Serveis de Seguretat

Carlos Borrego

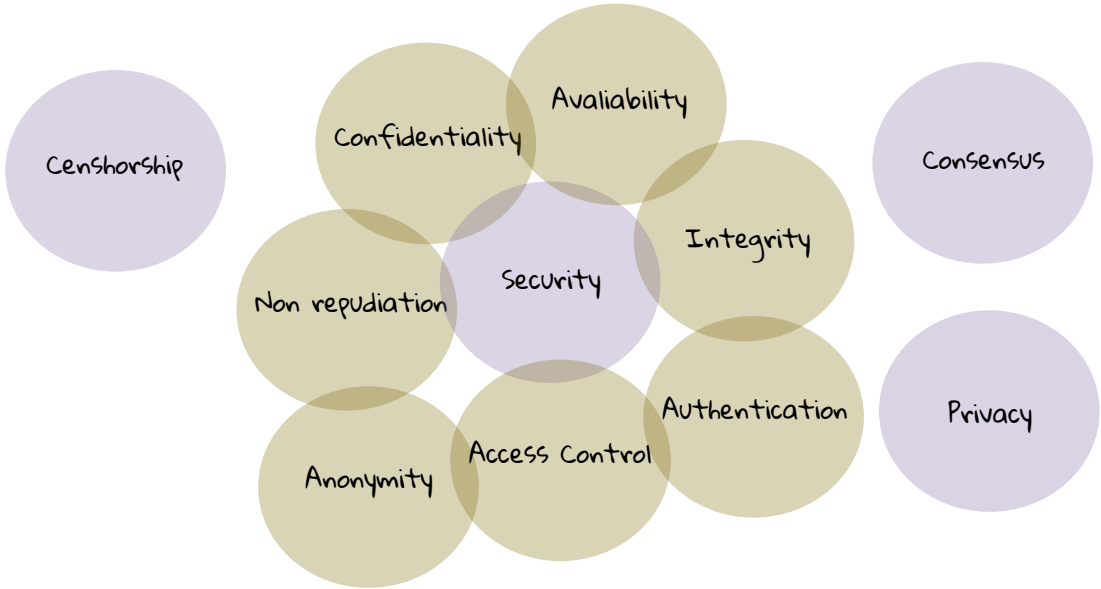
Carlos.Borrego@uab.cat

Departament d'Enginyeria de la Informació i de les Comunicacions
Universitat Autònoma de Barcelona

