A Framework for Systemic Privacy Protection in a Pervasive Platform

JAN POREKAR, KAJETAN DOLINAR
SETCCE - Security Technology Competence Centre
Jamova 39, SI-1000, Ljubljana
SLOVENIA

BORKA JERMAN-BLAŽIČ
E5 – Laboratory for Open Systems and Networks, Institute Jozef Stefan
Jamova 39, SI-1000, Ljubljana
SLOVENIA

Abstract: - Pervasive environments pose extended security and privacy threads if compared with traditional systems. Many privacy enhancing and trust management techniques have been studied in recent years. In the paper we present the DAIDALOS IST FP6 Integrated Project[1] approach to enabling privacy in pervasive information systems. In DAIDALOS privacy enabling is approached in a systemic and manageable fashion. To enable privacy we use a fusion of techniques that bring together various technologies and research disciplines from the field of privacy engineering: automatic agent negotiation, identity management, and trust management. As a solution to the complex problems imposed by pervasive environments we propose privacy enabling architecture of the DAIDALOS platform. Privacy enabling solutions are in service to user communication and exploit the system feedback loop where experience gained in one communication cycle is fed back via updating of the reputation models. Entities involved in communication first have to negotiate privacy agreements based upon trustworthiness, afterwards appropriate virtual identities are created or selected and in the last phase privacy agreements violations are considered and trustworthiness of the communicating entities are lowered.

Key-Words: - Privacy, Pervasive Systems, Trust, Identity Management, Negotiation, Virtual Identity

1 Introduction

Pervasive or ubiquitous systems have been a subject of intense conceptual research in recent years [2][3]. The number of electronic devices connected to the network is expected to rise exponentially and will eventually outnumber humans living on the planet. Mobile devices such as laptops or personal digital assistants and cellular phones will increase in number, standard household appliances and machines will be connected to the network and new intelligent appliances and biosensors will emerge. The vision of pervasive systems is to integrate all those different devices in a world where computer technology will disappear from everyday lives and will become invisible. A world where computer systems will seamlessly adapt to user context and will help user achieve task by inferring one's intent. A world where a digital representation of user, user's data and his digital workplace will constantly be copied across various network nodes in order to follow user in his real world geographical movements.

Realization of such a vision calls for a broad and systematic approach where elements can operate in a coherent and stable framework; the elements are there, however the full integration has yet to be tamed. A typical setup for a pervasive system includes the following elements (in terms of functional requirements):

- *sensors*: omnipresence of cameras, microphones, movement detectors, etc. and tracking devices, e.g. RFID, mobile phone;
- *smart items*: processing units and sensors embedded into objects of everyday life (household appliances, traffic utilities, etc.) making possible for the objects to react on their surroundings;
- *smart spaces*: physical spaces equipped with sensors and smart items;
- *integrated networking & mobility*: integration of various network technologies for support to interoperability of wired, wireless, and ad hoc networking;
- *context*: digitally represented smart space along with additional parameters attributed to

persons or physical objects (as for example temperature, humidity, blood pressure, etc.) most often in function relative to user;

- *personalization*: computer aided automation for human-computer interaction;
- *intelligence*: a logic for management of resources and processes of smart spaces to make possible context awareness and personalization in a consistent and seamless way.

The main objective of DAIDALOS project is not to develop a pervasive system but to setup a framework where the elements of pervasive system can serve to provide a service oriented platform with emphasis on network operability. The framework should open an area of business opportunities for smaller or bigger operators so that they can exploit their network facilities in context of service oriented business models. Nevertheless, in the values of the business models the project has incentive to keep pace with emerging paradigm of pervasiveness; however, as emphasis is made on framework and networking and less on peripherals, the aspects of integration (the last three bullets) prevail over material installations (the first three bullets) taking also into account features of service oriented platform. The functional blocks of DAIDALOS pervasive platform are the following:

- service discovery, composition and management
- context management
- personalization & learning
- runtime environment with support for deployment of services, session management, event mechanisms, rules mechanisms, and security in general
- privacy protection

The networking functionality is taken as granted on pervasive level and provided by lower work packages.

