can only try to hide their behaviour by making their network stations do more things than necessary at other times than necessary. For example a user can order a whole newspaper or several newspapers instead of a single article, and he can do so at any time before he wants to read them.

F. Pichler (Ed.): Advances in Cryptology - EUROCRYPT '85, LNCS 219, pp. 245-253, 1986.

This is an easy but expensive measure and not suitable for services like telephony.

So the only way to decrease user observability in a comfortable and cheap fashion seems to be to design a network for anonymity and not to try to realize anonymity afterwards.
The standard requirements on an ISDN, i.e. high performance and reliability, have to be met, too.

In the following chapters we will describe the existing proposals for anonymous networks in a systematic way and some options how they can be adapted to meet the stringent requirements on performance and reliability.

1 Basic concepts for anonymous networks

1.1 A closer look at anonymity

What we would like to realize is absolute anonymity against every possible attacker. But an attacker can control all network stations, all lines, and even the communication partner and so absolute anonymity is theoretically impossible. Therefore we need reasonable models of possible attackers.

There are several possible attackers: the administration, foreign states, companies, one's neighbours and communication partners. During the design of an anonymous network these possible attackers have to be translated into terms of stations and lines. A station is always under control of its owner and might be under control of everybody who has had access to it so far, e.g. its manufacturer, because he might have installed a Trojan Horse [PoKl_78, Thom_84]. Trojan Horses are a serious problem in stations with high complexity, e.g. switching centers. In simple user stations they can be detected more easily (if this is tried). Lines are assumed to be owned by the PTT. Normally they can easily be observed by the PTT or an eavesdropper, but by physical measures such an attack can be made much more difficult.

Given a model of the attacker we have to define what we want to keep hidden from him. A strong possibility is to keep the sender and the recipient of a message secret. A weaker possibility is to keep only their relationship secret, i.e. sending and receiving of physical messages is observable, but it is infeasable for an attacker to link the physical message sent by the sender and the physical message received by the recipient.

1.2 Recipient anonymity

Receiving a message can be made completely anonymous to the network by delivering the message to all stations (broadcast). If the message has an intended recipient, a so called addressee, it has to contain an

attribute by which he and nobody else can recognize it as addressed to him. This attribute is called an implicit address in contrast to an explicit address, which describes a place in the network.

Implicit addresses can be distinguished according to their visibility, i.e. whether they can be tested for equality or not. An implicit address is called invisible, if it is only visible to its addressee and is called visible otherwise [Waid_85]. Invisible implicit addresses can be realized with a public key cryptosystem. A message is addressed by encrypting it (or a part of it) with a public key of the addressee. Each station decrypts all messages with each of its private keys and uses the message redundancy to decide which messages are addressed to it.
Conversely, if you have any invisible addressing scheme, you can do public key distribution: If you want to communicate a n bit key to your partner, choose n messages randomly, and address them to your partner if the corresponding key bit is 1, and address them not to your partner otherwise. Send these n messages in one explicitly addressed message to your partner.

Visible implicit addresses can be realized much easier: Users choose arbitrary names for themselves, which can then be prefixed to messages.

Another criterion to distinguish implicit addresses is their distribution. An implicit address is called public, if it is known to every user (like telephone numbers today) and private if the sender got it secretly from the addressee either outside the network or as a return address or by a generating algorithm the sender and the addressee agreed upon [FaLa_75, Karg_77].
Public addresses should not be realized by visible implicit addresses to avoid the linkability of the visible public address of a message and the addressed user.

Private addresses can be realized by visible addresses but then each of them should be used only once.

1.3 Unlinkability of sender and recipient

This form of anonymity can be realized by a special network station, a so called MIX, which collects a number of messages from the senders, changes their encodings and forwards the messages to the recipients in a different order.
This measure hides the relation between sender and recipient of a message from everybody but the MIX. By using more than one MIX to forward a message from the sender to the recipient, the measure hides the relation from every attacker in the network who doesn't control all the MIXes [Chau_81].

