FIDIS

Future of Identity in the Information Society

Title:	D14.4: Workshop on "From Data Economy to Secure Logging as a Step towards Transparency"
Author:	Sven Wohlgemuth (ALU-FR)
Editor:	Sven Wohlgemuth (ALU-FR)
Reviewers:	Patrick McKelvy (SIRRIX)
	Els Soenens (VUB)
Identifier:	D14.4
Type:	[Report]
Version:	1.0
Date:	Wednesday, 20 February 2008
Status:	[FINAL]
Class:	[Public]
File:	fidis_wp14_d14.4_Workshop_From_Data_Economy_to_Secure_Logging_as_a_Step_towards_Transparency_FINAL.doc

Summary

This workshop was the kick-off meeting for the WP14 work on privacy evidences as an instrument for enforcing privacy policies after the disclosure of personal data. It aimed at coordinating the work on the deliverables D14.5 and D14.6 and to present the corresponding contributions of their participants.

This workshop was held on September 11th, 2007, at the FIDIS 2nd Research Event in Athens, Greece. The agenda, presentations and minutes are available on the internal FIDIS pages of WP14.

Copyright Notice:

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Institut de recherche criminelle de la Gendarmerie Nationale	France
19. Netherlands Forensic Institute	Netherlands
20. Virtual Identity and Privacy Research Center	Switzerland
21. Europäisches Microsoft Innovations Center GmbH	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

Versions

Version	*Date*	*Description (Editor)*
0.1	11.09.2007	• Initial release (Sven Wohlgemuth, ALU-FR)
0.2	19.12.2007	• Version for the internal FIDIS review (Sven Wohlgemuth, ALU-FR)
1.0	20.02.2008	• Revised report according to the comments of the internal FIDIS review (Sven Wohlgemuth, ALU-FR)

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
1 Executive Summary	Sven Wohlgemuth (ALU-FR)
2 Workshop on "From Data Economy to Secure Logging as a Step towards Transparency"	Sven Wohlgemuth (ALU-FR)
Annex 1: Participants	Sven Wohlgemuth (ALU-FR)

Table of Contents

1 Executive Summary

Privacy in Ambient Intelligence assumes users trust in service providers. Personal as well as context data is collected by sensors, cameras and RFID readers, e.g., in the METRO Extra-Future Store. The use of loyalty cards maps collected data to users and transforms context data to personal data. Users are neither able to decide on the access of personal data nor to verify the collection and use of personal data, since they are not aware of every collection. Current privacy-enhancing technologies focus on the collection of personal data but not on the usage of personal data.

The identification of requirements for mechanisms for the enforcement of privacy policies and the verification of their enforcement regarding the collection and processing of personal data is the objective of WP14. Privacy evidences, to be used in case of dispute between users and service providers, are proposed on this workshop as a step towards the enforcement of privacy policies. A precondition for privacy evidences is the logging of service provider activities concerning the collection and use of personal data.

This workshop has shown that such log data has to be authentic, i.e., it must faithfully reflect reality and not allow parallel realities. Since log data consists of personal data, e.g. the IP address of user's personal device, the log data itself is personal in nature and must therefore be kept confidential.

The requirements for secure logging will be presented by the WP14 deliverable D14.6 "From Regulating Access Control on Personal Data to Transparency by Secure Logging".

2 Workshop on "From Data Economy to Secure Logging as a Step towards Transparency"

2.1 Objectives

This workshop was the kick-off meeting for WP14 work on privacy evidences as an instrument for ex post enforcement of privacy policies. It aimed to coordinate the work on deliverables D14.5 "Experimental Study on Profiling in Business Processes" and D14.6 "From Regulating Access Control on Personal Data to Transparency by Secure Logging" by presenting the corresponding contributions of their participants.

2.2 Agenda and Slides

The workshop was held during the 2nd FIDIS Research Event on September 11th, 2007 in Athens. The following presentations have been given:

