Challenges of Identity, Authentication, and Discovery Management in a Ubiquitous environment: The DAIDALOS perspective

James Clarke, Stephen Butler
LAKE Communications
Ireland

Shane Dempsey, Micheal Crotty, Jonathan Brazil
Waterford Institute of Technology
Telecommunications Software & Systems Group
Ireland

Christian Hauser, Martin Neubauer
Institute of Communication Networks and Computer Engineering
University of Stuttgart
Germany

Aleksej Jerman Blazic
SETCCE
Slovenia

Abstract

DAIDALOS, which stands for **D**esigning **A**dvanced **I**nterfaces for the **D**elivery and **A**dministration of **L**ocation independent **O**ptimised personal **S**ervices, is a project within the European Commission's Sixth Framework Information Society Technologies Programme[1]. While the first phase of the project is for 2.5 years, DAIDALOS[2] could potentially have a full duration of ten years if the first phase is carried out successfully. This is because the DAIDALOS project is a new type of project unveiled in the Sixth Framework called an Integrated Project (IP), whose objectives are more forward-looking involving high-risk research with an emphasis on larger projects with longer timeframes than in the previous Framework programmes.

1. DAIDALOS Objectives

The overall objective of DAIDALOS is to develop and demonstrate an open architecture based on a common network protocol (IPv6) to:

- Design, prototype and validate the necessary infrastructure and components for efficient composition and distribution of services over diverse network technologies beyond 3G,
- Integrate complementary network techno-logies to provide pervasive and user-centred access to these services,
- Develop an optimized signalling system for communication and management support in these networks,
- Demonstrate the results of the work through strong focus on user-centred and scenario-based development of technology.

The DAIDALOS consortium is comprised of a mix of telcos, manufacturers, academic and SME participants. The telco members of the consortia include T-Systems, Eurescom, Portugal Telecom, Telenor, Telefonica, ERA Poland, Telecom Italia, France Telecom and OTE of Greece.

The consortium also includes four major telecommunications equipment companies (Lucent, Motorola, Siemens and NEC), and BMW is participating as a major user-related company targeting the problems of future multimedia service distribution to its customers.

The SMEs in the consortium include companies involved in the areas of wired and wireless customer premises equipment (LAKE Communications), data protection and secure communication (HW Communications, United Kingdom, SETCCE, Slovenia), IP communication over broadcast networks

[1] More information on IST can be found at http://www.cordis.lu/ist/
2 More information on Daidalos project can be found at http://www.ist-daidalos.org.

(UDCast, France), service platforms (Agora, Spain), and context services (Comnac Gmbh, Germany).

There is also a strong participation from Academic partners and Research Institutes including the Telecommunications Software & Systems Group (TSSG) at Waterford Institute of Technology, the University of Aachen, University of Stuttgart, Universidad Carlos III de Madrid (UC3M), Fraunhofer FOKUS, among others.

2. Designing Personal Services

DAIDALOS services will be strongly tailored to users' context and preferences. Such information exposes high risks when intercepted by unauthorized party. DAIDALOS initiative is developing a sophisticated framework of identity management, authentication processes and data protection mechanisms to embody strong requirements from international and national legislation for privacy. The DAIDALOS identity and privacy policy management architecture facilitates the pseudonymous use of services both broadcast and unicast while permitting integrated billing and the escrow of identities for law-enforcement purposes.

In addition, DAIDALOS is applying this framework to provide a platform for ubiquitous computing. A key tenet of ubiquitous computing is support for a wide variety of devices and services.

Some of the key challenges that need to be addressed are:

- Protocol heterogeneity. Ideally, the discovery components would have to support only one service discovery protocol in a single networked environment. In reality, however, given the nature of the pervasive systems, several discovery mechanisms are likely to be used on different devices and networks. Given this environment, discovery should facilitate inter-working between a finite set of service discovery, and interoperability protocols. Furthermore, pervasive environments should enable seamless transition between different networked environments while maintaining the same level of service and functionality including data protection.