1.4 Sender anonymity

A powerful scheme for sender anonymity is superposing sending which is published in [Cha3_85, Cha8_85] and is called DC-net (dining cryptographers net) there.
Each user station generates at least one keybit for each message bit and sends each keybit to exactly one other user station over a secure channel. To send one bit every user station adds modulo 2 (superposes) all generated and received keybits and its message bit if there is one. The sums are sent over the network and added up modulo 2. The result is distributed to all user stations. The result is the sum of all sent message bits, because every keybit was added twice. Therefore the scheme realizes a multi-access channel with collisions. For its efficient use a medium access protocol [Tane_81] preserving anonymity is needed. Two of them are mentioned in [Cha3_85].
If an attacker controls all lines and some of the user stations, he gets no information about the sender of a message among the other users, as long as their key graph, i.e. the graph with the users as nodes and the keys as edges, is connected.
Superposing sending requires the exchange of a tremendous amount of randomly chosen keys. To reduce costs, pseudorandomly generated keys can be used instead, reducing information-theoretic [Sha1_49] to complexity-theoretic security.

The expensive generation, distribution and superposing of keys (and messages) of the concept of superposing sending can be avoided, if the network is designed for preventing attackers from physically observing all lines connecting a user with the rest of the world.
A simple and efficient way to do so is to connect the user stations by rings, which are in wide use for local area networks. If an anonymous medium access protocol is used, a user station is only observable if its two neighbour stations collude or the lines are tapped. The latter attack can be prevented by an appropriate cable run [Pfi1_83, Pfit_84]. Possible medium access protocols are slotted ring with sender remove and token ring, both with exhaustive service [Höck_85, HöPf_85].

2 Performance

The two main performance characteristics of networks are throughput and transfer delay. Their importance depends on the services the network should offer. Throughput and delay are less critical for services like electronic mail, only throughput is critical for services like file transfer, only delay for services like telephony and both are critical for video telephony.

2.1 Some remarks on the basic concepts for anonymous networks

Analyzing the performance of the concepts of chapter 1 must go along with considering how they would be implemented physically.

In local areas with a few hundred stations the performance of a ring network implemented as a physical ring is about as good as or even better than that of an equally expensive usual star or bus network [Bürl_84, Bürl_85, Mann_85]. However, performance and reliability of ring networks with more than 10000 stations become inacceptable.

In [Cha3_85] David Chaum suggests implementing superposing sending on a physical ring network. Each message bit requires two circulations around the ring: in the first round the user bits are successively superposed by the users, in the second round the resulting bit is broadcasted.
This implementation seems quite efficient, because under the assumption of uniformly distributed traffic it increases the average expenditure of transmission only by a factor of four compared with a traditional ring access protocol in which the recipient removes the message from the ring, whereas on a star or tree network the factor is the number of stations. But the amount of transmission on each line, i.e. the required bandwidth, is the same for all implementations, so implementations on stars or trees might still be better if their delay time is shorter. The nodes of such networks can be less complex than normal switching centers and constructed in a way that the overall delay in the network is only proportional to the logarithm of the number of stations whereas in ring networks it is always proportional to the number of stations [Pfi1_85].
As throughput and reliability of any network based on superposing sending can't be greater than that of a ring network, these networks can't be built with more than 10000 stations either.

In the MIX network, several factors are to be considered: How many and which stations act as MIXes and how many MIXes are used per message?
As expenditure of transmission of a message grows quadratically with the number of MIXes chosen for it, this number must not be too large. Especially not all stations can be chosen as MIXes for all messages.
To guarantee short delay for time critical services the throughput of a station that acts as MIX must be very high because it must always have enough messages to mix. These lots of messages must be decrypted and rearranged and forwarded. So a MIX must be extremely powerful and complex, and therefore there can only be a limited number of MIXes in the network.
If the MIX network is implemented using some user stations of an existing physical network as MIXes, each message must pass the physical network several times which adds additional delay to that occuring in the MIXes. But using the switching centers of the physical network as MIXes can not be recommended either, because the probability that they collude is too great (and the assumption that they are independent becomes altogether absurd in states with a telecommunication monopoly like the FRG).

