Massimo Felici (Ed.)

Communications in Computer and Information Science 182

Cyber Security and Privacy

Trust in the Digital World and
Cyber Security and Privacy EU Forum 2013
Brussels, Belgium, April 2013
Revised Selected Papers

Springer

CSP forum

Communications
in Computer and Information Science 182

For further volumes:
http://www.springer.com/series/7899

Massimo Felici (Ed.)

Cyber Security and Privacy

Trust in the Digital World and
Cyber Security and Privacy EU Forum 2013
Brussels, Belgium, April 18–19, 2013
Revised Selected Papers

Springer

Editor
Massimo Felici
Hewlett-Packard Laboratories
Security and Cloud Lab
Long Down Avenue
Bristol BS34 8QZ
United Kingdom

ISSN 1865-0929 ISSN 1865-0937 (electronic)
ISBN 978-3-642-41204-2 ISBN 978-3-642-41205-9 (eBook)
DOI 10.1007/978-3-642-41205-9
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2013951507

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Foreword by SecCord

Security and Trust Coordination and Enhanced Collaboration[1] (SecCord) is a project funded under the EU's Seventh Framework Programme for Research (FP7). It is a coordination and support action that brings together researchers with the aim of enhancing collaboration, increasing impact of results, improving effectiveness and identifying direction for future research in trustworthy information and communication technology (ICT).

The focus of SecCord is to increase the influence of the trust and security (T&S) research community in the EU. To boost their influence, the research projects supported by the framework programme need to work together within its context, rather than act as singular entities. They can contribute to the larger programme where collaboration and cooperation are critical to enriching and raising the awareness and impact of their research activities. The need for such collaboration will grow as time goes on as greater effectiveness and pay-back are sought, with better structures and support for clustering of T&S projects.

SecCord is exploring ways to bring the researchers together by developing and enhancing project clusters and other collaboration activities already in place in the trust and security research space, by providing a programme of opportunities for currently active and newly funded projects to engage in fruitful debate, developing and sharing state-of-the-art ideas and knowhow and identifying further issues and openings to be explored. Membership of the cluster community will be extended to other projects and groups with T&S needs or dependencies, particularly in areas concerned with health, legal, social and economic research and also to parallel national T&S initiatives.

The goal of SecCord is to provide the coordination and services for EU T&S research to realise this collaboration through five inter-related objectives:

1. **Support for enhanced collaborative networking:** building on the current collaborations between the T&S projects, evolving the clustering activities, gathering of state-of-the-art ideas and knowledge and extending membership to other projects and initiatives with T&S needs.
2. **Analysis of results and coordination of research impact:** conducting a detailed analysis of the work of the projects, demonstrating the dividends, outputs and benefits resulting from the investment in T&S research and providing evidence of valuable and meaningful results and potential impact.
3. **Awareness and dissemination of research results:** providing greater visibility of T&S research programme through a high-profile annual conference and a T&S research web repository that provides a central focus and exchange for T&S

[1] http://www.seccord.eu/

research information and links; the goal is that these become a recognisable brand; visibility and outreach will be extended by building on an already established community of interests to include relationships with industry and T&S initiatives of member states.

4. **Research-to-industry impact:** providing leverage to the potential and impact of T&S project results by maintaining a catalogue and showcase of results, and by interpreting and matching them against use-cases of current and foreseen market needs covering a wide spectrum of social considerations—legal, economic and personal.
5. **Identify T&S strategic directions:** providing context for the impact and visibility of the research programme—a strategic outlook of the emerging and developing T&S issues, challenges, requirements and priorities, with attention being given to legal, social and economic as well as technical concerns.

These proceedings collect contributions from the Annual T&S conference, Cyber Security and Privacy EU Forum[2] (CSP EU FORUM 2013), organised in cooperation with the trust and security unit of DG CONNECT. The aim is to establish the Cyber Security and Privacy EU Forum as the main trust and security EU research-to-industry dissemination channel. Alongside the CSP 2013, the SecCord project has established an Advisory Focus Group (AFG) of academic and industrial experts in trust, security and privacy for ICT. Its co-location with the CSP EU FORUM supported the discussion of relevant emerging research issues or topics. The aim of the forum is also to avoid fragmentation of similar efforts, to enhance collaboration, to increase research impact and to improve effectiveness in identifying and elaborating research priorities. The CSP EU FORUM therefore is a means to support discussions and to gather feedback on research priorities. Such discussions and feedback will inform future European research agenda in trustworthy ICT. CSP EU FORUM 2013 was organised in collaboration with the European Association for e-Identity and Security (EEMA) and Trust in Digital Life (TDL), and was hosted by the European Commission in Brussels during April 18th–19th, 2013.

August 2013 Paul Malone

[2] http://www.cspforum.eu/

Preface

Many thanks for taking the time to contribute to the *Trust in the Digital World and Cyber Security and Privacy EU Forum* event which took place in Brussels during April 18–19, 2013. The conference programme consisted of fifteen different tracks involving a variety of presentations and panel discussions covering the key challenges and strategies available to effectively manage employee, citizen, and corporate trust. The conference provided an opportunity for those in business, public sector, research and government who are involved in the policy, security, systems, and processes surrounding trust.

This two-day conference organised by EEMA, TDL and CSP EU FORUM, hosted by DG CONNECT of the European Commission and in partnership with the SecCord project, invited presenters, panellists and exhibitors to contribute to this collection of selected papers. Two types of papers were solicited to be published in the post-proceedings of the conference:

- Practical Experience Reports and Tools presenting in-depth description of practitioner experiences, case studies and tools
- Research Papers presenting recent original research results providing new insights to the community.

Papers submitted were peer-reviewed by (at least three) programme committee members and experts. The peer-review process provided authors with valuable feedback in order to improve their papers. The selected papers grouped in thematic parts of these proceedings capture just a snapshot of the two-day conference, which provided an opportunity to present and debate on-going cyber security and privacy research and development in Europe. These proceedings intend to inform researchers, practitioners and policy-makers about research developments and technological opportunities for innovation in cyber security and privacy.

I would like to thank all people who made the publication of these proceedings possible, in particular the authors, the Programme Committee members and reviewers, the conference organisers and the supporting organisations.

August 2013 Massimo Felici

Organization

Organising Committee

Frances Cleary	TSSG, Waterford Institute of Technology, Ireland
Paul Malone	TSSG, Waterford Institute of Technology, Ireland
Michele Bezzi	SAP, France
Massimo Felici	Hewlett-Packard, United Kingdom
Fabio Massacci	University of Trento, Italy
Tom Curran	TSSG, Waterford Institute of Technology, Ireland

Programme Committee and Reviewers

Julio Angulo	Sweden
Claudio A. Ardagna	Italy
Karin Bernsmed	Norway
Michele Bezzi	France
Shahriar Bijani	United Kingdom
Marco Casassa Mont	United Kingdom
Stéphane Cauchie	Spain
Antonio Celorio	United Kingdom
Jim Clarke	Ireland
Tom Curran	Ireland
Ernesto Damini	Italy
Argen de Landgraaf	The Netherlands
Francesco Di Cerbo	France
Zeta Dooly	Ireland
Massimo Felici	United Kingdom
Olga Gadyatskaya	Italy
Bushra Hasnain	United Kingdom
Sven Herpig	United Kingdom
Keith Howker	Ireland
Martin Gilje Jaatun	Norway
Fernando Kraus	Spain
Juan Lorenzo Del Castillo	United Kingdom
Paul Malone	Ireland
Fabio Massacci	Italy
David Núñez	Spain
Federica Paci	Italy
Nick Papanikolaou	United Kingdom

Wolter Pieters	The Netherlands
Henrik Plate	France
Thomas Quillinan	The Netherlands
Sathya Rao	Switzerland
Christoph Reich	Germany
Thomas Ruebsamen	Germany
Carsten Rust	Germany
Suksant Sae Lor	United Kingdom
Stuart Short	France
Yannis Stamatiou	Greece
Tim Storer	United Kingdom
Mark-Alexander Sujan	United Kingdom
Vasilis Tountopoulos	Greece
Luca Viganò	Italy
Nick Wainwright	United Kingdom
Markus Wehner	Germany
Harald Zwingelberg	Germany

Trust in the Digital World
and
Cyber Security & Privacy EU Forum

Hosted by
DG CONNECT

Brussels, Belgium,18th-19thApril 2013

Organized by

Contents

Security and Privacy Technology

Security and Privacy Policy

Cloud Computing

Towards Trustworthiness Assurance in the Cloud

Francesco Di Cerbo[2(✉)], Pascal Bisson[1], Alan Hartman[3], Sebastien Keller[4], Per Håkon Meland[5], Micha Moffie[3], Nazila Gol Mohammadi[6], Sachar Paulus[7], and Stuart Short[2]

[1] THALES Services SAS, Paris, France
pascal.bisson@thalesgroup.com
[2] SAP Product Security Research, Mougins, France
{francesco.di.cerbo, stuart.short}@sap.com
[3] IBM, Haifa, Israel
{hartman, moffie}@il.ibm.com
[4] THALES Communications and Security, Paris, France
sebastien.keller@thalesgroup.com
[5] Stiftelsen SINTEF, Oslo, Norway
per.h.meland@sintef.no
[6] Paluno, University of Duisburg-Essen, Essen, Germany
nazila.golmohammadi@paluno.uni-due.de
[7] FH-Brandenburg, Brandenburg, Germany
paulus@fh-brandenburg.de

Abstract. Cloud- and service-oriented computing paradigms are intrinopaque to their users, as they cannot inspect providers' implementations, and important concerns about aspects like security, compliance, dependability can arise. Therefore, users have to make trust decisions with respect to software providers, with the hope that there will not be any detrimental consequences. To contrast this situation, the paper proposes a framework to define, assess, monitor and make explicit the elements of a service that render it trustworthy. This paper relies on a number of recent scientific contributions, and aims at supporting informed decisions on obscure service implementations by machine-understandable statements about their objective (trustworthiness) characteristics. Such statements would innovate upon many aspects of service operations, from discovery to composition, deployment and monitoring. To demonstrate this, the paper presents a concept for a Trustworthy Service Marketplace.

1 Introduction

Embracing the Cloud implies to demand to a third party the operation of services needed for a certain business application. This means to lose the complete control on a part of the business process execution, to achieve a flexibility and a simplification of maintenance operations. On the other hand, such a situation presents at least a number of concerns. Especially due to the intrinsic lack of control implied by the cloud model. Security [1] and other aspects like (data) privacy, performance and correctness may be difficult to assess beforehand, for

M. Felici (Ed.): CSP EU FORUM 2013, CCIS 182, pp. 3–15, 2013.
DOI: 10.1007/978-3-642-41205-9_1,

instance during an evaluation of different services. This lack of assurance with respect to a service's characteristics is one of the reasons why cloud offerings are not being exploited to their fullest extent [2] in critical domains like healthcare, financial, pharmaceutical and so on.

This proposal aims at defining new means for stating a service's characteristics, in a machine-understandable way. Such descriptions, verified by a third party, would then be used to enhance existing service-related operations, such as discovery, provisioning and monitoring. In particular, relying on recent contributions towards the definition of a model for analysing objectively a software/service in terms of its "*trustworthiness*" [3,4], we propose an extension for the Digital Security Certificate [5] concept. This enhanced certificate would contain also measurable evidences for each claim, therefore we refer to our extension as a "trustworthiness" certificate (DTwC). This can then be used for monitoring a service's execution, to gather up-to-date information to complement/verify what was stated in certificates, thereby, for instance, triggering corrective actions in case of detected issues.

The application of this framework would bring innovations with respect to many existing cloud/service-related operations. In particular, in this paper we present a concept for a next-generation service marketplace. Therefore, it will be possible to create more sophisticated support tools, that allow fine-grained matching of user requirements with available offerings, thereby exploiting the new assurance information conveyed by the DTwC.

The paper is structured as follows: Section 2 presents the model for defining a service's trustworthiness aspects, while Sect. 3 illustrates the different approaches to measure them. Section 4 depicts the ongoing effort to define the DTwC, while Sect. 5 outlines the means to monitor/manage services at run time. Lastly, the aforementioned concepts are applied to a service marketplace use case (in Sect. 6), and Sect. 7 concludes the paper.

2 Trustworthiness and Its Attributes

Trustworthiness is a broad-spectrum term with notions including reliability, security, performance, and user experience as parts of trustworthiness [6]. It has been defined as assurance that the system will perform as expected [7]. Li et al. defined trustworthiness of software as worthy of being trusted to fulfil requirements which may be needed for a particular software component, application or system [8]. We consider *trustworthiness* concept as "outcome oriented", where trustworthiness is the probability that the system will successfully meet all of the trust requirements or trust concerns of an end-user.

Trustworthiness of a system is a major factor in its acceptance by organizations and end-users. Trustworthiness is an important quality, which needs to be fostered and engineered to the system while under development. Though, trustworthiness can be interpreted differently, through different acceptance criteria based on priority and requirements of different users and organisations.

Trustworthiness may be evaluated with respect to different targets like, the confidentiality of sensitive information, the integrity of valuable information, the availability of critical data, the response time or the accuracy of outputs.

Therefore, what contributes to the trustworthiness of a system will depend on the domain, context and eye of the beholder. For instance, while trustworthiness in healthcare may emphasize safety and privacy attributes, trustworthiness in high performance computing is more an indicator of the system's Quality of Service (QoS) guarantees. Related literature mostly studies trustworthiness from a security perspective while assuming that single properties (certification, certain technologies or methodologies) of services lead to trustworthiness. Compared to this approach, we reasonably assume that such a one-dimensional approach is insufficient to capture all the factors that contribute to a system's trustworthiness and instead we consider a multitude of attributes. We have therefore identified a pool of attributes that can work as indicators of the overall trustworthiness.

Trustworthiness attributes influence different moments of the software life-cycle, from software design and implementation, to deployment and execution, up to its end-of-life phase. However, some attributes can be measured only at software execution time, while others belong specifically to the development process, or to the end-of-life management, like for instance the privacy preservation of sensitive information at software termination.

As a consequence, we speculate that by selecting a relevant set of attributes in the early development life-cycle of the system, it is possible to design it in a way so that there will be mechanisms to ensure, evaluate and monitor trustworthiness. We call this *trustworthiness-by-design* (TwByD), and the idea is that trustworthiness must be considered in all development phases and built into the core of the system rather than bolted on as an afterthought. TwByD is a collection of reusable development process building blocks that can be added to existing software engineering methodologies.

These building blocks consist of method descriptions, for instance guidelines, patterns and check-lists that will ensure that the right mechanisms are put in place to ensure trustworthiness. The mechanisms contributing to trustworthiness can be implemented in different ways and sometimes the designer will have to balance the trade-offs between somewhat competing trustworthiness attributes. In such cases, the designer can perform a cost-benefit analysis in order to determine whether the cost incurred (effort) from increasing a particular trustworthiness attribute would be economically justified (result in increased revenues).

We have defined trustworthiness attribute as a property of the system that indicates its ability to prevent potential threats from becoming active, i.e. a resilience assurance that it will not produce an unacceptable outcome. Table 1 gives an overview of a pool of trustworthiness attributes, which has been organized into a set of categories, e.g. security, compatibility and dependability. The attributes in this pool are further detailed by Gol Mohammadi et al. [3].

Table 1. Trustworthiness attributes from [3]

Trustworthiness attribute category					
Security	Compatibility	Data related quality	Dependability	Performance	Usability
Attributes					
Accountability	Openness	Data Integrity	Accuracy	Throughput	Satisfaction
Auditability	Reusability	Data reliability	Availability	Response time	Learnability
Traceability		Data validity	Maintainability		Effectiveness
Confidentiality		Data timeliness	Failure tolerance	Efficiency of use	
Integrity			Reliability		
Safety			Scalability		
Non-repudiation			Flexibility/ robustness		
Trustworthiness attribute category					
Compliance	Cost	Configuration related quality	Complexity	Correctness	
Attributes					
		Stability	Composability		
		Completeness			

3 Trustworthiness Metrics and Evidences

As defined in the previous section, multiple stakeholders can have different ideas on a software's trustworthiness. Therefore, there is a need for a structured and acknowledged model for describing trustworthiness attributes, as well as having at one's disposal a set of acknowledged methods, mechanisms and means (later on referred to as measures or metrics) for measuring the previously defined trustworthiness indicators, so that their evaluation can produce tangible results of the trustworthiness characteristics of a software. We call such results the trustworthiness evidence.

There are a number of types of evidences that can be used for demonstrating trustworthiness. In this paper, we will concentrate on the following types of evidences for trustworthiness:

1. Measures for defined trustworthiness attributes of the to-be-developed software/service/application,
2. Measures for the successful application of development practices that have a positive impact on the trustworthiness of the to-be-developed software/service/application,
3. Measures for the application of software patterns that help achieve trustworthiness of the to-be-developed software/service/application,
4. Re-use of software components that have already been subject to a trustworthiness evaluation.

We will detail our approach for each of these elements in the rest of this section.

3.1 Measures for Defined Trustworthiness Attributes

As presented in Table 1, Gol Mohammadi et al. [3] collect a set of software attributes that contribute to the trustworthiness of the software to be developed. This represents a set of attributes that in some sense describe generic non-functional requirements for any software to fulfil certain trustworthiness expectations.

Of course, each of these generic non-functional requirements needs to be detailed during the requirements engineering activities to specify the exact level and expected quality of the attribute. One way of detailing such a requirement engineering step is to define a metric for each trustworthiness attribute for the software in question. For example, the attribute "Openness" might be specified in the percentage of interfaces that are adhering to standards that are accepted on an industry-wide basis.

The development of metrics for different attributes yields various levels of complexity. For some attributes, the development of metrics might be easy and straightforward - and maybe even relatively generic for any type of software (such as the example of Openness), whereas for others, the to-be-developed metric is very specific for the software in question (such as, for example, Confidentiality). Therefore, we cannot deliver a complete common set of metrics that apply for every software. Rather it is necessary to define a process for the identification of metrics in the requirements engineering phase.

A generic way of developing metrics is the so-called "Goal-Question-Metric" approach. It has been defined by Basili and Rombach in 1988 [9]. It describes a generic approach to develop metrics in the software development area. For each to-be-achieved Goal (i.e. the different trustworthiness attributes of the software), a set of Questions is identified that helps identifying what supports achieving the Goal and subsequently Metrics that measure the gradual fulfilment of the Goal (or sub-goals thereof). An important success factor for these metrics to be helpful in due course of the development process (independently of using agile or more traditional models) is that the metric must be able to be applied during the development process itself, i.e. at different stages of the software development.

Yet it seems very unlikely that requirements engineers will develop individual metrics for each and every trustworthiness attribute for each software they aim to develop, consequently, it is our aim to simplify this process by preparing a set of questions for each trustworthiness attribute with corresponding potential metrics, or parametrized metrics that only need to be specified in more detail - eventually maybe also using plug-ins for existing requirements engineering tools. This is subject to ongoing research.

3.2 Measures for the Successful Application of Development Practices

Besides measuring the outcome of a development project, it is also very helpful to measure the capabilities and practices that support the goal of developing trustworthy software. Bishr et al. [4] have analysed existing development models together with best practices for trustworthy development. It turns out that none of the models investigated actually fully assures the development of trustworthy software on its own today. Consequently, individual activities - herein called "(trustworthy) development practices" must be identified that help towards developing trustworthy software. These are, e.g.:

- Threat Modelling
- Trustworthiness criteria acceptance test case development
- Training and education of software engineers
- Application of "trustworthy software principles"
- Formal modelling of trustworthiness attributes

The set of development practices needs to be further investigated, e.g. by "distilling" these activities from the development models analysed in [4] and by widening/adapting the scope for those models that focus on "security" rather than on "trustworthiness". This is subject to ongoing research.

The application/completion of the development practices, once identified, can be measured using classical process-driven software metrics. Examples are: percentage of software components subject to threat modelling, percentage of high/medium risks identified in threat modelling that are addressed with corresponding measures, percentage of software engineers trained/certified using specific "trustworthy development" courses, percentage of software components covered by formal trustworthiness attributes modelling etc.

3.3 Measures for the Application of Trustworthy Software Patterns

A commonly used approach in industrial software development is to use so-called software patterns. In many cases, even if a functional or non-functional requirement is identical to previous situations, software cannot be re-used for a number of practical reasons, such as e.g. different code base, different language, different project structure and so on. But since the requirement is always the same, the same (and industry-accepted, and/or scientifically proven) solution will/should apply. Such software patterns are commonly used in many places, such as for searching, indexing, or session management. Software patterns may also be used for trustworthiness related requirements, and there are a number of already available security-related software patterns that could be adapted/completed to fulfil the trustworthiness attribute requirements. Such patterns are, for example:

- Input Encoding and Output Sanitization
- Secure Communications
- Federated Authentication

A good source for security patterns is [10] or [11]. The development/adaptation to trustworthiness patterns is subject to ongoing research.

Metrics related to trustworthiness patterns still need to be investigated, first ideas are related to measuring the coverage of the pattern in the software project, the percentage of requirements addressed using proven/established and accepted patterns vs. individual solutions, or the quality of the implementation of the patterns.

Given the relatively good usability of the pattern approach, both for certification as well as for formal modelling, though, we expect this area of activity to be of great importance for the development of trustworthy software in the future.

3.4 Re-use of Software Components

Another popular industrial practice in industrial software development is software reuse. Since the adoptions of so-called components-of-the-shelf (COTS) from Component Software Engineering [12], the availability of *units of reuse* that can be integrated in third-party applications is a reality that finds application also in service-oriented and cloud computing.

In particular, the (black-box) re-use of publicly available components could be seen as an evidence of the application's trustworthiness, or a means for its enhancement. The main reasons are that, firstly, the adoption in a software's architecture of a component with a good reputation or acknowledged trustworthiness mitigates some possible concerns about a part of the software implementation. Secondly, if a component was already evaluated (e.g. by a Common Criteria certification process), it could be possible to build up on this previous knowledge for demonstrate the trustworthiness of a part of the application. Otherwise, a dedicated (and possibly costly) evaluation activity should take place to give visibility to that part of the application trustworthiness features.

However, a number of points must be addressed, in order to measure to which extent trustworthy components contribute to an application's trustworthiness. For instance, considerations could be made regarding the integration of components into the software architecture or about its information flows, possibly taking into account aspects like component granularity. Therefore, the definition of metrics related to re-use of software components is subject of future research.

4 The Digital Trustworthiness Certificate

Once a software is developed and implemented with a certain TwByD methodology, and/or measured with respect to its trustworthiness aspects, all its trustworthiness claims and evidences need to be represented in a consistent, usable and convenient way. To this extent, and looking at experiences like the Digital Security Certificate [5], we are developing a concept for a Digital Trustworthiness Certificate (DTwC). The concept consists of a machine-understandable digital

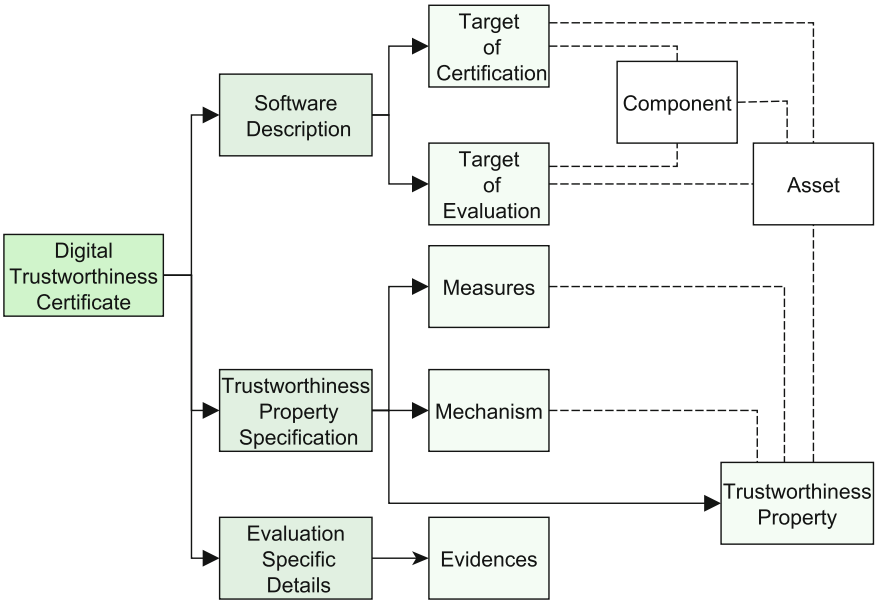

Fig. 1. Initial conceptual model for a Digital Trustworthiness Certificate.

artefact that conveys different trustworthiness information, like attributes, metric interpretation and evidences about a software. It would also contain conditions and prerequisites under which a software can operate as stated by the certificate. In particular, the machine understandability of the artefact will permit its usage in machine-driven scenarios like software (especially service) discovery, provisioning, monitoring and so on. The correctness of the certificate will be ensured by a specific life-cycle model, that will be designed; intuitively, it could follow approaches like Common Criteria [13].

The structure of the Digital Trustworthiness Certificate would comprise three main elements (see Fig. 1).

Firstly, a *software description*, which depicts a general architecture for the software, as well as an identification of the relevant assets, like for instance input parameters; this description would contain similar contents as the software description in Common Criteria. In contrast to it, however, an element of novelty is represented by an explicit determination of the software components that are evaluated, among those as part of a software being certified. This choice is necessary to ensure machine understandability to the description, and to allow modularity, e.g. with respect to composition of a certified component into a software architecture. So, the software description will be captured by a section called "Target of Certification" (TOC); another section will determine which parts of the TOC were evaluated as part of the certification issuing activities, and this is called the " Target of Evaluation" (TOE).

Secondly, *trustworthiness property specification*, that would detail:

1. the trustworthiness features (related to attributes previously defined), with a syntax that would enable the identification of components or assets affected;
2. the mechanisms with which the trustworthiness features are achieved;
3. the corrective measures (*controls*) that reinforce the trustworthiness properties, and on which components/assets they apply.

Finally, it would include a *evaluation-specific* section that contains evaluation-collected evidences that support the trustworthiness property specification. The evidences might come from design-time or run-time assessments. Evidences could be collected by means of metrics as defined in Sect. 3. Importantly, this section would also describe how the evidences support trustworthiness properties: we plan to describe here concretely that an evidence E supports trustworthiness property P, and the assumptions or conditions under which E was chosen, among possibly existing alternatives.

5 Trustworthiness Monitoring

Dynamic runtime monitoring, assessment and management of services enables users to extend their trust decisions into runtime and adjust to the changing landscape of cloud capabilities, customer requirements and online threats. Runtime management of trustworthiness consists of the three main tasks shown in Fig. 2.

The system is an autonomic control loop where measurements are taken on the system, analysed for threats, and if necessary, appropriate plans are chosen and executed to mitigate the threats. The approach taken, based on Mape-K

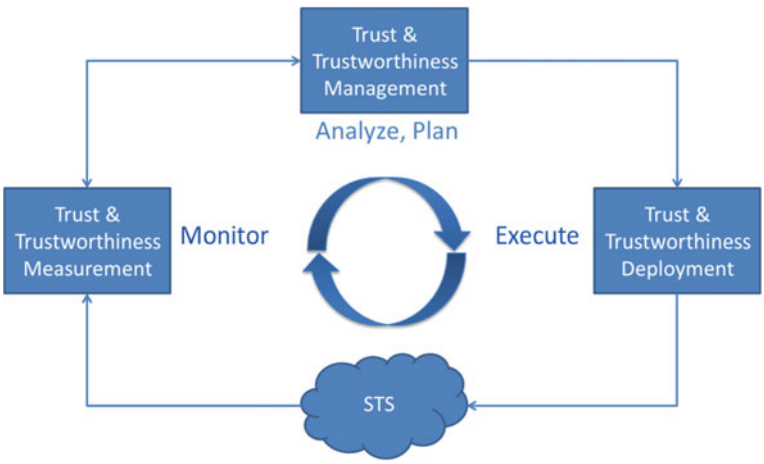

Fig. 2. Runtime management of Trustworthiness for a Software or Socio-Technical System (referred as STS), including its actors.

autonomic control loop architecture [14], manages itself and dynamically adapts to change in accordance with business plans, policies and objectives. The main task of the measurement component is to produce metric values to measure attributes (such as reliability, average response time etc.). It does so by processing simple properties and events that can be directly measured on the system. For example, system properties can include system uptime, response time and events may include system crash. The management component is responsible for analysing the attributes and metrics provided by the measurement component. This component chooses the best plan to execute based on predefined business plans, policies and objectives. The plan is then sent to the deployment component which executes the plan on the system. For example, allocating additional resources from the cloud, using a different service, etc. The management system is configured by the user and includes business plans, policies and objectives. These include mitigation actions that can be applied as well as triggers for their execution. The user may also configure specific properties and events to monitor at runtime as well as specific attributes and metrics to compute. The user can also provide the system with a certificate containing machine-understandable statements about the service's objective trustworthiness elements. Using the certificate the runtime system will be able to:

1. Measure properties and listen to events that are defined in the certificate.
2. Compute metrics (based on those properties and events) and relate to attributes defined in the certificate.
3. Execute predefined actions/tests in order to collect and compute specified metrics. Note that tests can only be executed if some testing environment is given and that executing tests on live system may have an impact on the deployed system.
4. Validate expected metric values of attribute to those dynamically measured. It is necessary for the system to be able to compare the actual runtime deployment to the certification/testing environment and accommodate the expected results to the actual deployed system and environment.
5. Provide a dynamic evaluation containing results and values for attributes that were measured at runtime. The evaluation will include attributes metrics and values measured over time and will specify the dynamic environment in which the service was deployed and evaluated.

The system must be able to identify statements related to a specific service or application and distinguish them from runtime environment. For example, the system will be able to distinguish a crash that is due to the service itself or due to the cloud environment. The resulting runtime output can be consumed by the marketplace in following Sect. 6. For instance, once the marketplace has consumed several runtime evaluations it can present consolidated results, that could provide a dynamic view about how the trustworthiness characteristics of a service varies over time.

6 Use Case: The Trustworthy Service Marketplace

A usage scenario for the described trustworthiness framework is represented by the Trustworthy Software Marketplace (TWM). The availability of machine-understandable trustworthiness information, captured by the DTwC, enables the design of innovative operations that take into account the trustworthiness properties of marketplace offerings. Therefore, TWM would include enhanced service discovery operations, based on functional and non-functional aspects of offerings. In particular, TWM users can understand which non-functional characteristics (trustworthiness properties) are part of an offering, and where and how they are implemented: this information comes from statements, as well as from evidences of the presence/implementation of these characteristics that are part of the DTwC.

One of the planned TWM functionalities would permit users to specify their (trustworthiness) requirements in offering discovery operations, in order to understand which offerings match their functional and non-functional needs. This functionality, called Decision Support System, opens to the possibility to express user-specified prescriptions for offerings (similarly to Common Criteria Protection Profile[1]) to be used as part of the discovery process, for instance to model domain-specific requirements.

Moreover, other advanced services can be designed, relying also on the privileged role of TWM in connecting users, software providers and "deployment actors"(i.e., cloud providers for service offerings, or mobile platform owners for mobile apps). The TWM could instruct a secure (trustworthy) deploying of a selected offering, in its operational scenario: as an example, considering web service offerings, the deployment target in this case would be a cloud service provider.

However, an offering's trustworthiness properties might require specific conditions to be met, for instance in terms of dependencies availability. For this reason, another under-design TWM functionality would manage securely offering dependencies, thus to ensure that the trustworthiness of an offering does not get invalidated by a wrong fulfilment of dependencies; this functionality complements with the secure deployment previously described.

7 Conclusions

The importance of providing assurances for cloud-based solutions is an essential element in convincing businesses to move from traditional structures and benefit from operating in this manner. This paper has outlined an approach that seeks to overcome the complexity of satisfying user's requirements (and consequently alleviating potential disruption) and expectations. By providing means for business services to communicate information on functional and non-functional aspects

[1] see for examples http://www.commoncriteriaportal.org/pps/

of their offerings the end-users decision making process are facilitated and compliant solutions can be discovered (and composed) and deployed in a secure manner.

This approach develops a notion of trustworthiness incorporating a security perspective and broadening this to other factors in a socio-technical system which may otherwise be overlooked. A set of trustworthiness attributes should be pertinent to a chosen domain and be measurable to the extent that deviations can be identified and addressed.

The Digital Trustworthiness Certificate is the catalyst for ensuring that this information is made available to a service marketplace. Monitoring and management of services in runtime not only caters for the dynamicity of the marketplace but also updates the DTwC allowing for the possibility of taking more informed decisions and lessening the uncertainties in the cloud. The ultimate goal is to provide the necessary elements that lead to a trustworthy marketplace, where service trustworthiness attributes can be assessed and prioritised on a cost-benefit basis.

Acknowledgment. This work was partly supported by the EU-funded project OPTET [grant no. 317631].

References

1. Gartner: Forecast overview: Public cloud services, report G00234817 (2012)
2. Lotz, V., Kaluvuri, S., Di Cerbo, F., Sabetta, A.: Towards security certification schemas for the internet of services. In: 5th International Conference on New Technologies, Mobility and Security (NTMS), pp. 1–5 (2012)
3. Gol Mohammadi, N., Paulus, S., Bishr, M., Metzger, A., Koennecke, H., Hartenstein, S., Pohl, K.: An analysis of software quality attributes and their contribution to trustworthiness. In: 3rd International Conference on Cloud Computing and Service Science (CLOSER), Special Session on Security Governance and SLAs in Cloud Computing-CloudSecGov, available in SCITEPRESS Digital Library, to appear in Springer, SSRI, Aachen (2013)
4. Paulus, S., Gol Mohammadi, N., Weyer, T.: Trustworthy software development. In: De Decker, B., Dittmann, J., Kraetzer, C., Vielhauer, C. (eds.) CMS 2013. LNCS, vol. 8099, pp. 233–247. Springer, Heidelberg (2013)
5. Kaluvuri, S., Koshutanski, H., Di Cerbo, F., Mãna, A.: Security assurance of services through digital security certificates. In: 2013 IEEE 20th International Conference on Web Services (ICWS), pp. 539–546. IEEE (2013)
6. Mei, H., Huang, G., Xie, T.L.: Internetware: a software paradigm for internet computing. Computer **45**(6), 2631 (2012) [Online]. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6197170
7. Avizienis, A., Laprie, J.-C., Randell, B., Landwehr, C.: Basic concepts and taxonomy of dependable and secure computing. IEEE Trans. Dependable Secure Comput. **1**(1), 11–33 (2004)
8. Li, M., Li, J., Song, H., Wu, D.: Risk management in the trustworthy software process: a novel risk and trustworthiness measurement model framework. In: Fifth International Joint Conference on INC, IMS and IDC, 2009. NCM'09, pp. 214–219 (2009)

9. Basili, V.R., Rombach, H.D.: The TAME project: towards improvement-oriented software environments. IEEE Trans. Softw. Eng. **14**(6), 758–773 (1988)
10. Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Buschmann, F., Sommerlad, P.: Security Patterns: Integrating Security and Systems Engineering, vol. 7. Wiley, New York (2006)
11. Paulus, S.: Basiswissen sichere software, report (2010)
12. Szyperski, C., Gruntz, D., Murer, S.: Component Software: Beyond Object-Oriented Programming. Addison-Wesley, New York (2002)
13. The Common Criteria Recognition Agreement: Part 1: Introduction and general model, September 2012, version 3.1 revision 4. NIST, vol. 49, p. 93 (2012) [Online]. http://www.commoncriteriaportal.org/cc
14. IBM Corporation: An architectural blueprint for autonomic computing, report (2006)

Security and Privacy in Mobile Cloud Under a Citizen's Perspective

Dimitris Geneiatakis[1(✉)], Ioannis Kounelis[1,2], Jan Loeschner[1], Igor Nai Fovino[1], and Pasquale Stirparo[1,2]

[1] Institute for the Protection and Security of the Citizen, Joint Research Centre (JRC), European Commission, Ispra, VA, Italy
[2] Royal Institute of Technology (KTH), Stockholm, Sweden
{dimitrios.geneiatakis, ioannis.kounelis, jan.loeschner, igor.nai-fovino, pasquale.stirparo}@jrc.ec.europa.eu

Abstract. Cloud usage has become a reality in users' everyday habits (even if sometimes unconsciously), and security and privacy issues in this context have already been subject of consideration by scientific, business and policy-makers communities. However, the increasing use of mobile phones, and, generally speaking mobile smart devices, to access the Cloud, introduced recently in the area the concept of Mobile Cloud. Scope of this paper is to address the security and privacy aspects of the mobile cloud phenomenon, under the citizen perspective, taking as driving example the context of commercial mobile transactions.

