Privacy in Context
A panel discussion
Karen Sollins
Overview

- Sollins: Introduction, some thoughts for framing
- Panelists: Tschofenig, Sowell, Clark
- Discussion: Everyone
Information privacy concerns the protection of information about individuals and other entities. The environment for privacy is dynamic, reflecting social shifts..., varying and evolving attitudes..., and discontinuities... as well as technological change.

Toward Better Usability, Security, and Privacy of Information Technology, National Research Council, 2010
Introduction

The Scenario

System:
(2) Senders
Alice
Bob
Malice

(1) Communication Network
Msg from Alice
Msg from Bob
Msg from Malice

(3) Recipients
Carol
Accomplice
The basis

- From perspective attacker interested in:
  - What communications occur
  - Patterns of communication
  - Manipulation of communication

- Perspective
  - All possible observations must be considered
  - Focus on items of interest (IOI): subjects, messages, actions
  - Can learn (actor, action, object)
  - Later can learn attributes/values of an IOI
Definition of anonymity: attacker cannot sufficiently identify the subject from with a set of subjects, the anonymity set.

- Shared observable attributes

Definition of anonymity delta: specifies subject’s anonymity difference between

- Subject’s anonymity given the attacker’s observations
- Subject’s anonymity given the attacker’s a priori knowledge only
Unlinkability

- Definition of unlinkability: given two IOIs, from within the system the attacker cannot sufficiently distinguish whether they are related or not.

- Reconsidering anonymity:
  - Anonymity: unlinkability of subject and attribute
  - Consider attribute of “having sent a message $m$”
  - New def. of Anonymity: whether subject is anonymous within the “sender-of-$m$ anonymity set”
Definition of undetectability: from the attacker’s perspective, the attacker cannot sufficiently detect whether a particular IOI exists or not. (Example: steganography)

Unobservability of communication (IOI)

- Two parts
  - Subjects not involved can know nothing about the IOI or subjects
  - Subjects involved can only know about the IOI itself, but nothing about the other subjects (preserves anonymity)

Definition: (a) preserves undetectability of IOI from all uninvolved subjects, (b) preserves anonymity of all subjects in IOI including other participants in the IOI.
Unobservability

Universe

System:
(2) Senders

(1) Communication Network

(3) Recipients

Alice
Bob
Malice
Carol
Accomplice

Unobservability sets

Msg from Alice
Msg from Bob
Msg from Malice

Msg from Carol
Msg from Accomplice
Accountability and anonymity: extremes from each other

Pseudonymity
- Identifier used instead of real identifier
- Can be used for subsets of IOIs and attributes
- Can be used in credentials
- Can be used for: person, role, relationship, role-relationship, transaction
- Fills the gap between accountability and anonymity
What next:

- Hannes Tschofenig, NSN: Privacy and Standards
- Jesse Sowell, MIT: Privacy and Regulation
- Dave Clark, MIT: Privacy and Accountability
- Open discussion