Tuesday, September 11th, 2007	
09h00-09h20	Sven Wohlgemuth (ALU-FR): From Data Economy to Secure Logging as a Step towards Transparency Ambient Intelligence environments lead to a collection of contextual and personal data for personalised services which is unaware for their users. This stems from the deployment of RFID tags of goods, sensors and cameras observing the users in, e.g., a shop such as the "Future Store" of the METRO AG. Therefore, users are not able to decide on the disclosure of their data. Either they do not participate in such environments or they have to trust service providers to use their personal data according to the privacy policy. The concept of usage control, with obligations as rules, for a desired use of personal data is an approach allowing users to control the use of their personal data. It has been shown that current privacy mechanisms support access control over personal data but not its use. Privacy policy languages, such as P3P or EPAL, support obligations but do not offer the possibility for users to verify whether obligations have been enforced. The aim is to identify requirements for a mechanism which generates privacy evidences in order to offer users proof that they can trust service providers. Log data are the foundation for privacy evidences, since they should reflect the enforcement of obligations and identify the misuse of personal data should it occur. This talk presented the requirement of the authenticity of log data and an approach toward generating them using a secure logging protocol.
09h20-09h40	Eleni Kosta (ICRI): Legal Requirements of Secure Logging From the view of legislation, log data is also personal data and, as such, must be protected. This talk focuses on the two main legal requirements of the "right to access log data for users" and the "right to be informed". This also means that there should be integrity control over logging activities, the collected data must be authentic and the logging activities

	must be accountable. Timestamps and trust services such as the eSignature Directive are proposed. The talk further introduces privacy principles and security criteria which have to be fulfilled by a secure logging system in order to pass legal evaluation.
09h40-10h00	Martin Meints (ICPP): International Security Standards and Logging This talk introduces the definition of logging according to the ISO/IEC 270xx series of security standards as well as CobiT and ISO/IEC 15408. It concludes that third party (e.g. user) interests are not covered, though protocol data from enterprises is increasingly used by the state. It points out that if logging mechanisms according to these standards are used, the administrator of the system has unlimited access to the data logged.
10h00-10h20	Stefan Berthold (TUD): Technical Aspects of Secure Logging – Requirements, Approaches, Limitations This talk focuses on the semantic interpretation of log data and its interpretable presentation to users lacking security knowledge. Stefan Berthold presented the concept of lattices for semantic interpretation and the of town maps for presentation.
10h20-10h30	Rani Husseiki (SIRRIX): D14.5 Experimental Study on Profiling in Business Processes This talk introduces the experimental study according to its goals (detecting the misuse of personal data) and approach. Students apply for various loyalty programs and make minor mistakes in their names. For example, if an address is sold to an advertising company, it is possible to determine who sold the personal data. The results will be summarized by a survey.
10h30-11h00	Coffee break
11h00-12h30	Coordination of D14.5, D14.6 and proposals for the 5th work plan The results of the discussion include a sketch of the table of contents of D14.6, its schedule and an agreement upon a publication for the 5th work plan to summarize the results from WP14. Concerning the 5th work plan, a study of the means by which users can verify the logging of data and only view their own details, was proposed and discussed. The proposal needs refinement before presenting it for the 5th work plan.

The slides are available at http://internal.fidis.net/interactive/filemanager/files/workpackages/?dir=wp14%2Fworkshop_d14.4.

2.3 Results

The contributions of the participants in WP14 have been presented, discussed and fixed. Regarding D14.5, a method for the experimental study has been presented and discussed with regard to the participants in the study (students), the kind of personal data to be given to the

service providers (modified e-mail addresses and names) and the point at which usage of this data becomes a violation of privacy in a legal sense. Regarding the latter, it was agreed that legal advice from FIDIS partners should be pursued.

Regarding D14.6, a sketch of the table of contents and the schedule was discussed and fixed by the contributors. Legal requirements will be taken into account regarding whether log data can be used as evidence of the misuse of personal data. Secure logging is the foundation for preserving privacy in logging while generating privacy evidence. A result of the discussion is that log data is also personal in nature and should therefore be kept confidential.

2.4 Further Steps

Concerning D14.5, the field study will start in November 2007.

Concerning D14.6, the scenario and trust model for privacy are the starting points of this deliverable and will be written by ALU-FR as an orientation for: the identification of legal (ICRI) and technical requirements (TUD, ALU-FR), the presentation of related work on logging in general (ICPP) and secure logging (ALU-FR), the identification of additional security mechanisms (TUD) and the outlook (TUD, ALU-FR).

Annex 1: Participants

The participants of the workshop are listed in the following table:

Contr. No.	Organisation	Surname	First name
1	ICSS	Andronikou	Vassiliki
2	TU Dresden	Berthold	Stefan
3	ICRI	Coudert	Fanny
4	VIP	Dubuis	Eric
5	ICRI	Dumortier	Joseph
6	NFI	Edelman	Gerda
7	SIRRIX	Husseiki	Rani
8	ISRI	Kollanyi	Bence
9	TU Dresden	Köpsell	Stefan
10	ICRI	Kosta	Eleni
11	KU	Martucci	Leonardo
12	MU	Matyas	Vashek
13	ICPP	Meints	Martin
14	ICRI	van Alsenoy	Brendan
15	VaF	Vyskoc	Jozef
16	ALU-FR	Wohlgemuth	Sven