Keywords: Cloud · Cyber-security · Mobile devices · Mobile cloud

1 Introduction

Cloud usage has become a reality in users' everyday habits (even if sometimes unconsciously) and security and privacy issues in this context have already been subject of consideration by scientific, business and policy-maker communities. However, the increasing use of mobile phones, and, generally speaking, mobile smart devices to access the Cloud, introduced recently in the area the concept of Mobile Cloud. According to a generally well-accepted vision, mobile cloud refers to an infrastructure where both the data storage and data processing happen outside of the mobile device [1]. This view does not indeed add so much to the common view of cloud, in fact, according to it, smart-phones here are seen only as interfaces to get access to the cloud. In the real world, however, the role of smart devices in cloud operations is a lot more than that of mobile interface: smart-phones in fact can be used as storage resource for the cloud, memorizing data and making it available to the cloud when needed. Moreover, they can simultaneously establish mobile-to-mobile direct connections, share directly information and computation results with other phones, and at the same time interact with the traditional cloud. In that sense, especially considering their computational resources (quad-core processors are not rare in this domain), we

M. Felici (Ed.): CSP EU FORUM 2013, CCIS 182, pp. 16–27, 2013.
DOI: 10.1007/978-3-642-41205-9_2,

believe that mobile phones can and must be considered as full, even if peculiar, nodes of the cloud infrastructure. The criticality of these "special nodes" is generally due to the following considerations:

1. Being mobile by nature, they are exposed full-time to a potentially adverse environment
2. The need, for mobile applications, to cut the development costs to maintain the price appealing for the mobile-application market, is often translated into a quick-prototyping approach, rather than a careful cyber-security oriented code development
3. Being the smart-phone strongly linked to their owner, a successful exploitation of a smart-phone can directly impact the security and privacy of its owner

Scope of this paper is to address the security and privacy aspects of the mobile cloud phenomenon, under the citizen perspective, taking as driving example the context of commercial mobile transactions. Particularly, we focus on cloud services accessed by mobile devices (SaaS - Software as a Service) and the first-level connection between mobile devices and their access point. The structure of the paper is the following: Section 2 describes the reference use case scenario. In Sect. 3 we categorize mobile cloud vulnerabilities in order to map a set of threats on the use case scenario to which the citizen might be exposed (e.g. profiling, proximity marketing and behavioral analysis). In Sect. 4 we use the scenario to present a set of effective countermeasures. Finally, in Sect. 5 we conclude our findings.

2 Use Case Scenario

In order to better demonstrate the risks and threats for a citizen when using a mobile cloud, we base our explanations on the following scenario.

A citizen, Maria, with a mobile device (e.g. an Android smart-phone) is visiting Milan during her vacation. As she is new to the place, she would like to explore the city and see the most well-known monuments and tourist attractions. In order to do so, she uses the mobile application of her choice and using GSM/3G she connects to the Internet and is able to search for sightseeings. She picks up the most common location as her next place to visit, but she then realises that it is too far to go on foot. As a result she buys a ticket for the subway using the corresponding application.

The ticket mobile application is an interface to a cloud through a mobile device. The payment itself is delegated to a third-party payment service, while the ticket company keeps on their servers proof and details of the ticket purchase. The citizen also receives on her phone a valid barcode and NFC tag to be used for ticket control. As a result, before entering on the subway she swipes her phone at the NFC readers, her ticket is validated and she can proceed on using the means of transport.

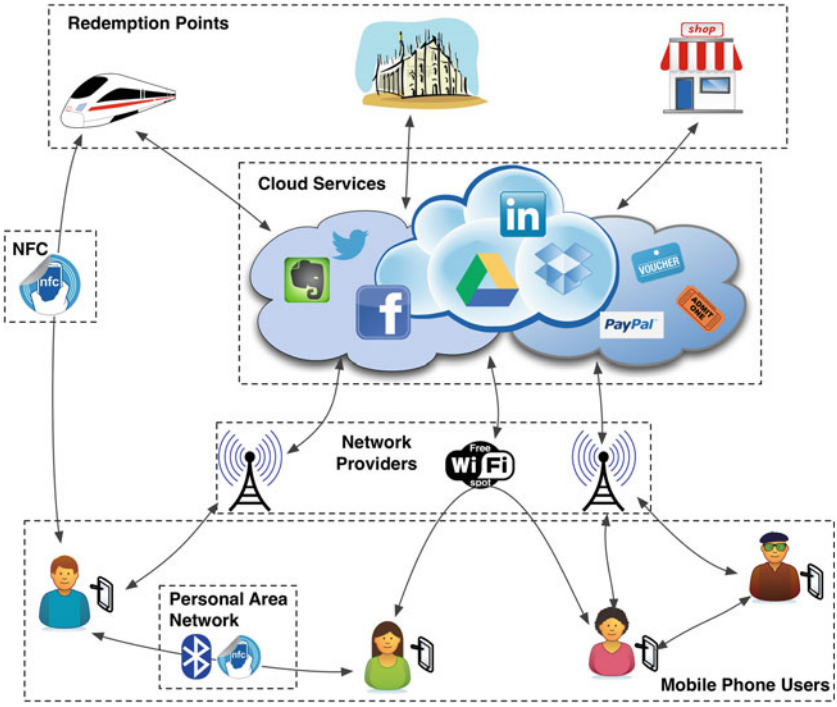

Fig. 1. High level mobile cloud layered interaction scheme

Later that day, she is with her friend in a cafeteria and in order to avoid using the 3G connection, since she has reached the data plan limit, she switches to Wi-Fi connecting to the open wireless network of the shop. While connected she chats with her friends online while in the mean time uses a cloud storage application to send pictures.

Finally, as she had bought by mistake more than one subway ticket, she wants to give one of them to her friend. The tickets are anyway anonymous and no authentication of the user is required. The transfer of the ticket is done over Bluetooth to her friend's device. Her friend can now use the ticket as if she had bought it himself. In this case it is of the ticket provider's interest to be able to verify the validity of the ticket and to also be able not to allow misuse and illegal duplication of the tickets. Figure 1 provides an overview of all the actors, services and infrastructures typically involved in mobile cloud operations.

3 Vulnerabilities and Threats

Scope of this section is to present a general overview of threats and vulnerabilities affecting the mobile cloud infrastructure under a citizen's perspective. We are looking at those vulnerabilities related to the "last mile" of the infrastructure, i.e. the mobile device. As defined by Bishop in his book [2], a threat is a *potential*

violation of security. Such violation does not need actually to occur for there to be a threat. The fact that the violation might occur means that those actions that could cause it to occur must be guarded against (or prepared for). Those actions are called attacks.

3.1 Communication Vulnerabilities

Due to the nature of mobile devices, all communications happen via several wireless communication protocols, and todays' smart-phones have deployed on board many different wireless communication capabilities. Unfortunately every (new) feature brings, along with many technological advantages and benefits, a series of vulnerabilities and possible threats. All wireless protocols are prone to the following major classes of threats:

- *Eavesdropping* is the unauthorized interception of information. It is passive, suggesting simply that some entity is listening to the communications. If data is sent unencrypted over any wireless communication channel, eavesdropping becomes very trivial.
- *Spoofing* is the impersonation of one entity by another. It lures a victim into believing that the entity with which it is communicating is a different entity.
- *Tracking* refers to the possibility for an attacker to remotely determine the exact or approximate location of a mobile device. Because mobile devices by their nature emit radio signals and their physical addresses, which have to be both unique and known to communicating parties, that are subject to location-tracking threats.
- *Denial of Service* (DoS), a long-term inhibition of service, refers to the ability of an attacker to prevent a server from providing a service. The denial may occur at the source or at the destination (by blocking the communications from the server), or along the intermediate path (by discarding messages from either the client or the server, or both).
- *Data Corruption, Manipulation or Insertion* is the result from an entity changing information. Unlike eavesdropping, this threat is active. An example of this could be the man-in-the-middle attack, in which an intruder reads messages from the sender and sends a modified versions to the recipient, in hopes that the recipient and sender will not realize the presence of the intermediary.

Although the above listed threats apply to the computer world as well and are not exclusive to the mobile world, the easiness to carry attacks in order to exploit such threats increases drastically in the mobile world, as all wireless communications are broadcasted, therefore lacking of any physical protection mechanism. In the following paragraphs we provide an overview of the major weaknesses affecting the communication channel available in modern smart-phones.

GSM Connections: Vulnerabilities of the GSM protocol are mainly related to serious flaws in the cryptographic algorithms A5/1 and A5/2, other than to the

fact that it authenticates only the subscriber against the network and not vice-versa. Since the first attack against A5/1 proposed by Anderson in 1994 [3], both algorithms A5/1 and A5/2 used for link-level encryption of voice data in GSM have been practically broken [4]. Moreover interception attacks have been shown to be easily possible with off-the-shelf hardware, making feasible to set up a cellular base station to pose as a legitimate one [5]. The price of needed equipment has dropped significantly; with a low budget it is possible to buy the hardware needed such as Universal Software Radio Peripheral (USRP), daughterboard, antennas, etc., while the software to run on top of it is free and open source: OpenBTS and GNURadio. By setting up a fake base station, all the nearby phones could be automatically connected to it, as by default the phones choose to connect to the base station with the most powerful signal. Upon connecting, the attacker can act as a man-in-the-middle, eavesdropping all incoming and outgoing communication and even creating fake ones. It is possible for example, to send a Short Message Service (SMS), SMS Spoofing, or make a call pretending to be a specific number, making the victim believe that someone else is communicating with him/her. In this context, the SMS represents a high risk solution when used as (extra) security feature, e.g. Transaction Authentication Number (mTAN) sent over SMS by the banks to their customers.

Wi-Fi Connections: Wi-Fi is the common name used when referring to the implementation of the standard IEEE 802.11 for wireless local area network (WLAN). Wi-Fi vulnerabilities are mainly related to the authentication method used. Particularly the WEP authentication protocol has been broken due to a flaw found in the RC4 algorithm, which is at the base of WEP. In 2001 Fluhrer et al. [6] demonstrated a weakness in the use of the initialization vectors (IVs) used with RC4, resulting in a passive attack that can recover the RC4 key after eavesdropping on the network.

Near Field Communication Protocol: The NFC is a bidirectional proximity coupling technology, which allows data transfer between devices on a short distance (up to 10 cm). Other than supporting contactless smartcard systems, NFC extends the above with peer-to-peer functionality standardized in [7,8]. NFC has three operative modes: (1) Reader/Writer, (2) Card Emulation, and (3) Peer-to-Peer. NFC technology, brought to mobile phones, opens new attacks and threats scenarios. According to [9], NFC-enabled devices can be susceptible to threats like eavesdropping, data modification, corruption, insertion, man-in-the-middle (MITM), DoS, and phishing. Although more a design/standard issue than a proper vulnerability, the NFC standard does not offer link level security, a part from NFC-SEC [10] that provides security standard for peer-to-peer NFC communication (does not include reader/writer and card emulation mode [11]), the wireless signal is not encrypted.

3.2 Application Layer Vulnerabilities

According to [1] mobile Internet is expected to overwhelm the usage of land line Internet. This is not only because of evolution of smart-phones and underlying infrastructure, but also due to easy management of the mobile applications. This is supported by mobile applications stores, such as *Google play store, Itunes*, etc., which follow the one-stop shop model, where a user can acquire the desired application and install it directly on his phone without any interventions. These stores gain users' trust. Each of these stores before publishing an application scrutinize it for identifying possible malicious activities by using particular security techniques, such as Google's Bouncer.

However, on a side, it's almost impossible to be 100 % secure on the safeness of an application. For instance, in 2012 was presented a technique to bypass *Google's* Bouncer security checks [12]. A similar problem was faced also by *Apple's store* [13]. These facts show that even the existence of security mechanisms at the store side do not guarantee the security (e.g., lack of malicious operations) in the provided applications. On the other side, to make things even worst, end-users can in any case try to install applications from non-verified repositories.

Malicious software (malware) [14] is a type of software designed to manipulate users' data depending on its attributes. Under the umbrella of malware can be found multiple types of malicious software such as backdoors, rootkits, spyware, etc., that might violate users' privacy. In the past malware was affecting mainly the availability or/and the integrity of the information system, while currently it can affect the confidentiality as well. Without loss of generality, mobile malware applications can be classified in two main categories:

Trojanized applications: In this type of malware the attacker is able to modify the application's code and insert the malicious code as illustrated in Fig. 2. Afterwards, the attacker uploads the new modified application in the store, where unsuspicious users can install and use it, without recognizing the malicious operations executed by it. This can be accomplished by using the Soot framework instrumentation tool [15] that enables the reverse engineering Android applica-

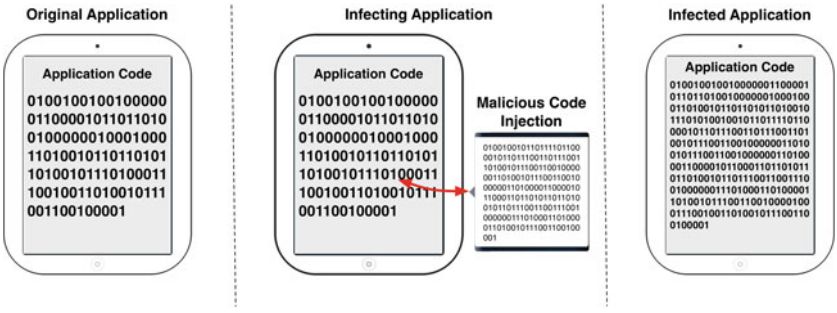

Fig. 2. An example of mobile *trojanized* application

tions. As a result a malicious user can modify the provided application in order to add particular type of code.

Malicious applications: In this type of malware the attacker develops a particular application which is able to manipulate personal data or execute other malicious functionalities on the smart-phone by design (e.g., send out users' photos).

The plethora of personal information managed (created, modified, deleted) by mobile applications, the always online nature of mobile devices and their integration with the cloud, makes the smart-phones, especially in the cloud context, an interesting target for attackers. For example, spying applications can collect user's position or steal his personal contacts and sell them to marketing companies. A detailed analysis for existing mobile malware can be found in [16].

According to Kaspersky security bulletin for 2012 [17] malware main target is smart-phones and particularly those which run Android OS. Consequently, the mobile users have to face the following threats in the context of mobile application security:

Privacy invasion and data loss: the fact that mobile applications manage a wide range of personal information such as unique identifiers, location, call history, text messages, emails, etc., generates new opportunities for profiling users' preferences. Legitimate applications can use personal information to provide powerful features and benefits. However, the opportunity to misuse that information exists as well. This is, for instance, the case of *Twitter application*, which was sending out users' personal information (contacts), without notifying the user [18]. In the worst case scenario personal information can be totally lost if the malware is allowed to execute the corresponding operations. In other cases mobile malware takes the advantage of the fact that applications can be granted with more permissions than what they actually need and consequently can manipulate personal information stored in the phone.

Toll fraud: The malware developers create such software driven by different aims, however, as reported in [16] among main incentives is financial return. In these cases, malware achieves profit by leveraging the mobile phone billing system mainly by sending sms to premium rate services without the users? consent. Alternatively, malware can focus on other financial related applications for exploitation. As illustrated in [19], applications include personal information in different states, which a malicious user is able to extract with existing tools.

Furthermore, considering the fact that smart-phones are becoming the central repository of user's personal data, there is an urgent need for mechanisms protecting the content of mobile devices as high number of phones are lost or stolen. In [19] Stirparo et al. show different techniques in order to extract personal information when you have physical access to a smart-phone. For instance, if a smart-phone is lost a malicious user can root it and data can be extracted via the android device bridge (adb) using the following command.

```
adb pull /system/app/data.dem /tmp/
```

In this example, the malicious user is able to store the file *data.dem* to the */tmp* directory in his computer. Even if the stored information is encrypted

other tools for analyzing operating system's memory can be used in order to identify personal data. Alternatively, this information can be extracted and then decrypted *off-line* using well-know decryption tools, such as the Cain and Abel tool.

3.3 Attack Scenarios

The above mentioned vulnerabilities and threats are not just theoretical but as a matter of fact are in most cases easy to replicate and provide a good investment/profit ratio from the attacker's point of view.

Taking the use case scenario described in Sect. 2, an attacker could be eavesdropping on the GSM network, and therefore interfering with the communication of our character. The attack could either be passive in order to gather information for the victim's physical movements or active altering data of the transaction on the attacker's benefit. In the first case, the attacker could be interested to find out that the victim bought a subway ticket. He may for example be interested in locating the victim and stealing her laptop. In the second case the attack has no physical encounters. It may be a financial attack, stealing the victim's credit card or making her buy tickets from a fake website. Of course, the same two attacks can also occur in the case of the open Wi-Fi network by monitoring the internet traffic or over a Bluetooth local area network in order by sniffing on the transferred files (steal the subway ticket in this case).

Besides financial gain, the attacker may be interested in more indirect attacks. Performing session hijacking to the victim's personal social sites, may result into taking in control her personal digital life. The attacker may be able to alter personal and sometime private information of the victim that will result in harming her public profile. Although these attacks don't have direct economical gain, they occur during personal rivalries or even more important business intelligence.

The passive version of this attack is to monitor the user and profile her. Profiling can also be used for the purposes described above with the only difference that the user usually does not understand that she is been profiled. Profiling refers to collecting user's habits, interests and in general preferences in everyday choices; from the music someone listens to, to the cafeteria she prefers to hang out, etc. This information can be then used combined in order to perform a specific personalised attack on the victim, using in most cases social engineering skills, to gain the victim's trust and then exploit it according to the attacker's interest.

Another attack that can take place is a phishing attack on the NFC tags. An attacker can replace a legitimate NFC tag (the one for ticket validation for example) with a rogue one that injects code on the user's phone and then manages to take control.

Finally, eavesdropping can be performed in a physical way as well. As shown in [20] with a mobile application and a normal camera of an average phone, a user can monitor all the letters the victim is typing from a not so close distance. As a result stealing credentials, personal information or just messages can be

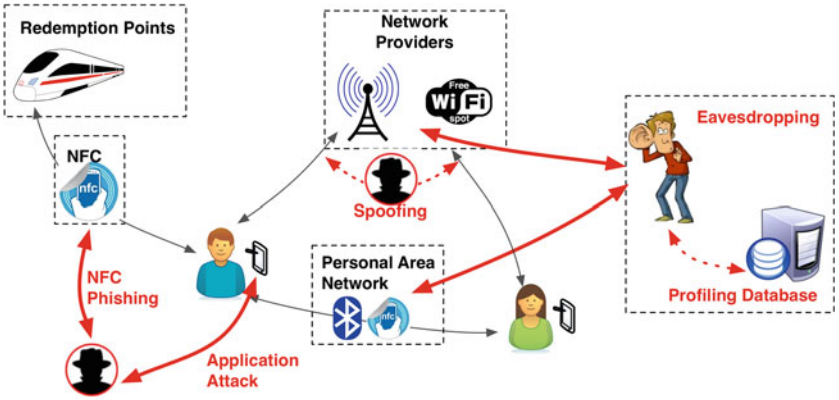

Fig. 3. Attack scenarios

achieved in this way especially in crowded places like means of transport or tourist attractions. All the attack scenarios are illustrated in Fig. 3.

4 Countermeasures

Successful countermeasures aim at preserving the three pillars of security services, also known as the CIA model: confidentiality, integrity, and availability. *Confidentiality* refers to preventing the disclosure of information to unauthorized individuals or systems. Data *integrity* means maintaining and assuring the accuracy and consistency of data over its entire life-cycle and, finally, *availability* refers to the ability to use the information or resource desired. For any information system to serve its purpose, the information must be available when it is needed, therefore the communication channels used to access it must be functioning correctly.

4.1 Communication Layer

To minimize the risk of being victim of attacks targeting vulnerabilities that affect communication protocols, it is important to determine a priori in the design phase which communication protocols will be used in the Cloud architecture that has to be developed and deployed, and therefore applying the proper countermeasures. For example, in order to avoid connecting to a compromised base station, 3G (or 4G if available) connection should always be used. As the 3G protocol allows mutual authentication, the base station will have to be authenticated and thus a compromised base station will not be accepted as a legitimate one.

When moving to Wi-Fi connection, WPA2 must be enforced as compulsory authentication method, since it uses AES-based encryption mode with strong security. As underlined in Sect. 3.1, the specification do not envisage link-level

encryption except for the peer-to-peer mode, therefore it is fundamental that developers implement cryptography in their solutions.

4.2 Applications Layer

To eliminate the risk of personal data manipulation Android and iOS operating systems follow different approaches. Particularly, Android OS provides strong application isolation. By default applications are not allowed to execute functions that affect other applications or the user. Applications have to declare in a manifest all sensitive operations that can be accomplished during their execution, which the user should endorse during installation. Android does not offer any capacity to users for dynamically enabling permissions.

On the other hand, iOS since version five, does not incorporate any functionality to avoid data manipulation. iOS in fact, protects users' data through developer license agreement. In the latest release iOS enables users to enhance the control of their personal data by requiring applications to get explicit permission before accessing them.

However, as described in Sect. 3.2 the underlying security mechanism can be by-passed, thus various researches have been published in order to enhance the security and privacy levels in the mobile platforms. Particularly, [21] focus on the static analysis of the executable part of the mobile application to identify any permission manipulation. An alternative approach is followed by [22–24] in which users are able to define their policies for accessing personal data. Other solutions such as [25] focus on application repackaging. In this approach the compiled applications are analyzed and injected with particular code at the bytecode level in order to monitor all the access of personal data.

4.3 User Behavior

Security measures and mechanisms are developed with the aim to provide protection to the end user. However, it is very often the case that the end user is the weakest link in the security chain. Especially in the case of mobile devices, where the users tend to forget that the smart-phone they are using is not just a telephone but a computer with powerful capabilities. This is either due to the fact that they are not aware of the security risks of mobile applications and how to manage their security and privacy settings [26] or because the extra security features change their user experience and interface in such a way that it makes the original application hard to use. The latter is completely aligned with Saltzer and Schroeder principle of *"psychological acceptability"* [2].

5 Conclusions

Mobile Cloud is the new *frontier* of modern ICT. It represents the most evident proof of the technology convergence that is in act in the telecommunication and, more in general, in the ICT world. On one side the massive use of mobile

devices to get access to the Internet and to perform cloud oriented operations constitutes a great opportunity to deliver new and more advanced services to the citizen. On the other side, the economic model on which the mobile cloud is built, based on cheap mobile applications development, rarely fits with the need for high security level in a field in which citizen's privacy and security should be indeed the most important parameter to be taken under consideration. On top of this, the scarce attention of the end-user to the security issues (in average a smart-phone, for the end-user, is still "only" a phone), is an amplifier for the threats described. In this paper we provided an overview of these threats and of the vulnerabilities affecting the mobile world, under a cloud perspective, providing a set of "best practices" which should help the end-user in mitigating the exposure to the described threats.

References

1. Mobithinking: Global mobile statistics 2013 part a: Mobile subscribers; handset market share; mobile operators (2013) [Online]. http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#subscribers
2. Bishop, M.: Computer Security: Art and Science. Addison Wesley Professional, Boston (2003)
3. Anderson, R.: A5 (was: Hacking digital phones), Usenet communication on sci.crypt, alt.security and uk.telecom (1994)
4. Barkan, E., Biham, E., Keller, N.: Instant ciphertext-only cryptanalysis of GSM encrypted communication. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 600–616. Springer, Heidelberg (2003)
5. Meyer, U., Wetzel, S.: On the impact of gsm encryption and man-in-the-middle attacks on the security of interoperating gsm/umts networks. In: Proceedings of 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC 2004, vol. 4, pp. 2876–2883 (2004)
6. Fluhrer, S., Mantin, I., Shamir, A.: Weaknesses in the key scheduling algorithm of RC4. In: Vaudenay, S., Youssef, A. (eds.) SAC 2001. LNCS, vol. 2259, pp. 1–24. Springer, Heidelberg (2001)
7. ISO/IEC 18092 / ECMA-340: Near Field Communication Interface and Protocol (NFCIP-1), ECMA International Std. (2004)
8. ISO/IEC 21481 / ECMA-352: Near Field Communication Interface and Protocol (NFCIP-2), ECMA International Std. (2004)
9. Haselsteiner, E., Breitfuß, K.: Security in near field communication (nfc). In: Workshop on RFID Security (2006)
10. NFCIP-1 Security Services and Protocol - Cryptography Standard using ECDH and AES, ECMA International Std. (2008)
11. Coskun, V., Ok, K., Ozdenizci, B.: Near Field Communication (NFC): From Theory to Practice. Wiley, New York (2012)
12. Miller, C., Oberheide, J.: Dissecting the android bouncer (2012) [Online]. http://jon.oberheide.org/blog/2012/06/21/dissecting-the-android-bouncer/
13. Ducklin, P.: Apple's app store bypassed by russian hacker, leaving developers out of pocket (2012) [Online]. http://nakedsecurity.sophos.com/2012/07/14/apple-app-store-bypassed-by-ussian-hacker-leaving-developers-out-of-pocket/
14. Mell, P., Kent, K., Nusbaum. J.: Guide to Malware Incident Prevention and Handling [Online]. http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf

15. Bartel, A., Klein, J., Le Traon, Y., Monperrus, M.: Dexpler: converting android dalvik bytecode to jimple for static analysis with soot. In: Proceedings of the ACM SIGPLAN International Workshop on State of the Art in Java Program Analysis, SOAP '12, pp. 27–38. ACM, New York (2012)
16. Felt, A.P., Finifter, M., Chin, E., Hanna, S., Wagner, D.: A survey of mobile malware in the wild. In: Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, SPSM '11, pp. 3–14. ACM, New York (2011)
17. Kaspersky security bulletin 2012. The overall statistics for 2012 [Online]. https://www.securelist.com/en/analysis/204792255/Kaspersky_Security_Bulletin_2012_The_overall_statistics_for_2012
18. Mobile apps take data without permission [Online]. http://bits.blogs.nytimes.com/2012/02/15/google-and-mobile-apps-take-data-books-without-permission/
19. Stirparo, P., Kounelis, I.: The mobileak project: forensics methodology for mobile application privacy assessment. In: Proceedings of the International Conference for Internet Technology and Secured Transactions, pp. 297–303. IEEE (2012)
20. Maggi, F., Gasparini, S., Boracchi, G.: A fast eavesdropping attack against touchscreens. In: Proceedings of 7th International Conference on Information Assurance, IAS' 12, pp. 320–325. IEEE December 2011
21. Bartel, A., Klein, J., Le Traon, Y., Monperrus, M.: Automatically securing permission-based software by reducing the attack surface: an application to android. In: Proceedings of the 27th IEEE/ACM International Conference on Automated Software Engineering, ASE, pp. 274–277. ACM, New York (2012)
22. Schreckling, D., Kstler, J., Schaff, M.: Kynoid: real-time enforcement of fine-grained, user-defined, and data-centric security policies for android. Inf. Secur. Tech. Rep. **17**(3), 71–80 (2013)
23. Kodeswaran, P., Nandakumar, V., Kapoor, S., Kamaraju, P., Joshi, A., Mukherjea, S.: Securing enterprise data on smartphones using run time information flow control. In: Proceedings of the 13th International Conference on Mobile Data Management, MDM '12, pp. 300–305. IEEE Computer Society, Washington (2012)
24. Xiao, X., Tillmann, N., Fahndrich, M., De Halleux, J., Moskal, M.: User-aware privacy control via extended static-information-flow analysis. In: Proceedings of the 27th IEEE/ACM International Conference on Automated Software Engineering, ASE, pp. 80–89. ACM, New York (2012)
25. Berthome, P., Fecherolle, T., Guilloteau, N., Lalande, J.F.: Repackaging android applications for auditing access to private data. In: Proceedings of the 7th International Conference on Availability, Reliability and Security (ARES), pp. 388–396 (2012)
26. Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E., Wagner, D.: Android permissions: user attention, comprehension, and behavior. In: Proceedings of the Eighth Symposium on Usable Privacy and Security, SOUPS '12, pp. 3:1–3:14. ACM, New York (2012)

Bringing Accountability to the Cloud: Addressing Emerging Threats and Legal Perspectives

Massimo Felici[1], Martin Gilje Jaatun[2],
Eleni Kosta[3], and Nick Wainwright[1(✉)]

[1]Hewlett-Packard Laboratories, Long Down Avenue, Bristol BS34 8QZ, UK
nick.wainwright@hp.com
[2]SINTEF ICT, Trondheim, Norway
[3]Tilburg University, Tilburg, Netherlands

Abstract. This paper is concerned with accountability in cloud ecosystems. The separation between data and data subjects as well as the exchange of data between cloud consumers and providers increases the complexity of data governance in cloud ecosystems, a problem which is exacerbated by emerging threats and vulnerabilities. This paper discusses how accountability addresses emerging issues and legal perspectives in cloud ecosystems. In particular, it introduces an accountability model tailored to the cloud. It presents on-going work within the Cloud Accountability Project, highlighting both legal and technical aspects of accountability.

Keywords: Accountability · Data governance · Cloud computing

1 Introduction

Cloud computing has emerged as a new paradigm used across industries for deploying technological resources. Economic forecasts show that cloud computing will enable efficient, competitive and cost-effective deployments of computational resources in order to accommodate emerging user needs [1]. Alongside many business benefits both for consumers and providers of information services, cloud computing presents new challenges in terms of security and trust. Personal data is duplicated across cloud resources making them more accessible and less subject to loss. Unfortunately, personal data is also exposed to security threats and lack of trust across cloud supply chains [2].

Cloud consumers and providers are exposed to various problems. For instance, from a resource viewpoint, it is necessary to improve data management processes and to a certain extent to automate them. The increasing amount of data and resources requires new mechanisms enabling cost-effective management while guaranteeing critical features like security and privacy. One of the essential characteristics of cloud computing is rapid elasticity – "*Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand*" [3]. This involves horizontal (connecting different resources such that they work as a single logical unit) and vertical (increasing the capacity of a

M. Felici (Ed.): CSP EU FORUM 2013, CCIS 182, pp. 28–40, 2013.
DOI: 10.1007/978-3-642-41205-9_3,

single unit by adding additional resources to it) scalability of cloud computing. Unfortunately, scalability of code and data still remains among the main challenges affecting quality of services and interactions among customers and providers [1]. From security and trustworthiness perspectives, some of the issues that consumers and regulators are mostly concerned about are things like lack of transparency and control in cloud service provision. The international dimension of some situations (for instance, foreign government surveillance) may involve dealing with further complexities from a legal perspective. Other challenges in cloud computing relate in particular to multi-tenancy, which "*raises multiple concerns that implicit impact on the quality of the cloud systems and in how far the respective characteristics can be fulfilled*" [1]. Such challenges are perceived as barriers and are limiting the adoption of cloud computing.

Accountability has emerged as a critical aspect of data protection [4]. Recent research on accountability [5] has identified its essential elements (e.g. organizational commitments, mechanisms for privacy policies and assurance reviews). Unfortunately, a generally accepted definition of accountability is still beyond any consensus [6]. Without a well-defined concept of accountability, it is difficult to interpret accountability from an operational viewpoint of analysis in cloud ecosystems. However, within the on-going debate on a definition of accountability, this paper is concerned with how accountability information enables data governance in cloud ecosystems. The relationship between accountability and information is also referred to as information accountability: "*information usage should be transparent so it is possible to determine whether a use is appropriate under a given set of rules*" [7]. Accountability provides a means to unlock the cloud potential by addressing relevant problems of data protection emerging in cloud ecosystems [8].

This paper discusses emerging issues (focusing on data governance and protection) in cloud ecosystems and presents relevant legal perspectives. The separation between data and data subjects as well as the exchange of data between cloud consumers and providers increases the complexity of data governance in cloud ecosystems. This problem is worsened by emerging threats and vulnerabilities in cloud ecosystems. This paper discusses how accountability addresses emerging issues and legal perspectives in cloud ecosystems. In particular, it introduces a model of accountability addressing both technical and legal perspectives in cloud ecosystems. This paper is organized as follows. Section 2 discusses the problem of data governance in cloud ecosystems. Section 3 describes some emerging data protection problems in the cloud. It highlights how cloud computing requires new information mechanisms orchestrating data governance and relationships among stakeholders. Section 4 introduces our model of accountability in the cloud. Section 5 discusses relevant data protection issues drawn from legal perspectives. Section 6 highlights some remarks.

2 Data Governance in Cloud Ecosystems

Cloud computing has transformed the way information technology is delivered, promising rapid, efficient, and cost-effective deployment of computational resources across different industries, geographic areas and application domains. More recently,

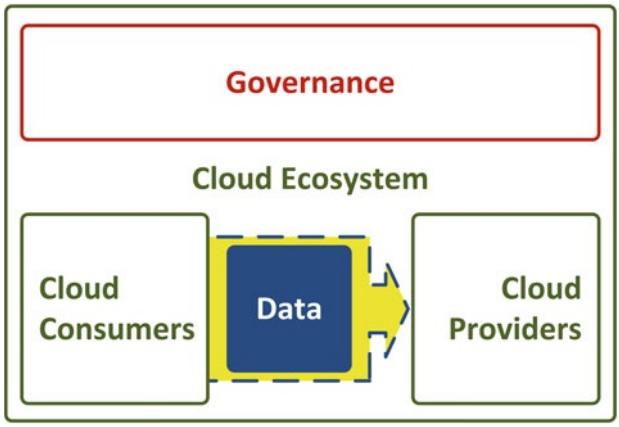

Fig. 1. Cloud ecosystem

the scope of cloud computing has expanded to include 'big data', the increasingly large amounts of data held by cloud service providers that is the raw material on which new and innovative cloud services are founded. However, alongside its numerous business benefits for consumers and providers of information services alike, cloud computing presents new challenges in terms of security, privacy and trust. The transfer of personal or confidential data into the cloud may provide the opportunity for innovators to create new services, offering operational advantages such as improved accessibility and reducing the probability of catastrophic loss. At the same time this may make data more vulnerable to unauthorised access or modification. The broader issue is essentially one of loss of transparency and control in what happens to data once moved to the cloud. As stewardship of data becomes shared between users and potentially complex chains of cloud providers, the former have to place trust on the cloud ecosystem and its governance (see Fig. 1). This has proven to be a significant barrier limiting the adoption of cloud computing – one that can be lifted by ensuring that there is accountability throughout the cloud ecosystem.

Accountability is emerging not only as an essential aspect of data protection (for several decades it has been regarded as a privacy principle), but also in particular within the deployment of cloud computing as argued by the Article 29 Data Protection Working Party[1] – "*In IT accountability can be defined as the ability to establish what an entity did at a certain point in time in the past and how. In the field of data protection it often takes a broader meaning and describes the ability of parties to demonstrate that they took appropriate steps to ensure that data protection principles have been implemented*" [18].

[1] Under Article 29 of the Data Protection Directive, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data is established, made up of the Data Protection Commissioners from the Member States together with a representative of the European Commission. The Working Party is independent and acts in an advisory capacity. The Working Party seeks to harmonize the application of data protection rules throughout the EU, and publishes opinions and recommendations on various data protection topics.

Accountability, if implemented by cloud service providers, can unlock further potential cloud services by addressing relevant problems of data stewardship and data protection in emerging in cloud ecosystems. Governance is the process by which accountability is implemented in the cloud. All the actors involved in the cloud – service providers, consumers of cloud services (whether individual end-users, businesses, public organisations and even other cloud service providers), and those directly involved in IT governance have a role to play in making cloud services accountable for how data is used and managed in the cloud.

3 Emerging Challenges in Cloud Ecosystems

This section discusses by means of examples emerging challenges and issues in cloud ecosystems. Cloud services are not isolated, they exist in an ecosystem where all the parts interact and rely on each other. Figure 2 illustrates the main challenges and threats that we will discuss in the remainder of this section.

The governance challenges in cloud computing are in part related to the complex provider supply chains in such ecosystems, for instance, where the Software-as-a-Service (SaaS) application that a user interacts with may be based on another provider's Platform-as-a-Service (PaaS) solution, which in turn may be running on yet another provider's Infrastructure-as-a-Service (IaaS) offering. To complicate things even further, services and data may be replicated horizontally among multiple providers, making it extremely difficult to determine where your data is at any one time. As if the complexity of the Cloud ecosystem supply chains was not enough, the scale

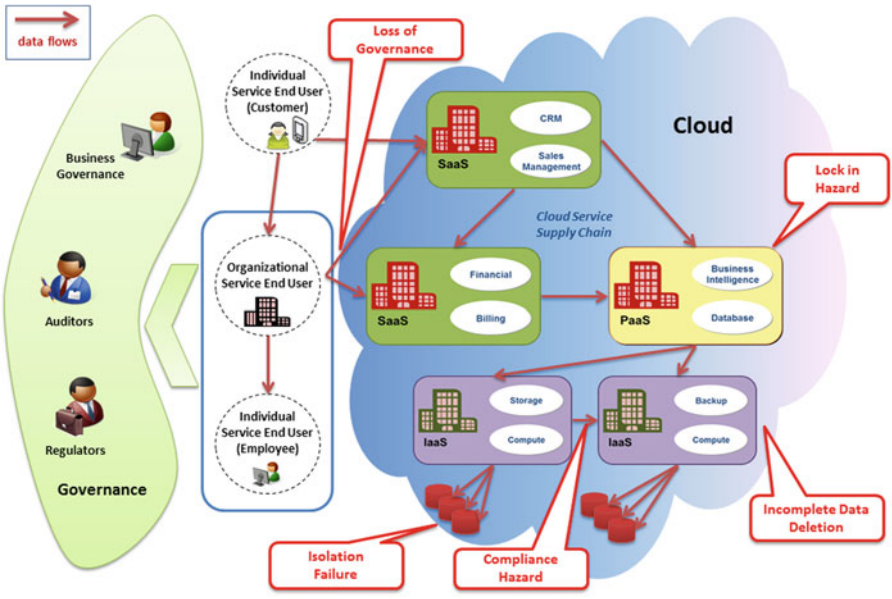

Fig. 2. Threats in a cloud ecosystem

of cloud operations is daunting. Economy of scale is one of the most often quoted arguments for the viability of cloud computing, and the major cloud provides operate data centres of a size which is downright intimidating. Finally, the vast amounts of data on individuals available to cloud providers enable them to perform sophisticated data mining operations, revealing things about us that we may not even know ourselves.

