Category: IT Security & Ethics

Anonymous Communications in Computer Networks

Marga Nácher
Technical University of Valencia, Spain

Carlos Tavares Calafate
Technical University of Valencia, Spain

Juan-Carlos Cano
Technical University of Valencia, Spain

Pietro Manzoni
Technical University of Valencia, Spain

INTRODUCTION

In our daily life no one questions the necessity of privacy protection. Nevertheless, our privacy is often put at risk. The first problem has to do with the fact that privacy itself is a concept difficult to define. As a matter of fact, in many countries the concept has been confused with data protection, which interprets privacy in terms of the management of personal information. Nowadays, the term *privacy* is extended to territorial and communications protection.

We will focus on the privacy of electronic communications. When referring to this type of communication, the first aspect we think about is security. In fact, this concept is widely discussed, and nowadays we often hear about threats and attacks to networks.

Security attacks are usually split into active and passive attacks. We consider that an active attack takes place when an attacker injects or modifies traffic in the network with different purposes, such as denial of service or gaining unauthorized access. Unlike active attacks, a passive attack takes place whenever the attacker merely inspects the network by listening to packets, never injecting any packet. Malicious nodes hope to be 'invisible' in order to collect as much network information as possible just by using timing analysis and eavesdropping routing information. A way to avoid this type of attack is to anonymize both data and routing traffic. In this manner we can hide the identities of communicating nodes and avoid data flow traceability.

Various scenarios can be devised where anonymity is desirable. In a commercial transactions context, if we think about an off-line purchase, we accept that some users prefer to use cash when buying some goods and services, because anonymity makes them more comfortable with the transaction. Offering anonymity to online commerce would increase the number of transactions.

Military communications are another typical example where not only privacy but also anonymity are crucial for the success of the corresponding mission.

Finally, if we attend a meeting where some delicate matter is being voted on, it could be necessary for the identities to remain hidden. Again, in this case, anonymity is required.

BACKGROUND

In order to talk about anonymity, first we have to establish the terminology to be used. An important work on this issue is Pfitzmann and Hansen (2000); based on this work, we can establish a classification of anonymity degrees: A node is considered exposed when its identity information is known. If its identity is not the real one, the node is pseudonymous. Furthermore, if it is unlinkable to some kind of relevant information, we achieve anonymity with respect to that information; as an example we can consider the relationship between end-to-end peers or the peers themselves. Finally, when the communication is not perceived, we can say that it is undetectable; and if it is undetectable for any external node and also anonymous for every participant, the communication is unobservable.

In the literature, there are various works based on different networks topologies as the Dining Cryptographers (Chaum, 1988) or MIXes (Chaum, 1981) in order to provide anonymous communications in fixed networks.

PEER ANONYMITY

In this article we will discuss the different degrees of anonymity provided by means of different proposals found in the literature, emphasizing those issues that are still unsolved.

General Approaches

Anonymity has been treated differently depending on the network characteristics and goals. We believe that the two most relevant generic proposals are the Dining Cryptographers network and the MIX network.

Dining Cryptographers Network

The Dining Cryptographers network (DC-net) (Chaum, 1988) achieves sender anonymity in the following way: some pairs of participants share a secret bit. Each participant calculates the sum of all the bits that he shares, and if he wants to transmit, he inverts that result. All the nodes send the result of the sum or the inverted one (if necessary). If no one (or an even number of participants) transmits, the sum of all these transmissions is zero. In cases where one participant (or an odd number of them) transmits, the sum will be one. Each participant could share a key of n bits with another participant, one bit per round. So, the ith bit of each such key will be used in the ith round.

However, this approach is restricted to small networks since only one node can transmit in each round. In large networks the probability of having more than one node wishing to transmit in a specific round increases, and so collisions will render this mechanism impractical.

Furthermore, the anonymous bandwidth of a DC-net is limited by the slowest participant. Overall, DC-nets provide strong anonymity elegantly, but suffer from efficiency and scalability problems.

Herbivore (Goel, Robson, Polte, & Sirer, 2003) is a protocol based on DC-nets that tries to solve the scalability problem by splitting the network into sub-groups (called cliques), but it requires global topology control. In terms of efficiency, results are actually quite poor.

MIXes Network

In 1981, Chaum proposed the use of MIXes to anonymize electronic mail users and messages. The main goal for a single MIX is to hide the correlation between incoming and outgoing messages within a large group of messages by delaying or reordering them. In order to do this, encryption and padding mechanisms are applied.

There are several MIX variants:

- A pool MIX only sends part of the incoming messages, keeping the other parts for later rounds. Hence, it uses the reordering technique. It is called a "timed MIX" if the event that triggers the flushing is the expiration of a timeout. In cases where the trigger is the arrival of a message, the MIX will be referred to as a "threshold MIX."
- A stop-and-go MIX (or continuous MIX) delays messages according to an exponential distribution, which does not depend on traffic. Hence, if the number of users is low, the degree of anonymity is also low.

A MIX network can consist of a set of predefined routes, called cascades, or free route networks, where routes are selected by users. Berthold, Pfitzmann, and Standtke (2001) establish that this last type of networks is flexible, scalable, and extendable. However, it is less secure due to the intersection of different anonymity sender/recipient groups,

Figure 1. Example of DC-net