- Model extensibility. The system should allow for extension of the models used to represent the (enabling and third party) services and devices. Primarily, this will allow the platform to support arbitrary standards for device and service interoperability. This is further extended to support potential new innovative types of services and devices as they emerge.

- Scalability. The discovery components must scale from simple, ad hoc peer-to-peer environment to the level of an enterprise network. For example the system must be capable of being used in large geographically diverse corporate networks to find a suitable printer service and at the same time enable direct file exchange between two user devices in proximity.

- Context-aware discovery. The discovery components should be capable of filtering the results of a discovery request, based on the state and context of the target object. For example, for performance reasons, a PDA may wish to send email via the service, which has the shortest queue of pending messages. Another example would be an urgent business document needs to be printed quickly, which requires discovering the printer that can print greater than 6 pages per minute and has a short queue size i.e. Less than two pending jobs.

- Security and Privacy. How to instil confidence to the users that they are interacting with are genuine providers, and not some shady third party. Conversely, how to ensure users are bona fide, and prevent service theft and fraud. This is further complicated by the requirement for pseudonymous service usage. The ubiquitous nature of the developed applications based on the pervasive systems platform requires close attention to user privacy and security issues. In order to support the user best according to his current context, pervasive systems have to handle a considerable amount of personal data. This requires a sound control by the user regarding retrieval, storage, disclosure and processing of this sensitive data. Intelligent inference of further items of context information from raw (indirect) context data being provided by network of sensors even increases this problem.

3. Building Trust in Pervasive Systems

In the area of privacy and security, trust plays an important role. Pervasive systems are a logical evolution from today's mobile communication systems delivering simple end-to-end services. In complex multi entity environments of personalized services it is mandatory evaluating the trust situation of these systems and to compare it to the situation of future pervasive systems.

Today mobile communication systems assign clear roles to the participating peers. On the one hand, there are untrusted consumers and on the other hand, there are large operators as service providers. Communication services are mostly provided by a single network operator, which may also provide some value added services, e.g., location-based services. This single provider is well known and an abuse of personal user information would cause a significant loss of credibility.

A wide-spread trend in mobile systems is on open philosophy like in the Internet. Beyond publicly available interface specifications, this also means - in its final consequence - that everyone may participate in the system not only as an information consumer but also as a content or service provider. Thus, it can be assumed, in future, there will be many service providers for certain services. This service providers and services themselves could even have a limited lifespan, lasting for a fraction of time. Services may appear and stop to exist; they may be dynamically modified and provided by arbitrary entity. Similar to today, there are many free e-mail providers, and it is very likely in the future, there will be many service providers of context-aware services. This situation can lead to varying or even diminishing trust of users in (service) providers.

Although privacy and security from a user's point of view is crucial regarding acceptance of pervasive systems, security needs of service providers must not be neglected. These needs, e.g., non-repudiation, are often in conflict to the needs of the users, e.g., pseudonymity. Thus, trade-offs have to be found which are accepted by users as well as by service providers. This is called multilateral security.

Following these arguments, the traditional trust model of mobile communication systems, in which the users fully trust their single provider, is no longer suitable for future systems. Thus, new protection mechanisms have to be adopted, which satisfy the security needs of both service providers and users in the global environment of pervasive systems.

4. Privacy Policy Negotiation and Virtual Identities

In DAIDALOS, a consistent security and privacy framework considering multilateral security on different layers will be developed. This framework will be evaluated in close cooperation with other activities (context management, personalization, etc.) in order to balance security/privacy functions and the system's functionality (Figure 1).

For privacy purposes, the link between a user's identity and his personal information, e.g. context information, must be concealed. On the other hand, regarding multilateral security, the users must be accountable for their actions requiring the use of pseudonyms instead of anonymity. Furthermore, there is a changeover from the often used client-server paradigm whereas private users are only clients initiating a communication. In future systems, it must be possible that private users — who are only known by a pseudonym — also provide their own services.