Isolation Failure. Multi-tenancy means data from several customers are stored and processed on the same infrastructure, and improper protection may expose confidential data. An example of isolation failure would be if it was possible to log into anyone's account without a password. Isolation failures do not always arise due to provider errors. Cloud consumers might misconfigure their services, effectively making data which should have been private publicly available on the internet. A specific case of the data isolation challenge comes when a given employee (say, of Acme Inc.) uses an Enterprise SaaS application for work-related transactions, but at the same time also uses an eGoverment/eHealth app in the capacity of a private citizen (see Fig. 3). This is challenging on several levels; not only is there a risk of mixing personal information and sensitive business information on the same device (which is strictly speaking not a cloud challenge), but the eGovernment SaaS service and the Enterprise SaaS service may actually be based on the same IaaS service (as Fig. 3 illustrates).

This highlights that isolation failures could both have consequences for personal data (individuals accessing data belonging to other individuals) and sensitive company data (one company accessing another company's trade secrets) and even combinations of the two (Acme Inc. accessing the personal eHealth data of their employees).

Compliance Hazard. Data protection laws prohibit transferring personal data from EU to jurisdictional domains without sufficient protection. Determining what constitutes "*sufficient protection*" might not be something the average cloud user should be expected to manage, but even if a local provider is chosen, there is a high likelihood that data is transferred across borders. Data flows in the cloud ecosystem are dynamic,

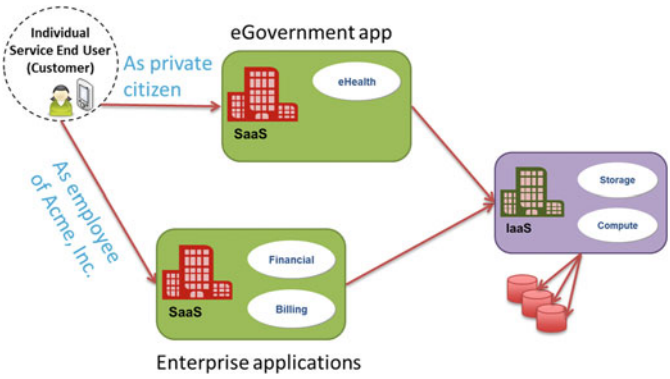

Fig. 3. Example of data isolation problem

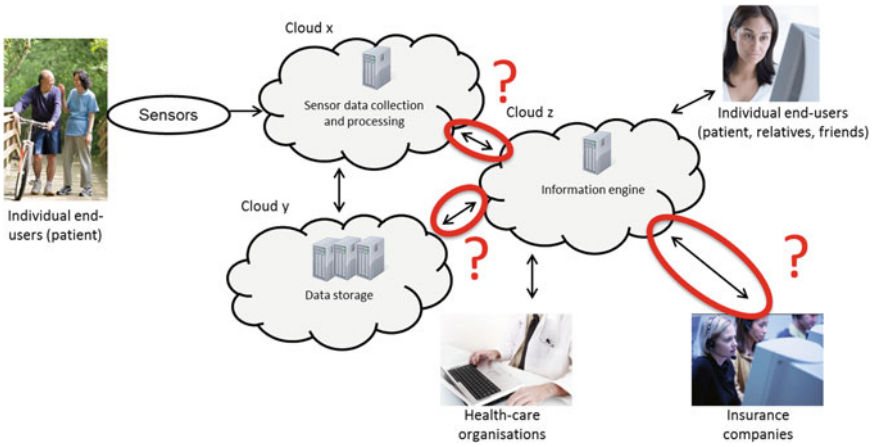

Fig. 4. Example of data flows in a cloud ecosystem

and may go both horizontally (e.g. between IaaS providers) and vertically (e.g. from Saas to PaaS to IaaS).

Figure 4 illustrates an example where an (imagined) SaaS application in cloud X gathers medical sensor data from home-based patients, passes partially processed data on to another SaaS application in cloud Z, and uses IaaS storage services from cloud Y for long-term storage and backup. Cloud Z may be using the same IaaS services as Cloud X, but it could just as easily be using a completely different cloud. Cloud Y could, in turn, use yet another cloud service to back up the data in their data centres.

Figure 4 also shows that some statistical data is transferred to insurance companies; here it will be important to ensure that the data is properly and fully anonymized, or that the patients have given consent for this use of their data (note that consent may not be required if data are really anonymous, however this could be subject to ethical practices described in professional codes of conduct).

Incomplete Data Deletion. Redundant data storage and data migration may lead to multiple copies being stored on multiple physical infrastructures, and a command to delete a particular piece of data may take a month to take effect (due to data being duplicated across different data centres). Furthermore, some providers state that data may remain in backup logs for 90 days or more, or even indefinitely (i.e. stored forever) [10].

Lock-in Hazard. Proprietary formats may make moving from one cloud provider to another difficult, if not impossible. Data transfer costs may also be prohibitive, and serve as a lock-in feature in itself. There are examples where it is cheap to upload data to a given service, but comparatively expensive to download. This can be the case where a customer is allowed to upload a small amount of data for free every month; a small trickle of data over the years translates to a data deluge when it has to be moved all at once. It may be even more dramatic when a cloud service provider goes out of business – when the Megaupload file sharing service was shut down due to copyright infringement, a large number of innocent customers lost access to their files and

images without warning [9]. Some standard terms offered by cloud providers can also leave consumers with little control on how to migrate their data or their accounts, e.g. allow providers to terminate consumers' accounts for any reason at any time, with no advance notice.

Loss of Governance. The challenge related to loss of governance may be seen a combination of all issues discussed in this section, but maybe in particular for a business user of cloud services. When a business places its data and processes in the cloud, control is necessarily ceded to the cloud provider, but the SLA for this service does not necessarily also cover governance services from the CSP, unless this has been specifically negotiated. Furthermore, control of what happens further down the provider chain is not something that automatically can be assumed; this should be clear even from the simple examples we have provided.

4 Accountability in Cloud Ecosystems

Recent research has identified basic features of an accountability-based approach [5], and has highlighted the complexity of accountability [6]. Different definitions of accountability have been proposed (e.g. see [5–8] for relevant discussions on accountability). This paper is concerned with the problem of supporting and achieving accountability in practice. The following definition captures a shared understanding of accountability based on reviewing previous related work and discussion within the Cloud Accountability Project:

Conceptual Definition of Accountability: *Accountability consists of defining governance to comply in a responsible manner with internal and external criteria, ensuring implementation of appropriate actions, explaining and justifying those actions and remedying any failure to act properly.*

Governance here is the processes which devise ways of achieving accountability. The conceptual definition of accountability encompasses different understandings drawn from different disciplines. It is intentionally generally applicable across different domains. Further to this generic definition, we tailor the conceptual definition of accountability to data protection in the cloud. Thus, the following definition contextualises the notion of accountability (i.e. Conceptual Definition of Accountability) and makes it relevant to the problem of data governance in the cloud.

Definition of Accountability for Data Stewardship by Cloud Services: *Accountability for an organisation consists of accepting responsibility for the stewardship of personal and/or confidential data with which it is entrusted in a cloud environment, for processing, storing, sharing, deleting and otherwise using the data according to contractual and legal requirements from the time it is collected until when the data is destroyed (including onward transfer to and from third parties). It involves committing to legal and ethical obligations, policies, procedures and mechanisms, explaining and demonstrating ethical implementation to internal and external stakeholders and remedying any failure to act properly.*

Fig. 5. Accountability attributes, practices, mechanisms and tools

The definitions highlight the main conceptual aspects of accountability. They characterise the necessary practices emerging in organisations that take an accountability-based approach (with respect to specific attributes of accountability). An analysis that deconstructs the accountability definitions highlights a model consisting of *accountability attributes*, *practices*, *mechanisms and tools*. Figure 5 shows how they form together a model of accountability for cloud ecosystems.

The central elements of this model are:

- **Accountability attributes** – conceptual elements of accountability as used across different domains (that is, the conceptual basis for our definition, and related taxonomic analysis)
- **Accountability practices** – emergent behaviour characterising accountable organisations (that is, how organisations operationalize accountability or put accountability into practices)
- **Accountability mechanisms and tools** – diverse mechanisms and tools that support accountability practices (that is, accountability practices use them).

5 Legal Perspectives of Data Protection in Cloud Ecosystems

The Data Protection Directive [12] lays down rules for the processing of personal data and recognizes specific rights of individuals on their personal data, while ensuring that such data can move freely within the internal EU market. When data can be linked directly or indirectly to an individual (the so-called data subject) they qualify as personal data. Only data that are truly anonymous are excluded from the provisions of the Directive [13]. Great amounts of information can be found in cloud ecosystems, some of which qualifies as personal data, while some does not. When information in cloud ecosystems refers to an identified or identifiable natural person, then the Data Protection Directive may apply. Important territoriality issues arise, which will not be further discussed within this work.

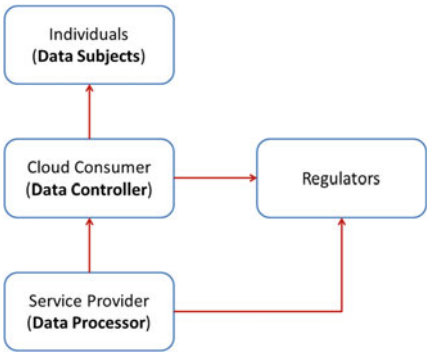

Fig. 6. Data subject, controller, processor and regulator

The European data protection legal framework distinguishes between two principal actors (besides the data subjects): the data controller and the data processor. The data controller is the one who defines the means and the purposes for the processing of personal data, while the data processor carries out the processing on behalf of the controller. This distinction is of great importance as the data controller (and not the data processor) is the party who carries the obligations described in the Data Protection Directive and also the party required to define the details of the data processing. Cloud computing raises significant challenges in identifying who are the responsible entities, in order to assign accountability obligations, since usually multiple actors are involved. Figure 6 shows an example of accountability relationships for cloud ecosystems drawn from a data protection viewpoint (note that other relationships creating different governance models are possible too).

The Directive contains general principles for processing personal data that have to be respected, which balance the interests both of data controllers and of data subjects [14]. These principles include fairness and data quality (data should be correct and up-to-date), purpose specification and use limitation (data may only be processed for previously specified purposes), and legitimate ground (processing must be based for instance on user consent, a contract, a legal obligation, or vital interest of the data subject). Of special importance is the principle that the design of data-processing systems be aimed at processing either no personal data at all or as little as possible (data avoidance and data minimisation) [15]. Consent will often be the legal basis for processing personal data in cloud computing, but special attention must be paid to the processing of health and medical data: the processing of these is in principle prohibited, unless special grounds apply. Figure 4 (in Sect. 3) shows an example in which the cloud providers collect and process personal data of persons, who in many cases are also patients. In such cases, the rules on the protection of sensitive data have to be taken into account, with attention for the special requirements that relate to health and medical data [11].

The Data Protection Directive also addresses the issue of data security, imposing a statutory obligation on data controllers to ensure that personal data are processed in a secure environment. Moreover, the Directive contains rules for the transfer of personal

data to third countries, an issue of great importance in all trans-border applications. The transfers of data between cloud computing providers, which are located in different countries, raise issues on the trans-border flows of personal data. Specifically, questions arise on the entities that have to take into account data protection from the design of the system and on who is responsible for the integrity and security of the data. Especially when several providers are involved in applications that transfer personal data of users in a way that leaves the control of the developer of the system, the identification of the responsible parties becomes difficult [17]. The European Commission has proposed the replacement of the Directive with a Regulation, which aims at ensuring a consistent level of protection for individuals among the 27 European Member States and at providing legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises [16]. Although the draft General Data Protection Regulation will take several years before coming into effect, developers of cloud computing systems and applications have to take into account the envisaged amendments and changes in order to make sure that they will comply with the future legislation as well. The draft Regulation introduces the concept of joint controllers and creates stricter accountability obligations for data processors. Of particular relevance are requirements to implement 'data protection by design and by default' and to execute Data Protection Impact Assessments for all operations that present specific risks.

6 Discussion and Concluding Remarks

This paper highlights accountability as an enabler for cloud ecosystems. In order to make accountability meaningful, it is useful to distinguish between accountability attributes, practices, mechanisms and tools. Figure 7 illustrates the contextual relevance of the accountability (in terms of the model basics, i.e. attributes, practices,

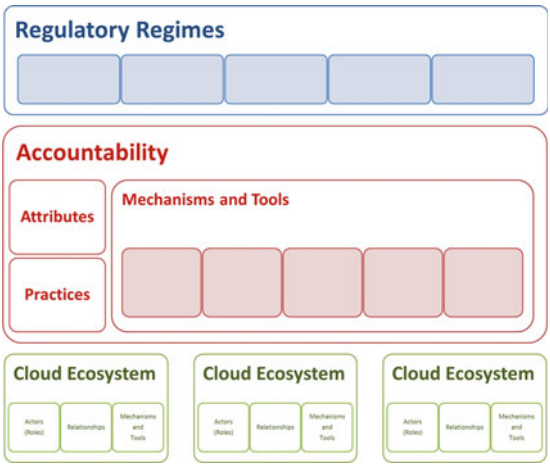

Fig. 7. Accountability context

mechanisms and tools) between cloud ecosystems with respect to regulatory regimes (e.g. Data Protection Directive).

The attributes of accountability identify relevant concepts, e.g. responsibility, liability and transparency, that support accountability (other attributes can be observability, verifiability and attributability). Accountability practices concern different operational aspects of cloud ecosystems. That is, despite the supporting elements, accountability practices differ across cloud ecosystems. Emerging relationships among attributes and practices of accountability, supported by specific mechanisms and tools (e.g. technical tools like software implementing security controls and policies as well as legal mechanisms like sanctions), enable cloud ecosystems to position and comply with relevant regulatory regimes. This stresses an operational interpretation (that is, what work practices and other domain-specific factors show being accountable) of accountability in cloud ecosystems. The different attributes of accountability and their contextual practices enable various mechanisms and tools in cloud ecosystems.

The emerging accountability model enables the analysis of accountability relationships among cloud actors. The attributes of accountability (e.g. responsibility, liability and transparency) highlight accountability relationships among cloud actors. The analysis of such accountability attributes enables us to understand how accountability relationships emerge in cloud ecosystems. For instance, let us consider responsibility in order to analyse emerging relationships among cloud actors. A Cloud Service Provider (CSP) is responsible to its customers, as specified in contracts between them, for the way personal data are stored and managed. Similarly, the CSP is responsible to Data Protection Authorities (DPAs) to comply with data protection legislation – the extent of such responsibility varies depending on the CSP's role in managing personal data. Each CSP's employee is responsible to the provider (employer), but not directly to Customers and DPAs. This is an example of how the elements of accountability enable us to analyse emerging relationships among cloud actors. Different accountability relationships emerge among actors in cloud ecosystems. Chains of accountability consist of the sets of relationships existing between any two actors in a cloud ecosystem. The characterization of accountability and the analysis of the emerging relationships among actors allow us to identify opportunities (in terms of mechanisms and tools) to support accountability in cloud ecosystems. Our accountability characterization of cloud ecosystems involves the identification of the main actors and the analysis of their relationships with respect to the attributes of accountability. The emerging accountability model enables cloud ecosystems that need to comply with regulatory regimes constraining their application domains. It supports diverse mechanisms and tools throughout chains of accountability relating actors one another.

In conclusion, this paper has discussed the problem of data governance and protection in cloud ecosystems. The problem has been explained from two different viewpoints: a technical one discussing emerging threats affecting data governance in cloud ecosystems, and a legal one highlighting the complexity of the EU Data Protection Directive constraining the provision of cloud services. This paper is concerned with addressing both perspectives by supporting accountability in cloud ecosystems. The paper has introduced a model of accountability in the cloud that enables diverse mechanisms and tools, which support organisational practices for being accountable.

Acknowledgments. This work has been partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD – http://www.a4cloud.eu/) Cloud Accountability Project. Figure 2 Threats in a Cloud Ecosystem is taken from a presentation by Siani Pearson. Figure 4 Example of data flows in a cloud ecosystem is based on original by Karin Bernsmed. We also would like to thank the contributions to the accountability conceptual framework of our partners within the Cloud Accountability Project: Daniele Catteddu, Giles Hogben, Amy Holcroft, Theofrastos Koulouris, Ronald Leenes, Christopher Millard, Maartje Niezen, David Nuñez, Nick Papanikolaou, Siani Pearson, Daniel Pradelles, Chris Reed, Chunming Rong, Jean-Claude Royer, Dimitra Stefanatou, Vasilis Tountopoulos, Tomasz Wiktor Wlodarczyk.

References

1. European Commission: Advances in Clouds – Research in future cloud computing. Expert Group Report, Public version 1.0. European Union (2012)
2. ENISA: Cloud computing: benefits, risks and recommendations for information security. European Network and Information Security Agency (2009)
3. Mell, P., Grance, T.: The NIST Definition of Cloud Computing. NIST Special Publication 800-145 (2011)
4. Article 29 Data Protection Working Party: Opinion 3/2010 on the principle of accountability, 00062/10/EN WP 173 (2010)
5. The Galway Project: Accountability: A compendium for stakeholders. The Centre for Information Policy Leadership (2011)
6. Guagnin, D., et al. (eds.): Managing Privacy Through Accountability. Palgrave Macmillan, Basingstoke (2012)
7. Weitzner, D.J., et al.: Information accountability. Commun. ACM **51**(6), 82–87 (2008)
8. Pearson, S.: Toward accountability in the cloud. IEEE Internet Comput. **15**(4), 64–69 (2011)
9. Stilgherrian: Collateral damage in the copyright wars. http://www.abc.net.au/unleashed/3787384.html. Accessed June 2013
10. Bennett, C., Molnar, A., Parsons, C.: Forgetting, Non-Forgetting and Quasi-Forgetting in Social Networking: Canadian Policy and Corporate Practice. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2208098. Accessed 28 Jan 2013
11. Dumortier, J., Goemans, C.: Legal challenges for privacy protection and identity management. In: Jerman-Blažič, B., Schneider, W., Klobučar, T. (eds.) Security and Privacy in Advanced Networking Technologies. NATO Science Series, III: Computer and Systems Science, vol. 193, pp. 191–212. IOS Press, Amsterdam (2004)
12. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281, 23 Nov 1995, pp. 0031–0050 (1995)
13. Kuner, C.: European Data Protection Law – Corporate Compliance and Regulation, p. 51. Oxford University Press, Oxford (2008)
14. Walden, I.: Privacy and data protection. In: Reed, C., Angel, J. (eds.) Computer Law: The Law and Regulation of Information Technology, 7th edn. Oxford University Press, Oxford (2011)
15. Holznagel, B., Sonntag, M.: A case study: the JANUS project. In: Nicoll, C., Prins, J.E.J., van Dellen, M.J.M. (eds.) Digital Anonymity and the Law – Tensions and Dimensions, Information Technology and Law (No. 2). TMC Asser Press, The Hague (2003)

16. Proposal for a General Data Protection Regulation, COM (2012) 11 final, 25 January 2012
17. Löhr, H., Sadeghi, A.-R., Winandy, M.: Securing the e-health cloud. In: Veinot, T. (ed.) Proceedings of the 1st ACM International Health Informatics Symposium (IHI'10), pp. 220–229. ACM (2010)
18. Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, 01037/12/EN, WP196 (2012)

Introducing Life Management Platforms and Collaborative Service Fusion to Contextual Environments

Mario Hoffmann[1(✉)] and Pekka Jäppinen[2]

[1]Fraunhofer AISEC, Garching, Germany
mario.hoffmann@aisec.fraunhofer.de
[2]Lappeenranta University of Technology, Lappeenranta, Finland
pekka.jappinen@lut.fi

Abstract. The approach presented in this position paper aims at collaborative service fusion and provisioning in user-centric environments in the future Internet of People, Things, and Services (IoPTS). Our approach connects dynamic gathering of user requirements and feedback with community based service fusion in any phase of a service life cycle. These highly adaptive services allow agile service creation and exploitation embedding the users by fusing his or her cloud based daily activities within intelligent environments. We propose two fundamental new building blocks: On the one hand a life management platform in our approach empowers users to manage service fusions, profiles, and access policies in a secure, trustworthy and unified way increasing their independency, privacy and possibilities to manage lives after personal priorities by personalized information flow. On the other hand the introduction of a service fusion engine supports automated access to personal consumer data and requirements for specifically authorized services and market places. Note: We think that with respect to recent discussions on profiling citizens and consumers user control and consent need to be re-balanced. As such the proposed life management platform is supposed to enable users to manage personally identifiable information.

Keywords: Life management platforms · Personal clouds · Service fusion · Contextual environments · Security and privacy by design · Identity management

1 Introduction

According to Gartner, the top ten strategic technology trends for 2013 comprise "Personal Cloud", "Hybrid IT and Cloud Computing", and "Integrated Ecosystems". One of the top ten critical tech trends for the next five years is "Hybrid cloud services". Gartner says combinations of private and public clouds will be composed of services from multiple providers. Private clouds improve agility and will dominate. Gartner expects that you could end up with hybrid environments with dozens of specialty providers. A second trend that is already visible today is the widespread

M. Felici (Ed.): CSP EU FORUM 2013, CCIS 182, pp. 41–52, 2013.
DOI: 10.1007/978-3-642-41205-9_4,

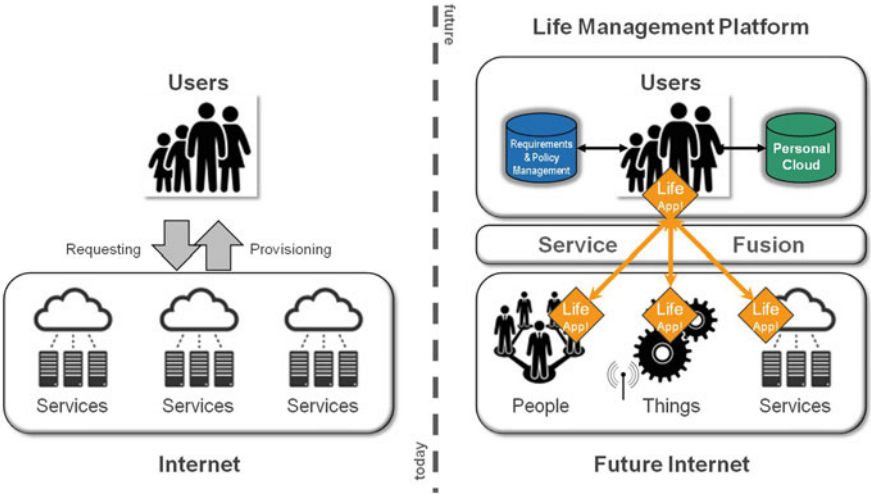

Fig. 1. Life management platform and service fusion in future internet

adoption of "app"-based application development and distribution models that couple inexpensive or free applications with a simple model for acquisition, installation and maintenance of applications. According to Flurry Analytics, end users of Apple iOS- and Android-based mobile devices downloaded more than 1.76 billion new applications onto their devices in the Christmas holiday week of 2012 alone [1]. More generally, the number of Internet-connected devices is also growing at a rapid pace: estimates by network infrastructure and service manufacturer Cisco estimate the number of Internet-connected "things" at the end of 2012 to be 8.7 billion and expect this number to grow to 50 billion by 2020 [2, 3].

We are heading for designing, developing and putting into operation cloud-based as well as mobile operated services in such a way that it enhances the life of end-users on their way into an ambient lifestyle, in which they have to deal with hundreds of sensors and actuators in contextual environments. We propose a platform that connects dynamic gathering of user requirements with community based service creation in every phase of a service lifecycle resulting in highly adaptive services. The two key components, namely a life management platform as well as a service fusion engine, are shown in Fig. 1.

2 Contextual Environments

The following use case illustrates central challenges for our framework and will be used as a template for evaluation and requirements elicitation as well as a basis for further technical developments. The use case refers to an international hotel where different visitors (a businessman as well as a family on vacation) discover both seamless support by the Life Management Platform (LMP) as well as direct and user induced service fusion. The use case is just an example. Further application scenarios from Automotive, Ambient Assisted Living, and Social Networks will be investigated in future research.

2.1 Use Case Example

Time 17:00–18:00: Frank enters his hotel room. It has been a long day at the conference where he has been in contact with many new potential investors and networking contacts. When he enters the room, his LMP connector (e.g. an app on his tablet or mobile phone) already on his way up to the hotel room has been in contact with the hotel services and has personalized his room. The curtains are half open, the lights are off and the television has his favorite TV channels in the sequence he prefers. The new contacts' personal cards as well as additional personal information has been exchanged and synchronized directly with the LMP backend. Figure 2 below illustrates the seamless service fusion taking place in this situation.

Note: What kind of organization serves as a host for a LMP is, indeed, an important question. Probably service providers of social and business networks would consider themselves as LMP providers already. Alternatively, LMPs could be provided by your company, your city, an independent institution such as a data protection office or association, and, finally, self-hosted at home.

Time 18:00–19:00 in another room at the hotel: Family Frost's members, Allen, Mary, Louise and Peter immediately sat down on the two king-size beds in the hotel room. They had been travelling for more than 10 h and were exhausted. Similar to the process above the room was personalized to the family preference profile. During the flight it became evident that Louise (aged 10) was not feeling so good. The sensors in her blouse had the last hours read that her temperature was a bit higher than usual and that the body stress also was higher. Mary could read this on her tablet since Louise and herself shared the personal information on Louise. As a result of the readings, the LMP and the hotel services system offered Mary the possibility to have somebody from the hotel go to the pharmacy nearby to buy some medication for Louise to make her feel better. Meanwhile Peter was getting hungry. So Allen and Peter studied the hotel's menu card. Peter suffered from severe nut allergies, and the hotel menu had already taken that into account when offering the family as such a selection of their preferred dishes and drinks.

Time 22:00–24:00 in Frank's room: Frank was now back in the room after dinner and a social gathering at the conference. However, he was not feeling tired and after a talk with his wife at home, he decided to watch a movie – simultaneously with her. They could choose for example to watch a recommended movie from the hotel

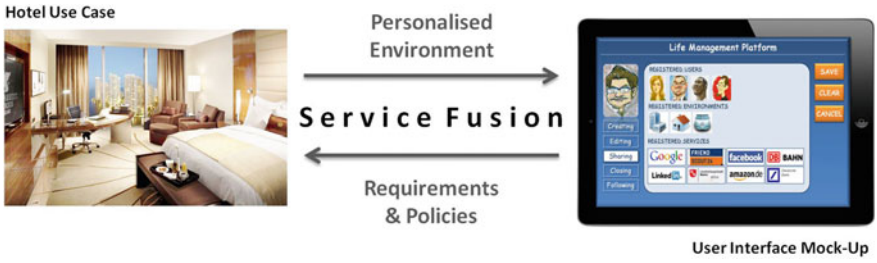

Fig. 2. Seamless service fusion and life management platform

services or from their common cloud movie service. Sharing of a hotel movie with a person outside the hotel was not a problem but would cost a small fee. After a little talk they decided to watch a comedy and kept their templates open for a personal chat.

Three days after: Frank was leaving the hotel after a really good conference. In the lobby he met the Frosts that he had seen several mornings for breakfast. Louise was feeling much better and the family had a tremendous good vacation. As soon as everybody checked out, the private data, preferences and personal information was removed from the hotel data bases leaving only necessary contact information.

Note: The integration of LMPs and service fusion in such application scenarios relies on service providers who act according to data protection laws and respect policies and purposes attached to personally identifiable information (PII). We observed that most service providers (whose business model does not rely on selling PII) are not reluctant against integrating privacy preserving technologies but configuration is still much too time consuming and complex.

2.2 Implications

The intuitive hotel scenario above has shown several use cases how hotel guests could benefit from dynamic and (semi-)automated matching of preferences and needs with available contextual services. Hotel rooms have been set up according to personal preferences, healthcare for the ill daughter has been suggested, restaurant menus have been adapted to intolerances and allergies, and services can be even shared with people outside. These are all examples of seamless service fusion between the personalized LMP management profiles and the hotel as a service provider (in this case) – see Fig. 3.

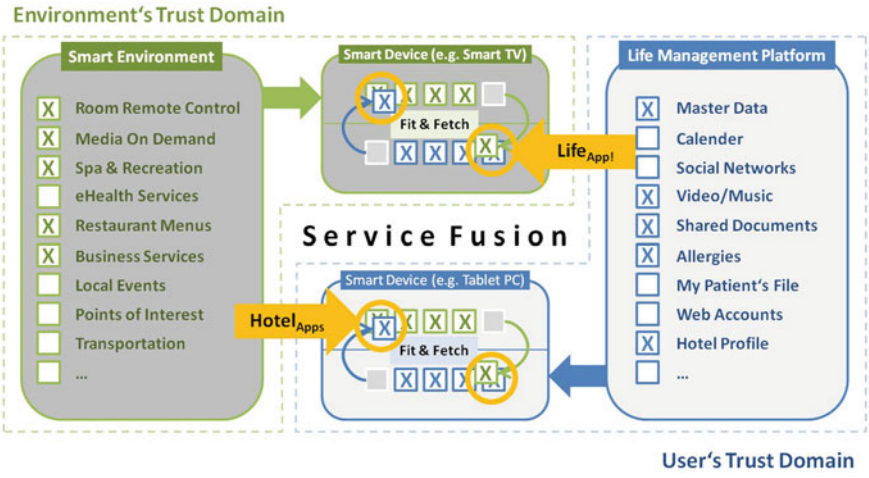

Fig. 3. User induced service fusion

Major implications comprise: (1) Interoperability of services of different domains and contexts, (2) transparency and usability taking end-users into account (and their small willingness to deal with privacy configurations), (3) balancing protection goals including confidentiality, integrity, and availability, and (4) considering limitations, e.g. in protecting personally identifiable information once the information itself has been disclosed.

3 State of the Art

3.1 Personal Information and Life Management Systems

Current Internet services such as the Amazon web store gather personal information via registration and monitoring of user behaviour in the service. This information is stored in the company services databases. Companies that provide third parties with access to their identity management platform usually do so by providing an authentication interface to their centrally managed services. Examples for this at the time of writing include authentication services provided by Facebook, Twitter and Google.

Federated and distributed user identity and profile management approaches do not rely on centralized provisioning of user identity and profile information. The Digital.me project uses a personal server approach, where data is fetched from users' personal server and the access can be controlled from computer or mobile phone. Jäppinen developed the mobile phone-based personal data storage concept ME, which was enhanced by Oyomno into ME2.0 [4, 5]. The recently established FutureID FP7 project is concerned with the development of a European identity management infrastructure that is privacy-aware, trustworthy, accountable, ubiquitously applicable and usable. It focuses exclusively on establishing a generically applicable infrastructure.

Digital identity today offers federated authentication and domain to domain authorization using mechanisms such as OAuth 2.0 [6]. In a multiparty interaction where users' data are being exchanged, it is often essential to guarantee users' awareness and consent and such mechanism is offered by User Managed Access (UMA) - a profile of OAuth 2.0 [7]. The evolvement of cloud computing opens up opportunities for leveraging complex digital identity ecosystem and at the same time brings up challenges such as privacy [8], large scale attack vectors [9] etc. scaling up to a degree that requires to go beyond state of the art in order to tackle and prevent such vulnerabilities.

The ABC4Trust (Attribute-based Credentials for Trust) project addresses the federation and interchangeability of technologies that support trustworthy yet privacy-preserving Attribute-based Credentials. In contrast to present solutions, this project focuses on revealing minimal information of the user required by the application, without giving away full identity. The recently started CloudSpaces project focuses on personal clouds and addresses service provisioning for personal clouds and privacy-aware data sharing in the personal cloud domain. Bussard and Pinsdorf describe the need for a lifecycle model for data privacy in service ecosystems [10].

3.2 User-Initiated Service Creation, Adaptation and Fusion

Web2.0 tools have enabled users to become content providers already. Zhao takes this user generated content into the next level: User generated services [11, 12]. According to Zhao current tools and platforms make it possible for technology-oriented users to become developers. This view was also acknowledged by the eMobility Technology Platform in its view on the Future Internet [13, 14]. Thus a user centric approach that allows consumers to have more control on contextual and personal information flow is needed. Different Mashup tools like YahooPipes or Omelette, an FP7 project, represent semi-automatic tools. Although end-user engagement is one objective of Omelette, it does not link users and developers together as a LMP aims to do. The FP7 project Socios addresses social networking but it misses the user created service aspects.

Future trends include semantics, context-awareness, revenue sharing (new business models) as well as trust and privacy issues as enabling technologies for user generated services. The LMP deals with these issues but emphasizes a bit more of the social co-creation aspects than everybody-as-developer approach. This approach is supported by Hyrynsalmi et al. [15]. In Schultz et al. the role of developers has been studied [16]. Two aspects, direct user needs and new business models (pricing of applications) are seen extremely important for successful service creation. In Kim et al. the developer perspective is further studied [17]. In addition to the economic (business model) and social (user needs) elements the authors emphasize the meaning of suitable software and tools.

A number of research projects have addressed service creation, adaptation and fusion in different forms in recent years. The SPICE project developed, prototyped and evaluated an extendable overlay architecture and framework to support easy and quick service creation, test and deployment, especially focusing on 3G beyond and IMS network infrastructures. The COMPOSE project focuses on providing services that combine real and virtual worlds through the convergence of the Internet of Services with the Internet of Things.

4 A New Service Ecosystem

Our framework aims at accelerating service development in the future Internet of People, Things, and Services by having direct links from user needs into the development cycle. Development is guided by an agile development process resulting in contextual services. The use of the services is managed by the Life Management Platform. The overall concept is presented in Fig. 4.

The App and Service Continuum consists of four pillars: (1) Life Management Platform, (2) Personalized Dashboard, (3) Smart Services Infrastructure, and (4) AppContinuum. The pillars are topics of R&D on their own, the integration and interworking is the key achievement. Through the Life Management Platform we envisage a user controlled provisioning of requirements and personalizable information. Service fusion brings together the information across clouds, and uses it through a dynamic adaptation process to generate personalized and contextual services. The

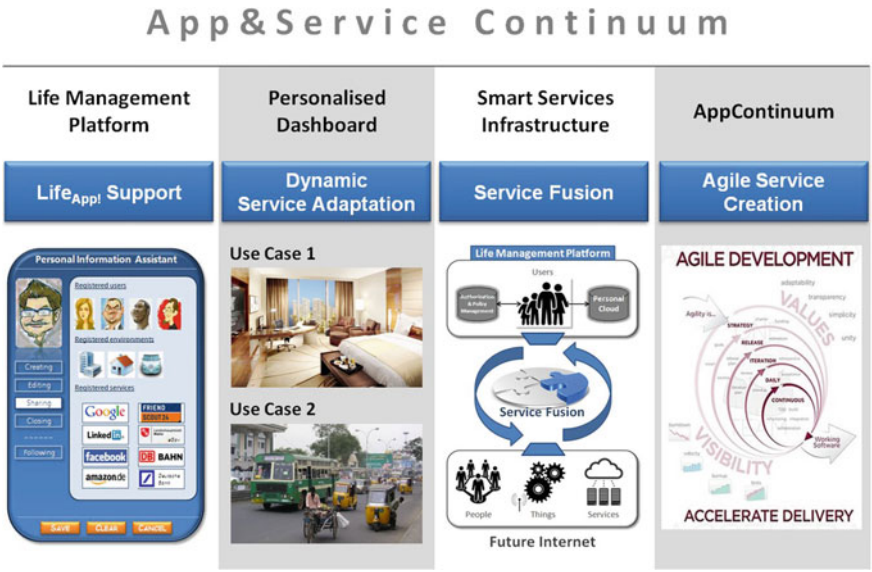

Fig. 4. App and service continuum

App and Service Continuum enables the agile development of services and creates the business incentives for contributors to this new ecosystem.

4.1 Life Management Platform and $Life_{App!}$ Support

The Life Management Platform is characterized by the introduction of a so called $Life_{App!}$. This supports the approach of – instead of only sending unprotected profile information to a service provider – providing an app for downloading figuratively him- or herself. This app, the $Life_{App!}$, contains not only the required subset of profile information and preferences but also policies for their usage and validity.

Prospects for the user: The user mainly benefits from transparency and user centric control mechanisms. This includes for example purpose binding, i.e. the user is basically able to monitor and control that his or her data is only used for the service(s) intended. Further, it is possible to control the life cycle of the information provided. This is important to be able to grant and revoke access rights depending on context changes. Note: Since many users are not interested in monitoring and analyzing usage of personally identifiable information by themselves the security model allows delegating compliance to privacy to independent and trusted third parties.

Prospects for the service provider: Trustworthy communication between the user's frontend and the service backend is secured by the $Life_{App!}$. In the service provider's infrastructure the $Life_{App!}$ runs in an isolated and trusted execution environment. The $Life_{App!}$ receives updates performed in the user's Life Management Platform in real-time, profile information is always up-to-date, inconsistencies can be avoided. The

$Life_{App!}$ is, finally, supposed to be open to integrate compliance rules such as technical implementations to fulfill data protection laws or provider‘s security policies. So, all information and components necessary to maintain and control the information life cycle are coherently consolidated at one place, the $Life_{App!}$. More information about the Life Management Platform can be found in [18].

