Security and privacy in a pervasive world – The Daidalos approach

James Clarke
Waterford Institute of Technology
jclarke@tssg.org

Christian Hauser
hauser@ikr.uni-stuttgart.de
Martin Neubauer
neubauer@ikr.uni-stuttgart.de
Institute of Communication Networks and Computer Engineering, University of Stuttgart

Daidalos is a European project funded under the Sixth Framework Programme, which aims to integrate a range of heterogeneous networks and to develop pervasive systems on top of them to provide the user with transparent access to personalised communication and information services. Security and privacy are key to the development of such a system. This article addresses some major questions on how to build trust and confidence in pervasive systems where many entities play different roles, mostly for some limited amount of time, and where a significant amount of personal data travel through the network.

Daidalos aims at a platform to allow third party providers to easily deploy pervasive services. As an example of a pervasive service, imagine that you are walking along, watching a video on a handheld device. You enter a room with a large public display, and the video is automatically switched to it, which transparently charges you a couple of cyber-cents. However, this simple example raises a number of important questions. How does the system know that you are entering the room and that you want to use a large display whenever available? How does it know your charging account? How does it know whether you are authorised to use the large display and that the use does not reveal any sensitive data?

The dynamic nature of pervasive systems

Questions like this raise a crucial issue of pervasive systems – privacy and security. It is obvious that such systems will have access to confidential personal information in order to adapt according to the user's personal situation. For achieving privacy, users must be aware of how and where personal data are processed and used. Furthermore, users must be confident that they are interacting with genuine providers.

The dynamic nature of pervasive systems makes these processes even more complicated. While the user is on the move, there will be new services appearing in the vicinity of the user. Moreover, the actual network a user is associated with changes quite often. In addition, it is a widely acknowledged fact that future telecommunication systems will be opened to many providers – network, service and content providers. Thus, a user will frequently be confronted with new providers and will have to be authenticated to each of them. Today, trust relationships are static and security settings require significant effort to configure. In a dynamic pervasive system with mobile users – acting also as providers – this is no longer appropriate. As one goal of pervasiveness is to minimise the user's interaction necessary to control the system, Daidalos strives for automation of these processes as far as practicable.

Virtual Identity

For this, a consistent security and privacy framework based on multilateral security is being developed. For achieving privacy protection, the link between a user's identity and his/her personal information must be concealed. However, users must be accountable for their actions. This necessitates the use of pseudonyms rather than anonymity. In Daidalos, we refer to this pseudonym together with the information disclosed in the context of it as a Virtual Identity (VID). A user can have multiple VIDs. These VIDs are controlled by a software component named Privacy Agent, which acts on behalf of and is controlled by the user, implementing the right of informational self-determination.

When a service is first encountered, a privacy policy must be negotiated bilaterally with the service prior to the use. This privacy policy is the basis for a VID of user's choice, which the service can then use to interact with him/her and access his/her data. Based on the negotiated privacy policy and the chosen VID, the access rights to personal context information are automatically configured. These three building blocks – privacy policy negotiation, identity management and access control to context information – take the burden of understanding the most critical privacy impacts induced by pervasiveness. Moreover, they are taking the necessary configurations away from the user and thus support pervasiveness.

Challenges of the VID approachThere are a number of complex issues that Daidalos is tackling with the VID approach including the protection of the user's VIDs between services, or at least the notification of the user of any VID linking leading to privacy risks. The VID approach has to be supported from the very first stage in design and onwards. Beneath the communication system – including the authentication and authorisation – the VIDs of a user must not be linked whilst being capable of nevertheless guaranteeing legal enforcement and charging of pseudonymous users.

Another challenge is the effect of the VID approach on the personalisation and user preferences of the pervasive system, which need a substantial effort to build up knowledge about the user's wishes. Compartmentalising the profile into separate VIDs makes it more difficult to identify preferences. Furthermore, if a preference is identified for one VID, it cannot automatically be transferred to any other VID for the same user. This scenario could be confusing to a user who in general will not keep track of which preferences have been identified for which VIDs.

Conclusions

Overall, Daidalos presents a sophisticated system approach that will tie different technologies and innovations together in a seamless way with security, privacy, cost, quality of service and efficiency factored into the process. Concerning privacy protection in pervasive environments, it is very important to consider holistic solutions taking into account the application as well as the network, which can be done in Daidalos due to the shared competence of the partners in all those areas. Note, that this article can only address one part of the complete Daidalos security and privacy architecture. More details about this part can be found in our paper presented at the Eurescom Summit 2005 [1].

Daidalos is also participating within the Security and Dependability Task Force (www.securitytaskforce.org) set up within the SecurIST project (www.ist-securist.org) in helping to frame the strategic roadmap for Security and dependability in Framework Programme 7. The Security Taskforce’s goal is to provide Europe with a clear European level view of the strategic opportunities, strengths, weakness, and threats in the area of Security and Dependability. It will identify priorities for Europe and mechanisms to effectively focus efforts on those priorities, identifying instruments for delivering on those priorities and a coherent time frame for delivery.

Further information about EU project Daidalos is available at www.ist-daidalos.org

References

[1] J. Clarke, S. Butler, C. Hauser, M. Neubauer, P. Robertson, I. Orazem, A. Jerman Blazic, H. Williams, Y. Yang: “Security and Privacy in a Pervasive World”, EURESCOM Summit 2005, Ubiquitous Services and Applications - Exploiting the Potential, Conference Proceedings, 27-29 April 2005, Heidelberg, Germany, VDE Verlag, Berlin, Offenbach (ISBN 3-8007-2891-5), pp. 315-322