Attacker models, traffic analysis and privacy threats in IP networks

Ralf C. Staudemeyer
University of Applied Sciences Schmalkalden

Christian Omlin
University of South Africa

Attacker Models, Traffic Analysis and Privacy Threats in IP Networks

R. C. Staudemeyer[1,2], D. Umuhoza[1,2], C.W. Omlin[2,3]
[1] Department of Computer Science & [2] Center of Excellence for IP and Internet Computing,
University of the Western Cape, 7535 Bellville, RSA
[3] Department of Mathematics & Computing Science, University of the South Pacific, Suva, FIJI ISLANDS

***Abstract*— In this position paper, we present attacker models and discuss threats that attackers pose to privacy in IP Networks. These models abstract from implementation details and network infrastructure. We distinguish between passive and active attacks and discuss solutions that provide protection against such attacks. We conclude that protection against passive attacks can only be guaranteed if we can achieve unobservability of all communication. In a network in which communication is unobservable the only remaining threats are active attacks; these however can be detected and countermeasures can be initiated.**

Category: Personal Communications (B5)

I. Introduction

In the context of security and privacy in IP based networking ”senders” send ”messages” to ”recipients”. An attacker may be interested in monitoring what communication is occuring, what communication patterns exist or even attempt to manipulate the communication.

We can make the assumption that an attacker is not able to get information about the content of the messages thanks to strong data encryption. Traditionally, security has consisted of three main components: confidentiality, integrity and availability. We need to address all three issues to secure a system. In the business domain, there are two further components, - authenticity and accountability - , that are less relevant in this context.

The realm of privacy, however, has largely been neglected. In particular, attackers may monitor communication (e.g. conduct traffic analysis), look for communication patterns and manipulate communication. This paper addresses privacy issues. We want to ensure anonymity and unlinkability; ideally we would also achieve unobservability. The terms are defined as follows [1]:

- Anonymity ensures that users are not identifiable within a set of users, the so-called anonymity set. This only holds if the set is greater than one.
- The aim of unlinkability is to ensure that any two or more terms in a system remain uncorrelated indefinitely.
- Unobservability of a communication system is ensured if the state of any item of interest is indistinguishable from any item of interest at all.

This position paper is organized as follows: We first provide an introduction to traffic analysis; thereafter a literature survey of privacy enhancing protocols, attacker models and privacy attacks. We then discuss alternative attacker and attack models. We emphasize that our analyses describe attacks and attackers in their *abstract form*, i.e., independent of specific network protocols, routing node configurations, etc. Finally, we end with concluding remarks regarding future research.

The particular contributions of our attacker and attack models as follows: First, we define the term attacker more precisely than in previous literature. The attack model is intended to be comprehensive of all possible privacy attacks we are aware of which act on datagram-based communication networks and which are independend from any particular network protocol. Such a model will aid in the development of privacy-enhancing protocols and help to determine the kinds of attackers against which existing software protects. Second, we provide a list of possible attacks that can be launched against a message-based communication system such as the Internet. We examine all the ways in which an attacker might attempt to correlate a flow of messages from a particular sender to a particular recipient.

II. Traffic Analysis

Traffic analysis is the process of capturing, interrupting and analyzing messages on a network. The aim is to gather information about the network and its users from observed communication patterns. This technique is also applicable to encrypted messages. Large numbers of captured messages make traffic analysis more effective. Traffic analysis can reveal even more information if it is possible to modify either the flow of traffic or the messages themselves.

It is important to note that traffic analysis on its own is not very useful; but in combination with apriori knowledge it becomes a very powerful tool. The mere fact that two machines exchange messages might not be all that interesting on its own. The situation changes dramatically when we can map machines to locations. For instance, if we know that one communication node is a company that is seeking funds and the other is seeking to make acquisitions, then we can arrive at further conclusions. We might be able to tell in which departments the machines are located, that they are exchanging email messages and we may even be able to identify sender and recipient.

