# Secure ubiquitous computing based on entity recognition*

Jean-Marc Seigneur, Stephen Farrell, Christian Damsgaard Jensen,
Distributed Systems Group,
Department of Computer Science,
Trinity College, Dublin 2, Ireland.

***Ubiquitous computing cannot always use traditional enrolment schemes, especially in mobile ad-hoc networks (MANETs) and global computing infrastructures. In this extended abstract, we argue that entity recognition is more general than authentication and that ubiquitous computing environments benefit from the entity recognition approach. Entity recognition schemes do not always require an enrolment phase but rather a process where more or less attention is paid to surrounding entities depending on their estimated importance. Different applications may require different ways to recognise collaborators, so we propose a pluggable recognition module (PRM) as an interesting design approach in this area.***

In ambient intelligence (AmI) environments [6], where ubiquitous computing, ubiquitous communication and intelligent user interfaces are combined, it has been envisaged [1] that real people would have a digital-self acting on their behalf. These digital entities are more likely to be artificial intelligence agents following the real person they are representing – kind of ubiquitous roaming entities. As in real life, digital entities will encounter unknown entities while roaming from place to place. A fundamental question concerns the representation of entities including their naming and subsequent identification as well as their association with real-world principals. We believe that, in this context, it is more beneficial to take an approach based on entity recognition, rather than solely on traditional authentication schemes like PKI or Kerberos [2].

Our expectation is that entities are in general virtually anonymous to the extent that identity conveys little information about likely behaviour. What is important as a prerequisite is not really "Who exactly does this entity represent?" but "Do I recognize this entity as a trustworthy collaborator, whomever it represents?" We assume virtual pseudonymity and therefore we do not require the ability to establish the identity of a given entity in absolute terms, e.g. through globally unique and meaningful X.500 [10] "distinguished names". Instead, we simply require the ability to recognise other entities, e.g. through their name, location, digital signatures or other means. Collaboration amongst virtually anonymous entities is an approach to security in the global computing infrastructure. The Resurrecting Duckling security policy model [5] is an example of entity recognition; ducklings know that their mother is the first entity who sent the imprinting key when they were born. They must be able to recognize when the entity with which they interact is the one who sent the imprinting key, no more. This extended abstract discusses how recognition should be done to meet the requirements for ubiquitous computing environments.

Ubiquitous computing environments imply MANETs but include all other kinds of networks as well. For example, the current IPv4 based, NATed, Internet will most likely provide the foundation of any global computing environment. Many authentication protocols have been developed to verify the identity claimed by a principal. We are currently studying recognition requirements [9] that especially arise in MANETs and ubiquitous computing and which do not arise in more traditional networking contexts.

From the above, adaptability to an entity's capabilities and to legacy authentication solutions is required. Hence we assume an entity recognition module into which different recognition schemes can be plugged. The design of that PRM would be leveraged from other work such as pluggable authentication module (PAM) [4] implemented in Java2 with JAAS [3] amongst others. Auto-configuration, implied by initial collaboration with unknown entities, would be achieved by choosing and/or negotiating the appropriate recognition scheme. Privacy of the to-be-recognized entity must be taken into account during the negotiation, in addition to the security of the recognizing entity.

To us, entities are virtually anonymous: any identifier can work as long as it allows for referencing the entity involved over the required lifespan. This means that the "real" identity in absolute terms is not needed. Therefore recognition intrinsically favours privacy by divorcing the recognition and representational aspects of identity.

The following table describes the current authentication process (AP) and our entity recognition (ER) process.

* This work, still in early stage, is carried out as part of the IST-2001-32486 SECURE project [8].

| Authentication Process (AP) | Entity Recognition (ER) |
|---|---|
| A.1. **Enrolment**: generally involves an administrator or human intervention | |
| A.2. **Triggering**: e.g., someone clicks on a Web link to a resource that requires authentication to be downloaded | E.1. **Triggering** (passive and active sense): mainly triggering (as in A.2), with the idea that the recognizing entity can trigger itself |
| A.3. **Detective work**: the main task is to verify that the principal's claimed identity is the peer's | E.2. **Detective work**: to recognize the entity to-be recognized using the negotiated and available recognition scheme(s) |
| | E.3. **Retention** (optional): "preservation of the after effects of experience and learning that makes recall or recognition possible" [7] |
| A.4. **Action**: the identification is subsequently used in some ways. Actually, the claim of the identity may be done in steps 2 or 3 depending on the authentication solution (loop to A.2) | E.4. **Action** (optional): the outcome of the recognition is subsequently used in some ways (loop to E.1) |

First of all, human intervention in step A.1 goes against the aim of limiting human intervention in AmI environments. ER is better from this point of view.

