

Privacy Authentication – persistent non-identification in Ubiquitous environments

Stephan J. Engberg, Morten B. Harning

Open Business Innovation
Stengaards Alle 33D, 2800 Kgs. Lyngby, Denmark
Stephan.Engberg@obivision.com Morten.harning@obivision.com
www.obivision.com

Abstract. Identity management across Ubiquitous and Telecom environments is suffering from serious privacy problems as both persistent device identifiers and user identifiers lead to high levels of linkability. A new approach to Privacy authentication in wireless environments is proposed turning the IETF Mobile IP proposal for wireless communication into persistent non-identified IP sessions without telecom providers knowing any persistent device or user identifiers. A new Privacy Authentication Unit holding a data component to an Identity Disclosure Process act as an IP-session authenticating agent towards the subscribing telecom provider based on a zero-knowledge authentication process with a wireless device.

Keywords: Privacy Authentication, Session authentication, Pseudonymous, Identity Disclosure, Persistent Non-identification, Zero-knowledge Authentication, Accountability

© All rights reserved - October 2002. This paper covers elements of a patent-pending privacy framework. Latest version available at <http://www.obivision.com/papers/Papers.html>

Introduction

In ubiquitous computing macro (long-distance GSM, UMTS etc.) wireless communication is integrating with micro (local Bluetooth, infrared etc.) wireless communication as part of users general identity end environment management.

Since wireless-transmitting devices in normal circumstances cannot hide their precise location from for instance triangulation or simply closeness to a specific receiving station any persistent device or user id involves problems as they establish linkability in location tracking.

Non-persistent session-only device identifiers can be established using known principles like DHCP where the device request an identifier, randomly generated identifiers or reuse identifiers from some sort of pool etc. These principles are well known and technically easily to transfer to wireless.

Using mix nets or trace-eliminating solution, devices could in theory communicate anonymously or pseudonymous provided they have the necessary computation, secure key-storage and power to do the necessary encryption etc.

However Absolute Anonymous approaches to basic authentication are meet with strong resistance in especial law enforcement and the market adoption of anonymous communication solutions have also proven difficult.

Unsolved problems related to multi-identity management as well as legal and telecom provider requirements for device traceability and accountability make the above approaches to wireless anonymisation possible in theory but far from reality and available. As we move towards ubiquitous computing new privacy authentication solutions are needed.

Especially the macro wireless infrastructure is a privacy hostile environment requiring device-identifiers (Mac-addresses or others) and moving to integrate digital signatures in for instance mobile phones to

provide mobile authentication incorporating both persistent user and device identifiers without any additional privacy protection except light encryption.

In addition the issue of customization of ubiquitous environments add to the privacy problems. Depending on the authentication schemes and identity management, customisation risks implementing an increasing level of highly linkable personal data stored outside the control of users. The customisation issues are potentially more troublesome in microenvironments as significant amount of personal data and preferences are to be shared among devices.

Users are in strong need of portable devices able to do identity management and coordination in both micro and macro environments without sacrificing privacy. For mobile phones, PDAs or other devices used in macro communication to provide a privacy platform for managing ubiquitous computing on a local level the devices and authentication solutions needs to be altered in such a way that devices are not constantly linkable either by persistent device or user identifiers.

In other words - macro environment needs a Privacy Authentication solution that is session-only but still provides enough accountability to make room for eliminating upfront device or user identifiers.

This position paper propose a new approach - Privacy Authentication - to provide pervasive privacy as part of a larger holistic privacy framework aiming to remove the need for identification or device identifiers in wireless infrastructure. All aspects cannot be covered in one paper and this paper concentrates on the basic issues relating to authentication in ubiquitous environments mixing micro and macro communication.

Overview

We want to establish a situation such that a mobile communication device can be turned into the root control device of individual identity management and environment control incorporating maximum levels of privacy. This is within existing environments without assuming public

or infrastructure acceptance of absolute anonymity. We could name such a device a Privacy Authenticating Device (PAD).

The outcome is a setup in which a PAD device can establish an authenticated wireless IP-session with the normal subscription telecom provider (STP) without the STP having any persistent device or user identifier to link one session with a PAD-device to the next and still have traceability in case the PAD-device user is involved in any criminal activity. The subscriber will under normal circumstances remain unidentified and only session traceable.

To achieve this we incorporate two new entities – a Privacy Authenticating Unit (PAU) and a Privacy Accountability data component (PACC).