An analyst can log frequency and time of all messages between two communication partners. The analyst can easily conclude if the session is interactive or non-interactive. The traffic frequency pattern of a non-interactive session is much more regular than that of an interactive session. An interactive session will have a very individual traffic pattern which is much like a fingerprint; further conclusions can be made about the kind of application that is running. A Web-browsing session and a SSH-session exhibit very different traffic patterns. In Web-browsing, users request html pages, read them and request new pages; in a SSH-session, a message is sent after every keystroke.

In order to prevent message frequencies from revealing information about the type of connection, it is necessary to exchange messages continuously with equal maximum bandwidth to all potential communication partners. It is possible to achieve this by broadcasting a continuous stream of messages which includes dummy messages. Obviously, this is not very efficient and protects only against this kind of traffic analysis.

III. Related Work

The terms we use in connection with network communication privacy have been defined in [1].

There are few basic privacy-enhancing concepts. The concepts differ depending on whether we want to protect sender, recipient or sender and recipient from each other. In terms of anonymity, mutual protection guarantees that each member of the party remains anonymous with respect to others.

Important concepts are DC-Net and Private Message Service, which describe mechanisms for sending messages anonymously [2], [3]. With DC-Net, it is possible to construct a broadcast-round-based protocol where members of the round can unobservably publish exactly one message per round. This is called ”superposed sending”.

The following synopsis of the DC-Net-Algorithm is paragraphed from [5]:

Let $P = P_1, P_2, ...P_n$ be the set of participants and let $(F, \oplus)$ be a finite abelian group in which all computations will be carried out.

The protocol goes as follows:

- Initialization:
  Each participant securely shares secret keys (chosen at random from F) with some other participants. We denote the secret key shared by P_y and P_z by $K_{y,z} (= K_{z,y})$ and define the set G composed of all pairs (P_y, P_z), such that P_y and P_z share a secret key. Notice that if $(P_y, P_z) \in G\ then\ (P_z, P_y) \in G.$
- Message Transmission:
  In order to send a message M, P_i broadcasts:
  $$M \oplus \sum_{\forall_j s.t. P_i, P_j \in G} sign(i-j) * K_{i,j}$$
  Where $sign(x) = 1\ if\ x > 1$ and -1 otherwise
- ”Noise” Transmission:
  All other participants, P_j, broadcast:
  $$\sum_{\forall_j s.t. P_j, P_k \in G} sign(i-j) * K_{j,k}$$
- Computing the Message:
  All interested participants can obtain M by adding $\oplus$ all broadcasted messages. The fact that the sum of all broadcasted messages equals M can be seen by noting that all terms except M cancel out because of $sign(n)$ (i.e. for each term of the form $sign(j-l) * K_{j,l}$ we have $sign(l-j) * K_{l,j} = sign(l-j) * K_{j,l} = -sign(j-l) * K_{j,l}$).

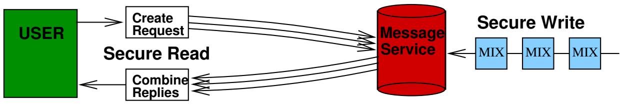

Fig. 1. Message Service

In order to quantify this scheme's security, we define a graph having n vertices, labelled 1,2,...,n (each representing a participant), with edges between nodes i and j if and only if P_i and P_j share a secret key. For example, if all participants share a secret key, the graph will be fully connected.

DC-Net can be extended to also provide support for the anonymous reception of messages [4]. The very basic concept to allow recipient anonymity is to broadcast or multicast a message.

Message Service or so-called anonymous information retrieval offers a method of reading an entry out of a database without anyone being able to track the message the reader was interested in. The suggested protocol can be modified to send messages to mobile recipients (Fig. 1) [3].

Anonymous information retrieval involves two steps:

- Messages are attached with an implicit address and sent to the service directly or by using another concept like mixing.
- The intended recipient requests the message from the message service using a special designed bit-vector protocol.