Criptografia i Seguretat

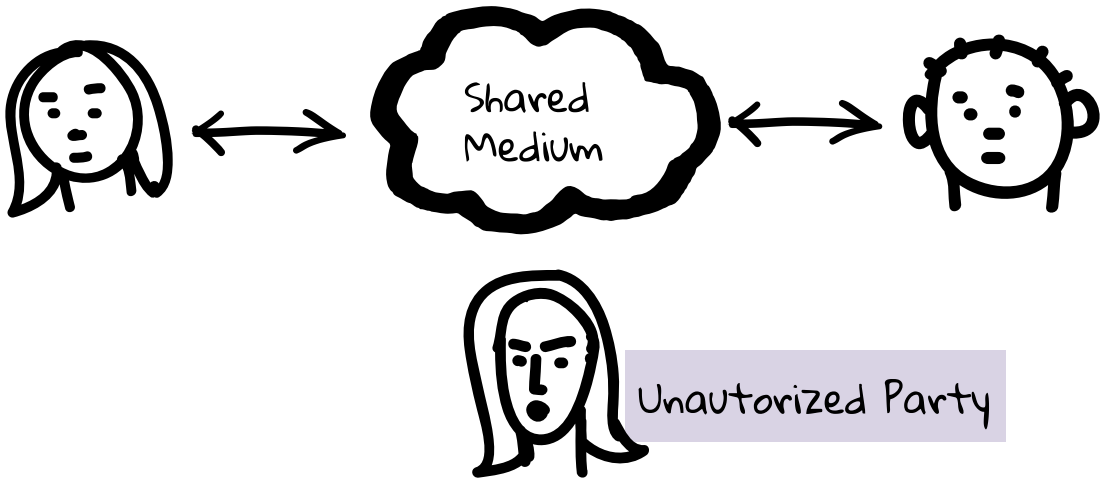
Content

Security+ Services



Confidentiality

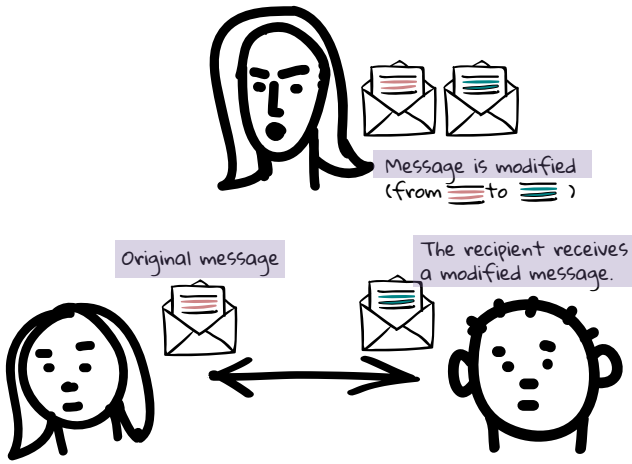
Confidentiality refers to **protecting information** from being accessed by unauthorized parties (specially when using a shared medium).



Once the secret has been revealed, there's no way to **un-reveal** it.

Integrity

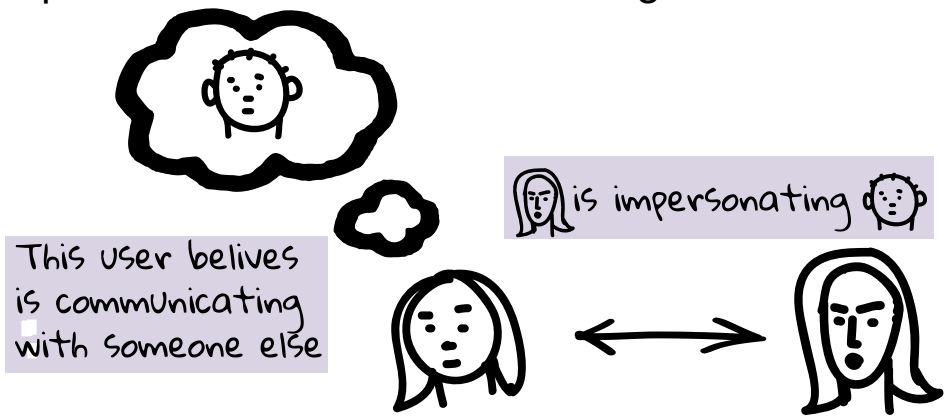
Integrity takes care of the **consistency** and accuracy of data during its entire life-cycle. A message that keeps its integrity means no process-in-the-middle has modify it.



An unauthorized party could modify a message. Integrity ensures that the message was originated from the intended sender and was **not modified** in transit.

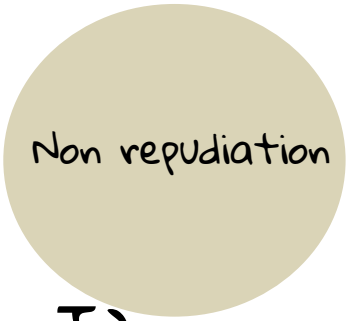
Authentication

Authentication is the process of recognizing a **user's identity**. It is important the processes remain authenticated, otherwise, a process could be implementing a certain protocol with another process different from the thought one.

