R. Rios, “Recipient Anonymity”, *Encyclopedia of Cryptography, Security and Privacy*, 2021.
http://doi.org/10.1007/978-3-642-27739-9
NICS Lab. Publications: https://www.nics.uma.es/publications

Recipient Anonymity

Ruben Rios[1] [2]

(1) Network, Information and Computer Security Lab, Universidad de Málaga, Campus de Teatinos, Málaga, Spain
(2) ITIS Software, Universidad de Málaga, Edificio Ada Byron, Ampliación Campus de Teatinos, Málaga, Spain

Ruben Rios
Email: ruben@lcc.uma.es

Related Concepts

Anonymity; Sender Anonymity; Unlinkability; Unobservability; Undetectability; Anonymous Communications;

Definition

Recipient anonymity refers to the ability of keeping the actual recipient of a message indistinguishable from all potential recipients. In the context of communication systems, a message recipient might be a person, a service or a computer device.

Theory

Anonymity can be defined as the state of being unidentifiable among a set of possible actors sharing similar attributes (Pfitzmann and Hansen 2010). Therefore, any actor involved in a communication system may want to be anonymous although this property is of special interest to senders and recipients since they are the main actors involved in a communication and their actions (i.e., sending and receiving messages) may reveal sensitive information about them. Anonymity can also be defined in terms of unlinkability. Sender and recipient anonymity can therefore be seen as the impossibility of linking a message to a potential sender and a potential recipient, respectively.

The set of actors with potentially the same attributes as the actor whose identity is to be preserved is called the anonymity set. When talking about recipient anonymity, we particularly refer to the recipient anonymity set. Recipient anonymity is achieved if an attacker cannot reliably determine after observing the system which of all the actors who received a message within a given period of time (i.e., the recipient anonymity set) is the actual recipient of a particular message. In principle, a large recipient anonymity set is relevant for recipient anonymity but it is not the only influencing factor.

The definition above captures the probabilistic nature of the process carried out by an attacker willing to identify the recipient of a message. The attacker may perform a passive or an active attack depending on whether he merely monitors network traffic or performs some actions to disturb the communication such as blocking or injecting new messages. After the attack, the adversary obtains a distribution of probabilities that link the particular message to potential recipients. Therefore, recipient anonymity is not only determined by the size of the recipient anonymity set but also by the uniformity of the probabilities. In other words, the level of uncertainty of the attacker when guessing who is the actual recipient. This is the reason why various metrics for quantifying anonymity are based on the concept of information entropy (Lu et al. 2019).

However, it might be the case that even when an entropy-based metric suggests strong recipient anonymity it does not necessarily imply strong anonymity for each particular recipient in the anonymity set, as suggested by Pfitzmann and Hansen (2010). In some situations, we might have that very few recipients are much more likely than the others and thus their anonymity is weak. This also indicates that recipient anonymity is context-dependent and thus depends on the particular type of attacker being faced. Consequently, recipient anonymity can be defined with respect to an external attacker or an internal attacker, including both intermediaries and data sources. Protection mechanisms will depend on the type of adversary that needs to be countered.

When protecting recipient anonymity, the first and most basic mechanism is to remove any identifiable information that may link the message to the recipient. However, without a destination address it is not possible to route the message through the network. It is therefore necessary to find an identifier that enables routing the message without revealing the actual identity of the recipient. A common approach is to use a multicast address (Shields and Levine 2000) rather than a unicast address so that the actual recipient remains anonymous among all the members belonging to the multicast group, that is, the recipient anonymity set.

A more sophisticated approach consists of using network overlays capable of hiding the correspondence between input and output messages. This idea was first proposed by Chaum (1981) and served as inspiration for many other schemes and tools available today. In essence, there is a network of devices that receive encrypted messages and forward equal-sized decrypted message only after each message has been mixed with a sufficient number of messages. Although mix networks were designed to hide the relationship between senders and recipients it also supports recipient anonymity with respect to external attackers. On top of that, the original data source may include an anonymous reply or return address for allowing the destination to respond to the data source (now the recipient) without revealing its identity.