A very important part of DAIDALOS pervasive platform is protection of privacy: the service oriented platform should prove reliable and trustworthy about personal information processing in order to justify the business models. As the pervasiveness implies complex installations with heavy data aggregation capabilities and powerful data processing the task to protect shared personal identifying information is far from trivial. (Compare for example [4].) No less than a very comprehensive and systemic approach can be enough to tame the tremendous impetus of pervasive systems for consuming personal identifying information. We will speak of the approach on this subject in the following chapters.

2 Systemic approach to enabling privacy in DAIDALOS

Security and privacy are being used as a constitutional part of the DAIDALOS platform. A couple of years back in distributed computing the security and privacy enabling mechanisms were in many cases added at a later stage, although lately it is becoming a standard to plan security from the first phases of system design. In designing pervasive platforms it is vital to plan privacy and security infrastructure from scratch as a fundamental part of the system and tune it all the time during the system development.

In DAIDALOS privacy protection is approached in a systemic and manageable fashion. When designing the system we have mimicked some of the natural mechanisms of relationships between principals (i.e. individuals, companies – natural or legal persons) as they appear in human society. There are three fundamental mechanisms which conduct relationships in any fair and efficient society of independent principals:

1. freedom of choice and self determination
2. trust and reputation
3. demand and offer

The first mechanism *allows* principal to find the most appropriate position in the society – to contribute and benefit to the highest and best possible degree. The second serves an instrument for principals to define the best possible associations (dependencies and collaborations) to other principals to be able to fully exercise all the benefits from the first point. The third means an establishment of dependency between individuals: principals depend on supply (which can finally be brought down to supply of material goods) and demand makes a principal a necessary member of society and worth of supply (support) by others; the third mechanism empowers the second for making reputation (and consequently trust) an important values, as mutual dependency makes possible sanctioning of members by levers of demand and supply.

The three mechanisms define a model for institution of privacy protection in DAIDALOS. The crucial good is privacy. The demand (supply) for (of) services is balanced by demand (supply) for (of) privacy: the higher the respect for privacy, the more interesting the service provider and the higher the demand for the service. The providers depend on the demand and individuals want supply – the deciding parameter is respect for privacy. The respect for privacy is being in demand, or in supply. The reputation and trust are implicitly important and the self determination and freedom of choice is provided by possibility for principals to have power over the degree and destination of personal identification information disclosure.

The three systems are used for the three mechanisms. The control over disclosure of personal identifying information is achieved by instrument of *virtual identities*: the whole set of personal identifying information available about a principal is organized around pseudonyms and each cluster is identified with one pseudonym, the cluster being a virtual identity. By using different virtual identities principal can engage in different transactions and (with some care) other principals not knowing the two are the same person. The trust and reputation systems are used to setup a web of trust where reputation is used in negotiating supply and demand of personal identifying information (negotiating the virtual identity), the negotiation being done by automatic agent systems.

3 Privacy Enhancing Cycle

Each principal is represented towards other principals exclusively and only by VID; true identity of a principal is never entirely transparent. In DAIDALOS each principal can be at the same time provider of a service or consumer (user) of a service; if a principal is interested in some service another principal provides then the first principal is user and the second one provider. The user is initiator of negotiation and the provider has to expect possible initiation accepts from users.

The following are the phases of setting up and running privacy protected communication between two unknown principals (user and provider):

1. acquiring reputation about an unknown principal from trusted peers;
2. negotiating disclosure of personal identifying information towards the principal (negotiating virtual identity);
3. selecting an appropriate virtual identity for the principal (evaluating threats for linkage of the new virtual identity to already issued virtual identities or other associated), setting up access control rights, and providing it to the principal;
4. running access control and recording logs on access to personal identifying information by the principal;
5. supervising usage of personal identifying information by the principal;
6. updating reputation of the principal after experience obtained upon supervision.

This cycle enables all three mechanisms written about in chapter 2. The reputation defines success of negotiation phase: if the reputation is low the negotiation will result in refusing the disclosure of personal identifying information (which means usage of the service by user, or if provider was unsatisfied, provisioning of service to user), which has direct consequences on demand and supply of the service. If on the other hand the negotiation was successful the user and provider setup and sign an agreement and exchange the virtual identities defined by negotiation. The relationship is established: both are known to each other by the virtual identities they have exchanged.