4.2 Personalized Dashboard and Service Fusion

The Personalized Dashboard is the main multimodal user interface to personalize the environment through contextual and global services. It illustrates the user‘s options which kind of user managed services are interoperable to interfaces provided by other people, things, and services. The Personalized Dashboard is the user’s frontend and interface to the Life Management Platform. The dashboard can be realized on PCs, tablets, smartphones or even Smart TVs or automotive head-up displays.

4.3 Smart Services Infrastructure and Dynamic Service Adaptation

The services, both contextual ones being provided by the environment as well as global ones being provided through the AppContinuum, are available on the Dashboard, and can there be combined together with the personal services of the user to form the requirements and recommendations for service adaptation. The user interaction itself is performed through the graphical interface on the Dashboard, but it relies on a semantic service description allowing the dynamic adaptation of services. Thus a graphical combination of two services either in form of a sequential order or in a logical combination of services is going to be translated into service adaptation, chaining and orchestration, performed in the Service Fusion Engine.

4.4 AppContinuum and Agile Service Creation

The AppContinuum is the main business incentive for contributors to the ecosystem. Not only can hotels or travel companies provide their own and specific service offers to their customers, these service offers can be enhanced through globally available services. While a bus company may offer trip and connectivity information, the service might be enhanced through augmented reality and translation services. Thus, being able to provide services on top of a rather traditional infrastructure is the key driver for business opportunities. The AppContinuum will make the services globally available and adaptable for other environments, thus going beyond the limitations of current AppStores. The feedback provided by the AppContinuum will stimulate agile service creation. Reports on usage pattern, non-fulfilled or partly fulfilled service adaptations will be made available to the developer community in near real-time, opening for service development combining adaptive methods and flexible AppStore components to answer the service adaptation needs.

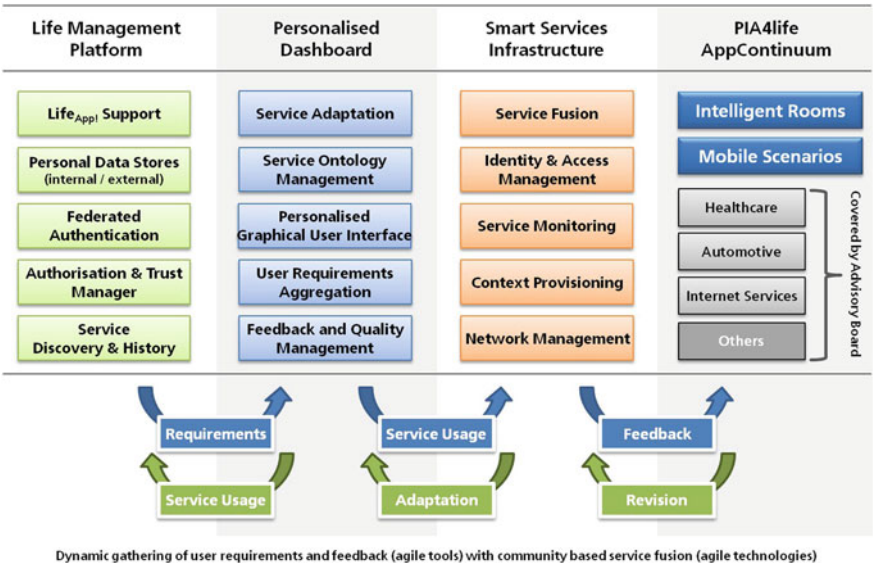

Fig. 5. Framework building blocks

5 Framework Building Blocks

The building blocks for the **Life Management Platform** summarized in Fig. 5. Life$_{App!}$ are supposed to support users (or authorized trusted third parties) to monitor and control sensitive information. Sensitive information will be stored confidentially and securely at internal and external Personal Data; here LMP will rely on Personal Cloud concepts and end-to-end encryption. Federated authentication is the next building block [19, 20]. The user, basically, will have the choice between three authentication mechanisms: (1) OpenID Connect,[1] (2) SIM-based authentication, and (3) eID-based authentication (e.g. Germany's new ID card). Most promising candidates for authorization & trust management are: Kantara's User Managed Access (UMA[2]) protocol, OAuth2.0,[3] U-Prove[4] technology, and the Higgins 2.0[5] framework.

Another building block is Service Adaptation. That means that the consumer has always specifically tailored access to dynamically orchestrated contextual services from other users, the ambient environment or service providers. Service adaptation is basically based on the fact that user requirements, embedded for example in preferences or given as direct feedback, are analyzed in the Service Monitoring component

[1] http://openid.net/connect/
[2] http://kantarainitiative.org/confluence/display/uma/Home
[3] http://oauth.net/2/
[4] http://research.microsoft.com/en-us/projects/u-prove/
[5] http://eclipse.org/higgins/

in a privacy preserving way. This feedback is then anonymously fed back into the developer community in order to fulfill the agile development life cycle process.

Finally, the third challenge is addressing Service Fusion. Through a graphical interface the user is able to select in drag and drop manner the source and type of information that will be given to the service. The service fusion engine, then, is responsible that this contextual information coming from users, the environment or services will be analyzed and merged. Much like the engines behind modern desktop environments, the service fusion engine has to recognize whether or not the provided information fits for the given service [21].

6 Discussion

The Life Management Platform inverts the relationship between service providers and users through the concept of the $\text{Life}_{\text{App!}}$. The $\text{Life}_{\text{App!}}$ effectively turns service providers into consumers of the end-user's $\text{Life}_{\text{App!}}$ This enables the end user to maintain control of her personal data and it frees service developers from having to rely on central identity and life management provisioning from commercial entities.

The next generation of digital identity ecosystem will require a number of aspects that the state of the art does not offer today. First, the scales of such ecosystems today require adopting billions of users (e.g. facebook). As an after-math of that such a system is generating an enormous amount of data (often referred as "big data") and the volume continues to grow. Therefore, the next generation identity ecosystem should have an autonomous capability of self-evolvement. Another important aspect would be, the business intelligence inferred from its data, because this will allow customizing services for the end users. Finally, it has to have a built-in robustness against large scale attacks and protecting the privacy of the users.

The current state-of-the-art in service creation, adaptation and fusion emphasize the increasing role of end users in the service creation loop, intuitive and self-adaptive tools as well as business models supporting co-creation of services. Many elements required for accelerated service development have been researched and implemented in past projects. Semantics, context-awareness, user and service profiling, user interfaces as well as trust and privacy issues in service creation and adaptation have all been extensively studied during the past years. The current trend of extending user generated content into user generated services requires, however, extensive combination of existing and development of new solutions. Three novel aspects characterize Life Management Platforms: First of all, end users are tied closely to the service development loop. The Dashboard provides users a way to adapt and fusion their own services and makes it possible to collect direct user needs for the actual developer community. Second, new revenue sharing business models between end-users and the open developer community make social service co-creation possible. Third, the Life Management Platform and service fusion engine combine many existing elements for service creation and exploitation and as such make the creation, adaptation and fusion of new services easier.

7 Future Research

Our approach of introducing Life Management Platforms and collaborative service fusion to contextual environments emphasizes strong user engagement in service fusion. The main idea is that existing services are orchestrated for new service offerings. If existing services cannot be fused, then user needs are recorded and submitted to the developer community. Following this approach, unaddressed needs of users can be connected with those who are able to provide the implementation of the required services.

Our research proposal also emphasizes the adaptability of services through the Life Management Platform. The Life Management Platform is supposed to enable the secure and user-controlled use of personal profiles and personal information in service execution. The Life Management Platform will make it easier for developers to create new services taking security, privacy and trust aspects into account.

As a service-oriented platform, LMP will be capable of interacting with a very wide range of systems and services. Value added services can be distributed, then, throughout the Internet and can be hosted directly on smart or "smart-proxied" devices via Internet of Things middleware systems.

Acknowledgements. We would like to thank the following colleagues and institutions for their support and fruitful discussions: Jari Porras (Lappeenranta University of Technology), Knud Erik Skouby, Henning Olesen, Lene Tolstrup Sørensen (Aalborg University), Atta Badii (University of Reading), Olaf Drögehorn (Harz University of Applied Sciences), Josef Noll (Movation), Mervi Himanen (Digital Living Finland Oy), Karsten Vandrup (SIA Latvisoft), and Sudhir Dixit (Hewlett Packard India).

References

1. Farago, P.: Holiday 2012 Delivers Historical Worldwide App Downloads, Flurry Blog. http://blog.flurry.com/
2. Evans, D.: The Internet of Things. How the Next Evolution of the Internet is Changing Everything. Cisco Whitepaper. http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (2011)
3. Soderbery, R.: How Many Things are Currently Connected to the "Internet of Things" (IoT)? Forbes Magazine Online. http://www.forbes.com/sites/quora/2013/01/07/how-many-things-are-currently-connected-to-the-internet-of-things-iot/
4. Jäppinen, P.: ME - Mobile electronic personality. Doctorate Thesis, Lappeenranta University of Technology (2004)
5. Oyomno, W.: Usable privacy preservation in mobile electronic personality. Doctorate Thesis, Lappeenranta University of Technology (2012)
6. Hardt, D.: The OAuth 2.0 Authorization Framework. IETF, October 2012
7. Hardjono, T.: User-Managed Access (UMA) Profile of OAuth 2.0, IETF draft, 27 December 2012
8. Bertino, E., Paci, F., Ferrini, R., Shang, N.: Privacy-preserving digital identity management for cloud computing. IEEE Data Eng. Bull. **32**, 21–27 (2009)

9. Riquet, D., Grimaud, G., Hauspie, M.: Large-scale coordinated attacks: impact on the cloud security. In: 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp. 558–563, 4–6 July 2012
10. Bussard, L., Pinsdorf, U.: Abstract privacy policy framework: addressing privacy problems in SOA. In: Camenisch, J., Kesdogan, D. (eds.) iNetSec 2011. LNCS, vol. 7039, pp. 104–118. Springer, Heidelberg (2012)
11. Zhao, Z., Laga, N., Crespi, N.: A survey of user generated service. In: Proceedings of IC-NIDC2009 (2009)
12. Zhao, Z., Laga, N., Crespi, N.: The incoming trends of end-user driven service creation. In: Telesca, L., Stanoevska-Slabeva, K., Rakocevic, V. (eds.) DigiBiz 2009. LNICST, vol. 21, pp. 98–108. Springer, Heidelberg (2010)
13. Jäppinen, P., Guarneri, R., Correia, L.M.: An applications perspective into the future internet. J. Netw. Comput. Appl. **36**(1), 249–254 (2013)
14. Guarneri, R., Jäppinen, P. (eds.): Strategic Applications Agenda, v.3.01, Future Internet E-Mobility, Working group on Leading edge applications (2010)
15. Hyrynsalmi, S., Mäkilä, T., Järvi, A., Suominen, A., Seppänen, M., Knuuttila, T.: App store, marketplace, play! - an analysis of multi- homing in mobile software ecosystem. In: Proceedings of IWSECO 2012 (2012)
16. Schultz, N., Wulf, J., Zarnekow, R., Nguyen, Q.-T.: The new role of developers in the mobile ecosystem: an Apple and Google case study. In: Proceedings of the 15th International Conference on Intelligence in Next Generation Networks, pp. 103–108 (2011)
17. Kim, H., Kim, I., Lee, H.: The success factors for app store-like platform businesses from the perspective of third-party developers: an empirical study based on a dual model framework. In: Proceedings of Pacific Asian Conference on Information Systems 2010, pp. 272–283 (2010)
18. Hoffmann, M.: An app approach towards user empowerment in personalized service environments. In: Lau, K.-K., Lamersdorf, W., Pimentel, E. (eds.) ESOCC 2013. LNCS, vol. 8135, pp. 149–163. Springer, Heidelberg (2013)
19. Hansen, M.: Top 10 Mistakes in system design from a privacy perspective and privacy protection goals. In: Camenisch, J., Crispo, B., Fischer-Hübner, S., Leenes, R., Russello, G. (eds.) Privacy and Identity 2011. IFIP AICT, vol. 375, pp. 14–31. Springer, Heidelberg (2012). http://www.csc.kth.se/∼buc/PPC/Slides/marit.pdf
20. Rost, M., Bock, K.: Privacy by design and the new protection goals. Datenschutz und Datensicherheit **35**, 30–35 (2011). https://www.european-privacy-seal.eu/results/articles/BockRost-PbD-DPG-en.pdf
21. Hämäläinenm, A., Jäppinen, P., Porras, J.: Service characteristics for service selection. In: Fourth International Conference on COMmunication System software and middlewaRE (COMSWARE), Trinity College Dublin, Ireland, 16–19 June 2009

Security and Privacy Management

Integrating Advanced Security Certification and Policy Management

Michele Bezzi[1], Ernesto Damiani[2], Stefano Paraboschi[3(✉)], and Henrik Plate[1]

[1] SAP Global Research and Business Incubation, 805 Avenue Dr M. Donat, 06250 Mougins, France
{michele.bezzi, henrik.plateg}@sap.com
[2] Universitá degli Studi di Milano, via Bramante 65, 26013 Crema, Italy
ernesto.damiani@unimi.it
[3] Universitá degli Studi di Bergamo, via Marconi 5, 24044 Dalmine, Italy
parabosc@unibg.it

Abstract. Recent models of software provisioning based on cloud architectures co-exist and interact with in-premises large and heterogeneous software ecosystems. In this increasingly complex landscape, organizations and users are striving to deal with assurance in all phases of software life cycle: acquisition, installation, use and maintenance. In this paper, we start by describing the notion of machine-readable security certificates, and discuss how they can be used for assurance-based software selection. Then, we introduce some models and tools for administrators for the automatic management of security policies, which include policy conflict detection. Finally, we discuss how these two approaches can be integrated for supporting organization to (semi-) automatically address the security requirements throughout the entire software life cycle.

Keywords: Service assurance · Security certification · Security policy management

1 Introduction

Recent models of software provisioning based on cloud architectures co-exist and interact with on-premises large and heterogeneous software ecosystems. One of the major differentiating factors between this scenario and traditional IT is the dynamic nature of cloud computing. In a cloud-based software ecosystem, thousands of services compete for being chosen by customers; also, customers' choices are usually short-term, in some cases coinciding with the duration of a single process instance. The ability of choosing services dynamically is perceived as a plus by users, because it enables them to select the "latest and best" services available, improving their productivity and competitiveness. However, the freedom of choice needs to be reconciled with the apparently conflicting requirement that customers carefully demand appropriate security controls when purchasing software systems. Such requirement cannot be ignored, as it is mandated by regulations like the United States Federal Information Security Management Act

M. Felici (Ed.): CSP EU FORUM 2013, CCIS 182, pp. 55–66, 2013.
DOI: 10.1007/978-3-642-41205-9_5,

(FISMA).[1] As early as 2009, the US General Services Administration (GSA) required that cloud computing services go through the formal approval process described in the National Institute of Standards (NIST) Special Publication 800-37. Unfortunately, NIST SP 800-37 process guidelines seem to assume a check-before-buy scenario, where software purchasers have a choice between multiple static systems they can evaluate against a set of acceptance criteria. The burden of going through a process like SP 800-37 can be alleviated if some accredited authority provides signed assertions (called *certificates*) regarding the security properties held by the entity (product, system, or services) to be purchased as well as the evidence supporting such assertions [1]. As we will discuss in Sect. 2, traditional security certificates are delivered as text documents to be read by human experts, like software buyers planning a purchase. Purchasers who choose certified entities rely on their security properties because they trust (i) the authority who signed the certificate attached to the entity and (ii) the evidence collection and assessment techniques the authority employed. In most cases, software systems are certified statically, i.e., by freezing their functionality and operational context. Once deployed, certified systems should be modified only under certain circumstances, lest their certification becomes invalid. Due to the dynamic nature of today's computing infrastructure (e.g., of clouds), this type of static certification cannot be used, since the infrastructure context will be constantly changing and invalidating static certificates. Given that static certifications can take months to produce, it is impractical to think that today's systems can be certified under this paradigm. Another approach that has been proposed is to trust technology suppliers (for instance, cloud providers) to collect and maintain all assurance information required by regulations like SP 800-37. This idea is based on the assumption that assurance evaluation is analogous to quality assessment, where certifications like ISO 9001 are periodically granted (and confirmed) to companies by accredited auditors. Between audits, customers trust their ISO-certified supplier's quality without considering changes that may have occurred from the last audit.

Unfortunately, this assumption is erroneous, because guidelines like the SP 800 series mandate software users to make sure that security properties hold *at the time of use*, rather than *at the time of certification*. This requirement is very difficult to satisfy in a cloud-based service marketplace, and in general with any dynamic software provisioning model.

In this paper we put forward the idea that without taking an entirely new perspective, complying with regulations when dynamically provisioning software (e.g. while accessing cloud services) may prove to be difficult or downright impossible, putting cloud customers working in highly regulated domains, like healthcare or the military, in the difficult dilemma of choosing between timeliness and assurance level.

Our perspective is based on two pillars: (i) a new generation of dynamic certificates, complemented by run-time monitoring and control (ii) accurate

[1] The FISMA Implementation Project was established in January 2003 to produce security standards and guidelines required by US legislation.

post-deployment monitoring of organization-specific configurations and security policies. Traditionally, security certificates have been manually written by security experts and administrators; here, we envision *online third parties* acting as authorities and taking part in dynamic certification and configuration control. After this introduction, we devote the next chapter by describing the notion of machine-readable security certificates, and briefly discuss how they can be used for assurance-based software selection (Sect. 2). Also, we provide a practical example of such certificates, focusing on test-based certification. Then, in Sect. 3 we introduce some models and tools for administrators for the automatic management of security policies, which include policy conflict detection. In Sect. 4 we discuss how these two pillars can jointly support organizations to (semi-) automatically address security requirements throughout the entire software life cycle. Finally, in Sect. 5 we draw our conclusions.

2 Toward Machine-Readable Security Certificates

Today, assurance evidence is collected by a wide range of formal, semi-formal, and informal evaluation methods, including verification of compliance to policies, system simulation, testing, code reviews, human "sign offs", and even references to supporting literature. Security certification schemes, such as Common Criteria (ISO 15408) [2] provide a widely adopted practical solution to address the trust deficit when evaluating and purchasing third-party software. A major goal of Common Criteria is to certify that the security policies claimed by developers are correctly enforced by the security functions of the product under evaluation. In Common Criteria, computer system users specify their security and assurance requirements, vendors implement and/or make claims about the security attributes of their products, and testing laboratories evaluate the products to determine if they actually meet the claims. A customer buying a certified product can rely on the "stamp of approval", by the certification authority who performed the assessment that a particular software system has some security features, conforms to specified requirements, and behaves as expected [1]. Until now, Common Criteria-style certification schemes have targeted static, monolithic systems, and require a medium/large investment of time and resources both vendors and customers. From the software customer perspective, the major issue is that security certifications are delivered in the form of natural language documents. Customers have to manually inspect and assess certificates to evaluate if they match their security requirements. With the increasing number of applications that can be quickly acquired and installed on-the-fly, (e.g., in the "app" marketplace), organizations face need a more effective way to provision and check security certificates. A "machine-readability" requirement emerges when software is discovered and consumed automatically, or at least with minimal human intervention. Current certification schemes are either insufficient or not applicable at all in these dynamic scenarios [3]. To address this gap, the Assert4Soa project has proposed a novel framework, supporting the production and consumption of machine-readable security certificates [4]. In the

Assert4Soa framework, the assessment of the security features of a piece of software is delegated to an independent third party, who evaluates the security properties by testing and/or using formal methods and issues a corresponding signed certificate (Assert). However, Assert certificates are expressed in a machine-readable format. Asserts are digitally signed statements written in an XML-based language (Assert4Soa language) which describes the certified security properties and the results of their assessment. Tests and/or models used in the evaluation are explicitly described in the certificate.[2] Accordingly, the consumer may use this information in the selection of the software, for example giving preference to software tested using standard test-suites. The Assert framework includes a discovery and match-making service, based on certificates. Users can define their functional and security requirements, using a special-purpose query language. The Assert query language supports queries based on type of evidence or proof used in the certificates. The Assert service discovery framework processes queries and ranks candidate services accordingly. While the Assert approach is a significant step toward dynamic certification, many problems remain to be solved, most of them pertaining to operations involving certificates. Today, certificate matching is a cumbersome process that assumes to be possible to establish partial orders among services whose properties were certified through different certification processes; also, ideally certificates need to be arbitrarily composed across process choreographies. In this paper, we tackle some open issues facing the development of an integrated framework of models, processes, and tools supporting the dynamic certification of assurance related to security, privacy and dependability properties, as well as the run-time control actions on configuration needed for preserving them. Certification has started to play an important role in the Service-Oriented Architecture (SOA) environment, to the aim of certifying service functional and non-functional properties. The framework we envision will be suitable for infrastructure (IaaS), platform (PaaS) and software application services (SaaS) in clouds. Our framework relies on multiple types of assurance evidence including testing, monitoring and model-based proofs.

2.1 Test-Based Service Certification

Test-based certification [5] of services involves three steps: (i) the specification of the security properties to be certified, (ii) the definition of the test units to provide evidence that each property holds, and (iii) test execution [6–8]. Dynamic security certification relies on machine-readable certificates available at run-time. Certificates contain information made available to the certificate issuer (the *certification authority*) for the definition of test cases. Such information can often be expressed as a model. Such model can be as simple as a WSDL interface; in this case, the certification authority uses black box testing techniques, such as equivalence partitioning or boundary value analysis. Alternatively, more detailed

[2] In some cases software vendors may prefer to remove this information to reduce the risk of possible disclosure of the internal functionalities of the software.

models, e.g. based on source code, can be used. In this case service providers provide source code to the Certification Authority (CA) only, but disclose the corresponding model to the general public. The certification authority can apply white box testing, considering all information on inputs, outputs, flow of execution, and internal state transitions. Test quality depends on the model's level of detail. A certificate based on a full implementation model is preferred ($\succeq$) over a WSDL (WSCL) model including test-based conditions only. In turn, the latter takes precedence ($\succeq$) over a bare WSDL (WSCL) model. When comparing models at the same level of detail, the outcome depends on users' preferences. Let us consider two certified services with the same functionality but different interaction patterns: a single-call service consisting of a single WSDL operation (hiding all conversation in the back-end) and a conversation service consisting of multiple operations and a WSCL file that specifies interactions. Here, the choice depends on user goals. A customer may prefer the single-call service, since a reduced number of interactions exposes to less risks. Another customer may prefer the conversation service, because it discloses less information per call. Below, we provide two examples [9] computed using different representations.

***FundTransfer* Service.** We consider a simplified banking service that implements a `Debit`(*info*,*amount*) operation. The service is described via a finite state model representing its WSDL interface and a stateful implementation. Let us consider a set of test units that aim to certify the security property *robustness against penetration by input malformation*. Figure 1 shows a portion of the `FundTransfer` WSDL concerning the `Debit` operation.

The customer calls the `Debit`(*info*,*amount*) operation passing two parameters: *info*, i.e. the reason for debiting the account and *amount*, the amount to be debited. The operation returns *result*, i.e. the new account balance if the customer's account balance is greater than the debit, or an error otherwise.

Figure 2 shows an abstraction of the `FundTransfer` service, where: (i) input condition [c1] includes the call to the operation `Debit` and requires *amount* to

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:description ...namespace...>
  <wsdl:types>
   <xs:import schemaLocation="FundTransfer.xsd"
     namespace="http://example.org/fundTransfer.xsd" />
  </wsdl:types>
  <wsdl:interface name="FundTransferI">
    <wsdl:operation name="Debit"
      pattern="http://www.w3.org/ns/wsdl/in-out">
     <wsdl:input
       element="xsFundTransfer:fundTransferReq"/>
     <wsdl:output
       element="xsFundTransfer:fundTransferResp"/>
    </wsdl:operation>
  </wsdl:interface>
</wsdl:description>
```

Fig. 1. A fragment of the WSDL file for the *Debit* operation in the *FundTransfer* service interface

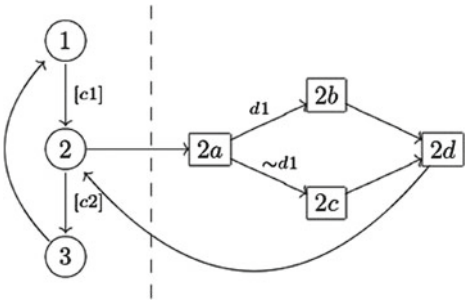

Fig. 2. Abstraction of the FundTransfer Service.

be greater than zero and less than a *max_amount*; (ii) output condition [c2] returns the output of `FundTransfer`, and requires the amount in the result (result.*amount*) to be equal to the one in the request (*amount*) and new balance (*result.balance*) to be equal to *balance* – *amount* or to 'error'. The right part of the model shows the internals, where a check on the account balance is performed. If *balance*≥*amount* (i.e., d1), the response is new balance (*result.balance*), otherwise (i.e., ∼d1) an error is returned. The certification authority (CA) dynamically tests the service to issue a certificate of its security properties, for instance *robustness* against *penetration by input malformation*. Test cases supporting the property can be automatically generated to the user's satisfaction, up to a complete coverage. Figure 3 shows the test cases.[3]

If all tests succeed, the CA releases a certificate of *robustness*.[4] Customers can check test cases quality against the model. The final assurance level depends on the certification model. In our example, the certificate could not be issued based on a bare WSDL model; test cases would become random pairs (*I,EO*) that do not consider internal states 2a, 2b, 2c, 2d.

***RemoteBanking* Service.** In many cases, users need to make sure that compositions (e.g., conversations or orchestrated processes) taken as a whole hold certain security properties. We will briefly discuss this type of certificates by considering a *RemoteBanking* service with a model including multiple operations and a WSCL conversation. Test cases certify the security property *integrity*, using RSA algorithm with a 1024 bit key, and a SHA-256 hash function.

Figure 4 shows the RemoteBanking WSCL. The customer calls `login`(*username,password*) exposed in the WSCL of the service. After logging in, the customer calls `fundTransfer`(*info*, *amount*), and waits for *result*. Then, she calls `confirm`(*id*) and waits for the final confirmation.

[3] For each test case, we show *input* (I) to the system (including related conditions) and *expected output* (EO).

[4] Our certificate is conditioned to users trusting the certificate-to-service binding. Such binding can be made trustworthy by a signature of the supplier, or even via a standard ISO/IEC 11889 Trusted Platform Module (TPM).

PROPERTY: ROBUSTNESS
CLASS ATTRIBUTES: `threat`=*malformed input*

$$TC1 = \begin{cases} I: & (random)\ 0 \leq amount \leq max\_amount\ [c1] \\ & balance \geq\ amount\ [d1] \\ EO: & result.amount = amount \\ & result.balance = balance - amount \end{cases} \quad (1)$$

$$TC2 = \begin{cases} I: & (random)\ 0 \leq amount \leq max\_amount\ [c1] \\ & balance < amount\ [\sim d1] \\ EO: & result =' Error' \end{cases} \quad (2)$$

$$TC3 = \begin{cases} I: & (random)\ amount \leq 0\ \vee\ amount \geq max\_amount\ [c1] \\ EO: & Fail \end{cases} \quad (3)$$

Fig. 3. Test cases for the `Debit operation` of the `FundTransfer` service