For a read operation of bit p using the bit-vector protocol the mobile recipient should create t random bit-vectors of length m. This is followed by creating a $t+1$ bit-vector by exclusive-or-ing the t random bit-vectors and then by flipping the p bit. This will create a set of $t+1$ bit-vectors that, when exclusive-ored together, will yield the bit-vector I_p with

$$I_p[j] = 0\ if\ j \neq p \mid 1\ if\ j = p$$

The bit-vector protocol works as follows:

- Choose $V_1, V_2 ... V_{i+1}$ such that $V_1 \otimes V_2 \otimes ... \otimes V_{i+1} = I_p$
- Read operations:
  Server 1:
  $$r_1 = \bigotimes_{V_1[i]=1} M[i]$$
  Server 2:
  $$r_2 = \bigotimes_{V_1[i]=1} M[i]$$
  Server t+1: ...
  $$r_{i+1} = \bigotimes_{V_{i+1}[i]=1} M[i]$$

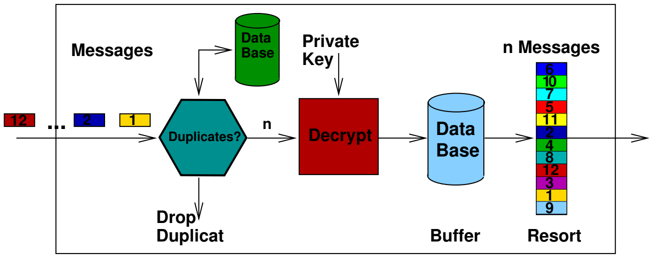

Fig. 2. Mixing

- Answer from Message Service:

$$r_1 \otimes r_2 \otimes ... \otimes r_{i+1}$$

It is assumed by the Message Service protocol that content privacy and data integrity is guaranteed. In addition Message Service servers are considered to be secure. Fault tolerance is not covered by this protocol.

A major disadvantage of Message Service is that it needs a minimum of three Servers with exactly the same database entries. Message Service also increases traffic in the network but becomes more efficient with the size of the database.

The MIX-network guarantees the anonymity and unlinkability of sender and receiver [6]. The mix scrambles, delays and reencodes a set of messages that an attacker cannot match incoming messages with outgoing messages (Fig. 2).

Initially the user encrypts his message m with an asymmetric method using the public key K_e of the receiver. Then the message is combined with a random part r_1 and encrypted with the public key K_1^{-1} of the mix used to send the message.

$$m = K_1(r_1, K_e(r_0, m))$$

The random part in the message is necessary to prevent an attacker from reencrypting the outgoing message with the known public key of the mix and tracing back the message. Additionally outgoing messages all have the same length by adding random bytes and an additional layer of encryption.

$$m = K_1(K_1(r_1, K_e(r_0, m)), RandomBytes)$$

To increase security in Mixing and to prevent that the owner of a mix can reveal the communication relation, multiple mixes must be used. The sequence is fixed by the encryption of the message using the individual public keys of the mixes. A message m using three mixes gets encoded in the following sequential manner:

$$K_1(r_1, K_2(r_2, K_3(r_3, K_e(r_0, m))))$$

Every MIX can only encrypt the outer frame of every message with its private key.

By using multiple MIXes it is sufficient if one of the MIXes is trustworthy. Only if all MIX-carriers work together can they reveal the communication relation. Multiple MIXes can be organized in fixed cascades or in free routes. Within a MIX-cascade a row of dedicated servers join and redirect traffic of a great number of users down a predefined route. In free routes, a network of MIXes is used. Distributed and equal client applications with MIXing functionality reroute and distribute the traffic equally over all possible routes. At the time of writing, neither strategy had proven superior.

Several adaptations of the MIX-concept have been introduced which add new functionality to the basic concept and resolve security and performance problems. These new functions include constant dummy traffic, the adaptive chop and slices algorithm and ticket-based authentication to prevent an attacker drawing conclusions from related packets travelling through the network [7], [10].