If during usage in phases 4 and 5 the principal was recognized to violate the negotiated agreement about handling personal identifying information then the reputation of the principal is updated and the following negotiations by whichever principal might result in lower demand, which gives us a sort of automatic sanctioning mechanism.

4 Daidalos Privacy Protecting Architecture

In order to make possible the cycle described in chapter 3 we use a conglomerate of many different approaches that constitute a privacy enhancing lifecycle. Four main architectural blocks have been defined as pillars of privacy enabling Daidalos architecture. These are:

- Identity Manager (see [5])
- Negotiation Manager (see [6])
- Trust Manager (see [7])
- Profile Manager

Functions of each of the blocks are as follows:

Identity Management

- creates and maintains virtual identities;
- maintains a database on history
  - of disclosures of personal identifying information by virtual identities,
  - and of usage of all existing virtual identities;
- estimates the threats behind disclosures by virtual identities according to the history
  - to prevent linking different virtual identities by society,
  - and other unintended disclosures.

Negotiation Management

- is involved in privacy policy definition languages and parsing
  - syntactical structures,
  - and semantic relation to personal identifying information;

- performs sane negotiation protocol encapsulated in an agent software
  - where statements of privacy policy are exchanged between peers,
  - but only statements relevant for current matter under discussion,
  - and possible is also anonymous credentials exchange;
- does flexible and optimal synchronization between negotiation techniques, as for example
  - pure anonymous credentials exchange,
  - or exchange of semantically enriched information using ontologies;
- performs complex decision making algorithms
  - to evaluate peer negotiation statements against local privacy policy,
  - and to make decisions, which are then encapsulated in response negotiation statements;
- provides framework for easy and scalable deployment of negotiation agents to negotiating parties
  - including anonymizers for indirect negotiation to protect customer's addresses,
  - including listeners for accepting negotiation requests.

Trust management

- determines trustworthiness of principals by combining several different techniques:
  - non-centralized reputation models,
  - certificates issued by trusted 3rd parties,
  - previous experience with communication;
- manages trustworthiness estimation strategies;
- enforces privacy through updating reputation models:
  - provides interfaces to agreement violation detection services,
  - update experience,
  - update opinions / reputation on entities involved in communication.

Personal Profile Manager

- stores, maintains and shares private data from
  - private information repository based on VIDs,
  - controlled by purpose, credential and privacy agreement based access control.

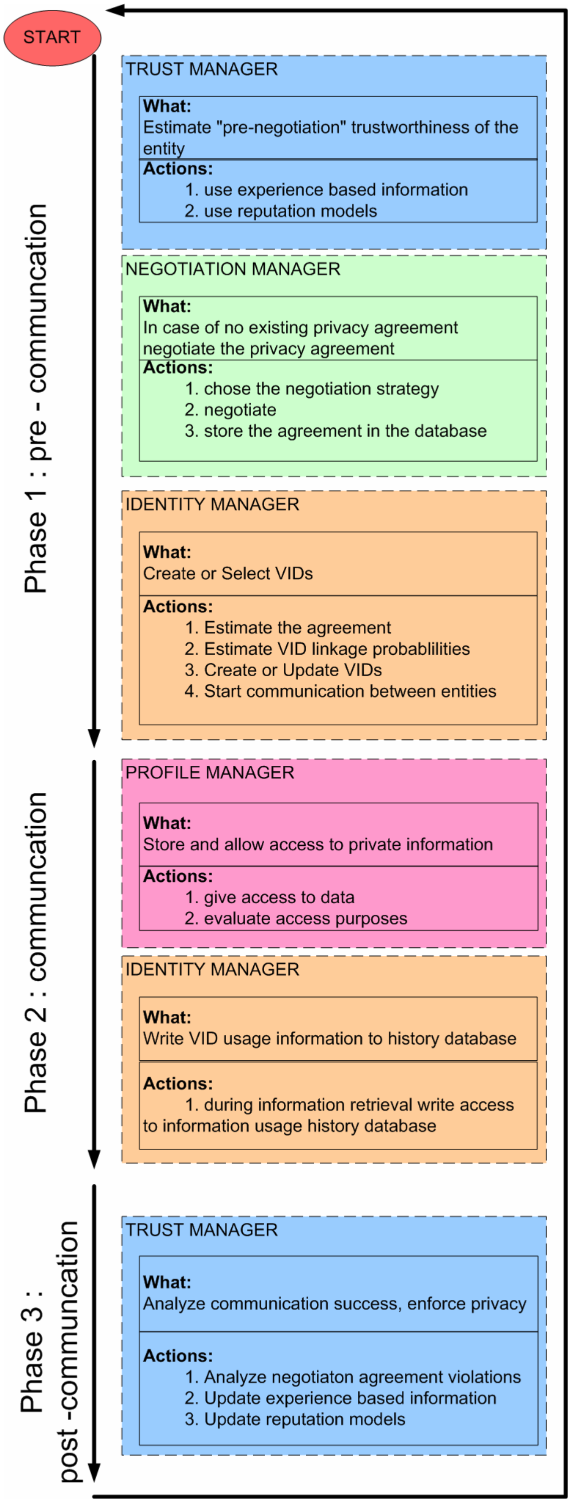
START
Phase 1 : pre - communcation
TRUST MANAGER
What:
Estimate "pre-negotiation" trustworthiness of the entity
Actions:
1. use experience based information
2. use reputation models
NEGOTIATION MANAGER
What:
In case of no existing privacy agreement negotiate the privacy agreement
Actions:
1. chose the negotiation strategy
2. negotiate
3. store the agreement in the database
IDENTITY MANAGER
What:
Create or Select VIDs
Actions:
1. Estimate the agreement
2. Estimate VID linkage probablilities
3. Create or Update VIDs
4. Start communication between entities
Phase 2 : communcation
PROFILE MANAGER
What:
Store and allow access to private information
Actions:
1. give access to data
2. evaluate access purposes
IDENTITY MANAGER
What:
Write VID usage information to history database
Actions:
1. during information retrieval write access to information usage history database
Phase 3 : post -communcation
TRUST MANAGER
What:
Analyze communication success, enforce privacy
Actions:
1. Analyze negotiaton agreement violations
2. Update experience based information
3. Update reputation models