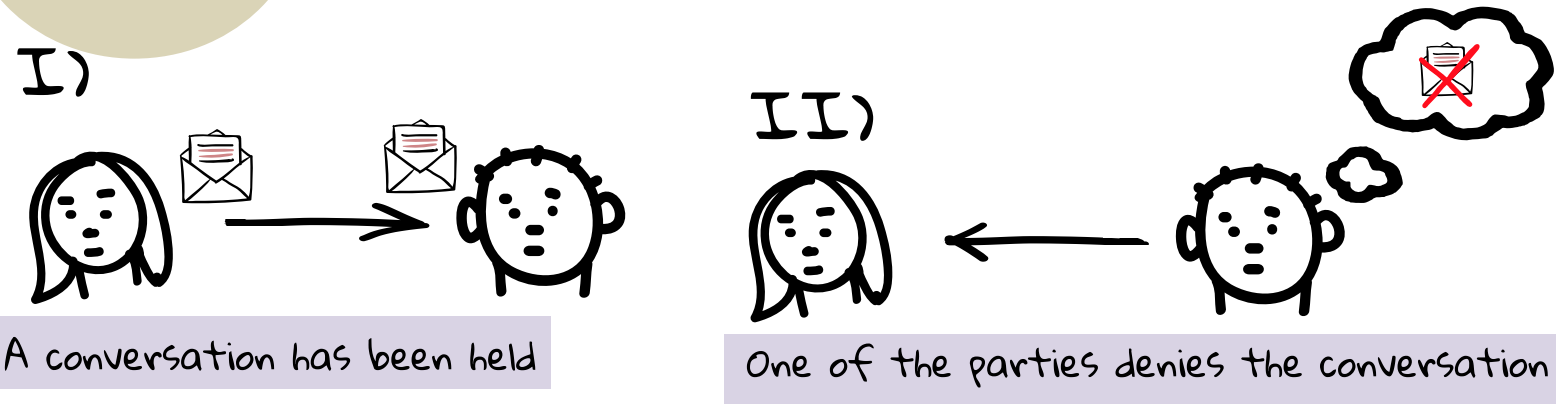


As in this figure, an impersonation attack is an attack in which an adversary successfully **assumes the identity** of one of the legitimate parties in a system or in a communications protocol.

Non-repudiation



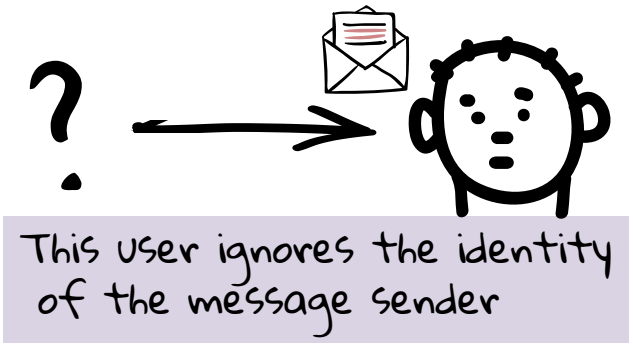
Assurance that the sender of information is provided with **proof of delivery** and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.



In order to implement this service, a **tangible evidence** connecting the identified party to a particular communication or action must be created.

Anonymity

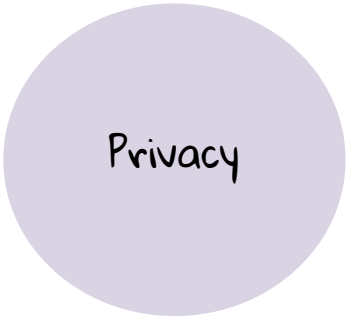
Anonymity refers to distributed systems where the user's **identity is unknown**. This can be a security service that eventually a process would like to implement. Anonymity can also be for both parties of the communication.



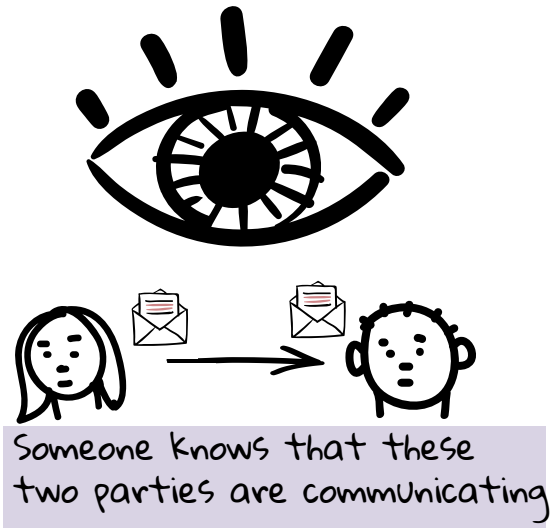
To Read:

The reasons you can't be anonymous anymore (By Bryan Lufkin 29th May 2017)
https://www.bbc.com/future/article/20170529-the-reasons-you-can-never-be-anonymous-again

Privacy

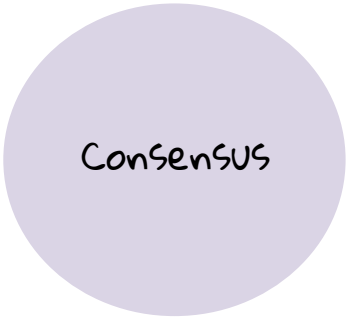


Digital privacy is the ability of the users to **seclude themselves** or information about themselves, and thereby express themselves selectively.