A good introduction to traffic analysis, attacker models and attacks on privacy-enhancing networks is given in [5], [9]. A solution based on the implementation of a Mix-based real-time proxy service that protects against some passive attacks was proposed in [10]. The authors include a comparison of existing systems with respect to resiliance against general passive attacks. An analysis of the success of various attacks based on traffic analysis on a number of privacy enhancing network implementations was presented in [11].

IV. Attacker Models

In this section we model the power of the attacker. Little previous work had been done.

Perfect protection protects against an omnipotent attacker. The omnipotent attacker is able to

- trace all data from point of creation to delivery,
- alter all data unnoticeably,
- alter whole system's functionality (until demolition).

We believe protection against attacks by an omnipotent attacker is unrealistic. A realistic attacker model must consider all possible attacks that can be expected during the lifetime of the observed system.

We distinguish the following powers an attacker might have:

- Attacker Distribution
- Internal/External Attacker
- Passive/Active Attacker
- Static/Adaptive Attacker
- Computing Power of an Attacker
- Non-Technical Attacks

An attacker may be able to control a subset of nodes (usually routers) of a communication system. These may vary from one to all available network nodes. An important aspect is the distribution of the controlled nodes within the network infrastructure. Depending on the distribution and relevance of the controlled nodes, an attacker can obtain a more or less complete view of the overall network traffic flow.

We distinguish between global and local attackers. A global attacker is able to access and observe all communication lines of the communication system. A locally present attacker has physical access to the senders and/or the recipients machine. It is important to consider that an attacker may be able control a subset of available communication lines or intermediate nodes. The relevance of this subset might vary strongly.

An internal attacker may be able to compromise the sender, the recipient or some intermediate nodes. Of special interest are intermediate nodes that provide routing or enhanced security functions. An attacker that is only able to compromise the communication medium itself is defined as an external attacker. An attacker who is only able to eavesdrop on the communication medium and observe the traffic flow is defined as a passive attacker. It is not possible to recognize a passive attack; but it may be possible to recognize the success of a passive attack if such an attack changes the behavior of nodes who collected additional information as a consequence of an attack.

An active attacker can modify network computations and transmitted messages. There may be restrictions on the kind of modifications an active attacker can execute. We can distinguish three kinds of changes of node behavior:

- interruption
- interception
- modification

Interruption cuts the connection between sender and recipient. With interception, an attacker is able to filter and store single packages. Modification enables an attacker to modify and introduce new packets. We might be able to conclude whether an attacker is able to modify packets in real-time or only with a noticeable delay.

In a static attack, the compromised resources are fixed after the attack has been launched. An adaptive attacker is able to control and modify resources during an attack. Only adaptive attackers are able to trace messages.

The computing power of an attacker may be limited or unlimited. An attacker with unlimited computing power is known as an information theoretical attacker. It is risky to assume that an attacker has only limited hardware resources at his disposal or lacks knowledge of powerful algorithms. It is acceptable, however, to make assumptions on the amount of money the attacker is willing to spend on an attack. We may also assume time restrictions on side of the attacker.

For instance, an attacker may bribe a trusted third party to manipulate part of the network infrastructure. This could give additional power and capabilities to an attacker that would not be available under normal circumstances.

Finally we must assume that there is a sufficient number of reliable participants within a network. Anonymity is not achievable for any participant of a network if all the other participants are controlled by an attacker.

V. Privacy Attacks

An attack may have at least one of two aims: observation of users of the communication system and/or interruption of services offered by a communication system. We give abstract descriptions of attacks that are independent of any specific concept.

A. Passive Attacks

A passive attacker is only able to eavesdrop on communication links and at intermediate nodes. It is the nature of attacks based on eavesdropping that they are not detectable as they are occurring. But it is possible to prevent them if the weaknesses of the observed network are known. The following attacks can be launched by an eavesdropper:

- Message Coding Attack
- Message Timing Attack
- Message Size Attack
- Message Counting Attack
- Communication Volume Attack
- Communication Pattern Attack
- Message Frequency Attack
- Brute Force Attack
- Long-Term Intersection Attacks

All messages that do not change their encoding during network transmission can be linked or traced by an attacker.