Finally, it is worth noting that there are some additional notions which provide stronger guarantees than recipient anonymity. These notions are undetectability and unobservability. Recipient undetectability means that an attacker cannot be sure whether or not a particular actor is a recipient. This is typically achieved by introducing large amounts of bogus traffic to cover real messages so that the attacker cannot sufficiently tell whether a message is real or not. Recipient unobservability augments that notion with anonymity even against other recipients, that is, not even recipients learn whether or not a particular recipient has received a message. A popular scheme called DC-Nets Chaum (1988) is capable of providing such level of protection by taking advantage of a tightly synchronized broadcast channel.

Applications

Anonymity is an important property that protects individual freedom, civil rights and democracy from infringement by totalitarian governments and private companies. Anonymity enables users to behave freely without discrimination or repression.

Recipient anonymity is convenient when using common internet services such as web browsing or email communications but also for resisting censorship. In all these situation, users may want to prevent third parties from learning with whom they are communicating not only because this may leak sensitive information about the user – social relationships, health condition, political ideas or religious beliefs, but also because it may result in prosecution, penalties or even physical harm depending on the type of data being accessed and who is the attacker. For example, a nation where freedom of speech and press are limited by law. Censorship-resistant systems (Khattak et al. 2016) can also benefit from recipient anonymity. In this context, recipient anonymity is paramount to keep the servers holding forbidden documents and allowing people to speak freely operational. Citizens should be able to gain unrestricted access to the servers but the identity and/or location of the servers must not be revealed even to legitimate users to avoid lockdowns by censors. Note that censors could pose as legitimate users of the censorship-resistant system in an attempt to track the servers.

Other contexts may also benefit from having recipient anonymity. For example, in wireless sensor networks it is critical to keep the identity of the data sink hidden from external adversaries. The reason for this is that an outsider may want to physically reach this device to compromise it and take control of the network or even destroy it thereby taking the whole network down. In this case, recipient anonymity is closely related to the concept of receiver-location privacy (Rios et al. 2016). This is also the case in other types of ad-hoc networks, where it is necessary to establish communication path with other parties while keeping the identity and/or location of the destination undisclosed.

Open problems and Future directions

Dealing with computational unrestricted attackers capable of controlling all communication links while keeping a low network overhead is a challenging problem. These attackers, which are typically referred to as global adversaries, demand for protection mechanisms that impose a great overhead either in terms of communication delays or bogus traffic injection. Therefore, finding lightweight anonymity solutions in the presence of powerful adversaries is an open problem.

Despite the number of metrics for measuring anonymity it is very difficult to actually assess the level of protection of the recipient since it very much depends on the information available to the attacker. Moreover, there might be various simultaneous attackers willing to identify the recipient each of which may have access to different information at the time launching the attack.

References

Pfitzmann, A. & Hansen, M. (2010) A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf

Lu, T.; Du, Z.; and Wang, Z. Jane (2019) A Survey on Measuring Anonymity in Anonymous Communication Systems, in IEEE Access, vol. 7, pp. 70584-70609, doi: 10.1109/ACCESS.2019.2919322.

Shields, C. and Levine, B (2000) A protocol for anonymous communication over the internet. In Proceedings of the 7th ACM Conference on Computer and Communication Security, Athens, Greece. Pages 33–42, doi: 10.1145/352600.352607

D. Chaum (1981) Untraceable Electronic Mail, Return addresses, and Digital Pseudonyms. Communications of the ACM, 24(2):84–88.

Chaum D (1988) The dining cryptographers problem: Unconditional sender and recipient untraceability. J Cryptol 1(1):65–75

Khattak, S; Elahi, T; Simon, L; Swanson, CM; Murdoch, SJ; Goldberg, I; (2016) SoK: Making Sense of Censorship Resistance Systems. Proceedings on Privacy Enhancing Technologies, 2016 (4) pp. 37-61. Doi: 10.1515/popets-2016-0028.

Rios, R.; Lopez, J.; Cuellar, J. (2016) Location Privacy in Wireless Sensor Networks, CRC Series in Security, Privacy and Trust, Taylor & Francis.