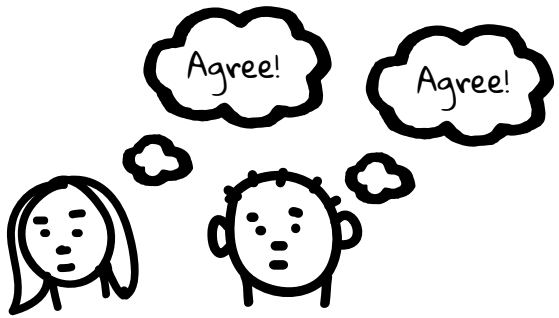


Digital Privacy is a collective definition that encompasses three sub-related categories; information privacy, communication privacy, and individual privacy.

Consensus

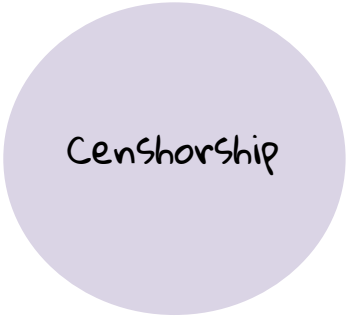


A consensus mechanism is used in distributed systems to achieve the necessary **agreement** on decisions among distributed processes or multi-agent systems.



This decisions may include single **data** values or a single **state** of the network.

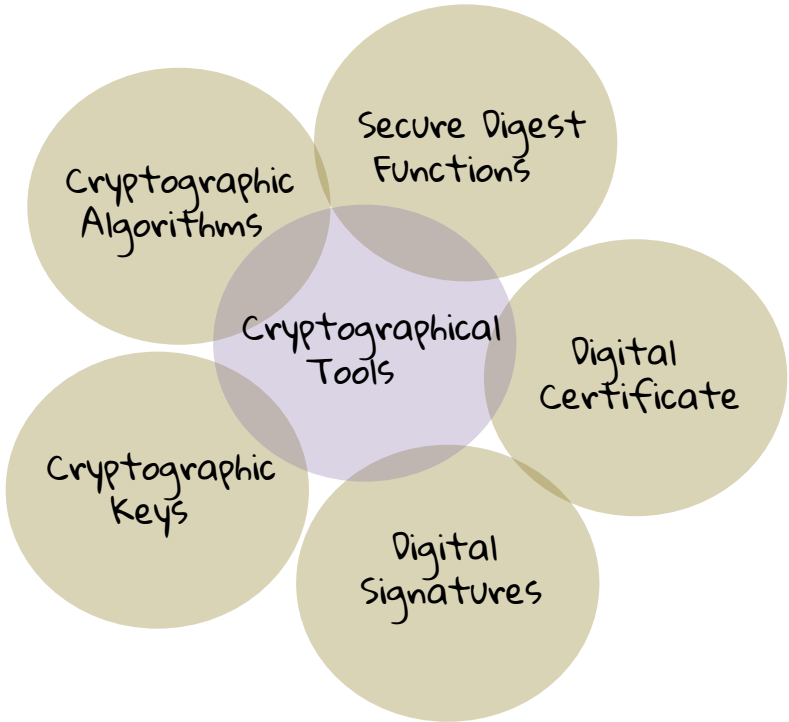
Censorship



Digital censorship is the **control** or **suppression** of what can be accessed, published, or viewed digitally enacted by regulators, or on their own initiative.

It may affect at the service itself or others that **announce** or help to **discover** them.

Cryptographical Tools



Serveis de Seguretat

Carlos Borrego

Carlos.Borrego@uab.cat

Departament d'Enginyeria de la Informació i de les Comunicacions
Universitat Autònoma de Barcelona

Criptografia i Seguretat