```
<?xml version="1.0" encoding="UTF-8"?>
<Conversation name="e-bank"
  xmlns="http://www.w3.org/2002/02/wscl10"
  initialInteraction="Start" finalInteraction="End">
  <ConversationInteractions>
    ...
  </ConversationInteractions>
  <ConversationTransitions>
    <Transition>
      <SourceInteraction href="start"/>
      <DestinationInteraction href="login"/>
    </Transition>
    <Transition>
      <SourceInteraction href="login"/>
      <DestinationInteraction href="fundTransfer"/>
      <SourceInteractionCondition href="success"/>
    </Transition>
    <Transition>
      <SourceInteraction href="login"/>
      <DestinationInteraction href="end"/>
      <SourceInteractionCondition href="failure"/>
    </Transition>
    <Transition>
      <SourceInteraction href="fundTransfer"/>
      <DestinationInteraction href="confirm"/>
    </Transition>
    <Transition>
      <SourceInteraction href="confirm"/>
      <DestinationInteraction href="end"/>
    </Transition>
    ...
  </ConversationTransitions>
</Conversation>
```

Fig. 4. WSCL file of the RemoteBanking service

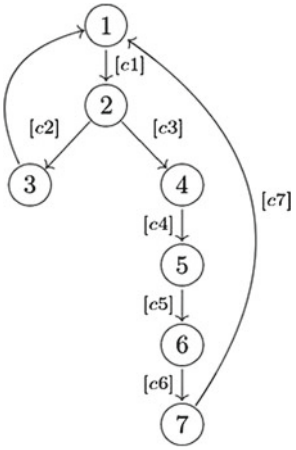

Fig. 5. Abstraction of the RemoteBanking Service.

$$TC1 = \begin{cases} I: \quad Message_i \ + \ Valid\ Signature \\ EO: decrypt_{P_i}[signature] = digest[Message_i] \end{cases} \tag{4}$$

$$TC2 = \begin{cases} I: \quad Message_i \ + \ Invalid\ Signature \\ EO: decrypt_{P_i}[signature] \neq digest[Message_i](fail) \end{cases} \tag{5}$$

Fig. 6. Test case for the RemoteBanking service

Figure 5 shows an abstraction of the RemoteBanking service, where conditions [c1],. . .,[c6] require input and output to be signed using RSA algorithm with 1024 bit keys, and a SHA-256 hash function. In addition, [c1] includes the call to `login`, while [c2] and [c3] model `login` output. [c4] and [c5] ([c6] and [c7]) model the call to `fundTransfer` (`confirm`) and its output.

Based on our model, the CA tests the composite service to certify its *integrity*. Here, only black-box test cases are generated (Fig. 6). We consider a set of i messages (Message_i) and the corresponding pairs (P_i, S_i) where P_i is the public key used to verify the signature, and S_i the corresponding secret key to generate it. The CA checks the signature of each message and verifies if the service rejects messages that are not properly signed.

Our technique can deal with orchestrations put together at run time, provided each services carries a certificate. In this case, the CA awards a temporary "virtual" certificate to the orchestration. Experimentation shows that the computation of virtual certificates is compatible with orchestration time [10].

3 Security Policy

The correct approach to the design of secure systems separates the security policy from the mechanisms responsible for the enforcement of security. A classical example is represented by access control, where there is a clear distinction between the authorization policy, which specifies if a user is authorized or forbidden to execute an action over a specific resource, and the control mechanisms, which guarantee that only actions authorized by the policy are executed on the resources under supervision.

Current systems rely on this separation between policy and mechanisms. Information system architectures often see the presence of several declarative policies, detailing the configuration of the many network and software components that cooperate in making the system secure. Even if each policy relies on a declarative specification, the number, size, distribution and heterogeneity of targets of the separate policies make their management quite difficult.

Today, the creation and maintenance of the policies is mostly a manual activity. Documentation about the implemented security policies, when it exists, is represented by information in spreadsheets or textual documents. The lack of support in the management of security policies is a significant problem for organizations, with several consequences. The maintenance of the security is quite expensive: every time there is a change in some security component or in a requirement, it is difficult to verify the extent of the impact of the change on the current system. The verification that all the security requirements are correctly considered in the implemented policy is typically hard, as policies in many independent elements of the landscape cooperate in the realization of system security. Finally, many organizations have to produce to authorities and other entities certifications about the compliance of their information system with a number of regulations. This activity is executed by external auditors, who have to analyze the security configuration of the information system with a long process. An additional problem is that auditors usually look at samples, while there is the need of a complete check of configuration settings.

A modern approach for the management of security policies should aim at delivering tools that support the security administrators and the subsequent maintenance of the security configurations of the many elements of the information system. The PoSecCo project is investigating the design and implementation of such an environment integrating a collection of tools supporting these needs. We provide a brief description of the approach followed by PoSecCo.

The representation of the security policies is based on a structure organized in three layers (*Business, IT, Infrastructure*)[11,12], at different levels of abstraction: the Business layer is the most abstract and describes the security requirements that motivate the security policy; the IT layer refines the security policy at the higher level and describes it in a formal way with reference to a conceptual model of the system; the Infrastructure layer maps the IT level policy to the specific modules and devices that compose the system and offers a logical representation of the configuration. The models in the three layers are

interconnected, to represent the binding between each element at one level with the corresponding elements in the other layers.

Our architecture can be adapted to the representation of heterogeneous security policies. The policies that received the greatest attention in the project are access control and data protection policies [13]. These policies are mapped in the Infrastructure layer to configurations for network devices and for systems with access control modules (operating systems, relational DBMSs, Web servers, and application servers). The fact that the same high-level policy is used to drive the configuration of several layers of the system offers the opportunity to adopt a "defense-in-depth" strategy, where consistent access control policies are implemented in separate modules of the system that are used together in the realization of a service, offering greater protection.

The advanced security management system helps the security administrator in the generation of the configuration, supporting a number of different targets [14]. Due to the large number of different devices that can contribute to the implementation of a security policy, the system has been designed to be extensible, facilitating the insertion of modules able to cover the devices and security components that may occur in a specific infrastructure.

An important service offered by the advanced security management environment is the ability to analyze the security policies, in order to detect inconsistencies or violations of generic integrity constraints. Semantic Web tools are particularly useful in this area, as they offer flexible representations of the policies, associated with reasoners able to efficiently apply consistency checks and return informative results about the outcome of the analysis. This analysis can be applied at every level of the policy (Business, IT, or Infrastructure), but the level that offers the best potential is the IT level.

Overall, the extensive collection of models and services that characterize these environments offer a significant help to the security administrator. In addition to the support in the construction of the security configuration, the system is also able to greatly facilitate the maintenance of the policies and the auditing activities.

4 Towards a Better Management of Security Assurance

We present here our vision for the integration of the tools and techniques developed within Assert4Soa and PoSecCo. A first aspect that can be observed is the complementarity between the goals of the two projects. The Assert4Soa project has developed techniques for the automatic verification of services and the management of certification authorities, supporting the high-level definition of the policies that have to be applied in the management of credentials and certified attributes. This increases the security of the system and improves its efficiency, as tedious and error-prone activities are managed by automated components. A classical application of these techniques occurs in the specification of

the integrity of the access control modules used in the system and in the guarantees about the integrity and trustworthiness of the credentials provided by the parties accessing the services. Another aspect that has to be correctly managed in order to guarantee the security is the consistency and completeness of the access control policy. The Assert4Soa project does not consider this aspect, which is the core goal of PoSecCo. Then, a clear integration opportunity arises form the combined use of the results of the two projects, which together promise to support a more robust (and more efficient in terms of management) approach for the construction of service-oriented applications.

Another interesting opportunity for the integration between the two projects derives from the extension of the policy analysis and automatic generation of configurations, provided by PoSecCo, with the ability to represent and automatically support the deployment in application infrastructures of advanced credential management and assurance services, provided by Assert4Soa.

A benefit that then derives from this integration is the ability to verify the correctness of the configuration and its compatibility with the access control and authorization policies of the application, extending the support offered by the tools developed by Assert4Soa. The support offered by PoSecCo tools in this scenario is particularly useful considering the delicate nature of credentials, which are relatively unfamiliar to most practitioners and require a precise setup in order to adequately provide their services. One of the obstacles that today limits the adoption of modern credential solutions like SAML in new systems is the concern about the level of support in the configuration and management offered by current middleware; this often comes together with an unclear understanding of the capabilities provided by these solutions. The combination of the solutions offered by Assert4Soa and PoSecCo can offer a significant support to the improvement of this critical component of service-oriented architectures.

5 Conclusions

A crucial aspect that characterizes both Assert4Soa and PoSecCo is the goal of supporting a security management process that is more efficient and at the same time able to improve the security. Both Assert4Soa and PoSecCo aim at improving the state of the art in security, offering methods and tools that at the same time increase the efficiency of the security management process and lead to a better representation in the system of the security requirements of applications. The development of the approaches and techniques discussed above is able to meet a clear demand, in the same way as modern software development solutions have been developed to answer to the needs of programmers.

Acknowledgements. This work is partially supported by projects PoSecco (Grant No. 257129 - www.posecco.eu) and Assert4Soa (Grant No. 257351 - www.assert4soa.eu).

References

1. Damiani, E., Ardagna, C.A., Ioini, N.E.: Open Source Systems Security Certification, 1st edn. Springer, Heidelberg (2008)
2. ITSEC: Common criteria for information technology security evaluation
3. Anisetti, M., Ardagna, C., Damiani, E.: Toward certification of services. In: International Workshop on Business System Management and Engineering (BSME 2010), Malaga, Spain, June 2010
4. Bezzi, M., Sabetta, A., Spanoudakis, G.: An architecture for certification-aware service discovery. In: 2011 1st International Workshop on Securing Services on the Cloud (IWSSC), pp. 14–21. IEEE (2011)
5. Anisetti, M., Ardagna, C., Damiani, E.: Fine-grained modeling of web services for test-based security certification. In: 2011 IEEE International Conference on Services Computing (SCC), pp. 456–463, July 2011
6. Baresi, L., Di Nitto, E.: Test and Analysis of Web Services. Springer, New York (2007)
7. Bozkurt, M., Harman, M., Hassoun, Y.: Testing web services: a survey. Technical Report TR-10-01. Department of Computer Science, King's College London, January 2010
8. Canfora, G., di Penta, M.: Service-oriented architectures testing: a survey. In: De Lucia, A., Ferrucci, F. (eds.) ISSSE 2006-2008. LNCS, vol. 5413, pp. 78–105. Springer, Heidelberg (2009)
9. Anisetti, M., Ardagna, C., Damiani, E.: Fine-grained modeling of web services for test-based security certification. In: Procedings of the 8th International Conference on Service Computing (SCC 2011), Washington, DC, USA, July 2011
10. Anisetti, M., Ardagna, C., Damiani, E., Saonara, F.: A test-based security certification scheme for web services. ACM Trans. Web (TWEB) **7**, 1–41 (2013). http://www.crema.unimi.it/Biblioteca/Note_pdf/163.pdf
11. Plate, H.: Policy and security configuration management. In: Fischer-Hübner, S., Katsikas, S., Quirchmayr, G. (eds.) TrustBus 2012. LNCS, vol. 7449, pp. 229–231. Springer, Heidelberg (2012)
12. Paraboschi, S.: Integrated management of security policies. In: Li, Y. (ed.) DBSec. LNCS, vol. 6818, pp. 12–13. Springer, Heidelberg (2011)
13. De Capitani di Vimercati, S., Foresti, S., Jajodia, S., Paraboschi, S., Psaila, G., Samarati, P.: Integrating trust management and access control in data-intensive web applications. ACM Trans. Web **6**(2), 1–44 (2012)
14. Casalino, M.M., Mangili, M., Plate, H., Ponta, S.E.: Detection of configuration vulnerabilities in distributed (Web) environments. In: Keromytis, A.D., Di Pietro, R. (eds.) SecureComm 2012. LNICST, vol. 106, pp. 131–148. Springer, Heidelberg (2013)

Security Property Lifecycle Management for Secure Service Compositions

Shahidul Hoque[1], Aneel Rahim[1],
David Llewellyn-Jones[2(✉)], and Madjid Merabti[2]

[1]Telecommunications Software and Systems Group,
Waterford Institute of Technology, Waterford, Ireland
{shoque, arahim}@tssg.org
[2]School of Computing and Mathematical Sciences,
Liverpool John Moores University, Liverpool, UK
{D.Llewellyn-Jones, M.Merabti}@ljmu.ac.uk

Abstract. We present an approach to deploying a security property life cycle management mechanism for secure service composition. A Security Property Determination Module component is introduced that forms part of the Aniketos project, in the context of a case study relating to an online payment system that has been developed using real services deployed within the Activiti BPMN service process engine. Both the theory behind the implementation as well as the implementation itself will be discussed, along with the lessons learnt and the potential for future improvements to the lifecycle mechanism. The mechanism integrates tightly with the verification processes of the Aniketos platform. It also allows the security property lifecycle to be managed at run-time without user intervention. The mechanism unifies the verification of imported properties and the digital signing and storage of properties associated with both atomic and composed services. These integrated capabilities form a novel approach discussed and situated in the context of the case study.

1 Introduction

Networked services represent a crucial component of the Future Internet vision, with users and service developers routinely invoking loosely coupled services to create larger applications in a dynamic way. However, in order for the technology to be used seriously, the security of these services must be maintained, and mechanisms and incentives are therefore needed in order to ensure that services fulfil the security capabilities they claim.

Security in this context is particularly challenging for a number of reasons. For a composed service the security capabilities of the system are a function of the

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant no 257930 (Aniketos). We would like to thank all partners for their helpful contributions to this work.

M. Felici (Ed.): CSP EU FORUM 2013, CCIS 182, pp. 67–78, 2013.
DOI: 10.1007/978-3-642-41205-9_6,

capabilities of the sub-services of which it's comprised. The relationship between the two is non-trivial and dynamic. Moreover, with the responsibility for sub-services shared between multiple providers, there is a need to trust each of these providers to fulfil their claimed security promises and to understand the overall trustworthiness of a system managed by multiple providers that might each be trusted in a different way.

The Aniketos project is tackling these challenges by considering the security of composite services in detail from design-time through to deployment and run-time [1]. It is an EU research project that addresses trustworthy and secure service composition with run-time monitoring and adaption of services. The Aniketos platform incorporates verification of atomic service security properties, validation of composite security properties (where the security of a composite service is inferred from the security of the atomic services from which it's constructed), run-time monitoring of security properties, run-time fuzz-testing of the service security and a threat model that ensures the security context of the service is taken into account.

However, in order to ensure the consistency of these various techniques and maintain the state of a service's security characteristics, the lifecycle of these security properties must also be understood and managed. During service composition, the security properties are subject to change due to both dynamic internal and external changes. These changes in security properties or changes due to threats are identified by the Aniketos platform and may also result in trustworthiness changes, and as such the security property bindings for a service need to be able to change and be managed over time. The Security Property Determination Module (SPDM) – one of the sub-components that forms part of the Aniketos platform – has been designed and implemented in order to achieve exactly this task: the dynamic management of the security property lifecycle.

In the remainder of this paper we will consider the SPDM and its role in ensuring service security. In the next section we consider the Security Property Lifecycle Management process in detail, and go on to consider its relationship with composite services in Sect. 3. Section 4 looks at the implementation of the SPDM, followed by a case study to illustrate its use in Sect. 5. In Sect. 6 we consider related work. Finally we conclude in Sect. 7 with a discussion about future work.

2 Security Property Lifecycle Management

Understanding and measuring the security of a networked service is a challenging task, not least because of the many different ways the term 'security' can be interpreted. In a service-oriented environment the challenge is increased due to the distinction between the service provider and service consumer: even if the provider claims a certain level of security compliance, how can the consumer be sure that there is any truth to the claim?

The Aniketos platform tackles these challenges using a number of techniques. Consistency of interpretation is achieved through the use of security contracts, which allow a provider and consumer to compare the security offered against the security required. For Aniketos, such a contract is effectively a list of security properties expressed in a form that allows *inclusion* to be determined. That is, it's possible to

determine whether one contract (the agreement template offered by the provider) is a subset of another (the consumer policy required by the consumer). However, while this ensures the provider can offer a security guarantee that the consumer can understand, it does nothing to address the question of whether the contract holds in practice.

A number of methods can be used to resolve this. For the strictest guarantee, formal methods can be used to verify mathematically that a certain security property holds for a given service. This requires that the service implementation (for example, the Java source or bytecode in the case of Aniketos) is available to be tested by the consumer. While this offers the strongest guarantee, it is not appropriate in all cases. For example, some properties will not be amenable to testing in this way (e.g. due to complexity or expressiveness constraints) or the implementation may not be available.

An alternative technique is that of runtime monitoring. In this case the behaviour of a service is monitored to ensure compliance with the security contract. For example, if a contract specifies that certain data must be transmitted encrypted, then this can be checked at execution time either through internal monitoring of service API calls (e.g. does it use socket or secure socket connections?) or external monitoring of data transmissions. Note that runtime enforcement can also be considered as a related activity, since blocking certain behaviour implies that it can also be identified.

The use of monitoring can also be tied to trustworthiness, since a service identified as violating a security policy may be considered less trustworthy than one that has hitherto always satisfied it. Trust information may be used by a consumer in making a priori decisions about the level of enforcement (formal analysis, monitoring) to apply.

Finally, security is also a function of context, and the question of whether a service is able to fulfil a security contract may depend on the threats that are present while the service is being used.

The Aniketos platform incorporates technologies related to all of these methods. They all interact with one another in a variety of ways. A particular challenge is therefore the management of the security properties that relate to a given service and its security contract. At any given time (either before, during or after service execution), it's important that a consumer should be able to understand the security properties for a service and the method of enforcement in order to be able to make an informed judgement about the likelihood the service will fulfil the security contract.

We achieve this using the Security Property Determination Module (SPDM) which provides rich lifecycle management of the security properties of the services available in the Aniketos Marketplace.

Figure 1 highlights how – during the security property lifecycle – each security property is given one of four different security property statuses: *unverified*, *verified*, *lapsed* or *certified*. This status changes over time due to the changes in the security properties. Before a security property is discovered or obtained from the agreement template (the user and service provider security negotiation document), the security property status is expressed as *unverified*. Subsequently, once the binding of the security properties to a service is completed, the property status is changed to *bound*. When the bound property has been verified through a formal process, its status again changes to *verified*. After verification, the security property can be associated with a certificate and the status is changed to *certified*. The security property lifecycle

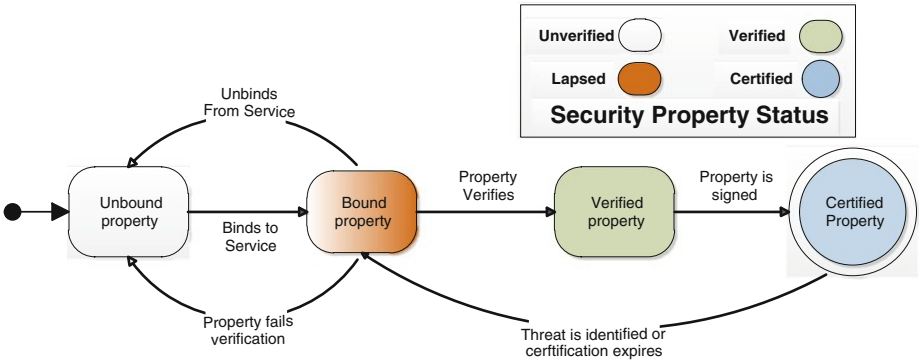

Fig. 1. The security property lifecycle

management includes verification of imported security properties, assigning digital certificates to the properties and storage of the properties for the associated services.

The SPDM registers each security property and starts managing its lifecycle just after each security property has been discovered and bound to a service or service composition. This occurs as the service developer uploads the service to the Aniketos Marketplace (the agreement template containing the security properties is uploaded along with the service description). The SPDM then sends requests to other components for performing verification of the property and – if successful – after receiving verification confirmation, the SPDM changes the status of the property to *verified*. An internal process then digitally signs the property and marks it as being *certified*, with the information stored by the SPDM along with a timestamp and time-limited cryptographic signature.

The signature may become invalid for one of two reasons. First, it may expire due to the time-limited nature of the certificate. Second it may become invalid due to changing threats in the environment. In either case the property is removed from certified status and returns to bound status, thereby triggering a reverification of the property. This security property lifecycle management process ensures the reliability of the properties and supports a strong trust relationship between the components of the Aniketos platform.

3 Composite Services

One of the key concerns of the Aniketos platform is tackling composed services that are built from multiple sub-services. When a service developer is constructing a composed service, it's likely information about the properties of the sub-services will already be known and registered with the SPDM. Through a combination of security property lifecycle management and composite service validation, the Aniketos platform is able to infer security property information for these composed services too.

This occurs as part of the verification process: the SPDM sends the security properties to a central exchange referred to as the Nested Composition Verification Module (NCVM). While this does not itself perform any verification, it negotiates

with other Aniketos modules in order to determine the result, which it then returns to the SPDM. In the case of an atomic service the NCVM directs the verification process to a Property Verification Module (PVM) that performs formal analysis of the service implementation (Java code) directly [1]. In the case of a composite service the NCVM determines based on a set of rules whether the property can be determined from the properties of its subservices. For example, an access control requirement stating a service must *not* access a particular resource can be checked by ensuring none of the services access it. The NCVM would therefore take a top-down approach, converting the request into multiple property requests relating to the sub-services.

For a third class of cases that require analysis of the composition itself, the NCVM directs the verification process to the Composite Security Validation Module (CSVM) [1]. The CSVM performs a formal analysis of the full composed service. This is particularly useful where the property to be verified depends in a complex way on the subservices and how they interact with one another. In particular, it applies where the property to be determined can't be decomposed into properties that must hold for the subservices. An example used in Aniketos is that of Separation of Duty properties.

However, both the PVM and CSVM are analysis modules in their own right, and their capabilities fall outside the scope of this paper. Instead, we wish to consider the second case in more detail and suppose that the property of a composite service is derivable as a function of its subservices. In the access control case described above the relationship between a service and its subservices is equivalent to the intersection operator. We note this isn't universally the case though; consider for example the case where a composed service is *required* to access a particular resource at some point during execution. In this case, we take the union operator, $\cup$, for performing the aggregation of the security properties of the atomic services participating in the service composition. This aggregation process achieves the required results since it removes the duplicate properties. More formally, the process determines whether the property P (the requirement to access the resource) holds for the composed service S^C using the union operator as follows.

$$P \in \bigcup_{i=1}^{N} \pi(S_i),$$

where $S^C = \{S_i | i = 1, \ldots, N\}$ and S_i is the ith service in the composed service S^C. The number of atomic services participating in the service composition is denoted by N and the set of security properties offered by the ith atomic service S_i is denoted by $\pi(S_i)$. Note the values of $\pi(S_i)$ may not be known at this stage. If so, the process may trigger further verification processes on sub-services in order to determine the result.

As discussed above, at runtime security properties are subject to changes due to internal (such as verification lapses) or external (typically context changes including threat notifications) triggers. After verification of each security property, it is cryptographically signed by the SPDM. The security property status is not changed if there is no valid signature found for a property.

A timestamp is being used to manage the cryptographically signed certificates associated with security properties. We refer to the time when the certificate is no longer valid as t_{expiry} and the cryptographically signed certificate associated with

security property p_i as $C(p_i, t_{expiry})$. The SPDM periodically checks each certificate $C(p_i, t_{expiry})$ and compares its t_{expiry} with the wall clock timestamp, t_{now}. Hence there are two possible situations for certificate management of the security properties.

1. If $t_{now} \geq t_{expiry}$, redirect the property to be verified with trust requirements.
2. If $t_{now} < t_{expiry}$, no action is required.

The dynamic changes that can cause a change in the property values can be summarised as follows.

1. A security property can change over time, for example due to a new vulnerability being discovered. In this case, if the security property has become invalidated it will require further reverification.
2. The binding of the security property to a service can change over time, such as when a service has changed its functionality and hence, it no longer offers a particular property. The most likely situation where this might occur is if a service composition replaces one of its sub-services for security reasons.
3. When new threats are identified and trustworthiness changes, the security property may change in character.
4. When a security property description is amended directly by the service developer.

4 Implementation

We have discussed the operations of the SPDM from a theoretical point of view, and considered its abstract relationship with other Aniketos modules. Figure 2 shows the

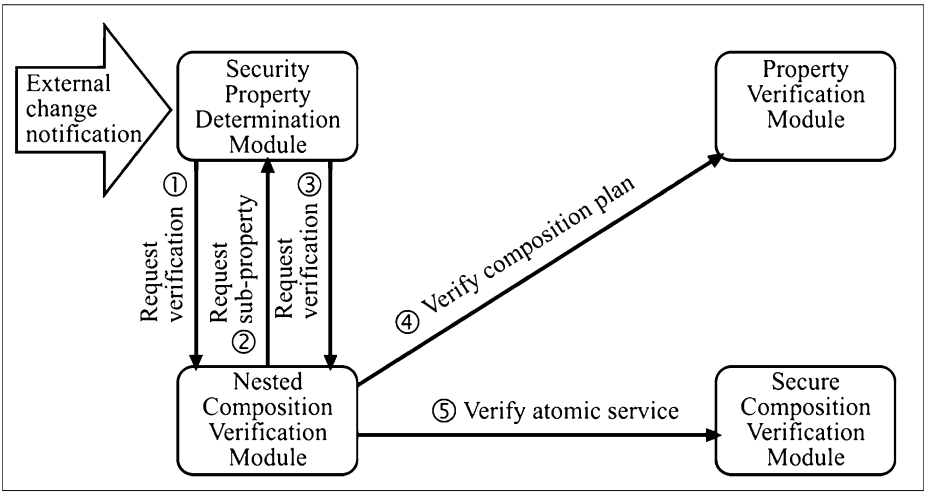

Fig. 2. Interactions among modules for verification within the security property lifecycle

component interaction view in relation to the SPDM's communication with other components for managing the security property lifecycle.

The SPDM deploys an internal database to register the security properties, binding the properties to the services along with the verification status. For practical reason, this database is extended to offer querying capabilities of the security properties with associated property status so that the relationship between the properties and services can be effectively understood.

As with all Aniketos modules, the SPDM is coded in Java deployed as an OSGi bundle in Apache Karaf and exposed as a Web Service using Apache CXF. The main relevant datatypes for the module are exposed through the **ISecurityProperty** and **IWebService** interfaces, which represent instances of specific security properties and the Aniketos-compliant services they can be associated with respectively.

The main API for the SPDM is then the **ISPDMService** interface. This – along with the two datatypes – can be seen in Fig. 3 (slightly abridged for brevity). As can be seen from these, the **IWebService** interface is effectively a means for accessing the service ID used to reference the service in the Marketplace. The **ISecurityProperty** structure provides access to the relevant fields including the property ID, freshness, and state (see Fig. 1) of the property. The service interface offers a collection of means

```
publicinterfaceIWebService {
    voidsetServiceID(String id);
    String getServiceID();
}

publicinterfaceISecurityProperty {
    String getPropertyID();
    voidsetPropertyID(String propertyID);
    String getPropertyValue();
    voidsetPropertyValue(String value);
    Date getFreshness();
    voidsetFreshness(Date freshness);
    SPStategetState();
    voidsetState(SPState state);
    X509Certificate getCertificate();
    voidsetCertificate(X509Certificate certificate);
}

