Alien terms and definitions

Erik Nordmark
erik.nordmark@sun.com

Wassim Haddad

From <draft-haddad-momipriv-problem-statement-01.txt>

Anonymity

- An entity "A" in a system has anonymity if no other entity can identify "A", nor is there any link back to "A" that can be used, nor any way to verify that any two anonymous acts are performed by "A".
- Might still be able to identify “A” as being part of a set; the anonymity set.
- Where a MAC or IP address/identifier is used, neither the communication peer nor any outside attacker should be able to link between the identifier and the user's identity.

Pseudonomity

- Pseudonymity is a weaker property related to anonymity.
- It means that one cannot identify an entity, but it may be possible to prove that two pseudonymous acts were performed by the same entity.
- A pseudonym is an identifier for a party to a transaction, which is not sufficient to associate the transaction with a particular user.

Unlinkability

- Two events are unlinkable if they are no more and no less related than they are related concerning the a-priori knowledge.
- Unlinkability ensures that a user may make use of resources or services without others being able to link these two uses together.
- Note that unlinkability is a sufficient condition for anonymity, but it is not a necessary condition.

Privacy

- Privacy is a more general term than anonymity.
- Privacy is the claim of individuals, groups and institutions to determine for themesleves, when, how and to what extent information about them is communicated to others.
- In wireless telecommunications, privacy addresses especially the protection of the content as well as the context (e.g., time, location, type of service, ...) of a communication event.