In DAIDALOS infrastructure the set of personal data is controlled by a Security and Privacy Manager, which is acting on behalf of the subject and is controlled by him. Thus, Security and Privacy Manager reflects the right of informational self-determination. As the set of personal data need not to specify all information a user possesses it resembles a restricted view on the user at the recipient. Because this view is controlled and restricted we refer to it as virtual.

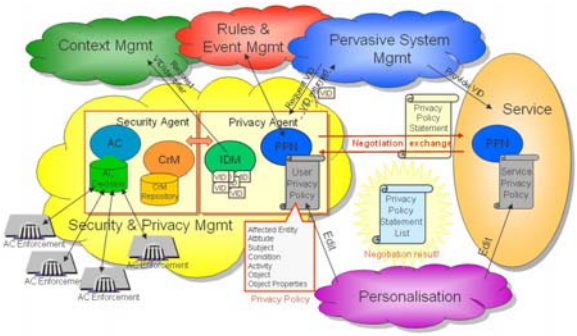

Figure 1: DAIDALOS privacy and security infrastructure.

DAIDALOS privacy concept mainly consists of four building blocks (Figure 1): Privacy Policy Negotiation (PPN), Identity Management (IDM), Credential Management (CrM) and Access Control (AC). Integrated components evaluate general privacy requirements, provide mechanisms for establishing agreements on how to manage user's data, handle user's pseudonyms and delegate and authenticate subject access rights. Main actors (users and services) in heterogeneous environments of pervasive systems use pseudonyms to hide their real identification. Pseudonyms are derived directly from processes taking into consideration subjects' preferences and common privacy information restrictions. At first, a subject privacy policy is negotiated using mechanisms provided by PPN (Negotiation Exchange) – where the negotiation process is defined by personal rules based on rules – with a new service prior to using it. This

policy is the basis for an identity the user chooses, and which the service can then use to interact with the subject and access its data. The identity is generated by IDM on direct basis of policy negotiation results. Moreover, derived identity is used to configure the access rights for the personal context information. Access control is delegated using credentials from CrM and enforced on the site by AC. Credentials present temporary tokens, which usually expire within short periods of time and disclose the purpose and rights (of access).

If each user can only use one pseudonym, it is very likely that his identity will eventually be revealed, as he is disclosing a lot of personal information linked to single pseudonym by using a variety of services during a long period of time. To avoid that, a user can use different pseudonyms. The respectively used pseudonym together with the information disclosed in the context of this pseudonym builds up a view on the user by some part of the system. In the remainder of this paper, we refer to this view as a Virtual Identity (VID), because it is a kind of identity — consisting of a pseudonym as identifier augmented by some attributes — under which the user appears in the system. VID concept is extended using granulation approach for supporting entities of a pervasive system. Disclosure of information exchanged between different system blocks is protected using appropriate encryption mechanisms and key distribution. Personal data therefore remains protected in the domain of functional blocks, while the performance of the overall system is not affected including steps of service accounting.

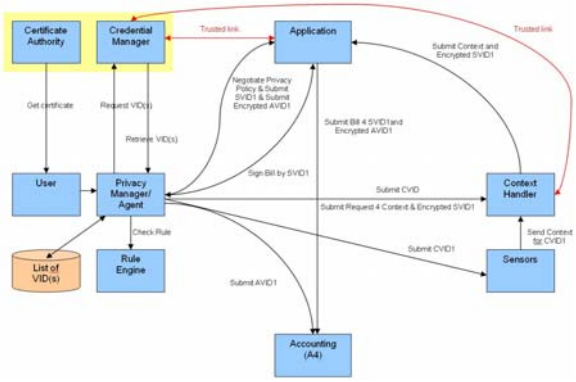

Figure 2: Usage of multiple identifiers in DAIDALOS infrastructure.

