Internet Engineering Task Force
Privacy
Internet Draft
Expires March 2006

Wassim Haddad
Ericsson Research
Erik Nordmark
Sun Microsystems

October 2005

Privacy Terminology
<draft-haddad-alien-privacy-terminology-00>

Status of this Memo

Abstract

This memo introduces the terminology for the main privacy aspects. The prime goal is to avoid situations where different interpretations of the same key privacy aspects result in different requirements when designing specific solutions, thus leading to an unnecessary confusion.

Table of Contents

1. Introduction

Privacy is becoming a key requirement to allow deployment of specific internet services. However, privacy has many aspects, which differ in scope, properties and limitations.

To avoid any possible confusion with regard to the meanings of privacy in some particular scenarios and to differentiate between requirements related to each scenario, privacy aspects have to be well defined before designing any solution. It is the intention of this memo to introduce the terminology for the main aspects of privacy.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [TERM].

3. General Terminology

Item of Interest (IOI)

An Item of Interest (IOI) represents what an attacker is trying to discover, learn, trace and possibly link to other IOI(s), in order to identify its target.
Examples of IOI include a subject, event, action (e.g., send, receive, move, etc), specific type of messages,...

Knowledge

In the field of privacy, knowledge refers to the information available to an attacker about its target. In terms of IOI, knowledge can be described by the probability of one or more IOIs.
We refer to any prior information available to an attacker about a specific target as background knowledge.

4. Privacy

Privacy is a fundamental human right. The most common definition of privacy is the one by Alan Westin: "Pivacy 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".

Privacy is a general term that involves several different aspects. These aspects enable features like hiding the node's address(es) (e.g., MAC and/or IP), name(s) (e.g., DNS), and/or location(s), in addition to hiding specific IOIs. One or more of these features can be obtained during one particular session.

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.

Consequently, neither the mobile node nor its system software

shall support the creation of user-related usage profiles. Such profiles basically comprise of a correlation of time and location of the node's use, as well as the type and details of the transaction performed.

The main privacy aspects are the anonymity, unlinkability,

unobservability and pseudonymity. Note that privacy can even be achieved by disconnectivity, i.e., not being connected to a network.

5. Location Privacy

Location privacy is the ability to prevent other parties from learning one's current and/or past location. In order to get such ability, the concerned (i.e., targeted :) node must conceal any relation between its location and the personal identifiable information.

In our context, location privacy refers normally to the topological location and not the geographic one. The latter is provided by other means (e.g., GPS) than an IPv6 address. But it should be noted that it may be possible sometimes to deduce the geographical location from the topological one.

6. Privacy Aspects

As mentioned above, privacy is a general term, which refers to many different aspects. In the following, we define the main privacy aspects and describe the different relations between them.

6.1. Anonymity

Anonymity is the state of being not uniquely characterized, i.e., identifiable, within a set of subjects (e.g., node, user) called the anonymity set. The set of possible subjects depends on the knowledge of the attacker and may vary over

time. Thus, anonymity is relative with respect to the attacker and is very much context dependent.

In the security field, anonymity is a property of network security. An entity "A" in a set 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 act are performed by "A".

From a user perspective, anonymity ensures that a user may use

a resource or service without disclosing the user's identity.

In wireless networks, anonymity means that neither the mobile node nor its system shall by default expose any information, that allows any conclusions on the owner or current use of the node.

Consequently, in scenarios where a device and/or network identifiers are used (e.g., MAC address, IP address), neither the communication partner nor any outside attacker should be able to disclose any possible link between the respective identifier and the user's identity.

6.2. Unlinkability

Unlinkability of two or more IOIs means that from an attacker's perspective, these IOIs are no more and no less related after his observation than they are related concerning his background knowledge.

For example, two messages (e.g., binding updates) are unlinkable for an attacker if the a-posteriori probability describing his background knowledge that these two messages are sent by the same sender and/or received by the same recipient is the same as the probability imposed by his a-priori knowledge.

From a user perspective, unlinkability ensures that a user may make multiple uses of resources or services without other being able to link these uses together.

6.3. Unobservability

Unobservability is the state of IOIs being indistinguishable from any IOI. This means that messages are not discernable from e.g., random noise. Consequently, unobservability deals with events instead of subjects.

From a user perspective, unobservability ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.

6.4. Relation between Anonymity and Unlinkability

In terms of unlinkability, anonymity can be defined as the unlikability of an IOI and any identifier of a subject. Consequently, unlinkability is a sufficient condition of anonymity but is not a necessary condition.

6.5. Pseudonymity

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 pseudonyms acts were performed by the same entity.

From a user perspective, pseudonymity ensures that a user may use a resource or service without disclosing its user identity, but can still be accountable for that use.

Consequently, a pseudonym is an identifier for a party to a transaction, which is not in the normal course of events, sufficient to associate the transaction with a particular user.

Hence a transaction is pseudonymous in relation to a particular party if the transaction data contains no direct identifier for that party, and can only be related to them in the event that a very specific piece of additional data is associated with it.

For more literature about the privacy terminology content, please refer to [ANON], [ISO99], [PRIVNG], [FREEDOM] and [ANON-PRIV]Ã.

7. Security Considerations

This document presents only terminology. There are no security issues in this document.

8. References

[ANON] A. Pfitzmann et al. "Anonymity, Unobservability, Pseudonymity, and Identity Management - A Proposal for Terminology", Draft v0.23, Aout, 2005.

[ANONPRIV] M. Schmidt, "Subscriptionless Mobile Networking: Anonymity and Privacy Aspects within Personal Area Networks", IEEE WCNC 2002.

[Freedom] A.F. Westin, "Privacy and Freedom", Atheneum Press, New York, USA, 1967.

[ISO99] ISO IS 15408, 1999, http://www.commoncriteria.org/

[LOPRIPEC] A. Beresfold, F. Stajano, "Location Privacy in Pervasive Computing", IEEE Pervasive Computing, 2(1):46-55, 2003 IEEE.

[PRIV-NG] A. Escudero-Pascual, "Privacy in the Next Generation Internet", December 2002.

9. Authors' Addresses

Wassim Haddad
Ericsson Research
8400, Decarie Blvd
Town of Mount Royal
Quebec H4P 2N2
Canada

Phone: +1 514 345 7900
E-Mail: Wassim.Haddad@ericsson.com

Erik Nordmark
Sun Microsystems, Inc
17 Network Circle
Moutain View, CA
USA

Phone: +1 650 786 2921
Fax: +1 650 786 5896
E-Mail: Erik.Nordmark@sun.com

Intellectual Property Statement

any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.
The IETF has been notified of intellectual property rights claimed in regard to some or all of the specification contained in this document. For more information consult the online list of claimed rights.

Disclaimer of Validity

Copyright Statement