publicinterfaceISPDMService {
    Set<ISecurityProperty>lookUpSecurityProperty(IWebService service);
    Set<IWebService>lookupService(ISecurityPropertysp);
    voidregisterService(IWebService service, ISecurityPropertysp);
    voidunregisterService(IWebService service);
    Set<ISecurityProperty>getProperties(IWebService service, SPStatestate);
    ISecurityPropertygetSecurityProperty(String serviceID, String sp_id);
    ISecurityPropertygetSecurityProperty(String sp_id);
    IWebServicegetService(String service_id);
}
```

Fig. 3. Interfaces of the SPDM datatypes and main SPDM service

for registering, searching and updating of security properties for specific services. Internally, methods that affect the state of services, such as the **registerService** method, are liable to trigger verification through a single call to the NCVM's **verifyProperty** method. This may also be called as a result of a property change caused by a timer event or threat change notification.

For an implementation of the security property lifecycle as described in the previous section, the overall sequence can be realized in the following phases.

1. Add/remove properties from agreement templates. The SPDM takes the security properties from the agreement templates of the Marketplace and registers them in its local repository.
2. Ensure verification of the properties. The SPDM sends the properties to the NCVM for verification. Whenever it receives verification results back from the NVCM, it updates the property status to verified (or failed). This process can be broken down further as shown earlier in Fig. 2.
3. Lookup services by name. The Marketplace may need to lookup services registered in the SPDM to determine their security properties.
4. Design-time service composition. Either searching the verified security properties of a service or searching for services offering a given set of security properties. This latter functionality is particularly useful to service developers constructing new composition plans having particular security requirements.
5. Design-time secure service composition. For creating secure composition plans, the verified security properties are needed along with trustworthiness. Hence the SPDM offers this feature with the help of the Trust Manager Module.
6. Runtime updates of security properties. From external components the SPDM can be asked to update the status due to changes in the environment. In addition, internally the SPDM ensures regular checking of verification status expiration.
7. Runtime reverification of security properties. When a verification lapses or a relevant threat is identified, the SPDM invokes verification.
8. Runtime adaptation and recomposition of services. When reconfiguration or recomposition of services is performed, the SPDM facilitates by providing details about the verified properties.

5 Case Study

To demonstrate use of the SPDM implementation within the Aniketos platform, we consider a simple case study relating to an online payment system. A service developer has constructed a simple service composition using two atomic sub-services: a service for locating activities based on geographical location, and a payment service. The structure of the service composition is shown using BPMN in Fig. 4. Here we can see that after the geosearch service has performed its search, the process then moves on to the payment service. However, a separation of duty (*sod*) security requirement (signified by the blue box) has been specified against the two services: the two services (search and payment) should not be fulfilled by the same provider.

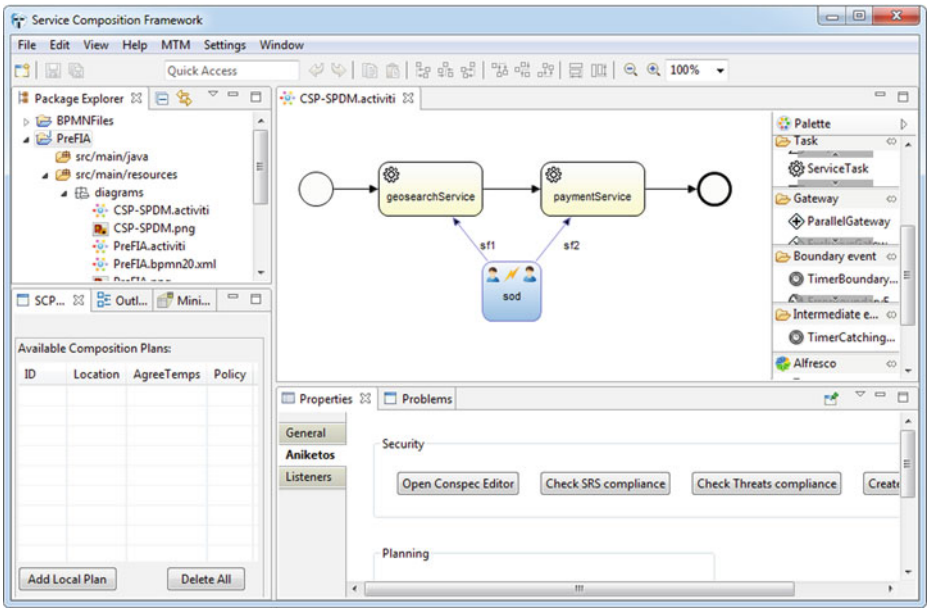

Fig. 4. Simple composed payment service

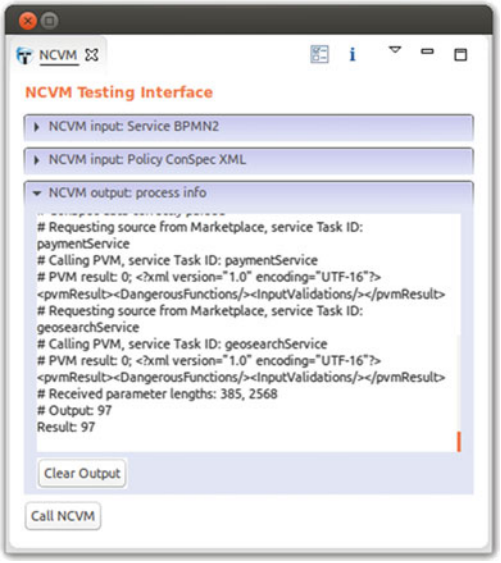

Fig. 5. Output from the verification process

Fig. 6. The SPDM cache contents directly after the verification process

On uploading this composed service to the Marketplace, the separation of duty property is registered with the SPDM to start its lifecycle, triggering verification. While the actual verification of these properties is performed by the CSVM – as we discussed in Sect. 3 – the process is orchestrated by the NCVM. The output of this process can be seen in Fig. 5. Because the atomic sub-services are also new and unknown to the SPDM, their properties are checked by the PVM, before a positive result for the overall composition is returned to the SPDM.

Having completed the process, we are able to query the SPDM cache to establish the properties that have been registered and their respective statuses. The output from this query can be seen in Figs. 5 and 6. Here the two services (*geosearchService* and *paymentService*) have been registered along with the *sod* property.

Future queries of the SPDM concerning the *sod* property for the composed service will result in a practically instant response, rather than having to complete the lengthy verification process, since the value will be stored in the cache until the freshness value expires. This allows the process to be significantly streamlined in terms of efficiency, while at the same time also ensuring that the lifecycle of the property can be properly managed with respect to time, trust and threat changes.

6 Related Work

The work proposed here crosses a number of areas, including vulnerability metrics, formal security analysis, security certification and common vulnerability and exposure databases. Some similar capability comes from the Common Vulnerabilities and Exposures (CVE) databases that track security notices, vulnerabilities and exploits for software and digital services, such as the US-CERT Vulnerability Notes Database[1] or the MITRE-run CVE.[2] These have existed for over two decades [2] and at a superficial level maintain similar information to that of the SPDM, including properties

[1] http://www.kb.cert.org/vuls/

[2] https://cve.mitre.org/

(vulnerabilities), related software, date of identification and so on. However, there are also important differences. First, vulnerability databases focus primarily on negative properties: that is, cases where software fails to match a basic standard security level. The properties therefore do not relate to requirements defined by policy and do not include positive assertions about the properties the software satisfies. Second, vulnerability databases are generally intended for human consumption. While there are automated techniques used in relation to vulnerability databases such as for correlation [3], data interchange languages such as the CVML [4] or combining databases [5], these again focus on vulnerabilities and are not intended to form a central store for security claims about a service or piece of software.

There has also been a great deal of work looking at security lifecycles [6, 7]. These mostly focus on the software development stages and the need to model, implement and test based on security requirements. The runtime elements of secure development lifecycles often focus on vulnerability detection and patching, rather than automated monitoring and compensating through service recomposition.

The ASSERT4SOA project has generated detailed results on the certification of security properties, with the work of Anisetti, Claudio and Ardagna being particularly relevant [8, 9]. An XML syntax is used to bind services with their properties and certified evidence used for assurance. Methods for querying and ordering these properties are also proposed. However, unlike our approach, the certification process does not appear to directly incorporate automated verification as part of the lifecycle.

More relevant to the work proposed here is the body of knowledge related to security monitoring [10], formal methods [11] and security contract specification languages [12, 13]. These all feed into this work, and different techniques can be used to affect the security lifecycle stages. The integration of such methods represents future work for the Aniketos platform as a whole.

7 Conclusions

In this paper we considered the Security Property Determination Module and its relationship with the security property verification process of the Aniketos platform. The SPDM manages the lifecycle of the security properties, forming an essential part of the overall security process. The module ensures that the correct properties are associates with the correct services and in the correct state, preventing outdates or incorrect security information being associated with a service.

Although the service has been developed and tested using a variety of test case studies, there remain a number of issues that we aim to address in future research. Aniketos utilises a number of techniques to tackle scalability and the SPDM represents one of them, by ensuring that previously verified properties do not need to be reverified needlessly while they remain valid. However, the verification process introduces scalability challenges and more work is needed in this area. A full evaluation of the lifecycle process is needed in order to determine efficiency, especially in order to understand the benefit of this caching in practice. In theory this should offer significant improvements over having to reverify security properties, but the benefits will depend on the level of re-usability that the properties support.

The association between composed security properties and the properties of sub-services also remains an area for on-going work. The relationship between the two is complex and providing a generalised solution is a challenge. The use of a finite automata policy language provides scope for a solution here.

Finally, while the SPDM implementation already provides a practical service within the Aniketos framework, other elements of the framework are still being developed and the full potential of the system relies on all platform components being available.

References

1. Rios, E. (ed.): Aniketos D1.5: Final Aniketos architecture and requirements specification. Aniketos Project (2013)
2. Neuhaus, S., Zimmermann, T.: Security trend analysis with CVE topic models. In: 2010 IEEE 21st International Symposium on Software Reliability Engineering, pp. 111–120 (2010)
3. Flizikowski, A., Majewski, M., Kowalczyk, Z., Romano, S.P.: Framework: applied security for heterogeneous networks. J. Telecommun. Inf. Technol. (2011)
4. Tian, H., Huang, L., Zhou, Z., Zhang, H.: Common vulnerability markup language. In: Zhou, J., Yung, M., Han, Y. (eds.) ACNS 2003. LNCS, vol. 2846, pp. 228–240. Springer, Heidelberg (2003)
5. Armold, A.D., Hyla, B.M., Rowe, N.C.: Automatically building an information-security vulnerability database workshop on information assurance. In: IEEE Workshop on Information Assurance, pp. 376–377. United States Military Academy, West Point, NY (2006)
6. Dai, L., Cooper, K.: A survey of modelling and analysis approaches for architecting secure software systems. Int. J. Network Secur. **5**, 187–198 (2007)
7. Amer, S.H., Humphries, M.J.W., Hamilton, J.A.: Survey: security in the system development life cycle. In: IEEE Workshop on Information Assurance. United States Military Academy, West Point, NY (2005)
8. Anisetti, M., Ardagna, C.A., Damiani, E.: Certifying security and privacy properties in the internet of services. In: Salgarelli, L., Bianchi, G., Blefari-Melazzi, N. (eds.) Trustworthy Internet, pp. 221–234. Springer, Milan (2011)
9. Anisetti, M., Ardagna, C.A., Damiani, E., Maggesi, J.: Security certification-aware service discovery and selection. In: Fifth IEEE International Conference on Service-Oriented Computing and Applications (SOCA 2012), pp. 1–8. IEEE, Taipei (2012)
10. Rudolph, M., Schwarz, R.: A critical survey of security indicator approaches. In: Seventh International Conference on Availability, Reliability and Security, pp. 291–300. IEEE, Prague (2012)
11. Weyns, D., Iftikhar, M.U., De la Iglesia, D.G., Ahmad, T.: A survey of formal methods in self-adaptive systems. In: Proceedings of the Fifth International C* Conference on Computer Science and Software Engineering - C3S2E'12. pp. 67–79. ACM Press, New York (2012)
12. Han, W., Lei, C.: A survey on policy languages in network and security management. Comput. Netw. **56**, 477–489 (2012)
13. Jiao, D., Liu, L., Ma, S., Wang, X.: Research on security policy and framework. In: Second International Symposium on Networking and Network Security (ISNNS'10), pp. 214–217. Academy Publisher, Jinggangshan (2010)

Data Privacy Implications for Security Information and Event Management Systems and Other Meta-Systems

Herah Khan[1(✉)] and Andrew Hutchison[2]

[1] University of Cape Town, Cape Town, South Africa
herah.k@gmail.com
[2] T-Systems International, Midrand, South Africa

Abstract. Security Information and Event Management (SIEM) systems collect security information from multiple input systems, with a view to correlating and interpreting events so as to conduct security analysis and inference. Our analysis of large SIEM event sets has shown that in many instances the source events also contain personal information resulting from activities performed by users. The treatment of privacy in such 'meta-systems' is a challenging and, as yet, largely unaddressed consideration in privacy debates. This paper uses the 2012 EU Draft Data Protection Regulation as a basis to develop a view of its implications for SIEMs and other meta-systems. Providers of SIEM services have an obligation to ensure that their 'meta-systems' adhere to the same requirements as other systems, and the complexity can be compounded if the SIEM is not located in the same country as the originating events. Recommendations for role clarification, notification requirements, anonymisation and data protection officer oversight activities are presented – with respect to requirements of the associated privacy specifications. By adhering to these privacy specifications, security objectives can be achieved while ensuring that the rights of individuals and obligations, in terms of data privacy requirements, are met even when centralised security events and other types of meta-data, are collected.

Keywords: SIEM · Privacy · Data protection · European Union · Regulation · Directive

1 Introduction

Detecting information security breaches, has sometimes been likened to trying to find a needle in a haystack. A multitude of security related events is generated by computing and security systems, but identifying those which could predict (or reflect) an attack is highly challenging. One technique for gaining the upper hand in this challenge is to centralise and consolidate security event information through the identifiable activity of Security Information and Event Management (SIEM).

M. Felici (Ed.): CSP EU FORUM 2013, CCIS 182, pp. 79–90, 2013.
DOI: 10.1007/978-3-642-41205-9_7,

SIEM represents a combination of Security Information Management and Security Event management, and supporting technology aims to conduct real-time analysis of security events, where these events are generated through system hardware, software and applications. Using a SIEM has many advantages, including improved organisation of (and insight into) log data, in turn enabling faster reaction [8].

While SIEM systems do not initiate security related events themselves, they are collectors and consolidators of a myriad of security events contributed by source systems connected into the SIEM. The issue under consideration in this paper is that, in our experience, these collected events are often observed to contain personally identifiable information, and for this reason the *data privacy implications* of SIEMs need to be carefully considered. In light of recent events in 2013, there has been a lot of scrutiny regarding the use of meta-data and its privacy implications when used by external bodies. SIEMS can be seen as a collector of meta-data, they process various information of other systems for purposes of security analysis.

A typical SIEM architecture consists of *agents* which collect and forward events from source systems to a central processing system. The *central collector system* typically logs the consolidated events, creating a security base which can be inspected and analysed for trends, baselines and anomalies. Analysis engines (which are rule based or predictive) are typically deployed with the central processing system to apply sophisticated data analysis techniques to the large volume of events arising. Techniques like big data processing can also be applied in this context. Large processing environments can benefit greatly from the use of SIEM systems and technology, to help comprehend the current processing and flows – enabling these environments to adopt and monitor policies which help them meet compliance frameworks [13].

Consideration of data protection issues for SIEMs, and other similar frameworks that collect valuable information from systems – from here on referred to as 'meta-systems' – has not been prioritised, with the focus of information protection largely being confined to the actual source systems from which events originate. While the source systems need to be seen and assessed in terms of data protection requirements, it is also necessary to ensure that other systems that are *receivers* and *collectors* of events from the source systems adhere to data privacy regulations too.

On the one hand *anonymisation* of security events can be a strategy to ensure that personal information is not revealed, but on the other hand this can inhibit some depth of analysis, unless the anonymisation is performed in a particular way. Techniques such as *blind security* enable analysis of anonymous events, without compromising their associated privacy, through the use of pseudonymisation. Events can be worked on in pseudonymous form after which they can be mapped back to their initial format (with full content) by the data owners, should the necessity arise and within appropriate organizational (or law enforcement) controls.

In this paper we consider the requirements for data protection as they relate to SIEM systems and other meta-systems collecting system information for purposes such as management, billing or analysis.[1] We use the EUs 2012 draft data protection requirements as a reference in this regard, and review the associated implications.

1.1 The Nature of Information in Meta-Systems

Security Information and Event Management systems are a particularly sensitive example of a meta-system, since they receive and consolidate security event information from multiple source systems. In our experience of providing large enterprise SIEMs for various corporations we have observed that the events processed by SIEMs identify users, domains, IP addresses as well as associated activities which have been performed.

This has led us to the contention that the processing of data within SIEM systems requires explicit data protection consideration, of a level which is equal to (or possibly even more stringent) than that of the primary systems feeding them.

Since a SIEM function can be performed as a service (possibly even cloud based) it is certainly possible that the SIEM system/service and the contributing systems, from which it receives events, do not reside in the same country. For multi-national companies and operations, the source systems feeding a SIEM may also reside in different locations. So while the SIEM may be subject to the national laws in which it is operated, the reverse path situation (as described earlier) may require different notification and forensic activity depending on the country where the actual source system to which the event(s) relate is located.

Based on the introduction of these themes and issues, the remainder of this paper focuses on those areas of the draft data privacy regulation which are most relevant to SIEMs, and provides interpretation of the implications of these for SIEMs and meta-systems.

The rest of the paper is organised as follows: in Sect. 2 we briefly overview various legislative documents concerning data protection and privacy in various areas of the world. In Sect. 3 we break down the 2012 Draft EU data protection Regulation in two parts; general and specific. Where applicable, relevant sections of the Regulation are discussed and their implications of ensuring privacy in meta-systems. While the final section summarises the conclusions of this paper.

2 Data Protection as an Issue

Widespread processing, and storage, of personal information in computer systems has led to data protection concerns. The far-reaching implications of data custodianship has been recognised in many countries, with associated directives

[1] This work was conducted as part of the European Union FP7 project MASSIF http://www.massif-project.eu

and regulations being implemented or planned. The European Union has been similarly engaged in considering how to ensure data protection, given the seriousness of this issue for individuals, in member countries. In 2002, the ePrivacy Directive [4] was enacted by the EU to harmonise with Directive 95/46/EC [3] ensuring the same level of protection regarding 'fundamental rights of processing personal data - but focused on the electronic communication sectorwhile ensuring the free movement of such data. This was further amended in 2009 bringing in considerable changes such as the *cookie amendment* in Article 5(3), requiring consent to store or access information on a users device rather than 'opt-out' as stipulated in the 2002 version. The European Parliament issued a draft regulation (in January 2012) for the reform of the European data protection rules proposed by the European Commission. It is the EU General Data Protection 2012 Regulation proposal [6] which refers here. The 2012 EU draft regulation is significant to SIEMs or meta-systems, due to the fact that it entrenches data protection principles within EU legislation, and applies the core benchmarks for the protection of personal data in [the] other subsequent instruments [10].

The objectives of this reform are supported by the European Parliament as documented in the European Commission memorandum on January 8, 2013 which is "to establish a comprehensive approach to data protection, to strengthen online privacy rights and to do away with the current fragmentation of 27 different national data protection laws which are costly and burdensome for businesses operating on Europes single market [7]".

Other relevant documents adopted and published by the Communication COM[2] in January 2012 is a Communication on "Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century" [5].

Implementation of EU Directives offers room for interpretation, and the existing directive on data protection [3] (agreed in 1995) has been implemented by EU member states with varying approaches. Consequently, different levels of data protection have also resulted. In contrast, the mandatory components of an EU Regulation, imply a level of harmonisation among member states.

Differing approaches to data privacy and protection are followed by the United States when compared to the European Union. While the United States focuses on self-regulation, the European Union enforces strict legal requirements [14].

In Germany, the German Government's draft bill challenges the idea of free movement of goods and services [11]. This is due to the proposal of a strict opt-in requirement, approaching privacy in a different manner from the Data Protection Directive [3] which focuses on ensuring the free movement of goods and services.

Internationally, the 2012 EU draft regulation is considered to be the central engine of a rising global data protection regime [1].

[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century

The most recent draft of the 2012 regulation aims at fully supporting a coherent and robust data protection framework, with strong and enforceable rights for individuals. The need for a high level of protection for all data processing activities in the EU, to ensure better legal certainty, clarity and consistency [7] is also implicit. For this reason, and due to an operational/legal focus on the European environment, this paper uses the 2012 draft EU data protection regulation as its reference base. It is noted however, that the principles are closely similar to emerging (or existing) legislation relating to data privacy and protection in many other countries.

As at the time of writing, the draft regulation on personal data protection is being considered in the European Council, with the intention of finalisation prior to June 2014, but this depends on the adoption process.

In the interim, this document outlines a set of guidelines by which meta-systems need to be assessed in terms of privacy and data protection.

An important principle of the EU draft regulation is the principle of *accountability*. This ensures better data protection implementation and enforcement, through compelling the controllers (who control the flow of data within systems) to take measures that are best suited and appropriate to implement the data protection principles, and consequently demonstrate what these measures were [10].

A further principle of the EU draft regulation is around the issue of *notification*. In general the notification requirements of the draft regulation on data privacy are inconsistent with respect to the eCommerce directive [4], and for ICT service providers a level playing field is sought in this regard. It is interesting to extrapolate how notification would apply for a meta-system, since users may not even be aware that their information is being propagated to a SIEM or meta-system. So while notification to relevant authorities is clear, the notification process to users (relating, for example, to a loss of their personal information) would have to use a reverse-path mechanism to notify each source system, and then trigger their notification process.

3 Detailed Considerations of Meta-System Implications

In terms of general requirements there are preliminary (and umbrella) matters to consider such as subject matter, scope, term definitions, principles of processing personal data, distinguishing between different categories of data, and measures based on automated processing.

3.1 General Provisions and Principles

From a SIEM perspective, these general provisions and principles[3] imply that when considering data processing issues for SIEMs and meta-systems:

[3] Articles 1-10 of Draft Regulation 2012/0011/EC

- SIEM roles need to be made explicit and confirmed: data subjects, personal data and the role of *processor* need to be agreed and demarcated.
- For the SIEM, the framework needs to define distinctly what personal data is; what categories exist within the framework; and their individual rules of processing and authorisation of use. This can be set up as a policy of the meta-system and with the definition of rule sets for handling personal data. An example scenario to consider is whether information regarding a user's query frequency, IP logs, and 'type' of querying – used to help profile for security analysis/log purposes – can be seen as personal data. If it is agreed as personal then certain measures but must be take to ensure the results produced are protected and *only* available for the purpose of security analysis. A possible solution would be to map the data to aliases that can only be linked back to the user ids by security administrators, this type of approach is used by TomTom.[4]
  Use of anonymisation should be considered, where security patterns can be identified, without the need to necessarily tie this back to an individual in the first instance. A relevant reference implementation for how anonymisation could work in a SIEM context is PINQ. PINQ is an example of a system that integrates differential privacy into a database query framework (C# LINQ) [9]. The approach enables users to write programs that produce statistical results and deductions, whilst relying on an underlying privacy mechanism ensuring some formal notion of disclosure control [12]. This can ensure data privacy is not compromised, but still allow the free necessary flow of data within the framework. It is considered that this could be a *bridge* to creating the type of anonymisation envisaged for SIEM systems as well. As mentioned earlier however, security insight maybe reduced in some instances through the use of anonymisation.

Another topic introduced in the draft data protection regulation is *conditions for consent*,[5] which is where actual consent needs to be retrieved from data subjects. From a SIEM perspective, this implies that processing of personal data in a SIEM must be limited to the minimum possible, for whatever purpose this is used for (this should be ensured by the Processor), and can only be stored after a periodic review is carried out to confirm its necessity of continued storage – unless it is solely for historical, statistical research. In a SIEM, all areas where personal data is kept need to be assessed and evaluated as to whether their storage is still necessary.

In terms of the draft data protection regulation, the conditions by which it is lawful to process data depend on the purpose and include the principle that processing of data can only be done with the consent of the data subject (and for an explicit purpose). This could mean that users need to be explicitly notified of meta-processing by SIEMs and/or other meta-systems.

[4] http://www.tomtom.com
[5] Article 7, Draft Regulation 2012/0011/EC

Consent is seen as the burden of the Controller: to ensure he/she has proof of consent from a data subject. For a SIEM this must be enforced too, and it falls under the area of documenting requirements of a controller.

In addition to the documenting of 'consent', a data subject needs to be provided with information from the Controller regarding the consequences of processing the data, for example for profiling. Thus constant communication between the Controller and related data subject is what needs to be considered. The challenge though is that there may not be a (direct) relationship between the SIEM system and its Controller, and the end users or systems being managed. So the issue of consent requires further consideration within the context of a SIEM type service.

3.2 Area Specific Implications for a SIEM Framework

There are four main sections applicable to meta-systems, and where more specific consideration will be provided. The areas we have identified are: data subject rights,[6] data security,[7] authorisation control[8] and personal data transfer.[9]

Data Subject Rights. The EU draft regulation refers to all rights concerning a data subject (an identified natural person). Issues such as the right to rectification of personal data are considered.

The rights of a data subject are implicated in a SIEM perspective too and this needs to be integrated considering the following factors:

- The system needs to determine what is defined as personal data within the framework, and by what and whose rights it can be accessed. The question can be applied to cookies, IP addresses, RFID tag numbers.
  An example of data fields used in a large production SIEM is shown in Fig. 1. One can identify user sensitive fields such as user location where personally identifiable information may be propagated.
  It is recognized that 'on-the-fly' pseudonymisation of event data can ensure that personal information is not exposed during SIEM/meta-system processing, but that the ability for efficient security analysis is preserved. An existing method implemented by Biskup et al. [2] has been documented whereby audit data is inspected for personal data and identifiers referring to real persons, and replaced by transaction-based pseudonyms. A similar approach could work for SIEM and other meta-systems. In the scheme of Biskup et al., pseudonyms are set as shares for a suitable adaptation of Shamir's secret sharing cryptography. If suspicion is created relating to certain events or actions then re-identification could occur under the control of the source systems Controller [2].

[6] Articles 11-21, Draft Regulation 2012/0011/EC
[7] Articles 30-32, Draft Regulation 2012/0011/EC
[8] Supervisory Authorities: Articles 39-49, 46-54, 55-63, Controller and Processor: Articles 22-29, Data Protection Officer: Articles 35-37 of the Draft Regulation 2012/0011/EC
[9] Articles 40-45, Draft Regulation 2012/0011/EC

IP Location Fields		
16, 23, 38	[Source/Destination]IPPrivate[2]	A binary indicator which specifies if the IP address in `SourceIP[2]` is private or empty string if it is public.
17, 24, 39	[Source/Destination]IPGeoCC[2]	Two letter country code of the IP address in `SourceIP[2]` or string "1918" if the IP address is private.
18, 25, 40	[Source/Destination]IPGeoASN[2]	Autonomous System Number (ASN) of the IP address in `SourceIP[2]` or empty string if it is private.
19, 26, 41	[Source/Destination]IPGeoLat[2]	Latitude of the IP address in `SourceIP[2]` or empty string if it is private.
20, 27, 42	[Source/Destination]IPGeoLong[2]	Longitude of the IP address in `SourceIP[2]` or empty string if it is private.
Descriptive Fields		
7	SensorNameDescription	Describes the sensor type in `SensorName` (e.g. domain controller, member server and workstation).
47	AccountType	Describes if the account type in `UserName2` is privileged, a system account or a computer account.
54	ServiceType	Determines the computer type in the `ServiceName` field and distinguishes between domain controller, member server or workstation.
63	CodeDescription	Provides a description in words for the codes in `StatusCode`, `SubStatusCode` and `ResultCode`.

Fig. 1. Extract of field data categories in a SIEM system.

– The aim of data protection legislation is not to curb or limit the processing of data. The most important goal for it is to actually allow free flow of personal information, but with the critical point of having awareness on the sensitivity of the data which requires safe-guarding to protect a persons fundamental rights [10]. Thus, the SIEM framework needs to embrace the concept to encourage this.
This can be done by making rule sets, implementing differential privacy in DBMS layers, or constructing management of all layers of the framework using cryptographic keys on the various levels to ensure the data privacy.

Some additional rights and documentation requirements relating to SIEMs are as follows:

– Users have more specific rights that need to be accommodated in the SIEM Framework, particularly the rights to object; to be forgotten; to erasure and to data portability (whereby a user can transfer his/her own data without consent of the Controller).
– Further documenting procedures need to be handled by the Controller, including the reasons for the rejection of a data subject request by a Controller if this is the case, and communication on all possible consequences of processing the data subjects data.
– If not handled correctly, particularly for concepts such as data erasure rights, this can be quite onerous for a SIEM and/or undermine the very types of activity that the SIEM is trying to detect or predict.

Data Security. The EU draft regulation for data protection refers to security of processing, and prescribes measures for data protection to ensure a certain common level of security. From a SIEM and meta-system angle, the articles imply that:

- From the data security perspective we have a list of specifications for automated data processing that needs adherence to ensure data protection. In light of this, a SIEM Framework needs to evaluate its control of equipment access, data media, storage, users, data access, communication, input, transport, recovery, reliability and integrity. For each of the preceding items mentioned, the SIEM framework needs to be assessed (where applicable) and checked to see if each principle is enforced; if it is reliable; and if it is documented.

In addition, measures to be taken against unauthorised disclosure or alteration of personal data are required. From a SIEM perspective, these articles imply that a security mechanism to ensure the prevention of unauthorised disclosure should be implemented in the SIEM Framework, in the form of user control and user monitoring for the SIEM system itself. This should be formed by first constructing an evaluation of the risks to the system, to determine what areas needs to be secured. In essence though, this re-inforces our earlier assertion that SIEMs need to be viewed (and scrutinized) as systems in their own right.

Authorisation Control. The EU draft regulation for data protection refers to forms of authority needed by a person or persons to enforce data protection and privacy as stipulated. From a SIEM perspective, these articles imply that:

- All persons falling under the definition of 'controller' and 'processor', need to adhere to the responsibilities, rights and need for process documentation.
- Supervisory authorities need to be set up to enable the rights of a data subject to be heard, and to ensure that data processors do not abuse the power over the data given to them for processing [10].
- Based on the draft regulation requirements, it is recommended to appoint a Data Protection Officer within the SIEM or meta-system framework, and for the SIEM system/processing to be seen in terms of other source systems as well. In this way the focus on ensuring data privacy and protection can be examined.

The draft regulation specifies additional responsibilities for certain bodies, and includes a specification for a 'consistency' mechanism[10] whereby the unity of application in terms of data processing needs to be ensured. In particular:

- The Controller and Processor need to perform a data protection impact assessment. This has to be formally structured, and falls under the Duty of the Controller with the Duty of the Supervisory Authority perhaps, to confirm its assessment validity.

[10] Section 3.4.7.2 Draft Regulation 2012/0011/EC

- Prior authorisation and consultation needs to be obtained by the Controller and Processor from the Supervisory Authority.
- Binding Corporate Rules need to be set by supervisory authorities to ensure protected transfer.
- The code of conduct needs to written up and decided on within the SIEM Framework by a supervisory authority or board.
- The concept of data protection 'seals and marks' is introduced for *certification*. The question is whether they can be extended towards SIEMs.
- A *consistency* mechanism with regard to processing operations needs to be explicitly created within the SIEM Framework. People categories that fall under authorisation control need to ensure a consistency when dealing with data between boards, this could be implemented in a SIEM Framework with universal 'data handling' policies.
- The European Data Protection Data Board is to consist of the heads of the supervisory authority of each Member State and of the European Data Protection Supervisor. This is needed to ensure the consistent application of this Regulation.

Personal Data Transfer. The EU draft regulation for data protection refers to conditions and principles concerning the transfer of personal data including international transfer. From a SIEM perspective, the implication is that:

- Privacy and Data protection must not be compromised regardless of the transfer of personal data. The need to ensure this can be done by assigning a global data protection officer, to whom all data protection officers of an organisation report.
- An effort is required to ensure harmonisation across different areas with varying legislation, especially if a multi-national scenario (such as outlined previously) is implemented.

With regard to handling personal data, various approaches are needed depending on the purpose it is being processed for, and the type of data. This is aligned with our premise that meta-systems, like SIEMs, form a special case of processing purpose, requiring particular consideration.

With regards to a SIEM Framework, is it structurally definable as to what types of personal data there could be (as mentioned previously when dealing with categories of data). These data set elements would then be handled specially in the flow of events within a SIEM Framework, and it would be necessary to ensure associated privacy levels, according to the purpose of data retrieval and the respective 'type' of data. Similar discrimination should be considered for other meta-systems involved in management, billing etc.

4 Conclusions

In this paper we have noted the importance of data protection, and that the requirements for *primary* processing systems are not necessarily easily extrapolated to (or implemented by) *meta-systems* such as SIEM systems.

Using SIEMs as an example of meta-systems, we have attempted to clarify the implementation of data protection and privacy for these, and to make explicit the associated requirements for a meta-system.

In particular, roles need to be clearly defined (for example processor, controller etc.) for a meta-system in the same way as they are for any other system. The SIEM or meta-system itself needs to be treated as a processing system of an organisation. This means that the data residing in the system needs to be made explicit, with the retention and storing/processing purposes made known and documented. A data protection officer should be assigned, with responsibility for the meta-system in the same manner as other systems.

Given the potential sensitivity of data collected by a SIEM this needs to be done very carefully. Techniques of anonymisation or aggregation can also be used where applicable. Rules for processing jurisdiction could either be agreed contractually with SIEM providers, or there may be ways to embed such meta-information into the processing rules of cloud or other service providers so that Service Level Agreements can be implemented to guide and control how security processing is conducted.

This paper has introduced the initial aspects that we believe need to be addressed, but it is evident that additional analysis and interpretation is required to ensure that the data protection rights of individuals are upheld in meta-systems too – while still enabling safe and secure system management.

Acknowledgments. The authors would like to thank Joachim Hoenig, Director of the Deutsche Telekom AG, Brussels Representative Office in Belgium.

References

1. Birnhack, M.D.: The EU data protection directive: an engine of a global regime. Comput. Law Secur. Rev. **24**(6), 508–520 (2008)
2. Biskup, J., Flegel, U.: Transaction-based pseudonyms in audit data for privacy respecting intrusion detection. In: Debar, H., Mé, L., Wu, F. (eds.) RAID 2000. LNCS, vol. 1907, pp. 28–48. Springer, Heidelberg (2000)
3. European Commission: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Brussels, 24 Oct 1995
4. European Commission: Directive 95/46/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Brussels, 12 July 2002
5. European Commission: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century, Brussels (2012)

6. European Commission: Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25 Jan 2012
7. European Commission: MEMO, Brussels, 8 Jan 2013
8. CRN: Siem: A market snapshot (2007). Accessed 10 June 2012
9. McSherry, F.: Privacy integrated queries: an extensible platform for privacy-preserving data analysis. Commun. ACM **53**(9), 89–97 (2010) (ACM Press, New York)
10. Gellert, R., Gutwirth, S.: Beyond accountability, the return to privacy? In: Guagnin, D., Hempel, L., Ilten, C., Kroener, I., Neyland, D., Postigo, H. (eds.) Managing Privacy Through Accountability. Palgrave Macmillan, New York (2012)
11. Hoeren, T.: The new German Data Protection Act and its compatibility with the European Data Protection Directive. Comput. Law Secur. Rev. **25**(4), 318–324 (2009)
12. Gehrke, J: Programming with differential privacy. Commun. ACM **53**(9), 88 (2010) (ACM Press, New York)
13. Jenkins, S.: Learning to love SIEM. Netw. Secur. **2011**(4), 18–19 (2011)
14. Steinke, G.: Data privacy approaches from US and EU perspectives. Telematics Inform. **19**(2), 193–200 (2002) (Regulating the Internet: EU and US perspectives)

Modelling of Integrated Trust, Governance and Access

safi.re: Information Sharing Architecture

William J. Buchanan[1(✉)], Omair Uthmani[1], Lu Fan[1], Niall Burns[1], Owen Lo[1], Alistair Lawson[1], James Varga[2], and Cassie Anderson[2]

[1]School of Computing, Edinburgh Napier University, 10 Colinton Road, Edinburgh EH10 5DT, UK
w.buchanan@napier.ac.uk
[2]miiCard, Elliot House, 8 Hillside Crescent, Edinburgh EH7 5EA, UK

Abstract. We live in a world where trust relationships are becoming ever more important. The paper defines a novel modelling system of trust relationships using Binary Decision Diagrams (BDDs), and outlines how this integrates with an information sharing architecture known as safi.re (Structured Analysis and Filtering Engine). This architecture has been used on a number of information sharing projects, including within health and social care integration, and in sharing between the police and their community partners. The research aims to abstract the relationships between domains, organisations and units, into a formal definition, and then implement these as governance rules, and using the trust relationship definition, and the rules.

Keywords: Information sharing · Trust · Governance · Binary Decision Diagrams

1 Introduction

In an increasingly connected world, data is becoming a key asset, especially within a Big Data context, where data from different domains can be brought together to provide new in-sights. Most of the systems we have in-place, though, have been built to securely keep data behind highly secure environments, and then have difficulty in integrating with other disparate systems. This is now a major barrier to using data in a wide range of applications. Along with this, information sharing has many regulatory constraints, which often disable information sharing across domains, but, with carefully managed information architectures, it is possible to overcome many of these problems. An important challenge is thus to support information sharing across different domains and groups, across multiple information systems. In the context of this paper, a domain is defined as the governance (and possible ownership) of a set of data, which is exposed to others through well-managed services.

The problem of providing governance around trusted infrastructures is highlighted by Boris Evelson who outlines that [6]:

M. Felici (Ed.): CSP EU FORUM 2013, CCIS 182, pp. 91–101, 2013.
DOI: 10.1007/978-3-642-41205-9_8,

> Big data is such a new area that nobody has developed governance procedures and policies, there are more questions than answers.

A feature of any trusted infrastructure is that the owner of the data is clearly defined, and this entity can differ from the actual governance of it. For example, in a health care system, the owner of the data can be the citizen, and the governance of the data is defined by the health care provider (such as the National Health Service (NHS) in the UK). In a full trust infrastructure, the citizen could have full rights to define who had access to their data.

The safi.re architecture has been used in a number of projects including within health and social care, including with the TSB-funded project with Chelsea and Westminster Hospital in London which focused on creating an e-Health Cloud within a hospital environment [1]. This used a novel method of defining the ownership of the data, and providing a rights infrastructure for the citizen (or patient) to define the rights of access to their data. This work has since been extended within a number of projects including the TSB Trusted Service project, which has focused on integrating both digital and human trust, to provide a fully integrated and holistic care infrastructure, and which integrates primary and secondary health care with assisted living [2–4].

Another important area for information sharing is within the holistic care, where information from different public sector agencies can be used to improve the care of citizens. This might relate to sharing information on a child for concerns posted within health, social care, education and policing, where concerns within just one of these domains would not be seen as a major concern, but when aggregated across several of these, it might result in the concerns being escalated to the point where an action plan is initiated [5]. The work has thus into projects which involve information sharing for Child Protection, and which integrate with a multi-agency approach. As there is information held within each of the public sector agencies, it is important that accesses are well managed and controlled for the rights for the access to data.

The next section outlines the safi.re information sharing and how information rules are defined. After this the paper outlines a novel method for the modelling of information sharing using Binary Decision Diagrams (BDDs), and show how this integrates with the architecture. The final sections outline the results of simulations and in the main conclusions of the work.

2 Architecture Outline

A major problem within many information infrastructures is the control of information between organisational boundaries. Normally this is defined with a security policy, but the scope of this is often just defined within an organisation. As more information crosses organisations and domain boundaries, it is becoming difficult to manage the number of possible ways that information can be shared and aggregated. A key element of this is the increasing requirement for trust between organisations and units, especially with the move towards cloud-based services. The safi.re (Structured Analysis, Filtering and Integrated Rules Engine) architecture overcomes these

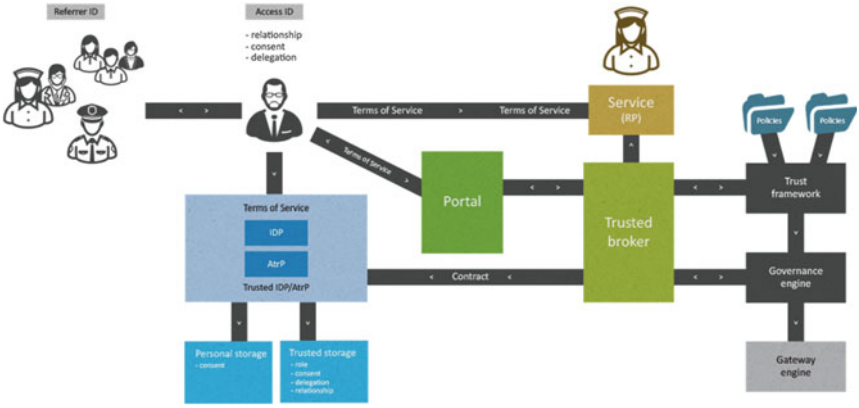

Fig. 1. Trust, governance and access framework

problems by creating a formal structure for the abstraction, governance and implementation of trust relationships and security policies. It can be used as a full end-to-end solution for policy abstraction, implementation and controlled access to services, or can integrate each of the elements as a Service to existing applications.

safi.re supports three basic components, each of which can operate as a stand-alone product or can integrate with existing systems. These are:

- **Safi.re TRUST**. This is a trust framework which abstracts the roles and services and defines their trust relationship. The export from this component is the requirements for the information sharing/service aggregation policy.
- **Safi.re GOVERNANCE**. This takes, as an input, the abstraction of the trust framework, and runs the rules required to define if an entity has the rights to access a given service.
- **Safi.re GATEWAY**. This takes the rules from the governance engine, and implements them within a real-time filtering system, which controls all the accesses to services between the domains.

In modern service-oriented infrastructures a user must gather claims to consume a service. Too often the service is bound to a specific authentication infrastructure which limits the scalability of the provision of the service. For more dynamic infrastructures there is no direct communication between the service and the gathering of the claims around identity and the attributes required to consume a service. Figure 1 thus outlines this process, where there are Terms of Service (ToS) between a user and their identity and attribute provider, another ToS between them and the service, and so on. It is the focus of the Trust and Governance infrastructure to define a contract which binds these terms of service together. This contract pre-defines the requirements for the claims to the service, and then is trusted to actually issue the contract for the user to consume the service.

3 Trust, Governance and Access

This paper is based on the integration of a formal trust framework and implemented rules, and then modelling of complex trust relationship between domains using a patent pending method of Binary Decision Diagrams (BDDs) [14]. BDDs are rooted, directed, acyclic graphs originally proposed by Lee [7] in 1959 and Akers [8] in 1978 to graphically represent Boolean functions. BDDs originate from binary decision trees which are rooted, directed trees that can be used to represent Boolean functions. For example, the decision tree illustrated in Fig. 2 represents the Boolean function f(x; y) = (x ∨ y).

3.1 Reduced Ordered Binary Decision Diagrams (ROBDDs)

In 1986, Randal Bryant proposed a solution to this problem in [9] by introducing algorithms for reducing binary trees and ordering the variables in a function. The process of reduction consists of merging any isomorphic sub-graphs for the decision tree. Any parent node which has child-nodes that are isomorphic is considered redundant and is removed. Applying this process to the decision tree for the Boolean

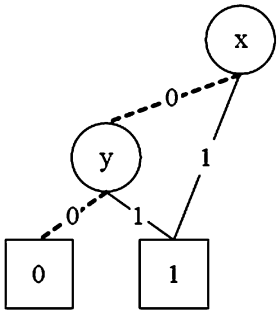

Fig. 2. Reduced Binary Decision Diagram for the function f(x; y) = (x ∨ y)

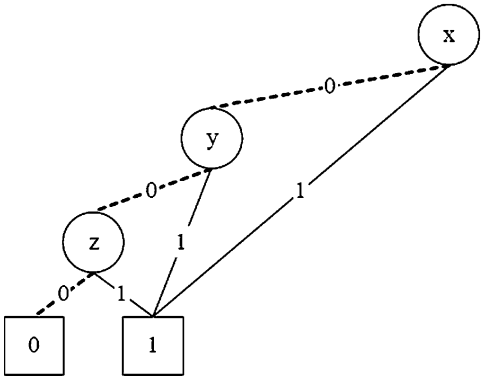

Fig. 3. Reduced Binary Decision Diagram for the function f(x; y; z) = (x ∨ y ∨ z)

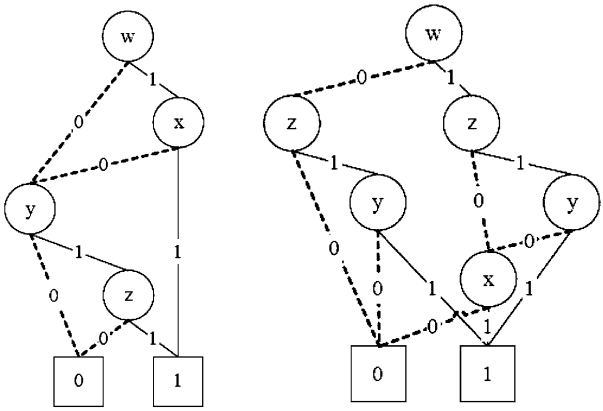

Fig. 4. Reduced Binary Decision Diagram for the function f(w; x; y; z) = (w ∧ x) ∨ (y ∧ z) with variable ordering of w; z; y; x

function f(x; y) = (x ∨ y), as illustrated in Fig. 2, it is evident that if the first node, x, is 1, then the value of the second node, y, has no effect on the terminal node value of the Boolean function: whether y is 0 or 1, the value of the terminal nodes is 1. This means that the where node x is 1, child-nodes of y are isomorphic. Node y can then be considered redundant here and removed. The result is the reduced decision tree illustrated in Fig. 3. Similarly, applying the reduction process to the decision tree for the Boolean function f(x; y; z) = (x ∨ y ∨ z), illustrated in Fig. 3, yields the reduced decision tree shown in Fig. 4. Reduced decision trees allow a much more compact representation of Boolean expressions than non-reduced decision trees.

Bryant also highlighted in [9] that the size of a decision tree for a given function is dependent on the ordering of the variables in that decision tree. For example, the decision tree for the Boolean function f(w; x; y; z) = (w ∧ x) ∨ (y ∧ z), given a variable ordering of w; x; y; z, is illustrated on the left-hand diagram in Fig. 4.

If the variable ordering for the same function was now changed to w; z; y; x, the resultant decision tree will be more complicated, as illustrated in the right hand side of Fig. 4. Hence, an optimal variable ordering will produce the simplest, and therefore smallest, decision tree for a given function, while sub-optimal orderings will produce larger and more complex decision trees for the same function. However, as shown by Bollig and Wegener in [10], determining the optimal variable ordering for a Boolean function is an NP-complete problem that often requires trial and error or expert knowledge of domain-specific ordering strategies.

Decision trees which have been reduced and ordered are referred to as Reduced Ordered Binary Decision Diagrams (ROBDDs), or commonly shortened to just Binary Decision Diagrams (BDDs). A key property of the reduction and ordering restrictions introduced by Bryant is that the resulting BDDs are canonical [13]. This means that the BDD for any Boolean function, for a defined variable ordering, will always be isomorphic. This property has made BDDs ideal for use in formal equivalence checking. In the electronic design automation process, for example, BDDs are frequently used to formally prove that two circuit design representations exhibit the same behaviour.

3.2 BDDs in Policy Modelling

A novelty of this paper is to exploit the unique properties of Binary Decision Diagrams (BDD) to model complex sets of policies, in a form that is readily machine-executable, and to extend these to the information-sharing domain. The work of Hazelhurst et al. [11] with firewalls identified key constituent fields in access-list rules and translated these into bit vectors representing BDD variables. This research applies a similar methodology to information-sharing where a set of information-sharing policies can be modelled as a decision diagram, once a specific variable ordering scheme has been selected. The modelling of a set of policies as a BDD provides a number of significant advantages, including providing an efficient lookup mechanism for an information-sharing request as well as providing a graphical representation of the overall policy set. As rule sets become larger and more complex, they become difficult to interpret and maintain [12]. Modification of the rule set, by either adding new rules or removing existing ones, or even changing the order of rules has a significant impact on the behaviour of the policy-based system. Hence, analysis and validation of large, complex rule sets is essential in ensuring that high-level directives are enforced. Further, exploiting the formal equivalence checking ability of BDDs, and the fact that they can canonically represent Boolean functions, multiple sets of policies can be compared to ensure that they have the same behaviour or identify areas where they behave differently. Large and complex rule sets, represented as BDDs, can, therefore, be efficiently modelled, analysed and validated.

3.3 Domain Modelling Using BDDs

The core of the patent is the linkage with the trust framework and the governance rules. In order to simply the access to data from domains, the method exposes only well-managed services to define the trust relationship. Within this the model defines a number of modelling elements, including:

- **Permission**. This is a simple permit or deny for access to a service.
- **Domain**. This relates to the domain that an accessor is contained within, and is used to create the holder to the domain ontology.
- **Organisation**. This relates to an organisation with a given domain.
- **Unit**. This relates to a unit with an organisation.
- **Role**. This defines the role that an accessor has in access a service within another domain.
- **Relationship**. This defines the relationship that the accessor has to the data being accessed.
- **Action**. This defines a CRUD (Create, Read, Update or Delete) access to a service and its associated data.
- **Attribute**. This defines an attribute of the object to be access, such as for a health record.
- **Object**. This defines the actual access target, such as for a specific person.
- **Context**. This defines the content of the investigation (which can be used to define certain risk levels for access privilege escalation.

- **Compliance**. This defines the audit/compliance reasons for the access.

The trust framework then defines the usage of each of these fields, and rules are written which implements them. A sample rule is thus:

> [Permit] [Police.Police_Force_A.*.Sergeant] with [*] relationship [R] [Unique_Identifier] of [Child] with [Abuse_Investigation] context from [Social_Care.Child_Protection_Agency_B.Records_Unit.Records_Admin] with Compliance [Human_Rights_Act_1998]

Overall the BDD model uses a binary representation for each of these fields, and which builds-up a rule definition with the binary representation of each of the possibilities for the fields. For example if there are four roles, we can represent them with:

- 00 – Constable
- 01 – Sargent
- 10 –Superintendent
- 11 – Chief Superintendent

These rules then use the BDD to determine if there are issues within the governance rules related to:

- **Redundancy**. This is where one set of rules is already included within the trust rules already defined.
- **Shadowing**. This is where a rule is higher up in the set of rules, and matches all the conditions that match in the current rule, such that the shadowed rule will never be activated.
- **Generalisation**. With this a rule is generalisation of another preceding rule if it matches all the packets of the preceding rule.
- **Correlation**. Two rules are correlated if the first rule in order matches some of the fields of the condition of the second rule and the second rule matches some of the fields of the condition of the first rule.

3.3.1 Simple Example

This example describes in detail the steps needed to translate a set of information-sharing policies to a BDD. List 1 shows a sample list of policies. A '*' or 'Any' is used to denote redundant fields, or redundant portions of fields. Redundant fields are not translated into binary as they represent variables that are not evaluated by the BDD and, hence, do not form part of the Boolean function. Where an entire field is redundant, it is entirely excluded from the binary representation and where only a portion of a field is redundant, only the relevant portion is translated while the redundant portions are shown using 'Xs'.

Listing 1:

Policy 1: This policy <permits> <ANY> requester, with <ANY> relation in <ANY> context, to request to <read> a <child's> <Health History Record> from the <Records Admin> of the <Records Unit> of <Child Protection Agency 'B'> under compliance of the <Data Protection Act>

Policy 1:

Compliance (DPA)	: 1
Requester (Any)	: not checked by BDD
Relation (Any)	: not checked by BDD
Context (Any)	: not checked by BDD
Object (Child)	: 1
Attribute (Health History Record)	: 01
Owner (SocCare.CPA-B.RecUnit.RecAdmin)	: SocCare : 10
	: CPA-B: 10
	: RecUnit : 10
	: RecAdmin : 10
Action (Permit)	: 1

The Boolean function corresponding to Policy1, ignoring redundant fields, is a logical conjunction of all of the above fields in the format shown in Listing 2. Listing 2 represents Policy1 expressed logically as an 'if–then' conditional statement and Fig. 1 illustrates Policy1 as a BDD.

Listing 2:

Permit: Compliance ^ Owner ^ Object ^ Attribute

Listing 3: Rule1 expressed as an if–then conditional statement.