A Virtual Identity composes a set of personal data for a specific service. This information is part of the overall user's context, which reflects his current situation, static personal data and preferences. Because Identity Management (IDM) needs not to be aware of the actual values of context information, IDM uses a formal description of the type of context to be disclosed. This context description is part of context ontology. Based on this description the Context Manager – a platform component providing the actual values and the context ontology – creates unique identifiers for each piece of context information (Figure 2). These Context Identifiers (CIDs) are then used in Virtual Identities to reference the real value and to make it accessible to other users and services at all. Furthermore, these Context Identifiers are used to specify the access rights for users and service in a flexible and highly dynamic manner as it is a pre-requisite for pervasive services.

For accountability and charging purposes, a Registration ID (RegID) is defined, which describes the user from his registration. Typically, the registration is done with the provider of Authentication, Authorization, Accounting, Auditing and Charging (A4C), which is comparable with today's Internet service provider. In this registration, it is described which services he can use, how many Virtual Identities he can use and whether he is a premium or a standard user. Further, the account to be charged is specified. These Registration IDs serve multilateral security, because on the one hand they guarantee the service provider that he will get the money for his provided service. On the other hand, based on the logging of service usages in combination with the used RegID, the user can verify (audit) the electronic receipts. Thus non-repudiation requirements of both, users and service providers, will be met.

5. Conclusions

Privacy protection based on the VID approach has a crucial problem: The VIDs of a user must not be linked by any service, or at least the user — or some entity acting on behalf of the user — is aware of any linking leading to privacy risks. A link of two VIDs can be based on unique application data appearing in the context of both VIDs, identical behavioural patterns traced and related to VIDs but also on unique data disclosed by the communication system. As long as disclosure of unique information by the communication system is not prevented, any application solution is ineffective regarding the VID approach. Moreover, the VID approach has to be supported from the very first stage in the design and onwards. Beneath the communication system, including the authentication and authorization system, the VIDs of a user must not be linked whilst being capable to nevertheless guarantee legal enforcement and charging of pseudonymous users.

DAIDALOS presents sophisticated system approach that will tie different technologies and innovations together in a seamless way automatically with security, privacy, cost, quality of service and efficiency all factored into the process of pervasive systems. Concerning privacy protection in pervasive environments, it is very important to consider holistic solutions taking into account the application as well as the network. DAIDALOS is a unique chance for doing so.

ABOUT THE AUTHORING ORGANISATIONS

LAKE Communications, an indigenous Irish SME company with over 100 employees, is a leading supplier of wireless & wired communication products. LAKE Communications are unique in the DAIDALOS consortium as a European SME Customer Premises Equipment provider of wired and wireless converged voice and data switches for the SOHO and COHO markets.

Waterford Institute of Technology is a publicly funded third level institute in the South East region of Ireland with 6,000 full-time and 4,000 part-time students enrolled on a broad spectrum of courses. The Telecommunications Software & Systems Group (TSSG) is the largest research group in WIT with staff and students working on a range of nationally funded and EU-funded research programmes and projects. Within DAIDALOS, Waterford Institute of Technology is concerned with the implications of operating multiple service providers and devices in dynamic service discovery.

University of Stuttgart, Institute of Communication Networks and Computer Engineering - The Institute of Communication Networks and Computer Engineering is leading the security and privacy activities in the pervasive systems part of DAIDALOS. Moreover, it is coordinating the overall security and privacy activities across the whole project.

Security Technology Competence Centre – SETCCE is a Jozef Stefan Institute spin-off research and development organisation, based in Slovenia, with the major focus on security in information system. Organization is actively participating in European based research programs and standardization bodies. SETCCE is a major partner for security and privacy in the pervasive systems part of the DAIDALOS project.

ACKNOWLEDGEMENTS

The project participants wish to express their appreciation of the co-funding and support provided by the European Commission DG XIII-B during the course of this project.