2.2 Hierarchical networks

As mentioned above networks which provide sender and recipient anonymity cannot be built for that number of stations an ISDN would have. To

achieve high performance, it seems reasonable to divide the network stations statically or dynamically into groups which perform one of the schemes of paragraph 1.4 and to support the possible groupings by a physical structure.

The simplest form of such a structure is the switched/broadcast network (SBNS), which has two levels, broadcast networks based on rings or superposing sending at the lower level and an arbitrary switched network as backbone [Pfit_83, Pfi1_83, Pfit_84, Pfit_85, Pfi1_85]. If the scheme of superposing sending is used, the SBNS can easily be generalized to a tree network. The partitioning into local broadcast networks can then be made variable by changing the depth of the backbone network [Pfi1_85].

2.3 Channel switching

So far only networks based on slotted rings with exhaustive service are suitable for services that require a continuous stream of information with short delay (channel switching), because once a station is allowed to use a slot, it can use this slot again and again as a channel.

The MIX network is inappropriate for such services, because of the delay during the transport of each message, and the networks based on the concept of superposing sending, because the basic medium access protocols don't guarantee exhaustive service.
New possibilities of increasing the performance of these network can be achieved by giving up one requirement on anonymity that seems unreasonable for channel switching services anyway: the requirement that the relationship between different messages of the same connection is hidden [Pfi1_85].

In a network based on superposing sending, channels can then be switched as in normal broadcast networks.

In a MIX network in its pure form the delay results essentially from the fact, that every MIX has to await all bits of a long packet, before it can decrypt it and send the first bit to the next MIX. This can be avoided, if a single message is used for setting up a connection and giving each MIX a key of a fast private key system used as a stream cipher. These private keys are used to encrypt the following messages of the initiated connection just as the public keys in the normal MIX network [Pfi1_85].

In a hierarchical network, channels are switched by concatenating channels of the different levels of the hierarchy.

3 Fault tolerance

So far, all networks are serial systems in the sense of reliability: all MIXes of a chosen sequence of MIXes, all stations of a ring, and

all stations taking part in superposing sending must work correctly. To fulfil the high reliability requirements on an ISDN, each scheme must be extended to include some fault-tolerance mechanisms. These mechanisms can work end-to-end, i.e. the sender retransmits a message if it doesn't receive an acknowledgement after a certain amount of time. Even if the sender chooses a different encoding of the message for each retransmission, the retransmitted messages can enable statistical attacks in some networks. Moreover, the performance of such mechanisms in terms of average transfer delay, variance of transfer delay, or usable throughput can be unsatisfactory. Therefore, it seems worthwhile to use mechanisms which avoid end-to-end retransmission wherever possible.

3.1 MIX network

If every MIX in a sequence of chosen MIXes can bypass the next MIX, a failure of one MIX (or more, as long as no two consecutive MIXes break down) can be tolerated. To bypass one MIX, its predecessor must not only get the message part for it but also for its successor. If it receives both message parts and this is done for every MIX, the length of the whole message grows exponentially. To avoid this exponential growth, the sender of a message chooses a different key (e.g. of a fast private key system) for each MIX. Together with its message part each MIX must get its key, that of its successor, and the addresses of the next two MIXes, all together encrypted with its own public key.

Let $A_1,\ldots,A_n$ be the sequence of addresses and $e_1,\ldots,e_n$ be the sequence of public keys of the chosen MIXes $M_1,\ldots,M_n$, A_{n+1} the address of the addressee $M_{n+1}:=A$ and e_A his public key, $k_1,\ldots,k_n$ the chosen sequence of keys, and N_i the message that M_i shall receive. The messages N_i are formed according to the following scheme, starting from the message content N that A shall receive:

$$
\begin{aligned}
N_{n+1} &= e_A(N) \\
N_n &= e_n(k_n, A_{n+1}), k_n(N_{n+1}) \\
N_i &= e_i(k_i, A_{i+1}, k_{i+1}, A_{i+2}), k_i(N_{i+1}) \qquad i=1,\ldots,n-1
\end{aligned}
$$

So M_i can get N_{i+1} and N_{i+2} out of N_i, but as long as at least two consecutive MIXes are not controlled by the attacker, the scheme is as secure as the original scheme [Pfi1_85].
The scheme can easily be modified to tolerate the failure of d consecutive MIXes instead of one for every fixed number d.