Fig1. Privacy enabling lifecycle schema: 3 phases of Daidalos communication process, with explanations of processes and architectural components involved.

5 Conclusion

The presented framework for systemic protection of privacy in pervasive environments is a subject of ongoing research and development in FP6 IST DAIDALOS project. Certain parts of the framework still deserve deeper understanding and more attention as for example which reputation models are the best for performance, reliability and security, and how to make possible for supervision over personal identifying information misuse after the virtual identities were already issued and disclosed and the access to data was already granted. Another parallel to human society helps us solve this issue in the first idea: special services can be provided in DAIDALOS service platform, so called *(privacy policy negotiation) agreement violation detection services*, which are provided by special principals, for example cyber police. The research in this area is still being done.

Disclaimer

The work described in this paper is based on results of IST FP6 Integrated Project DAIDALOS. DAIDALOS receives research funding from the European Community's Sixth Framework Programme. Apart from this, the European Commission has no responsibility for the content of this paper. The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

References:

[1] C. Kuhmünch, *D412, Revised Architecture for Daidalos Pervasive Systems*, DAIDALOS Consortium, 2005 March.

[2] D. Saha, A. Mukherjee, Pervasive computing: A Paradigm for 21st century, *IEEE Computer Society*, 2003 March.

[3] M. Satyanarayanan, Pervasive computing: Vision and Challenges, *IEEE Personal Communications, IEEE Computer Society*, 2001 August.

[4] M. Langeheinrich, Privacy by Design – Principles of Privacy Aware Ubiquitous Systems, *UBICOMP 2001*, LNCS 2201, pp 273 291.

[5] Jan Porekar, Kajetan Dolinar, Identity management and privacy issues in DAIDALOS pervasive environment, *Proceedings of 15th Wireles World Research Forum Meting*, 2005.

[6] Kajetan Dolinar, Jan Porekar, Aleksej Jerman-Blažič, Tomaž Klobučar, Pervasive systems: enhancing trust negotiation with privacy support, *Proceedings of International Workshop on Research Challenges in Security and Privacy for Mobile and Wireless Networks (WSPWN06): National Science Foundation*, 2006. p. 1-10.

[7] Audun Jøsang, Roslan Ismail, Colin Boyd, A Survey of Trust and Reputation Systems for Online Service Provision, *Decision Support Systems*, 00 (2006), p.000-000.