```
if      (Compliance = 1) ^
        (Owner = 10101010) ^
        (Object = 1) ^
        (Attribute = 01),
then (Action = Permit)
```

4 Results

This section offers an overview of the total processing times for a 2.6 GHz processor with 2 GB of memory, using a range of policy-set sizes. Two initial tests comprising of 1,000 policies and 10,000 are run in order to ensure that the test platform is stable. Following these, tests are run starting with a set of 100,000 policies and repeated at increments of 50,000 policies, until a maximum set of 1,000,000 policies is tested. During each test, measurements of percentage CPU utilisation, RAM usage and

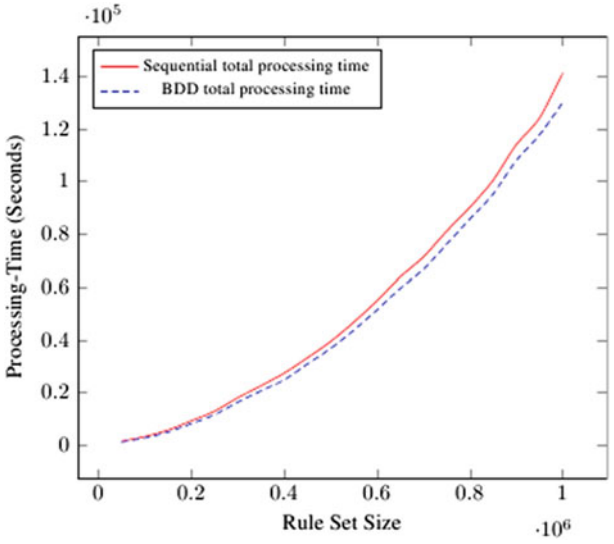

Fig. 5. Comparison of total processing times using sequential and BDD methods against increasing rule set size

latency are gathered for each stage of the policy verification process. Further, measurements for the anomaly detection stage are gathered for both sequential and BDD modes of operation.

As illustrated in Fig. 5, the total processing times increase with respect to increasing policy set size. Hence, with the same available resource configuration, it is expected that the total processing time will increase proportionally to the size of the policy set. In fact, as illustrated by the graphs in the figures mentioned, the rate of change of the total processing time increases with increasing policy set size, indicating a polynomial relationship.

A related observation from these is that the total processing times for the sequential method are higher than the total processing times for the method using Binary Decision Diagrams (BDDs). This result is expected, as the process using BDDs, due to their tree structure, involves fewer computations than sequential comparisons. Further, it should be noted that the total processing time for the sequential process increases at a greater rate than the total processing time for the process using BDDs.

5 Conclusions

This paper has outlined the safi.re architecture which integrates a trust framework and governance rules. As information opportunities increase with a sharing across domains, the modelling of polices is becoming important especially in identifying redundancy, shadowing, generalisation and correlation. The method defined in this

paper uses BDDs, which support a structured approach to the modelling, and which identifies problems in the governance rules.

As trust relationships are becoming a key focus within defining the security infrastructure between organisations, the complexity of these relationships is becoming a key factor. If we simplify these too much, it reduces the problem to simplistic rules which often do not reflect the actual inter-relationship between organisations. The long term goal must thus be to implement a trust infrastructure which can properly define the interaction between organisations, and this will require large-scale modelling of these. A key element of this will be the modelling of these governance rules between organisations as these will identify problems in the organisation of the governance rules. The BDD method outlined in this paper thus supports the next generation of trust relationships, and their related governance rules, and provides a method to reduce complexity of these.

While the BDD method has been applied to static modelling of policies such as in modelling network firewall rules, there is a need to model temporal rules, thus the modelling requires to be undertaken at frequent intervals in order to catch new rules which may conflict with existing ones.

References

1. Fan, L., Buchanan, W., Thuemmler, C., Lo, O., Khedim, A., Uthmani, O., Lawson, A., Bell, D.: DACAR platform for eHealth services cloud. In: 2011 IEEE International Conference on Cloud Computing (CLOUD), pp. 219–226 (2011)
2. Fan, L., et al.: SPoC: protecting patient privacy for e-Health services in the cloud. In: The Fourth International Conference on eHealth, Telemedicine, and Social Medicine, eTELEMED 2012 (2012)
3. Ekonomou, E., Fan, L., Buchanan, W., Thuemmler, C.: An integrated cloud-based healthcare infrastructure. In: 2011 IEEE Third International Conference on Cloud Computing Technology and Science (CloudCom), pp. 532–536. IEEE, November 2011
4. Lo, O., Fan, L., Buchanan, W.J., Thuemmler, C.: Technical evaluation of an e-health platform. IADIS E-Health (2012)
5. US Patent Application No 13/739074, The Court of Edinburgh Napier University, Short Title: Binary Decision Diagrams, IP Title: Improved Information Sharing, Submitted: 11 Jan 2013
6. Roger du Mars, Mission Impossible? Data Governance takes on Big Data, Boris Evelson, BI Trends and Strategies (2012). http://cdn.ttgtmedia.com/searchBusinessAnalytics/downloads/BI_Trends_+_Strategies_July_2012.pdf. Accessed July 2012
7. Lee, C.: Representation of switching circuits by binary decision programs. Bell Syst. Tech. J. **38**, 985–999 (1959)
8. Akers, S.B.: Binary decision diagrams. IEEE Trans. Comput. **C-27**(6), 509 (1978)
9. Bryant, R.: Graph-based algorithms for boolean function manipulation. IEEE Trans. Comput. **C-35**(8), 677–691 (1986)
10. Bollig, B., Wegener, I.: Improving the variable ordering of OBDDs is NP-complete. IEEE Trans. Comput. **45**, 993–1002 (1996)

11. Hazelhurst, S., Fatti, A., Henwood, A.: Binary decision diagram representations of firewall and router access lists. University of the Witwatersrand, Johannesburg, South Africa, Tech. Rep. TR-Wits-CS-1998-3 (1998)
12. Hazelhurst, S.: Algorithms for analysing firewall and router access lists. University of the Witwatersrand, Johannesburg, South Africa, Tech. Rep. TR-WitsCS -1999-5 (2000)
13. Bryant, R.E.: Symbolic boolean manipulation with ordered binary-decision diagrams. ACM Comput. Surv. **24**, 293–318 (1992)
14. US Patent Application: 13/739074
15. Hardt, D. (ed.): The OAuth 2.0 Authorization Framework, IEFT RFC 6749. http://tools.ietf.org/html/rfc6749.html (October 2012)

Security and Privacy Technology

A Marketplace for Business Software with Certified Security Properties

Midhat Ali[1,2], Antonino Sabetta[1(✉)], and Michele Bezzi[1]

[1] SAP Product Security Research, Sophia-Antipolis, France
antonino.sabetta@sap.com
[2] Computer Science Division—School of Science and Technology, University of Camerino, Camerino, Italy

Abstract. Digital marketplaces (e.g., the Amazon Web Service Marketplace or the Google Apps Marketplace), offer computation and data platforms as services to Independent Software Vendors (ISVs). ISVs, in turn develop applications and services on these platforms and sell these software products to customers, through the marketplace.

While these products are usually accompanied with descriptions of their functionality, it is hard for customers to reliably determine whether their security needs will be satisfied by a given product, (*a*) because its security properties are not expressed explicitly, or (*b*) because of lack of assurance that those properties are actually enforced.

While this limitation of today's marketplaces might be acceptable for private users, it represents an important obstacle to adopting the marketplace metaphor for the procurement of business applications, which need to comply with specific security and regulatory requirements.

Building on recent research results on service security certification, which are available as part of the Assert4Soa framework, in this paper we present a certification-aware Business-Software marketplace where software products have explicit, transparent, and verifiable certificates of security properties.

Our proof-of-concept provides business users with an infrastructure to search and compare cloud services based on security and assurance requirements.

1 Introduction and Motivation

Cloud platforms provide an easy way for software vendors to offer applications to their customers without the need to setup and maintain a costly IT infrastructure on their own. Because of the flexibility and the economic attractiveness of business models offered by the cloud paradigm, over the recent years, more and more companies are moving their offering to cloud-based solutions.

These cloud based applications are offered in an application marketplace, from where customers can choose the applications for their requirements.

Despite this growing popularity, security is a major concern for cloud adopters. In a survey [1], 65 % of respondents reported a higher number of security breaches in a cloud environment than their traditional infrastructure. Another recent

M. Felici (Ed.): CSP EU FORUM 2013, CCIS 182, pp. 105–114, 2013.
DOI: 10.1007/978-3-642-41205-9_9,

study [2] of the security incidents reported in the news in the first five years of cloud computing found that about 25 % of the 172 incidents considered could not be associated to any specific threat because their cause was unknown or not disclosed. These results lead CSA to conclude that cloud vendors should *be more transparent in order to make the cloud a more trustable, reliable and secure environment for both end-users and enterprises* [2].

Indeed, the problem of transparency is a consequence of the very nature of the cloud model, according to which infrastructure (IaaS), the platform (PaaS), or the application (SaaS) are offered as commodity services to customers. While this model frees customers from undesirable costs and overhead, it does not give them direct control or access to important information about the internals, the configuration, and the status of the systems they access.

The popularity of the marketplace metaphor exacerbates the problem even further. Cloud marketplaces, such as Amazon Web Service Marketplace or the Google Apps Marketplace, are organized as open ecosystems, where new vendors (be they one-person businesses, SMEs, or large corporations) enter the marketplace every day and with whom potential customers have never conducted business before. In such context, in which reputation alone cannot be reliably used to build trust, software procurement is problematic because important information about the security (or lack thereof) of candidate applications or services is not available. While private customers may not consider this problem as critical, it does represent a major stumbling block for businesses, who must ensure that their own customers' security is guaranteed and who risk reputation and financial loss in case of security incidents. To mitigate these risks, businesses strive to be in the position of proving that they performed due diligence to ensure that the software they use complies with the relevant security and data protection laws and regulations.

Approaches based on security certification can be used to tackle this problem and they are widely adopted in different industries, including software. However, the length and cost of existing security certification schemes do not match the fast lifecycle of typical cloud products. Also, the results of certification processes are usually expressed in a way that is not directly accessible and understandable by the typical customers of service and application marketplaces.

The research conducted in the Assert4Soa project [3] aims at defining a new, lighter-weight approach to certification, where finer-grained security properties of applications and services can be evaluated by independent 3rd parties and can be expressed in machine-processable artifacts (called Assert4Soas). One of the tangible results of the project is the Assert4Soa Framework, which defines the key components to build a certification-aware service repository from which services can be queried based on the security requirements expressed by the user.

In this paper we present a software marketplace targeting the procurement of business software. This marketplace uses the services offered by the Assert4Soa Framework to allow business customers to browse a catalog of certified applications and services. Through our system, users express their security

requirements and compare products based on their certified properties; also, the system automatically ranks the available candidates based on how well their certified properties match the user's security requirements.

Section 2 presents the key high-level requirements for such a marketplace and describes the design and realization of our prototype. Section 3 describes a typical usage scenario illustrating how such a marketplace would be used for procuring business software. Section 4 reviews some related work in this area; finally Sect. 5 concludes the paper.

2 A Certification-Aware Marketplace for Business Software

As discussed in the previous section, current marketplace deployments provide incomplete or no information about the security aspects of the applications they offer. To overcome this problem, the key idea of our certification-aware marketplace is to increase transparency by attaching explicit security certificates to the products offered on the marketplace. From the standpoint of a business customer, there are essentially three functional areas to cover, as outlined below.

Defining explicit security requirements. In order to take into account the security requirements of business customers, the marketplace should allow for expressing these requirements explicitly. In real-life scenarios, there may be different actors that could access this function besides the user that directly procures software from the marketplace (the *buyer*). In larger organizations there can be a central office in charge for defining the security policies that buyers must comply with when buying software.

Searching based on security requirements. Software buyers should be able to use the security requirements to search the marketplace for the software which meets the requirements. The process of matching requirements with the properties of the products offered on the marketplace should be as simple and quick as possible, and the security characteristics of each certified product should be readily accessible to the user.

Automated matching and approximate solutions. Among the results of a search, the buyers should be supported in finding the best fitting solution. If no candidate matches the security requirements exactly, the marketplace should suggest the closest match to the security requirements, ultimately allowing the buyer to take a rational decision based on all the information available both about the functionality and the security properties of each candidate.

To address these three high-level requirements, we developed a marketplace integrated with Assert4Soa [4,5]. Assert4Soa is a framework for security certifications that allows explicit definition of security properties of an application as well as a6 transparent view of the evaluation of these security properties. it also provides services for application discovery based on security properties

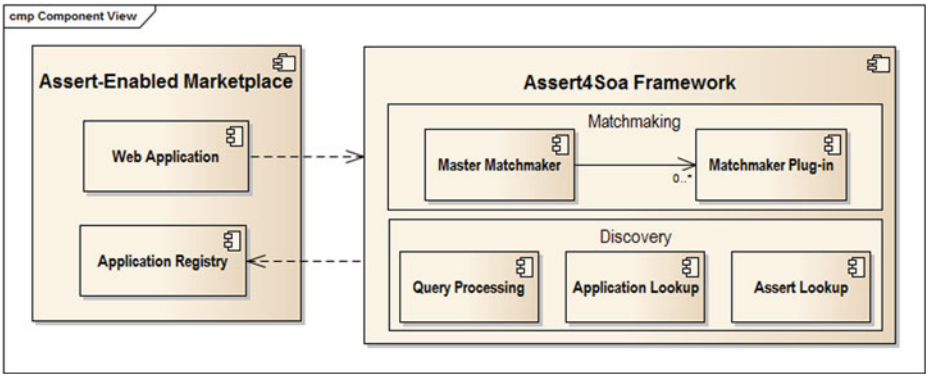

Fig. 1. Overview of the ASSERT4SOA-enabled marketplace

of the applications. As illustrated in Fig. 1, the certification-enabled marketplace consists of a Application Registry that contains the applications offered by the marketplace, and a Web Application to present this data to the user. Search queries flow from the web application to the discovery system of the ASSERT4SOA Framework, which searches the application registry based on the functional part of the query. This step produces an initial list of candidates that provide the required functionality, but whose security properties may or may not match the user security needs. This list is therefore processed by the Matchmaking subsystem, which compares the security properties of each candidate against the security requirements expressed in the security part of the query. An example query is shown in Listing 1 (abridged for the sake of clarity). This query language expresses a set of functional and security requirements. The functional part of the query is defined in the `RegistryQuery` element (lines 1–3), while the security part is represented in the `AssertQuery` element (lines 4–15).