3.2 Other networks

The ring network can be made fault tolerant by using a braided ring and special protocols [Mann_85]. A quantitative examination of the reliability improvement is given there.

Some remarks on the DC-net and the hierarchical anonymous networks can be found in [Pfi1_85].

4 Concluding remarks

The previous three chapters dealt with the design of a network with high performance and reliability which allows its users to send and to receive anonymously.
If using the network isn't free of charge the charges must either be paid anonymously with each use of the network (e.g. by anonymous numbered accounts [Pfit_84, Pfi1_83] or digital banknotes [Cha4_85,Cha8_85]), which seems rather troublesome, or measured anonymously (e.g. by safeguarded counters at user stations [Pfit_84, Pfi1_83]), or paid by flat rates.
As mentioned in the motivation, the content of a message can be hidden by using end-to-end encryption.

The initially mentioned services like electronic mail, ordering of newspapers or home banking can be implemented by higher protocols upon such a network.
If identification is required instead of anonymity, the well known authentication schemes can be used. Otherwise it is necessary to implement the services in a way which preserves the anonymity of the network. This must be proved in addition to proofs that the implementation fulfils its normal specification, e.g. security against fraud [WaPf_85].

It should be mentioned that many communication services where users nowadays have to identify themselves can be used in an anonymous way in the future, if there is a protocol that allows people to act under several pseudonyms and to transform documents that carry one of these pseudonyms into documents carrying another of their own pseudonyms, in a secure and anonymous way [Cha1_84, Cha2_85, Cha8_85].

Acknowledgements

We are grateful to David Chaum for sending us his drafts and for stimulating discussions and to Klaus Echtle and Birgit Pfitzmann for a lot of useful comments and discussions.

Literature

Bara_64 Paul Baran: On Distributed Communications: IX. Security, Secrecy, and Tamper-Free Considerations; Memorandum RM-3765-PR, Aug. 1964, The Rand Corporation, Santa Monica, California

Bürl_84 Gabriele Bürle: Leistungsvergleich von Sternnetz und Schieberegister-Ringnetz; Studienarbeit, Univ. Karlsruhe, 1984

Bürl_85 Gabriele Bürle: Leistungsbewertung von Vermittlungs-/Verteilnetzen; Diplomarbeit, Univ. Karlsruhe, Mai 1985

Chau_81 David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; CACM Vol. 24, Nu. 2, Feb. 1981, pp. 84..88

Cha1_84 David Chaum: A New Paradigm for Individuals in the Information Age; Proc. of the 1984 Symp. on Security and Privacy, IEEE, Apr. 1984, Oakland, California, pp. 99..103

Cha2_85 David Chaum: Showing Credentials Without Identification. Signatures Transferred Between Unconditionally Unlinkable Pseudonyms; Eurocrypt 85, Draft, received May 13, 1985;

Cha3_85 David Chaum: The Dining Cryptographers Problem. Unconditional Sender Anonymity; Draft, received May 13, 1985;

Cha4_85 David Chaum: Privacy Protected Payments. Unconditional Payer and/or Payee Anonymity; Draft, received May 13, 1985;

Cha8_85 David Chaum: Security Without Identification: Transaction Systems to Make Big Brother Obsolete; CACM Vol. 28, Nu. 10, Oct. 1985, pp. 1030..1044

FaLa_75 David J. Farber, Kenneth C. Larson: Network Security Via Dynamic Process Renaming; Fourth Data Communications Symp., Oct. 1975, Quebec City, Canada, pp. 8-13..8-18