By self-triggering (step E.1) we mean, for example, an entity recognition scheme that involves the recogniser monitoring the network and selectively carrying out detective work on (some of) the identities that are observed.

There is not an enrolment step at the beginning of the process but it does not mean that no enrolment is done. Actually, in step E.3, if the entity to-be recognized has never been met before, somehow what will be retained is going to be reused the next time this entity will have to be recognized. Depending on the recognition scheme, it should be more or less transparent, so more or less like the enrolment step in A.1.

Step E.4 is optional since it is not required if the entity recognition scheme was triggered externally.

As part of the outcome of any recognition scheme, meta-data should be included to achieve a sufficient level of confidence in the recognition. Knowing this information is available may help developers building auto-configuration and coping with false acceptance and false rejection for schemes which suffer such errors.

A number of different sensing, recognition and retention strategies can be envisaged for entity recognition schemes, e.g., reception of an acknowledgement packet from the wireless network interface provides a trigger that initiates recognition based on the IP address and records the fact that the sender replies to messages (retention). However, specifying such strategies is the subject of ongoing work and beyond the scope of this extended abstract.

We can show that any authentication process can be integrated into an ER scheme (by doing enrolment at step E.3) and can also show that some ER schemes are not authentication scheme and thus that the class of authentication schemes is a proper subset of the class of entity recognition schemes.

So, we should aim to develop a PRM where auto-configuration is present and a large spectrum of recognition schemes can be used.

Entity recognition, as described above, provides a new context in which we can see that some of the developments in authentication systems (e.g. Web self-registration) demonstrate a move away from the more traditional enterprise, administered network, and towards a secure ubiquitous computing environment. We expect that exploring this new context will lead to a variety of interesting approaches for handling network identities which are more suited to the current networking and application requirements.

[1] K. Ducatel, M. Bogdanowicz, F. Scapolo, J. Leitjen, and J.-C. Burgelman, "That's what friends are for. Ambient Intelligence (AmI) and the IS in 2010", in ***the congress of Innovations for an e-Society, Challenges for Technology Assessment Berlin, Deutschland, 17 - 19 Oktober 2001***, 2001, http://www.itas.fzk.de/e-society/preprints/esociety/Ducatel%20et%20al.pdf.

[2] J. Kohl and B. C. Neuman, "The Kerberos Network Authentication Service (Version 5)", Internet Request for Comments RFC-1510, 1993, ftp://ftp.isi.edu/in-notes/rfc1510.txt.

[3] C. Lai, L. Gong, L. Koved, A. Nadalin, and R. Schemers, "User Authentication and Authorization in the Java(TM) Platform", in ***the Proceedings of the 15th Annual Computer Security Application Conference, Phoenix, AZ, December 1999***, 1999, http://java.sun.com/security/jaas/doc/acsac.html.

[4] V. Samar and R. Schemers, "Unified login with PAM", Open Software Foundation, 1995, http://www.opengroup.org/tech/rfc/rfc86.0.html.

[5] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks", in ***Security Protocols, 7th International Workshop Proceedings, Lecture Notes in Computer Science, 1999***, pp. 172-194, B. Christianson, B. Crispo, and M. Roe (Eds.), 1999, http://citeseer.nj.nec.com/stajano99resurrecting.html.

[6] "Philips Ambient Intelligence", Website, http://www.research.philips.com/InformationCenter/Global/FArticleSummary.asp?lNodeId=712.

[7] "Merriam-Webster's Collegiate Dictionary", Website, http://www.m-w.com/.

[8] "Secure Environments for Collaboration among Ubiquitous Roaming Entities", Website, http://www.cs.tcd.ie/Jean-Marc.Seigneur/secure/index.htm.

[9] "Requirements for Recognition in Ubiquitous Computing", Website, draft, http://www.cs.tcd.ie/Jean-Marc.Seigneur/secure/ubiquitouscomputingrecognitionrequirements.htm.

[10] "The Directory: Overview of Concepts, Models and Service", ITU-T Rec. X.500, Information Technology - Open Systems Interconnection, 1993.