A timing attack observes the duration of communication between nodes and attempts to correlate patterns of network participation. Possible routes can be calculated using the round trip time of message sets entering and leaving the network at two observed points.

It is possible to correlate messages by their size if the size of the sent message is the same as that of the received message.

A counting attack observes the number of packets exchanged between two possible communication partners.

Communication volume attacks are a combination of message size attack and message counting attack. It detects the communication relation between two parties by observing the amount of transmitted data. It is applicable when messages are not delimitable within the traffic stream.

Communication pattern attacks can be launched by simply monitoring communication activity on any network device, i.e. the pattern of sending and receiving of messages. In general, an attacker can make the assumption that participants of a communication usually do not send and receive messages at the same time. Observations over long periods of time can reveal sets of possible communication partners.

Users always have distinct, individual behavior. For message frequency attacks an attacker analyzes the traffic flow of messages to fingerprint individual users and/or communication partners. This is most effective for real-time interactive communication. The attacker determines the message frequency between two endpoints by counting packets and recording the communication pattern.

An attacker may trace every possible path an observed message can take through a network and thus can construct a list of possible recipients. Given enough time, the number of possible sender/recipient pairs can be reduced. An attack proceeds as follows:

- The attacker follows the message from the sender to the first intermediate node where the number of possible outgoing messages m_t is $t > 1$.
- The attacker then tracks every message m_t the observed node releases to a new intermediate node or the recipient.
- The attacker repeats the above two steps until every message has been tracked to a recipient.

In the worst case, an attacker can match one sender to one recipient. In the best case, an attacker needs to follow t^d messages along $t^d - 1$ paths through a network and to their recipients in order to identify a pair sender/recipient.

An attacker may trace users over a long period of time by their online/offline behavior. Users exhibit an individual, characteristic usage pattern of network services. For instance, they get on and offline at specific times to check special webpages regularly, requesting email messages or reading a special newsletter. All transmitted data that serves unique purposes such as cookies, ID numbers, pseudonyms and any other data that is sent more than once uncovers a communication relation with a high certainty.

B. Protection against Passive Attacks

In order to provide protection against message coding attacks, the encoding must change during transmission. This can be done by encrypting the messages with k nested layers to members of the network or using per link encryption between routing nodes. A predefined message size of all network messages can protect against message size attacks; thus, smaller messages must use padding.

Ideally, the propagation of messages needs to be randomly delayed. The minimum delay can be defined by the maximum possible latency between two communicating network nodes. Another option that provides at least a guaranteed anonymity group is for routing nodes to wait for the arrival of a defined number n of messages from n different users and to forward them in one batch. Unfortunately, this method still causes delays in times of low traffic; thus, dummy traffic has to be transmitted in order to reduce such delays. It is difficult to overcome timing coincidences without wasting significant bandwidth.

Prevention of message counting attacks is possible if all network participants send and receive a standard number of messages. To provide protection against communication volume attacks it is sufficient to protect against message size and message volume attacks. Communication pattern attacks are dangerous attacks that are difficult to prevent. They require continous network participation of a sufficient great number of nodes. Message frequency attacks are most effective for real-time and interactive communication. A standardized, rigid message exchange pattern with the network would help to provide enhanced protection.

No guaranteed protection against brute force attacks or long-term intersection attacks exists. Keeping the number of possible recipients large during all times may make the success of such an attack less likely. This can be achieved by introducing dummy traffic. Protection against long-term intersection attacks remains a well-known open problem. Anonymous information retrieval for mobile nodes using the anonymous message service or a continous connectivity and message exchange with the network might be options to solve that problem.