Höck_85 Gunter Höckel: Untersuchung der Datenschutzeigenschaften von Ringzugriffsmechanismen; Diplomarbeit, Univ. Karlsruhe, Aug.1985

HöPf_85 Gunter Höckel, Andreas Pfitzmann: Untersuchung der Datenschutzeigenschaften von Ringzugriffsmechanismen; 1. GI-Fachtagung "Datenschutz und Datensicherung", Okt. 1985, München, IFB Band 113, Springer-Verlag, Heidelberg, pp. 113..127

Karg_77 Paul A. Karger: Non-Discretionary Access Control for Decentralized Computing Systems; Master Thesis, MIT, Laboratory for Computer Science, May 1977, Report MIT/LCS/TR-179

Mann_85 Andreas Mann: Fehlertoleranz und Datenschutz in Ringnetzen; Diplomarbeit, Univ. Karlsruhe, Okt. 1985

Pfit_83 Andreas Pfitzmann: Ein Vermittlungs-/Verteilnetz zur Erhöhung des Datenschutzes in Bildschirmtext-ähnlichen Neuen Medien; 13. Jahrestagung der GI, Okt. 1983, Univ. Hamburg, IFB Band 73, Springer-Verlag Heidelberg, pp. 411..418

Pfit_84 Andreas Pfitzmann: A switched/broadcast ISDN to decrease user observability; 1984 Intern. Zurich Seminar on Digital Communications, March 1984, Zurich, Switzerland, Swiss Federal Inst. of Tech., Proc. IEEE Cat. No. 84CH1998-4 pp. 183..190

Pfit_85 Andreas Pfitzmann: Technischer Datenschutz in diensteintegrierenden Digitalnetzen - Problemanalyse, Lösungsansätze und eine angepaßte Systemstruktur; 1. GI-Fachtagung "Datenschutz und Datensicherung", Okt. 1985, München, IFB Band 113, Springer-Verlag, Heidelberg, pp. 96..112

Pfi1_83 A. Pfitzmann: Ein dienstintegriertes digitales Vermittlungs-/Verteilnetz zur Erhöhung des Datenschutzes; Fak. f. Inform., Univ. Karlsruhe, Interner Bericht 18/83, Dez. 1983

Pfi1_85 Andreas Pfitzmann: How to implement ISDNs without user observability - Some remarks; Fak. f. Inform., Univ. Karlsruhe, Interner Bericht 14/85, 1985

PoKl_78 G. J. Popek, C. S. Kline: Issues in Kernel Design; Operating Systems, An Advanced Course, Ed. by R. Bayer et. al.; LNCS 60, 1978; Springer-Verlag, Heidelberg, pp. 209..227

Sha1_49 C. E. Shannon: Communication Theory of Secrecy Systems; Bell Syst. Tech. J., Vol. 28, No. 4, Oct. 1949, pp. 656..715

Tane_81 Andrew S. Tanenbaum: Computer Networks; Prentice-Hall, Englewood Cliffs, N. J., 1981

Thom_84 Ken Thompson: Reflections on Trusting Trust; CACM, Vol. 27, No. 8, Aug. 1984, pp. 761..763

Waid_85 Michael Waidner: Datenschutz und Betrugssicherheit garantierende Kommunikationsnetze. Systematisierung der Datenschutzmaßnahmen und Ansätze zur Verifikation der Betrugssicherheit; Diplomarbeit, Fak. f. Inform., Univ. Karlsruhe, Interner Bericht 19/85, Aug. 1985

WaPf_85 Michael Waidner, Andreas Pfitzmann: Betrugssicherheit trotz Anonymität. Abrechnung und Geldtransfer in Netzen; 1. GI-Fachtagung "Datenschutz und Datensicherung", Okt. 1985, München, IFB Band 113, Springer-Verlag, Heidelberg, pp. 128..141; Revised version appears in DuD, "Datenschutz und Datensicherung, Informationsrecht, Kommunikationssysteme", Vieweg Verlag, Wiesbaden