Sessions related to the same PACC are linkable by the PAU, but the subscriber can use additional PACCs within the same PAU or even additional PAUs to decrease linkability. Reducing linkability depending on identity management and communication management solutions likely but not necessarily lead to at least minor trade-offs of increasing cost or reducing convenience.

The PACC will determine how easily traceability to the real identity of the subscriber is in case of a specific session is investigated. This is in essence a social/political/legal question more than a technical question as desired outcomes can be encoded.

The encoding and the outcome of encoding are discussed in detail in another paper under preparation. For this paper is it relevant to mention two important aspects of the encoding discussion. One is the distinction between traceability of one session of a user vs. linkability between multiple sessions of the same user. Another is that no trusted party is assumed as even courts cannot be assumed as trusted parties in worst-case scenarios.

Interface Standard Environment.

We have in our considerations assumed IETF Mobile IP [1] specifications as the general interface specification. The RFC incorporates Subscription Units and Roaming Units as respectively the normal telecom provider with the subscription and billing entity and any foreign telecom provider through which a subscriber access his Subscription Unit. We will only consider the Subscription Telecom here, but the arguments are extendable to incorporate Roaming Units.

The goal was to operate within these specifications without having to change interface standards except internally in the device and Subscription Telecom. Changes in considerations can be necessary with other standard protocols and it may be impossible in some surroundings.

Privacy Accountability (PACC)

Key to Privacy Authentication is the existence of Privacy Accountability. The various properties of Privacy Accountability including how it could be established are not discussed in this paper even though it is highly relevant.

We assume the existence of a data component incorporating either identifying (a signature, a verified biometrics) or otherwise linking information together with a verified link to the public key of pseudonym. The data component is encrypted using multiple layers in such a way that it is not providing linkability by its existence and only through a series of steps including multiple trusted parts lead to disclosure of identity or other linking information.

One key goal is the ability to accept identity release of a single criminal while at the same time both prevent undetected mass-surveillance and even block it. This is not discussed in detail in this paper.

Relevant for this paper is the consideration that possession of a data component providing such properties is not in itself identifying as identity is not readily accessible nor is it clearly anonymous as linkability

exists. This is somewhere in between anonymous and identified but incorporating the better properties of both.

Privacy Accountability is structurally different from an Identity Escrow setup as in a PKI Certificate Authority as the unit in possession of the data component are only trusted to keep the data component in hiding until the disclosure process - for any reason – is required to initiate.

Privacy Authenticating Device (PAD)

A PAD-device can be any device able to communicate through wireless protocols. It is assumed to be a standard mobile phone, but could be a PDA, a portable computer, a car computer etc. In addition the PAD is incorporating the ability to do multi-identity management, multi-device management and the necessary encryption and communication operations involved. These operations should be controlled in a tamper-resistant environment such as a smart card together with additional protection.

In this paper, we only concentrate on the properties essential for the authentication procedure to work. This include:

- The ability to emulate standard interfaces without revealing a persistent device identifier. If a persistent device identifier is required this is generated, fetched, reused in a crowd in such a way that the protocol works but the device is not persistently identified.
- The ability to carry out a zero-knowledge authentication procedure with a PAU (Privacy Authentication Unit) in order to establish an authenticated IP-session.
- The ability to do any encrypted identity or device management on top of such a session without revealing further information.

The Privacy Authentication protocol

In the following we use the Mobile IP setup and protocol proposal from IETF (2377) as the example. The basic principle is an intermediation protocol requiring collaboration of the intermediated Subscription

Privacy Authentication

Telecom. As such the authentication protocol should easily be adaptable to any protocol as long as both the PAD-device and the Subscription Telecom is using protocols modified accordingly.

In the Mobile IP protocol a mobile device first establish an IP-session with a device identifier authenticates towards a Home IP-address of the Subscribing Telecom using a digital signature stored in the mobile device. The Subscribing Telecom is then acting as a proxy using the Home IP Address as the subscriber specific telephone-number and IP-gateway.

Mobile IP therefore assumes both persistent device and user identifiers. The persistent device identifier has no technical requirement to be globally unique. It could just as well be any randomly generated number unique within the local environment. The real problem is the Home IP Address, which is a globally unique and persistent User Identifier.