In general, protection against passive attacks requires a very rigid structure of user communication. Only an unobservable network offers protection against such attacks since neither nodes or nor messages are identifiable.

TABLE I
PROTECTION AGAINST PASSIVE ATTACKS

Attack	Proposed solutions
Message Coding	change coding during transmission k-nested encryption
Message Timing	1) batched forwarding of messages 2) random delay of messages ($delay_{min} \geq latency_{max}$)
Message Size	predefined message size padding small messages
Message Counting	receive and forward standard number of messages; use dummy messages
Communication Vol.	protect message size and communication volume
Communication Patt.	continous network participation
Message Frequency	standardized message exchange patterns
Brute Force	No clear protection dummy traffic
Long Term Intersection	No clear protection continous connectivity, dummy traffic, message service

C. Active Attacks

Active attacks are based on network disruption. An active attacker is able to change the state of the network, i.e. the attacker can interrupt the traffic stream, can delete or add packets and can modify messages by changing bits or timing.

Ideally, we would like to provide protection against the following types of active attacks:

- Message Tagging Attack
  - Manipulation of Message-bits
  - Message Replay
  - Message Delaying or Blocking
- N-1 Attack
- Broadcast Attacks
- Denial of Service Attack

Message tagging attacks require knowledge of both the originating and terminal nodes; messages are tagged at the former that the latter can spot. Since the entry node knows the sender and the exit node knows the receiver the communication relation is revealed. An attacker can change some bits in a message. We may distinguish if the manipulations are in the header or in the payload of a message.

Protection mechanisms may prevent an attacker from tracking a sent message. Resending it enables an attacker to follow the replay if the behavior of the copy through the network is identical to the behavior of the original message.

An attacker may delay or block messages and wait until the observed network becomes easier to monitor or to see if the observed recipient still gets messages. It is also possible for an attacker to mark the traffic stream itself by delaying or blocking certain packets.

All messages but one are generated by an attacker who blocks or manipulates all messages from other senders. Such an attack limits the size of the anonymity set to one i.e. it does not guarantee anonymity. Only the message the attacker wants to trace is unknown.

Broadcast attacks are based on the assumption that the intended recipient's reaction on receiving the message will differ from most other recipients.

An attacker might obtain information about the routes used by certain users by rendering some nodes inoperative. If at least one of these nodes is part of the route, the communication will get interrupted. This attack bases its success on the assumption that nodes which have a communication problem will behave differently from nodes which experience no problems.

Attacks can be combined and an attacker may obtain partial or probabilistic information by partially executing an attack.

Information can be inferred as follows:

1) with probability p, A is communicating with B or A is communicating with one of the users in the investigated group;
2) A is not communicating with B, C, D

A corrupt coalition of users or parts of the system may be able to trace certain users. It seem to be advisable to avoid centralisation. Ideally no point in the network reveals more information that any other point in the network.

D. Protection against Active Attacks

In this section, we assume an unobservable communication network. In order to protect against modification of message bits, we must ensure the integrity of header and payload, not only between end-users, but also between network links. It is adviseable to avoid centralisation within the network; ideally no node in a network reveals more information that any other node in the same network.

Redundancy of messages may help an attacker since manipulations stay undetected unless a system is able to clearly distinguish network failures and attacks.

In order to prevent replay attacks intermediate nodes may have a list of already processed messages and replayed messages are ignored. Another option is to share authenticated timing information with intermediate nodes. The second option also protects against delay attacks.

Authenticated sequence numbers and time-to-live values may also help to prevent attacks based on message replay or delay. But they can also reveal critical information about the connection to every intermediate node such as correlations between packets and distance to sender.

To prevent against blocking of messages a communication network must ensure continuous traffic exchange with end nodes. Intermediate nodes must ensure that messages come from a sufficient number of different senders to protect against N-1 attacks. This can be done by ticket-based authentication of messages. Protection is difficult if powerful attackers are able to build coalitions and launch distributed attacks. Nodes may use heartbeat traffic in order to detect a distributed N-1 attack. A standardized rigid network interaction pattern might help to prevent against broadcast attacks.

