Privacy Properties

What is Privacy?
What is Privacy?

• **Attacker** - interested in
  – monitoring what communication is occurring
  – what patterns of communication exist
  – or even in manipulating the communication

Anonymity

- **Anonymity**
  - the subject is not identifiable within a set of subjects, the anonymity set
  - from an attacker’s perspective means that the attacker cannot sufficiently identify the subject within a set of subjects, the anonymity set

Unlinkability

- **Unlinkability** of two or more *items of interest* (e.g., subjects, messages, actions, etc.)
  - from an attacker’s perspective means that within the system (comprising these and possibly other items), the attacker cannot sufficiently distinguish whether these *items of interest* are related or not.
• **Undetectability**
  – of an *item of interest* from an attacker’s perspective means that the attacker cannot sufficiently distinguish whether it exists or not

• **Unobservability** of an *item of interest*
  – *undetectability* of the *item of interest* against all subjects uninvolved in it
  – *anonymity* of the subject(s) involved in the item of interest even against the other subject(s) involved in that item of interest
Unobservability

- **Unobservability** of an *item of interest*
  - *undetectability* of the *item of interest* against all subjects uninvolved in it
  - *anonymity* of the subject(s) involved in the item of interest even against the other subject(s) involved in that item of interest

Pseudonymity

- **Pseudonymity** – the use of pseudonyms as identifiers
  - A *pseudonym* is an identifier of a subject other than one of the subject’s real names
Summary

Privacy

Data Protection

Anonymity

Unlinkability

Undetectability

Unobservability

Pseudonymity