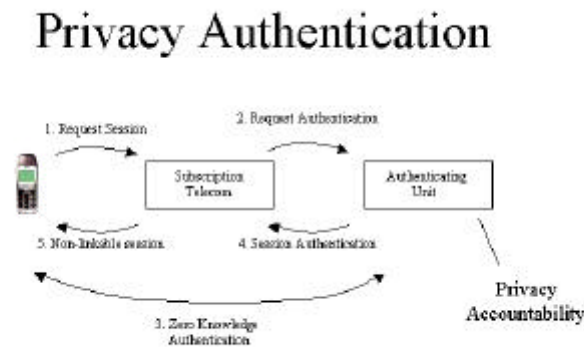


Fig. 1. Privacy Authentication

The authentication protocol is described on a generic level in the enclosed figure 1 with comments below.

1. The PAD-device initiates the request for a session using a session-only device identifier. An IP-session to the Subscription Telecom is established either directly or through a roaming Unit. Instead of providing the IP Home Address of the subscription – it request a new IP Home Address such the Home Address is not providing a persistent user identifier.

2. The Subscription Telecom receives a request for establishing a session together with a reference to the Privacy Authenticating Unit (PAU) able to authenticate the user. The Subscription Telecom establishes an IP-session through the Subscription Telecom to the Privacy Authenticating Unit limited to the authentication process only.
3. The PAD-device carry out a zero-knowledge authentication procedure with the PAU-unit so that the Subscription Telecom cannot infer anything more than one of its subscribers is using this specific PAU-unit. This procedure preferably uses a series of pre-agreed one-time-only identifiers together with a subsequent zero-knowledge authentication with a pseudonym known proving control of the private key of the pseudonym to the PAU-unit.
4. The PAU-unit can store the authentication sequence and thereby establish a trace to a previous stored PACC data component. Upon verification the PAU-unit can reverse-authenticate on behalf of the PAD-device a session identifier only.
5. The Subscribing Telecom now knows the PAU-unit has authenticated the Subscriber and can open the IP-sessions for general use. Payment can be either direct using digital cash, through a pre-paid, digital cash or post-paid solution with the PAU-unit.

Risks

Linkability can be achieved by physical surveillance of the device tracking sessions to the respective PAU-units and getting access to the various PACCs. As physical surveillance includes identification this solution is not protected against constant physical surveillance by law enforcement.

The quality of Privacy also depends on the encoded disclosure process and as the process is based on trusted parties it is vulnerable. The encoding process in itself is of course vulnerable and especially so if all

encoding is under surveillance. A weak disclosure process would too easily disclose identification and thereby remove the difference compared to Identity Escrow providing false sense of protection. A strict process would make disclosure very difficult and reduce the difference compared to absolute anonymity.

The setup is somewhat vulnerable but also resistant to identity theft. First of all because the PAD-device does not contain secrets that cannot be revoked simply by refusing to authenticate at the PAU-unit provided the individual has a backup entry to the PAU-unit.

Having some biometric in the disclosed information is one of the best protections against attempts to create ids in the name of another person. A biometric authentication to the client device can provide be part of both theft protection and voluntary identity theft.

Finally linkability between sessions can be achieved when carrying out a session switch with precise location tracking or long distance between users.

Outcome

With a basic wireless infrastructure transformed into never identified sessions the basic privacy risks of present protocols are significantly reduced. Especially within the passive PKI/CA-setup it is difficult to achieve similar properties.

When comparing this to the actual proposal version for an Anonymity terminology [3] this approach raise the question whether we need a distinction between different categories of pseudonyms, as the need for further identification seems limited. It might even increase privacy compared to a default anonymous approach with negotiation, as many negotiations are likely to result in identifiable information released.

The specific purpose of this proposal is to remove outstanding arguments against designing privacy into infrastructure. The intended goal is to change the existing technology trend towards increasing identification in favour of a trend towards investments, improvement, and matur-

ing of PET technologies by removing the major concerns that block the usage of PET technologies.

Another question is whether the one-dimensional approach to privacy building from anonymity up (for instance the Nymity Slider [2]) is not in reality pushing the development towards upfront identification or identity escrow as best case as the Privacy community is not providing realistic alternatives.

Conclusion

The paper demonstrates that it is possible - within existing interface standards - to change to persistent non-identified session-only wireless communication when accepting the existence of an identity disclosure process.

It is suggested that this persistent non-identified approach is preferable to an identified approach and at the same time provide a trend change incorporating PETs in infrastructure.

References

1. IETF RFC 2977 - <http://www.ietf.org/rfc/rfc2977.txt>
2. Goldberg, Ian. PhD Thesis - <http://www.isaac.cs.berkeley.edu/~iang/thesis.html>
3. Terminology - http://www.koehntopp.de/marit/pub/anon/Anon_Terminology.html