TABLE II

PROTECTION AGAINST ACTIVE ATTACKS

Attack	Proposed solutions
Manipulation Message bits	ensure message integrity
Message Replay	1) processed messages list 2) authenticated timing, sequence numbers and time-to-live
Message Delaying or Blocking	ensure continuous traffic exchange between end nodes
N-1	ensure sufficient number of messages from different senders; ticket-based authentification
Broadcast	standardized rigid network interaction pattern
DoS	known open problem

A very important fact to consider is that an attacker actively changes the state of a network. The act of changing the network state can be detected. The question is if attacks differ sufficiently from natural occurences that can happen in the network.

VI. Conclusion

Our work provides an analysis of attacker models and attacks on privacy that supports the better understanding, the evaluation and the development of privacy-enhancing technologies. We discussed various properties of an attacker that can be used to build a model with which to evaluate privacy enhancing networks.

We discussed passive and active attacks that can be lauched using traffic analysis. We conclude that protection against passive attacks requires very rigid communication behavior that guarantees network unobservability.

Protection against active attacks is nontrivial, but they can be detected since they change the state of the network. The question remains if they can be distinguished from benign network failures. This question warrants further investigation.

References

[1] A. Pfitzmann and M. Köhntopp. *Anonymity, Unobservability, and Pseudonymity: A Proposal for Terminology*, In H. Federrath, editor, Anonymity 2000, Volume 2009 of Lecture Notes in Computer Science, pages 1-9, Springer- Verlag, 2000.

[2] D. Chaum, *The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability*, Journal of Cryptology. Vol. 1, pages 65-75, 1988.

[3] D. Cooper and K. Birman, *Preserving Privacy in a Network of Mobile computers*, IEEE Symposium on Security and Privacy, pages 26-38, 1995.

[4] M. Waidner and B. Pfitzmann, *The dining cryptographers in the disco: unconditional sender and recipient untraceability with computationally secure servicability*, Proceedings of EUROCRYPT 1989, Springer-Verlag, LNCS 434, 1990.

[5] J. Raymond. Traffic Analysis, *Protocols, Attacks, Design Issues, and Open Problems*. In H. Federrath (Ed.), Anonymity 2000, Volume 2009 of Lecture Notes in Computer Science, pages 10- 29, Springer- Verlag, 2000.

[6] D. Chaum, *Untraceable electronic mail, return addresses, and digital pseudonyms*, In Communications of the ACM, Vol. 4, Nr. 2, 02/1981.

[7] A. Pfitzmann, B. Pfitzmann and M. Waider, *ISDN-mixes: Untraceable communication with very small bandwidth overhead*. Proceedings of the GI/ITG Conference on Communication in Distributed Systems. pages 451-463. 02/1991.

[8] O. Berthold, H. Federrath and S. Koepsel, *Web MIXes: A system for anonymous and unobservable Internet access*. In H. Federrath (Ed.): Designing Privacy Enhancing Technologies. Proc. Workshop on Design Issues in Anonymity and Unobervability, LNCS 2009, Springer-Verlag, Heidelberg 2001, 115-129.

[9] A. Back, U. Moller and A. Stiglic, *Traffic Analysis and Trade-Offs in Anonymity Providing Systems*. In I.S. Moskowitz editor, IH 2001, Volume 2137 of Lecture Notes in Computer Science, pages 245- 257, Springer-Verlag, 2001.

[10] O. Berthold, H. Federrath and M. Köhntopp, *Project: Anonymity and Unobservability in the Internet*, Workshop on Freedom and Privacy by Design / CFP2000, 2000.

[11] R. Song, L. Korba, *Review of Network-Based Approaches for Privacy*, Proceedings of the 14th Annual Canadian Information Technology Security Symposium, Ottawa, Ontario, Canada. May 13-17, 2002. NRC 44905.