```
1  <tns:RegistryQuery>
2   <Keywords>payment</Keywords>
3  </tns:RegistryQuery>
4  <tnsd:AssertQuery name="A1">
5   <tnsd:Condition relation="EQUALTO">
6     <tnsd:Operand1>
7      <tnsd:AssertOperand facetName="Assert"facetType="Assert">
8       //ASSERTCore/SecurityProperty/@PropertyAbstractCategory
9      </tnsd:AssertOperand>
10    </tnsd:Operand1>
11    <tnsd:Operand2>
12     <tnsd:Constant type="STRING">Confidentiality</tnsd:Constant>
13    </tnsd:Operand2>
14   </tnsd:Condition>
15 </tnsd:AssertQuery>
```

Listing 1. Sample Query (fragment)

The original scope of the Assert4Soa approach was restricted to web-services; consequently, some of its components were designed to target the WS-* technology space specifically. In particular, A-SerDiQuel [6] – the query language used in the framework – assumes that the functional description of services can be expressed in terms of their WSDL interface. To cover broader scenarios, where *applications* (not just web services) have to be considered, we defined an extension of A-SerDiQuel to cater for the discovery of generic software (services and applications), which may or may not have a WSDL Specification.

In response to a query like the one shown in Listing 1, the Matchmaking subsystem is capable of computing a score for each of the candidates that match the functional part of the query. This score is a measure of how closely the security properties of a candidate match the user's requirements. Because of the modular organization of the Matchmaking subsystem, different matchmaking strategies can be implemented as modules of the Matchmaking subsystem. The strategy we implemented in our prototype assigns scores as follows. For each candidate, each condition in the query is compared with the asserts associated to that candidate. The condition is given a real-valued score in the range $[0, 1]$ based on how well the properties expressed in the asserts match the condition at hand. More precisely, the score S_i of the condition i can take the following values.

1. Exact Match: an Assert4Soa of the solution exactly matches the security condition i: in this case the score S_i takes the value of 1.
2. Partial Match: the condition i is partially satisfied. For example, a security requirement of "confidentiality in-transit with AES-256" is only partially satisfied by a security property of "confidentiality in-transit with AES-128", because the *abstract property* "confidentiality" is satisfied but the mechanism used to satisfy it is weaker than the one requested. In this case, the score S_i takes a value α, where $\alpha \in (0, 1)$. The higher α is, the more tolerant is the matchmaking with respect to partial matches.
3. No Match: if no assert associated to the candidate matches i, then S_i is assigned a value of 0.

The final score S of the candidate is calculated as:

$$S = \prod_{i=1}^{k} S_i \tag{1}$$

where k is the number of conditions in the security query.

3 Typical Usage Scenario: A Walk-Through

The marketplace provide users the ability to search for applications on the store with multiple filters, including security properties, keywords and other store specific filters. The workflow below presents a usage scenario of the system, specifying how it caters for the requirements of the software buyers, who are responsible for buying business software respecting to the security requirements.

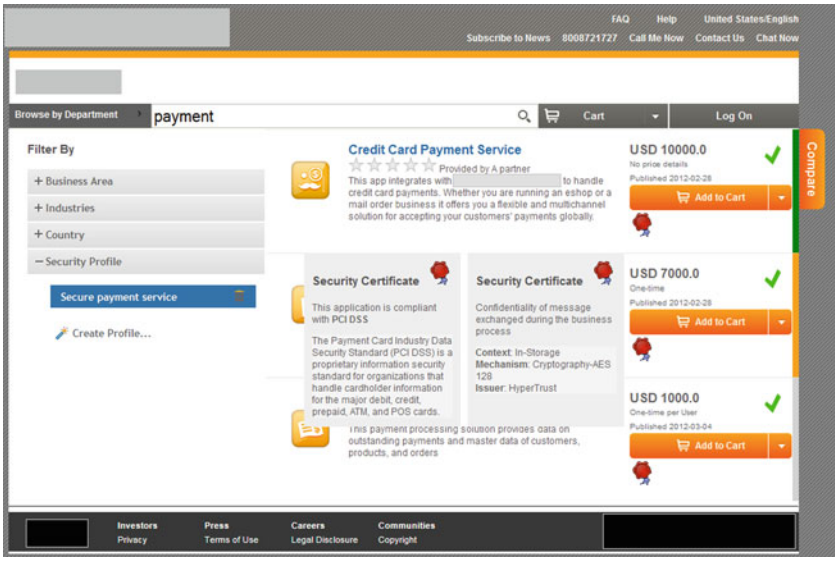

Fig. 2. Ranked search results

Searching for secure business software. As in all marketplace store-fronts, the user can search the repository of available applications and services, browsing by categories (business areas, industries) and/or specifying one or more keywords in the search field.

Differently from existing marketplaces, the security properties of the products in the result list represented explicitly as security certificates (Assert4Soas). The buyer can easily inspect them by clicking on the seal icon (Fig. 2). For each certified product, not only the information about the abstract security property is available (e.g., "confidentiality of stored data"), but also the mechanism used to achieve that property (e.g., "encryption") and its parameters (e.g., "cryptography algorithm used: AES with key-length 256 bits). Finally, information about the entity that evaluated the product at hand is available (the *certificate issuer*) together with the dates of issuing and validity (not shown in the figure, but visible in the "details" screen for each product).

Refining the search using filters (profiles). The possibility to review and compare the security properties of the different candidate products is already a significant step forward from existing marketplace instantiations. However, another important feature could be realized, leveraging the fact that Assert4Soas are machine-readable: the marketplace can offer automatic filtering of the candidates based on the user's security requirements. Of course, a preliminary step for such a feature is to allow users to specify what their security requirements are. For this purpose, our prototype offers a user-friendly interface (a "wizard"), partly shown in Fig. 3. The figure depicts the step of the wizard where the user can express the security properties that candidates must satisfy, and can indi-

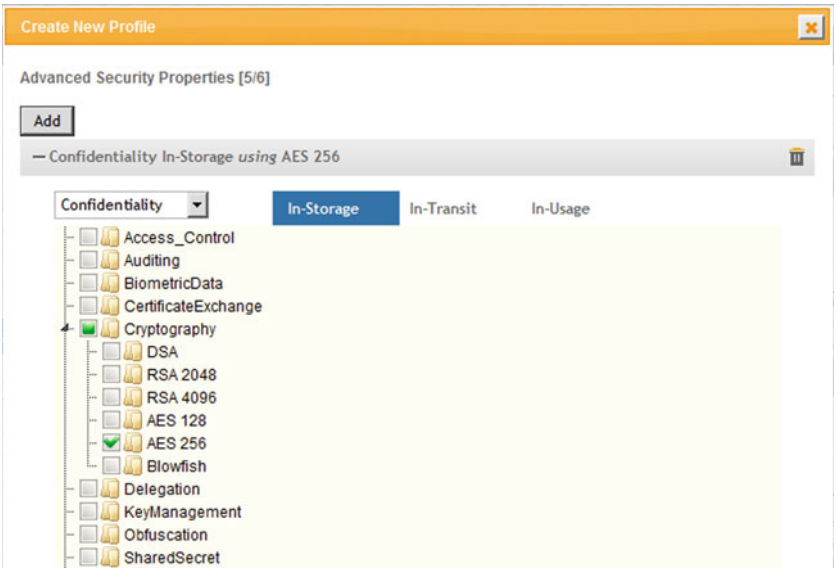

Fig. 3. Specifying security properties

cate what mechanism should be used to achieve those properties. At the end of the wizard, a new named "profile" is created and the corresponding button is added to the left-hand side menu. Different profiles can be applied at the same time: each may contain constraints of different nature, or coming from different sources. For example, centrally-defined corporate policies could be loaded automatically when the user logs onto the marketplace; in addition to those policies, the user can use the wizard to define additional customized profiles.

Under the hood, the active profiles are translated by the system into an `ASSERTQuery` like the one shown in Sect. 2. After applying one or more profiles, the candidate list is filtered to show only those that match (at least a part of) the constraints expressed in the active profiles. The results are also ranked (and color-coded) based on the suitability of a service with respect to the specified security criteria.

Finding the best match among candidate solutions. From the results list, it is also possible to compare two or more solutions side by side, to have a clear visual comparison of their security properties and to understand how they compare with the constraints of the active profiles (Fig. 4). The services are assigned a score as described in Eq. 1 of Sect. 2. The score is used to assign a color-coded bar below the title of the application (as in Fig. 4). The score is also visualized by a gauge, indicating in a intuitive way whether the corresponding candidate is a perfect match, a weak match, or a partial match (see the figure, from left to right). A weak match is a candidate that is certified for all the security properties required by the active profiles, but that achieves at least one of them using a mechanism other (weaker) than the one specified in the

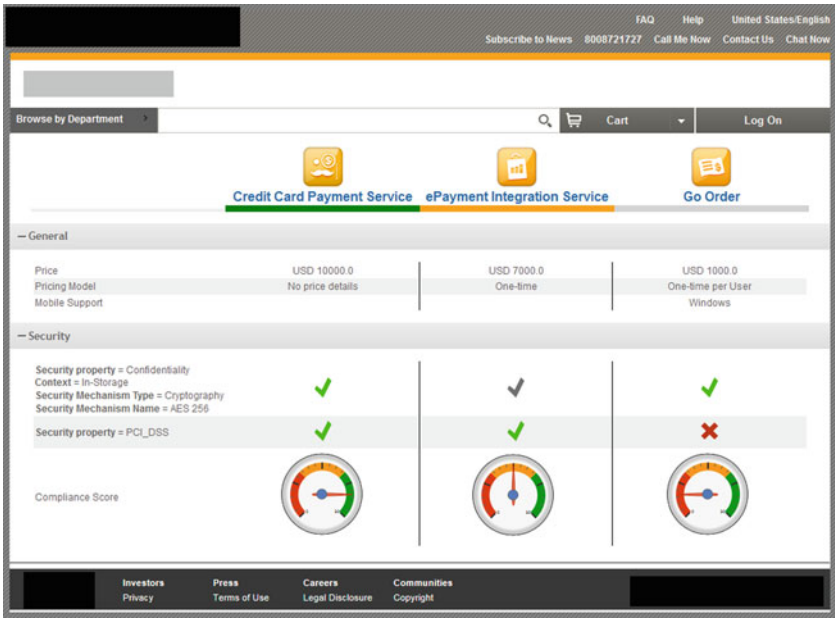

Fig. 4. Comparing the security properties of results

profile. A partial match is a candidate that achieves (perfectly) at least one of the properties required by the active profiles while missing at least one of the other required properties.

Services can also have additional Assert4Soas, which are not required to meet the security requirements; those Assert4Soas are mentioned separately (not shown in Fig. 4), below the comparison score.

4 Related Work

The problem of increasing the trustworthiness of digital marketplaces has received increasing attention especially in relation with the growing popularity of the mobile [7,8] and cloud markets [9]. While the role that marketplace owners can play in increasing trustworthiness is still subject to debate, these studies pointed out the necessity to provide additional transparency of the quality of apps. Security certification can play a major role for filling the trust gap between app-users and app-providers. Extensions to the "traditional security certification" model, which mostly addresses static software systems and relies on manual inspection of certificates, has been introduced to cope with the dynamic nature of modern service ecosystems [5]. In this context, the concept of certification-aware marketplace has been recently introduced in [10], where the authors discuss the use of lightweight certification and machine-processable certification artifacts as a mean to increase transparency and trust. In this paper,

we showed how this concept can be put in practice, based on the architectural framework presented in [5].

In addition, in [8], the authors advocate automated certification, but they also stress the fact that uniform, market-wide certification criteria may not be appropriate because different users may have different of requirements and a different understanding of those requirements. We share the conclusion of the authors that the choice of what policy to adopt should be left to the users, which is precisely the vision that our prototype embraces and realizes in practice.

5 Conclusions and Future Directions

Building on recent research results on service security certification, available as part of the Assert4Soa framework, we presented a certification-aware Business-Software marketplace where software products have explicit, transparent, and verifiable certificates of security properties. Our proof-of-concept provides business users with an infrastructure to search and compare cloud services based on security and assurance requirements. In this initial prototype, we covered basic use-cases leveraging essential services offered by the Assert4Soa Framework. More advanced features of the framework were not used. For example, the framework includes machinery to reason about composite services; also, more complex matchmaking strategies than the one presented here are made possible by the framework, taking into account the characteristics of the evaluation process followed to evaluate the certified security properties (not just the properties themselves). The extension of our prototype to benefit from these advanced features could be the subject of a future work.

At the time of writing, we are conducting a set of evaluation sessions, presenting the marketplace prototype to focus groups composed of security experts from the certification community, IT practitioners, and developers, with the goal of gathering feedback on usability, business relevance, quality, and potential for adoption.

The wide adoption of certificate-based tools is clearly dependent on a large availability of affordable certifications. We expect that the number of certified products will largely grow in the coming years, partly driven by the increasing number and complexity of data protection regulations. However, it should be also noticed that our approach could be already used by ISVs to describe the security features of their applications and services. Self-signed Assert4Soas, even produced without a 3rd party evaluation, are still useful to increase transparency and to allow machine-processability of security property description.

Acknowledgements. This work was partially supported by the EU-funded Assert4Soa project (grant no. 257351).

References

1. INTEL Corporation: What's holding back the cloud? (2012)
2. Cloud Security Alliance: Cloud computing vulnerability incidents: a statistical overview (2013)
3. Assert4Soa Consortium: Assert4Soa. www.assert4soa.eu (2010–2013)
4. Anisetti, M., et al.: ASSERT4SOA: toward security certification of service-oriented applications. In: Meersman, R., Dillon, T., Herrero, P. (eds.) OTM 2010 Workshops. LNCS, vol. 6428, pp. 38–40. Springer, Heidelberg (2010)
5. Bezzi, M., Sabetta, A., Spanoudakis, G.: An architecture for certification-aware service discovery. In: 1st International Workshop on Securing Services on the Cloud (IWSSC 2011), pp. 14–21. IEEE (2011)
6. Zisman, A., Spanoudakis, G., Dooley, J., Siveroni, I.: Proactive and reactive runtime service discovery: a framework and its evaluation. IEEE Trans. Software Eng. **99**, 1 (2013, PrePrints)
7. Barrera, D., Van Oorschot, P.: Secure software installation on smartphones. IEEE Secur. Priv. **99**, 1 (2010)
8. McDaniel, P., Enck, W.: Not so great expectations: Why application markets haven't failed security. IEEE Secur. Priv. **8**(5), 76–78 (2010)
9. Sunyaev, A., Schneider, S.: Cloud services certification. Commun. ACM **56**(2), 33–36 (2013)
10. Lotz, V., Di Cerbo, F., Bezzi, M., Kaluvuri, S.P., Sabetta, A., Trabelsi, S.: Security certification for service-based business ecosystems. Computer J. (2013)

Attribute Based Credentials Towards Refined Public Consultation Results and Effective eGovernance

Paul Spirakis[1,2] and Yannis C. Stamatiou[1,3(✉)]

[1] Computer Technology Institute and Press—"Diophantus", N. Kazantzaki Str., 26504 Patras, Greece
spirakis@cti.gr, stamatiu@ceid.upatras.gr
[2] Computer Engineering and Informatics Department, University of Patras, 26504 Rio, Patras, Greece
[3] Business Administration Department, University of Patras, 26504 Rio, Patras, Greece

Abstract. eVoting procedures are considered an effective eParticipation vehicle that helps governmental institutions shape policies according citizens' opinions. A major requirement, among other important requirements, of these procedures is the protection of citizens' anonymity. Although this requirement is sufficient for the purpose of gathering citizens' opinions, it nevertheless does not, directly, support procedures that allow a refinement of eVoting results according to citizens' *profiles* and it does not support the development of procedures in which only groups of citizens with specific profiles can participate. In this paper we argue that eVoting procedures that address these two aspects can be more effective for Government policy makers in reforming their tools and practices towards society and its citizens. We further propose enhancements of eVoting techniques that address these aspects, based on a new privacy preserving authentication technology, the *Attribute Based Credentials* or ABCs.

1 Introduction

eVoting and open discussions on the Internet on various proposals for changes or enhancements in governmental practices are a commonly used means employed by governments in order to sense citizens' attitudes and opinions towards their proposals for new practices and reform. Of course, anonymity (compulsory in strict eVoting procedures but voluntary on open discussion forums) is the common denominator of all of these processes as one of the major anchor points for protecting the individual's identity. However, there are situations where knowledge of certain characteristics (or attributes) of individuals' profiles may enhance the conclusions drawn from studying only the responses of the individuals. For instance, the ministry of education may open a discussion as to whether general entrance examinations at the Universities should be abolished and all students enter at the University schools of their choice, depending on their grades only.

M. Felici (Ed.): CSP EU FORUM 2013, CCIS 182, pp. 115–126, 2013.
DOI: 10.1007/978-3-642-41205-9_10,

Then a discussion result indicating that 90 % of the participants support the abolition of general examinations may provide some clue as to what the feelings of society are towards the examinations but a closer examination, according to individuals' profiles, may indicate that only 10 % of individuals who are university professors support the abolition and, thus, governmental authorities should be careful in implementing such a radical change without further discussion and elaborations. Moreover, there are also situations where knowledge of characteristics of individuals' profiles may be mandatory. For instance, the ministry of education may want to start a discussion about whether University infrastructures in a country are sufficient for a normal operation of Universities. In order to take as substantiated opinions as possible, the ministry decides to open the discussion only to professors and students who are at least at the 3rd year of their studies. This establishes that those who have had sufficiently many years of university life will participate so as to be in position to judge more accurately the University infrastructures and curricula.

Although all the examples discussed above indicate that having partial information about the profiles of individuals participating in a eVoting process is helpful, there is one major issue that should be taken care of: How can one prove, beyond doubt, something about a certain attribute of his/her credentials/profile without revealing the true identity even to the credentials service provider?

The goal of the paper is to address the integration of technologies that support *Attribute Based Credentials* or ABCs with technologies that are employed for *eVoting*. ABCs technologies (see [6,12,13]) allow an Identity Service Provider (IdSP) to issue a credential (or certificate) to a user, in a way analogous to a *Public Key Infrastructure* (PKI) issuing a classical certificate (see [37]). This credential contains attributes of the user such as address or date of birth but also the user's rights or roles as attributes. Using the credential, the user can prove to a third party that he possesses a credential containing a given attribute or role without revealing any other information stored in the credential. For instance, the user could use a government-issued anonymous ID credential to prove that he is of proper age, i.e., that he possesses a credential that contains a date of birth which is further in the past than 21 years. Thus, anonymous credentials promise to be an important cornerstone in protecting users' privacy in an eVoting environment while, at the same time, providing important enhancement in eVoting processes towards a more effective government policies reform. In the rest of the paper we address how anonymous credentials may enhance eVoting procedures and discuss the basic relevant technical aspects, which we will describe in more detail in the full paper.

The paper is organized as follows. In Sect. 2 we introduce some new eVoting procedures that rely on differentiation of individuals based on their credentials. In Sect. 3 we provide a brief review of the technologies involved in eVoting and ABCs. In Sect. 4 we discuss the details of integrating a specific eVoting protocol (see [33]) with ABCs. Finally, in Sect. 5 we discuss our conclusions and directions for future research.

2 Alternative eVoting Models Focused on Population Profiles

A voter within a certain population possesses a set of *attributes* (e.g. "sex" and "occupation") and for each attribute there is a certain set of allowed *values* (e.g. "male/female", "doctor/engineer/accountant"). Classical PKI certificates also provide a form of authentication (see, for instance, [37]) but the major drawback is that the authenticated individual is known to the certification authority after the authentication process is completed (i.e. anonymity is not provided).

The important assumption with regard to these attributes, to be justified in Sect. 3, is that each voter can *prove* the value of a certain characteristic (e.g. "sex", "occupation") without revealing his/her real identity using only a pseudonym, which he/she may change for different situations so as to avoid linking together his/her different actions in different eParticipation situations. Note that this assumption is not, normally, supported by current PKI technologies since in order to prove possession of, say, a role within society (e.g. occupation) one has to reveal his/her whole certificate. PKI only guarantees that the person presenting a certificate is the person claimed to be. Normally, there is no provision for preserving the privacy of the authenticated entity since the certificate contains all its attributes (see the discussion in Sect. 1.2 in Stefan Brands' seminal book [6]).

Our institute has already developed an eVoting platform, called *PNYKA* (see [3] for details), that is planned to be extended in order to encompass the new eVoting model proposed in this section, based on the ABCs technologies discussed in Sects. 3 and 4. Since our system employs the eVoting protocol in [33] which is discussed in Sect. 4 with respect to encompassing ABCs, our plan for the near future is ti augment the PNYKA system with ABCs capabilities in order to support the new eVoting models discussed in this section.

2.1 Enhancing Public Consultation Results Based on User Profile Information

In this subsection we address how public consultation procedures that take advantage of information on individuals' profiles may provide more information about voting results, beyond simple tallies. We assume, that the population can be divided into sets based on a particular attribute or attribute combination that characterizes them, e.g. "occupation", "sex", "educational level" etc. For simplicity, given a particular characteristic, we assume that the sets are pairwise disjoint (e.g. for the attribute "occupation", there is no member of the population that is both a "doctor" and a "computer engineer").

Let us assume that a question is posed by the government about a reform in financial policies. For instance, the question may be "Do you agree with publicizing on a bulletin board the names and incomes of all citizens (to aid transparency in financial administration)?" Based on the attribute based credentials public consultation and eVoting model, each voter casts his/her vote ("Yes" or

"No") and *proves* his/her occupation (or some other desired by the government) attribute or attribute combination. Then, the government may make more careful decisions about governmental policies, based on the refined results of such a public consultation procedure.

We will not expand on this issue but the benefits of using provable credentials can lead to refined, more accurate conclusions about citizens' opinions on major reform issues.

2.2 Public Consultation Procedures Directed to Populations of Certain Profiles

We now describe a public consultation scenario in which only voters with specific profiles are allowed to participate so as to be able to sample a particular class of individuals. At the same time, this scenario also provides an aspect of the attribute based credentials as a defence against orchestrated efforts to direct an open discussion towards a specific outcome. These efforts may come from either a malicious government or a massive citizen movement who want to impose a false opinion "on behalf" of the society. The defense consists in allowing participation only to the target individuals class and not outsiders who may either wish to spoil the results of a public consultation or are not sufficiently informed about the target of the consultation.

Assume that the government decides to open a public discussion on whether immigration should be allowed without any constraints or whether it should be constrained according to several government decided factors. Moreover, the government decides to sample the opinion of only young people so as to "listen" to how young people feel about immigration policies. Using attribute based credentials the government can set up an opinion polling procedure that allows people to state their opinion only if their age range falls within a predetermined target group (say, 18 to 25 years old).

Recently, within the context of the EU funded ABC4Trust project, a first step was taken towards the realization of user-profile based opinion gathering within the context of *university course evaluations*. This project's goal is to address the federation and interchangeability of technologies that support trustworthy yet privacy-preserving Attribute Based Credentials (ABCs). With respect to the context of the pilot, students are allowed to participate in the evaluation if they could prove, anonymously, that they are indeed students of the department offering the course, that they are registered to the course under evaluation, and that they have attended sufficient number of classes (details can be found in the project's site https://abc4trust.eu/).

2.3 Issues in Profile Based Consultation and eVoting Procedures

Although the public consultation and eVoting models discussed in this section, combined with minimal information disclosure of the participants, may offer a number of advantages with respect to classical procedures, it is possible, under certain circumstances, to lead to breach of anonymity of the participants.

For instance, as an extreme case, it is possible that among the individuals of a population, only one individual possesses an attribute with a certain value, disclosed in such a procedure. Then this individual is identified, indirectly, through this attribute value. Even if the attribute is shared by more than one individuals, if this set of individuals is small then identification may still be possible since search is limited to a candidate set of small cardinality.

To this end, our viewpoint is that such procedures should be carefully designed so as to avoid indirect disclosure of participants' identities. To this end, an important privacy concept has been proposed, the *k-anonymity* concept (see [36]). An information set provides k-anonymity protection if the information for each person contained in the set cannot be distinguished from at least $k-1$ individuals whose information also appears in the release. This property, depending on the choice of k, provides a level of protection against identification of participants in such profile-based procedures. The higher the value of k, the more privacy preserving the procedure is. Thus, before such a procedure is initiated, the authorities should check whether the chosen attributes are such that lead to sets of individuals revealing these attributes that are too small and, thus, can lead to the identification of individuals or groups of individuals. Alternatively, the authorities should choose the attributes over which to run these procedures so as to lead to large individual classes.

As another important issue, the chosen attributes over which the profile-based procedures should be conducted must be defined beforehand and not after the procedure is over. If the attributes are allowed to be chosen afterwards, then one can manipulate the results as desired.

Finally, a potential risk is that the authorities may use the results of the profile-based procedures for chastisement against specific individual classes, if the results are negative towards the authorities. To this end, profile-based procedures may not be appropriate for governmental elections in general.

3 Related Work on eVoting and Attribute Based Credentials (ABCs)

E-Voting systems must satisfy the same basic requirements as traditional voting systems. These requirements, see e.g. [22,33,35], are briefly presented in what follows: *Democracy* (only voters who have the right to vote can vote and one vote per voter is included in the election outcome), *accuracy* (the election outcome is correct and includes all valid votes), *secrecy* (a voter's vote cannot be seen by any other voter), *receipt-freeness* (no evidence is given to the voter that can be used in order to disclose the contents of his/her vote to another party), *uncoercibility* (protection from outside enforcement of opinion), *fairness* (the outcome of the election will be made public only after all votes have been received and tallied), *verifiability* (all critical stages of the election process are logged for later auditing and the election outcome can be verified by the voters), *verifiable participation* (the participation of a voter can be checked by the election authority,

in cases where voting is compulsory), and *robustness* (the election process cannot be hindered either accidentally or on purpose by outside intervention). These requirements are closely interrelated and often contradictory to each other, thus creating many technological, legal and organizational challenges for e-voting systems. Several reports highlight these limitations and challenges [1] and provide some first recommendations and guidelines [29].

Existing voting protocols can be divided in the following groups (see [33]):

1. Homomorphic: They are based on the use of encryption functions with homomorphic properties. An encryption function is homomorphic if, by multiplying two encrypted messages, the result is the same as encrypting the sum of the original messages. This allows the addition of all encrypted votes, without decrypting them, and at the end, the total vote is decrypted (see [16,33]).
2. Mix-nets: A mixnet is a multiparty computation-and-communication protocol that causes a large number of input messages to get shuffled into a random order in such a way that every party (as well as external verifiers) becomes confident that a shuffling was performed, but no party (nor even any t-element subset of corrupt colluding parties, provided that it is not too large) has any idea what the shuffle-permutation was (see [14]). This ensures secrecy (voter and vote cannot be combined) but presents limited efficiency in cases of large computations (large scale elections).
3. Blind Signature Schemes: The concept of blind signatures was introduced in [15] as a method to digitally authenticate a message without knowing the contents of the message. Several election schemes based on blind signatures have been proposed (e.g. [28,30]). However, they only offer atomic verifiability (not universal).
4. Heterodox schemes: They do not fit neatly into the "homomorphic" or "mixnet" camps, either because they use both ideas, or other ideas. Examples are [24,26] as improved in [33].

Many e-voting initiatives have been deployed across Europe, in all kinds of voting procedures, including large scale elections, with mixed results so far. Existing e-voting systems may be grouped in the following broad categories:

1. Systems that are developed within governmental initiatives: They are usually designed for large-scale national elections or referenda. The cases of Switzerland and Estonia are characteristic. In Switzerland, eVoting and especially Internet voting, was recently introduced as a complementary channel for elections and referenda, with great success [5,20]. One of the reasons might be that remote voting was largely practiced through postal voting for many years. The introduction of Internet voting came as an alternative and easier way to vote remotely and thus was rapidly accepted. In 2005, Estonia carried out the first Nation Wide online elections in the EU (see [18]). Similar efforts have also taken place in Spain, Belgium, UK, etc. Some more recent efforts are reported in [3,8,25,34].
2. Systems that were developed within EU funded projects (e.g. IST projects): In the past,several IST projects tackled e-voting, putting emphasis on innovative

ideas with regard to secure voting protocols, design methodologies, architecture models, but also highlighting social and legal issues. Some projects are: eVOTE (http://www.instore.gr/evote), CyberVote (http://www.eucybervote.org), e-poll (http://www.e-poll-project.net), True-Vote (http://www.true-vote.net), Webocracy (http://www.webocrat.org), etc.

3. Commercial systems: Several commercial e-voting systems are available in the market, mainly in USA and also in Europe and Australia. Some examples are: Pnyx, eBallot, and eVACS. Pnyx and eBallot are internet based commercial voting systems. Pnyx is also the outcome of an IST project funded by the EU (see http://www.scytl.com/) and is considered fairly successful [32]. eVACS was initially developed as a governmental system and operates on distinct isolated LANs and not through the Internet (see [4]).
4. Experimental - pilot systems: These systems were developed as experimental efforts, mainly by academic institutions. Usually, they are not integrated (they are pilots) and follow different approaches, covering specific issues with regard to e-voting. Such an example is e-VOX, which was developed in MIT (1997), as a thesis (Mark Herschberg's thesis "Secure Electronic Voting over the World Wide Web"). In 2003 the REVS voting system was proposed, improving several aspects of e-VOX (see [27]).
5. Open Source systems: Open Source systems are highly recommended for e-voting because they allow transparency and audit. Some examples are: GNU.FREE (Free Referenda & Elections Electronically) [21] and The Electronic Voting Machine (see [2,17]) which is developed by the Open Voting Consortium.

The *Attribute Based Credentials*, on the other hand, or ABCs for short, can be viewed as a set of cryptographic protocols which specify a user-controllable framework for defining and managing credential sets. These credential sets may be required for interactions with service providers (either private or governmental) in order to access personalized services that require access only to a subset of the users' credentials. Over the past 10–15 years, a number of technologies have been developed to build ABC systems in a way that they can be trusted, like normal cryptographic certificates, while at the same time protecting the privacy of their holder (e.g., hiding the real holder's identity). Such attribute-based credentials are issued just like ordinary cryptographic credentials (e.g., X.509 credentials – see [37]) using a digital (secret) signature key. However, ABCs allow their holder to uncover only a subset of the attributes contained in the original credential. Still, these transformed credentials verification procedure just like ordinary cryptographic credentials (using the public verification key of the issuer) and offer the same strong security.

Research has put forth a number of different proposals how to realize Attribute Based Credentials (see [6,11–13]) which are based on different number-theoretical problems and also differ somewhat in the functionality that they offer. There are two leading anonymous credentials systems: Idemix of IBM and U-prove of Microsoft. These two systems provide functionality for supporting user credentials with the following requirements: (1) Unforgeability (issuing), (2) Selective

disclosure with the user controlling the disclosed information set, (3) Soundness (no false claims about the validity of a credential), (4) No framing (showing transcript unforgeability), (5) Untraceability (showings with respect to issuing), (6) Unlinkability (between showings), and (7) Limited-show unlinkability, untraceability.

These two systems provide nearly the same functionality, using different cryptographic primitives. With regard to Idemix, it relies, mostly, on the hardness of the strong RSA problem while U-prove relies, mostly, on the difficulty of discrete logarithms. Also, credentials are represented in different formats. In what follows, we will sketch the use of credentials in eVoting using the description given by S. Brands in [6]. We will only use the basic credentials form in order to demonstrate our idea (more details will be given in a full paper). The discussion can be extended to work also with the more complex format given in [7] which have been incorporated in Microsoft's U-prove system as well as the other credentials format described in [9,10] which have been implemented into IBM's Idemix attribute based credentials system (see [11]). We refer the reader to the literature with regard to proofs that the properties listed above in bullets hold for both systems.For our purposes, we will provide a very brief introduction to the technicalities of the attribute based credentials in what follows.

Let us assume that to each individual correspond l attributes, such as for instance age, sex, marital status, nationality etc. To each such attribute a range of allowed values is assigned. If to these l attributes the values $x_1, x_2, \ldots, x_l$ are assigned (each value chosen from within the set of allowed values for the corresponding attribute), then these attributes are encoded, using the basic credential format, as a value $h = g_1^{x_1} \cdot g_2^{x_2} \cdot \ldots \cdot g_l^{x_l} \cdot h_0^{\alpha}$, with the elements $g_1, g_2, \ldots, g_l, h_0$ suitably generated by a *Credentials Authority* (CA – an analogous with the classical Certification Authority of PKIs) and publicly known to all credential holders. The value α is *randomly* generated by the credential holder (a different value for each one) is kept *secret*. Its role is to hide the values $x_1, x_2, \ldots, x_l$ of the credentials. For details, see [6,7]. Equipped with the credential $h = g_1^{x_1} \cdot g_2^{x_2} \cdot \ldots \cdot g_l^{x_l} \cdot h_0^{\alpha}$, there are techniques whereby the credential holder may prove properties about the values $x_1, x_2, \ldots, x_l$ without revealing more than the validity of the properties themselves or the values of attributes that are not required by the application.

4 How Digital Credentials can be Merged with eVoting

In this section we outline (details will be given in a full paper) how credentials may be employed in eVoting procedures in order to support the scenarios described in Sect. 2. We will demonstrate how eVoting results can be grouped into classes, depending on the values of a specific credential.

We assume that voters have encoded their credentials $x_1, x_2, \ldots, x_l$, as outlined in Sect. 3, in the form $h = g_1^{x_1} \cdot g_2^{x_2} \cdot \ldots \cdot g_l^{x_l} \cdot h_0^{\alpha}$. We also assume that the eVoting protocol employed is based on a homomorphic encryption function, such as the one given by Smith [33] which we will employ in demonstrating the integration of attribute based credentials into eVoting.

According to the protocol in [33], the ith voter's vote ends up encrypted with the ElGamal cryptographic protocol in the form $M_i = (g_0^r, h_0^r V)$, with V being the number corresponding to the vote cast by the voter and r being a random value. The values are set by the Election Authority. For details on the ElGamal encryption function see [23] as well as [33]. Our proposal is to proceed, as a next step, with the encryption of a credential value, in the same format as M_i. More specifically, let as assume that we wish to group votes according to the value of credential j, which has as possible values the number $d_{j,1}, d_{j,2}, \ldots, d_{j,k}$. We assume, for concreteness, that voter i has the value $d_{j,s}$, $1 \leq s \leq k$, for attribute j. Then voter i produces the ElGamal encryption $C_i = (g_0^{r'}, h_0^{r'} g_j^{d_{j,s}})$. Then the following product of ElGamal encryptions $M_i C_i = (g_0^{r+r'}, h_0^{r+r'} V g_j^{d_{j,s}})$ can be formed which includes both the value of credential j and the vote, encrypted in ElGamal form. As users cast their votes, the central election server accumulates these encryptions into a single product. Remember that our goal is to separate votes according to credential values. One way to accomplish this is to have each product of the form $V g_j^{d_{j,s}}$, for each distinct vote V, each distinct credential base g_j, and for each credential value $d_{j,1}, d_{j,2}, \ldots, d_{j,k}$ correspond to a distinct prime number. Thus, each triplet (vote, credential base, credential value) will be transformed to a distinct prime, when its three elements are multiplied together in $M_i C_i = (g_0^{r+r'}, h_0^{r+r'} V g_j^{d_{j,s}})$. Primes have the nice property of grouping together (each new prime value multiplying a product of primes, simply increases by one the exponent corresponding to this prime) without mixing with other primes, since they do not share common factors.

Now we should compute the correspondence $V g_j^{d_{j,s}} \leftrightarrow$ unique prime value. One way to accomplish this is to solve for $V$the following equations, where $w_{j,s}$ is the prime number corresponding to the second and the third elements of the triple (vote, credential base, credential value) of the product $V g_j^{d_{j,s}}$ and p is the prime number used in the ElGamal encryption function: $V g_j^{d_{j,s}} = w_{j,s} \mathrm{mod} p$. We solve for V by replacing $w_{j,s}$ with consecutive primes, for each possible credential value $g_j^{d_{j,s}}$. Thus, each time a combination $V g_j^{d_{j,s}}$ appears in the accumulated products $M_i C_i = (g_0^{r+r'}, h_0^{r+r'} V g_j^{d_{j,s}})$, it results in the prime value $w_{j,s}$. Consequently, in the end, the exponent of this prime will be equal to the number of individuals with credential value $d_{j,s}$ for credential j, who voted V.

Although we have not investigate the existence and size of solutions for the equations leading to the determination of the prime numbers, we experimented using the Maple software for performing arithmetic and algebraic computations. For the purposes of demonstration, let us assume that $p = 100000000379$ and that we have three possible values for credential, say, 1 with $g_1 = 111$. Let us, also, assume that these values are $d_{1,1} = 1, d_{1,2} = 2, d_{1,3} = 3$. Let us, further, assume that there are two possible votes V_1, V_2. Then we do the following:

1. For the combination $g_1 = 111$, $d_{1,1} = 1$, we need one prime value for vote V_1 and one prime value for vote V_2. Solving $V g_1^{d_{1,1}} = w_{1,1} \mod p \Rightarrow V \cdot 111 = w_{1,1} \mod 100000000379$ testing various prime values $w_{1,1}$, we obtain the

correspondence of V_1 to the (prime, value) pair (557, 34234234369) and of V_2 to the (prime, value) pair (1129, 25225225331).

2. For the combination $g_1 = 111$, $d_{1,2} = 2$, we need one prime value for vote V_1 and one prime value for vote V_2. Solving $Vg_1^{d_{1,2}} = w_{1,2} \bmod p \Rightarrow V \cdot 12321 = w_{1,2} \bmod 100000000379$ testing various prime values $w_{1,2}$, we obtain the correspondence of V_1 to the (prime, value) pair (19, 25452479603) and of V_2 to the (prime, value) pair (173, 52804155707).
3. For the combination $g_1 = 111$, $d_{1,3} = 3$, we need one prime value for vote V_1 and one prime value for vote V_2. Solving $Vg_1^{d_{1,3}} = w_{1,3} \bmod p \Rightarrow V \cdot 111 = w_{1,3} \bmod 100000000379$ testing various prime values $w_{1.3}$, we obtain the correspondence of V_1 to the (prime, value) pair (53, 86746790947) and of V_2 to the (prime, value) pair (313, 82108405283).

Then if, for instance, a voter with credential value for $g_1 = 111$ equal to $d_{1,2} = 2$ selects V_2, then the product $Vg_j^{d_{j,s}} = V_2 g_1^{d_{j,s}} = 52804155707 \cdot 111^2 = 173 \bmod 100000000379$ will appear in the accumulated (multiplicatively) encrypted (vote,credential) products $(\bmod p)\, M_i C_i = (g_0^{r+r'}, h_0^{r+r'} V g_j^{d_{j,s}})$. If another voter with the *same* credential value votes for V_2 too, then the exponent of the prime 173 will be increased to 2 etc. All computations are performed on the *encrypted* information, based on the homomorphic property of ElGamal.

Since it is mandatory that each individual can only cast a single opinion or vote, a mechanism is necessary for preventing multiple votes. This mechanism is provided by *scope exclusive pseudonyms* in Attribute Based Credentials. These are certified pseudonyms that are guaranteed to be unique per scope string and per user secret. By requiring a scope-exclusive pseudonym to be established in an application, a Verifier (e.g. a public consultation server) can be certain that only a single pseudonym can be generated, by an individual, for each credential or combination of credentials that are required in the application.

5 Conclusions

In this paper we have outlined how the emerging ABC technology can be integrated into traditional eVoting applications, such as public consultation and polling, using a concrete ABC credentials scheme and a concrete eVoting protocol. However, we believe that such integration can be performed with other ABC technologies and eVoting protocols, which currently is one of our major future research efforts. Our viewpoint is that ABC technologies will ultimately replace traditional PKI ones in a unified way and into a single *eID token* (see also [19,31] for a general discussion of eIdentity) that all citizens of a country will carry with them. Therefore, we believe that the time is now ripe for efforts that integrate ABC technologies with protocols that are employed for implementing all kinds of e-services in all sectors of citizens' daily lives.

As future research, it would be interesting to see how one can integrate ABCs with other eVoting protocols and systems, such as the ones discussed in Sect. 3.

Acknowledgement. The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under Grant Agreement no. 257782 for the project Attribute-based Credentials for Trust (ABC4Trust). We would, also, like to thank the reviewers for their insightful comments, which helped us improved greatly the contents of the paper.

References

1. ACM Special Issue on eVoting: The problems and potentials of voting systems. Commun. ACM **47**(10), 43–45 (2004)
2. Adams, J.: Opening Up E-Voting. O'Reilly Policy DevCenter (2004)
3. Antoniou, A., Korakas, C., Manolopoulos, C., Panagiotaki, A., Sofotassios, D., Spirakis, P., Stamatiou, Y.C.: A trust-centered approach for building E-Voting systems. In: Wimmer, M.A., Scholl, J., Grönlund, Å. (eds.) EGOV. LNCS, vol. 4656, pp. 366–377. Springer, Heidelberg (2007)
4. Boughton, C., Boughton, C.: Credible Election Software-eVACS. White Paper (2005)
5. Braendli, D.: The scope of e-voting in Switzerland. In: Proceedings of International Conference on E-Voting and Electronic Democracy: Present and the Future (2005)
6. Brands, S.: Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy, 1st edn. MIT Press, Cambridge (2000)
7. Brands, S., Demuynck, L., De Decker, B.: A practical system for globally revoking the unlinkable pseudonyms of unknown users. In: Pieprzyk, J., Ghodosi, H., Dawson, E. (eds.) ACISP 2007. LNCS, vol. 4586, pp. 400–415. Springer, Heidelberg (2007)
8. Burton, C., Culnane, C., Heather, J., Peacock, T., Ryan, P.Y.A., Schneider, S., Srinivasan, S., Teague, V., Wen, R., Xia, Z.: A supervised verifiable voting protocol for the victorian electoral commission. In: Proceedings of 5th International Conference on Electronic Voting (EVOTE 2012), pp. 81–94 (2012)
9. Camenisch, J.: Protecting (Anonymous) credentials with the trusted computing group's TPM V1.2. In: Fischer-Hübner, S., Rannenberg, K., Yngström, L., Lindskog, S. (eds.) SEC 2006. IFIP, vol. 201, pp. 135–147. Springer, Boston (2006)
10. Camenisch, J., Groß, T.: Efficient attributes for anonymous credentials. In: ACM Conference on Computer and Communications Security, pp. 345–356 (2008)
11. Camenisch, J., Van Herreweghen, E.: Design and implementation of the idemix anonymous credential system. Research Report RZ 3419, IBM Research Division, June 2002 (Also appeared in ACM Computer and Communication, Security 2002)
12. Camenisch, J., Lysyanskaya, A.: An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 93–118. Springer, Heidelberg (2001)
13. Camenisch, J., Lysyanskaya, A.: Signature schemes and anonymous credentials from bilinear maps. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 56–72. Springer, Heidelberg (2004)
14. Chaum, D.L.: Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM **24**(2), 84–88 (1981)
15. Chaum, D.L.: Blind signatures for untraceable payments. In: Proceedings of CRYPTO '82, pp. 199–203. Plenum Press (1982)
16. Cramer, R., Gennaro, R., Schoenmakers, B.: A secure and optimally efficient multiauthority election scheme. In: Fumy, W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 103–118. Springer, Heidelberg (1997)

17. The Electronic Voting Machine Project. http://evm2003.sourceforge.net
18. Estonian National Electoral Committee. http://www.vvk.ee/?lang=en
19. European Network and Information Security Agency: Privacy Features of European eID Card Specifications, February 2009. http://www.enisa.europa.eu/act/it/eid/eid-cards-en
20. The Geneva eVoting project. http://www.geneve.ch/evoting/english/welcome.asp
21. GNU.FREE: The FREE e-democracy Project. http://www.jasonkitcat.com/about/wheres-the-free-e-democracy-project/
22. Grewal, G.S., Ryan, M.D., Bursuc, S., Ryan P.Y.A.: Caveat coercitor: coercion-evidence in electronic voting. In: Proceedings of 34th IEEE Symposium on Security and Privacy, pp. 367–381 (2013)
23. Hoffstein, J., Pipher, J., Silverman, J.H.: An Introduction to Mathematical Cryptography. Springer, New York (2008)
24. Juels, A., Catalano, D., Jakobsson, M.: Coercion-resistant electronic elections. Cryptology ePrint Archive, Report 2002/165
25. Khader, D., Smyth, B., Ryan, P.Y.A., Hao, F: A fair and robust voting system by broadcast. In: Proceedinds of 5th International Conference on Electronic Voting (EVOTE 2012), pp. 285–299 (2012)
26. Kiayias, A., Yung, M.: Self-tallying elections and perfect ballot secrecy. In: Naccache, D., Paillier, P. (eds.) PKC 2002. LNCS, vol. 2274, pp. 141–158. Springer, Heidelberg (2002)
27. Lebre, R., Zúquete, A., Joaquim, R., Ferreira, P.: Internet voting: improving resistance to malicious servers in REVS. In: Proceedings of IADIS International Conference on Applied Computing (2004)
28. Okamoto, T.: Receipt-free electronic voting schemes for large scale elections. In: Christianson, B., Crispo, B., Lomas, M., Roe, M. (eds.) Security Protocols 1997. LNCS, vol. 1361, pp. 25–35. Springer, Heidelberg (1998)
29. Organization for the Advancement of Structured Information Standards (OASIS), eGovernment Unit - Cabinet Office UK (Editor), Election Markup Language - EML, Version 7.0, January 2011
30. Petersen, H., Horster, P., Michels, M.: Blind multisignatures schemes and their relevance to electronic voting. In: Proceedings of 11th Annual Computer Security Applications Conference, pp. 149–155 (1995)
31. Rannenberg, K., Royer, D., Deuker, A.: The Future of Identity in the Information Society – Challenges and Opportunities. Springer, Heidelberg (2009)
32. Riera, A., Puiggali. J.: Comments by Scytl on the SERVE security report. April 2004 (first version), March 2007 (last update)
33. Smith, W.D.: Cryptography meets voting. Version of January 2006
34. Storer, T., Duncan, I.: Electronic voting in the UK: current trends in deployment, requirements and technologies. In: Proceedings of 3rd Annual Conference on Privacy, Security and Trust (PST 2005) (2005)
35. Storer, T., Lock, R.: Accuracy: the fundamental requirement for voting systems. In: Proceedings of 4th International Conference on Availability, Reliability and Security (ARES 2009), pp. 374–379 (2009)
36. Sweeney, L.: k-anonymity: a model for protecting privacy. Int. J. Uncertainty Fuzziness Knowl. Based Syst. **10**(5), 557–570 (2002)
37. Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks

Extending Attribute Based Access Control to Facilitate Trust in eHealth and Other Applications

Jim Longstaff(✉)

Teesside University, Middlesbrough, England
j.j.longstaff@tees.ac.uk

Abstract. We describe a new model for Attribute Based Access Control (ABAC) which handles negative permissions and overrides in a single permissions processing mechanism. The model lends itself to the generation of explanations and permissions review, which can be used to foster end-user trust and confidence in the authorization system. We illustrate using a scenario in which a patient, with the assistance of an information specialist, develops consent directives for her medical records while receiving explanations and demonstrations. The model extends the approaches of ABAC and parameterized Role Based Access Control (RBAC) in that users, operations, and protected objects have properties, which we call classifiers. The simplest form of classifier is an attribute, as defined for ABAC; additional information is also handled by classifiers. Classifier values themselves are hierarchically-structured. A permission consists of a set of classifier values, and permissions review/determining an individual's risk exposure is carried out by database querying. The model has general applicability to areas where tightly-controlled sharing of data and applications, with well-defined overrides, is required.

Keywords: Attribute Based Access Control · Identity and access management · Enterprise information systems

1 Introduction

Trust is recognized as one of the essential factors in the use of computer systems. In authorization, if a user wishes to specify fine-grained controls over access to their data, trust can be gained through explaining the concepts based on a simple underlying model, and providing demonstrations of the access controls.

Attribute Based Access Control (ABAC) is generally considered as the way forward in authorization model research [17]. This reference suggests that implementations and applications will continue apace and also that there is a lack of a formal specifications base for ABAC. A comprehensive description of ABAC is provided in [9]. The central idea of ABAC asserts that access can be determined based on various attribute values presented by a subject. Permissions (often called rules) specify conditions under which access is granted or denied.

M. Felici (Ed.): CSP EU FORUM 2013, CCIS 182, pp. 127–137, 2013.
DOI: 10.1007/978-3-642-41205-9_11,

In this paper we present a new model of permissions which we call the Tees Confidentiality Model, version 2 (TCM2). It is based on a data model suggested by the ANSI standard for Role Based Access Control (RBAC) [1]. The basic RBAC model has the concepts of users being associated with roles, and roles being associated with permissions. Permissions are concerned with performing operations on protected objects. The TCM2 model has the same concepts of users, operations and protected objects; however these concepts now have properties, which we call classifiers, which are used for authorization. The simplest form of classifier corresponds to an attribute, as used in Attribute Based Access Control (ABAC) [9, 12]. User classifiers can take the role of parameters in parameterized RBAC; extended classifiers are defined for combinations of user, operation and protected object, and collection classifiers can be created to facilitate authorizations for collections of objects.

We have a totally different concept of permission to that of RBAC. Our permissions, which we call confidentiality permissions (CPs), in order to distinguish them from RBAC permissions, consist of sets of classifier values. The simplicity of the confidentiality permission format supports very-detailed authorizations and overrides.

TCM2 provides the capability of generating highly-targeted messages to specific users when they would expect to access data which has been denied. The messages could advise on using an override, or could give other information as appropriate.

The paper is organized as follows. Section 2 gives a description of the central concepts of TCM2 which includes examples of permissions and transactions in a notation appropriate for presentation. A comprehensive EHR scenario is presented in Sect. 3. An example of how permissions are processed is given in Sect. 4, while Sect. 5 compares our TCM2 model with current developments in ABAC and RBAC. Conclusions and references follow.

2 TCM2 Overview

2.1 Classifiers

Users, operations and protected objects are described by classifiers. Examples of user classifiers are User_id, UserName, UserRole, Team; for operations Op_id; for protected objects PO_id, PO_Type.

A classifier ordering is determined by the analyst, to indicate importance for matching classifiers. For example if User_id was deemed to be more important to UserRole when determining authorization, then a permission with a User_id value match would be preferred to another permission (not containing a User_id value) which matched by a UserRole value.

There is a type of override operation which allows a user to acquire a more specialized classifier value (if he was authorized to use this override).

2.2 Confidentiality Permissions

A CP is a set of classifier values, which can be provided by several mechanisms (stored database values, generator programs, external applications). Note that CPs

now encompass users, operations and protected objects, in contrast to RBAC permissions.

We now illustrate how CPs are used for authorization. The following CP represents the granting of read-and-append access to psychosis data for a clinician-user in the role "Psychiatrist", under normal (abbreviated "N") processing where no override has been used.

CP1 **Permit_CP (N)**:
{<UserRole, Psychiatrist>,
<Op_id, R_A>,
<PO_Type, Psychiatry>}

Other CPs may be derived using the classifier value hierarchies for every classifier present in a CP. For CP1 above, one derived CP includes the classifier value <UserRole, SeniorPsychiatrist>. Ranges of classifier values can be specified in CPs, as is illustrated later in CP11 – CP13.

A CP will match (i.e. qualify to authorize a transaction) if all its classifier values (describing the user, operation and object) are present in the transaction. Additionally, a CP will match if one of its derived CPs matches. For example the transaction described by

Active Classifier Values:
{<User_id, Fred>,
<UserRole, SeniorPsychiatrist>,
<Op_id, R_A>,
<PO_id, Alice_PsychiatryData >,
<PO_Type, Psychiatry>}

would be matched (and permitted) by permission CP1 above.

2.3 Deny Permissions, Override, and Deny Levels

Deny CPs are negative permissions which prevent access. These can be very detailed, for specific users and data, e.g.

CP2 **Deny_CP (L1)**:
{<User_id, Fred>,
<UserRole, Psychiatrist>,
<Op_id, R_A>,
<PO_id, Alice_PsychiatryData >}

CP2 denies (at Level 1 – see below) Fred access to Alice's psychiatry data when acting in the roles of Psychiatrist (and Senior Psychiatrist). However if authorized to override by the following CP

CP3 **Permit_CP (L1_Ovr)**:
{<User_id, Fred>
<UserRole, SeniorPsychiatrist >,
<Op_id, R_A>,
<PO_id, Alice_PsychiatryData >}

he could use this ‘CP Override’ to cancel the effect of the deny permission CP2, but only if he is acting in the role SeniorPsychiatrist.

Deny CPs are specified at increasing levels of power, called Deny Levels. A deny level contains deny permissions specified at lower deny levels. Therefore data could be denied to certain users who might be able to access it by Level 1 CP Override (if so authorized), whereas more sensitive data might be only available to more senior users who were authorized to override at Level 2.

Deny Levels can be used to implement a Break Glass emergency access approach [5]. The Break Glass approach to authorization has levels of access (pre-staged accounts, emergency levels) providing extra functionality which can be accessed in emergencies. In TCM2, emergency operations and data can be denied at deny levels 1, 2, 3, … etc., where each deny level represents an emergency level which can be accessed using CP Override.

2.4 CP Sets

CPs can be defined as having membership in separate, independent *Confidentiality Permission Sets*, or *CP Sets*. CP Sets can be used separately to determine authorisation, or combined. If a CP Set were to be used in conjunction with other CP Sets, they would first be analysed together for potential conflicts, which would be resolved according to analyst directives. They can be used for several purposes.

CP Sets can represent more detailed Break Glass emergency access than CP override by itself. Here CP Sets will represent access levels containing separately-designed permission sets which can be activated by a break glass override.

Representation of different levels of processing can be accomplished with CP Sets, e.g. Government and State regulations (CPS1), Consumer-specified directives (CPS2), and directives specified by Proxies for Consumers (CPS3). Therefore CPS1 authorizations can be preferred to CPS2 authorisations, if this is what the application requires.

In the examples that follow, normal access to health records (Sect. 3.2) could be provided by one CP Set, and the restrictions placed by an individual user on their own health records (Sects. 3.3−3.5) could form another CP Set.

3 HealthCare Scenario

3.1 Overview

We now give a comprehensive example of CPs, and briefly illustrate their processing in Sect. 4. The example concerns Electronic Health Record (EHR) data for a single patient Alice, and the consent directives represented by CPs which permit and restrict access to it. The patient develops the CPs through interacting with an information specialist.

3.2 Normal Access to EHR Data by Healthcare Professionals

For convenience we refer to this as access to Unrestricted Data (UD) for healthcare professionals. EHR data is to be made available to

(a) Healthcare professionals (HCPs) such as clinicians, doctors, and administrators who have a Legitimate Relationship or LR with the patient (specified by CP4).
(b) Additionally, all HCPs can exercise a Level 1 CP Override facility (CP5).

CP4 **Permit_CP (N)**: {<UserRole, HCP>, <LR, yes>, <Op_id, R_A>, <PO_Type, EHR>}	CP5 **Permit_CP(L1_Ovr)**: {<UserRole, HCP>, <LR, yes>, <Op_id, R_A>, <PO_Type, EHR>}

3.3 Access to Data Restricted by Consent Directive 1 (The Most Sensitive Data)

This data (several documents and database records), referred to as CD1 data, is to be made available to

(a) Certain individuals, Bob and Harry, when they are using role Senior Psychiatrist (CP6 and CP8).
(b) Bill, the author of this data, will also be able to access it, providing he is in a healthcare role, and has a Legitimate Relationship with the patient (CP6 and CP9).
(c) Other users on role Senior Psychiatrist, without an LR, on Level 2 CP Override, which is a privileged facility not generally available to healthcare professionals. (CP6 and CP10). (A message to Senior Psychiatrists would be displayed, indicating they could access restricted data by Level 2 CP Override.)

A further message is to be generated for the patient's GP, Fred, when he is denied access to this data through the matching of CP7. This message might say that the patient has restricted vital data from him, and suggest that he contacts a person who could access this data.

CP6 **Deny CP(L2)**: {<UserRole, HCP>, <PO_Coll_id,Alice_poc1>, <PO_Type, EHR>}	CP7 **Deny_CP(L2)**: { <User_id, Fred>, <UserRole, GP>, <PO_Coll_id, Alice_poc1>, <PO_Type, EHR>}	CP8 **Permit_CP (N)**: {<User_id, < Bob, Harry> >, <UserRole,SeniorPsychiatrist>, <Op_id, R_A>, <PO_Coll_id, Alice_poc1>, <PO_Type, EHR> }
CP9 **Permit_CP (N)**: {<User_id, Bill>, <UserRole, HCP>, <LR, yes>, <Op_id, R_A>, <PO_Coll_id, Alice_poc1>, <PO_Type, EHR>}	CP10**Permit_CP(L2_Ovr):** {<UserRole, SeniorPsychiatrist >, <Op_id, R_A>, <PO_Coll_id, Alice_poc1 >, <PO_Type, EHR>}	

3.4 Access to Data Restricted by Consent Directive 2

This (CD2) data (database records written by a particular clinician over a certain time period at a specific site) is to be made available to users as follows:

(a) All HCP users on Level 2 Override (if they are authorized to use it for this data).
(b) Senior Psychiatrist users on Level 1 Override, but only providing a precondition PC1 is true.

General messages indicating the availability of restricted data following override would be displayed. If the CP Level 2 Override were to be used, this would include a CP Level 1 Override, irrespective of the precondition evaluation).

CP11 **Deny_CP (L2)**: {<UserRole, HCP>, <Op_id, R_A>, <PO_id, Alice_EHR>, <PO_Type, EHR>, <PO_clinician_of_care, Bill>, <PO_EndDate, 01jan03>, <PO_Site, 2>}	CP12 **Deny_CP (L1)**: {<UserRole,SeniorPsychiatrist>, <Op_id, R_A>, <PO_id, Alice_EHR>, <PO_Type, EHR>, <PO_clinician_of_care, Bill>, <PO_EndDate, 01jan03>, <PO_Site, 2>}	CP13 **Permit_CP (L1_Ovr)**: {<UserRole, SeniorPsychiatrist>, <Op_id, R_A>, <PO_id, Alice_EHR>, <PO_Type, EHR>, <PO_clinician_of_care, Bill>, <PO_EndDate, 01jan03>, <PO_Site, 2>, <PC1, true>}
CP14 **Permit_CP (L2_Ovr)**: {<UserRole, HCP>, <Op_id, R_A> <PO_id, Alice_EHR>, <PO_Type, EHR>, <PO_clinician_of_care, Bill>, <PO_EndDate, 01jan03>, <PO_Site, 2>}		

3.5 Access to Data Restricted by Consent Directive 3

This (CD3) data (all psychiatric data) is to be made available to

(a) Senior Psychiatrists.
(b) Other HCP users via Level 1 CP Override.

CP15 **Deny_CP(L1)**: {<User_Role, HCP>, <Op_id, R_A>, <PO_id, Alice_EHR>, <PO_Type, Psychosis>}	CP16 **Permit_CP(N) :** {<UserRole,SeniorPsychiatrist>, <Op_id, R_A>, <PO_id, Alice_EHR>, <PO_Type, Psychosis>}	CP17 **Deny_CP (L1)**: {<UserRole,SeniorPsychiatrist>, <Op_id, R_A>, <PO_id, Alice_EHR>, <PO_Type, Psychosis>, <PO_clinician_of_care, Bill>, <PO_EndDate, 01jan03>, <PO_Site, 2>}

An additional message to Senior Psychiatrist users following the display of psychiatric data might alert to the availability of further (restricted) data (Consent Directives 1 and 2) through override. This would be to guard against possible oversight by the user, which might have serious consequences for the treatment of the patient.

3.6 An Authorization Example

As a consequence of the consent directives, consider an authenticated user (John) with an activated role of Senior Psychiatrist who queries the EHR for patient Alice, with whom he has an LR. For Normal Processing and Level 1 Override Processing, access to UD and CD3 data is permitted; for Level 2 Override Processing, UD, CD3, CD2, and CD1 objects are permitted.

4 CP Processing

Space restrictions only permit a brief illustration of how permissions are processed. CP processing depends on two principles. Firstly, a CP will match (i.e. qualify to authorize a transaction) if all its classifier values are contained in the transaction. Additionally, a CP will match if one of its derived CPs matches (An example of this was previously provided in Sect. 2.2).

The second principle concerns determining which of two CPs (taken from a set of Matched CPs) is the stronger or nearer match to a transaction. This Nearest Match CP would then have a higher priority in determining the authorization outcome. An elaboration of this principle follows.

A confidentiality permission is a set of classifier values. There is an ordering *cfiersq* on the classifiers that is set by the security architect and is a mapping of the set of integers 1, 2, 3, 4 … to the set of classifiers.

In order to compare two CPs *cp1*, *cp2* to find which one is the nearer match, we first determine the lowest classifier ordering number for each CP, namely $NCFIER_L(cp1)$ and $NCFIER_L(cp2)$.

If $NCFIER_L(cp1)$ and $NCFIER_L(cp2)$ are not the same then the CP with the lower classifier ordering number, i.e. the most important classifier specified by the security architect, is the nearer match. If they are the same then we consider the classifier values for these lowest ordering number classifiers, namely $VCFIER_L$ (*cp1*) and $VCFIER_L$ (*cp2*).

If $VCFIER_L$ (*cp1*) and $VCFIER_L$ (*cp2*) are not the same then we determine if they are related through the ancestor/descendant relationship and if so the descendant value takes priority and determines the Nearer Match CP.

If they do not have an ancestor/descendant association, or they are the same, then the whole process is repeated with the next lowest ordering number classifier for each CP, and so on, until the nearer match is obtained.

These principles can be used to directly determine the authorization outcome for a user, operation or protected object. Alternatively, by partially matching on user classifier values, they can be used to generate a sequence of Nearest Matched CPs which can be processed by database querying; this is illustrated in the examples below.

We now describe the processing of the transaction given in Sect. 3.6. The transaction is restricted to a single EHR for a single patient (Alice), and its sub objects. All Permit and Deny CPs specified the R_A operation. The initial set of Matched CPs, and the Nearest Match CP sequence (in order of strength of matching, and following Override CP removal for normal processing) are

Initially Matched CPs		**Nearest Matched CPs (no overrides)**		
CP4	Permit_CP (N)	CP4	Permit_CP (N)	1
CP5	Permit_CP (L1_Ovr)	CP6	Deny_CP (L2)	7
CP6	Deny_CP (L2)	CP11	Deny_CP (L2)	2
CP10	Permit_CP (L2_Ovr)	CP12	Deny_CP (L1)	4
CP11	Deny_CP (L2)	CP15	Deny_CP (L1)	3
CP12	Deny_CP (L1)	CP16	Permit_CP (N)	5
CP14	Permit_CP (L2_Ovr)	CP17	Deny_CP (L1)	6
CP15	Deny_CP (L1)			
CP16	Permit_CP (N)			
CP17	Deny_CP (L1)			

The match strength is indicated in ascending order, starting with the weakest (i.e. 1). Processing this Nearest Match CP sequence authorizes the retrieval of UD and CD3 objects. During demonstrations of the effects of permissions to the patient, it can be pointed which CPs permit or deny access to data, e.g. a particular CD1 object is denied by CP6, while a CD3 object is permitted by CP16.

Now suppose overrides are used. The same initially-matched CPs are returned. However on applying CP Override at Level 1 (involving deletion of L2_Ovr CPs), removing delete-related CPs and applying Nearest Match, the sequence of Nearest Matched CPs shown below is obtained: processing this sequence also determines that access is permitted to UD and CD3 data. If L2_Ovr is used, the indicated sequence is obtained: these CPs authorize access to UD, CD1, CD2, and CD3 data.

Nearest Match CPs (L1_ovr)			**Nearest Match CPs (L2_ovr)**		
CP4	Permit_CP (N)	1	CP4	Permit_CP (N)	1
CP5	Permit_CP (L1_Ovr)	2	CP5	Permit_CP (L1_Ovr)	2
CP6	Deny_CP (L2)	7	CP6	Deny_CP (L2)	5
CP11	Deny_CP (L2)	3	CP10	Permit_CP (L2_Ovr)	6
CP12	Deny_CP (L1)	4	CP14	Permit_CP (L2_Ovr)	3
CP16	Permit_CP (N)	5	CP16	Permit_CP (N)	4
CP17	Deny_CP (L1)	6			

5 Related Work

TCM2 has a number of similarities with our previously published TCM work [14, 15]. Role is treated as an application concept, and similar overrides are proposed. Also, the previous TCM papers have described design and processing strategies for permission types, but not for dynamic authorization involving individual permissions, as has been presented in this paper.

In the original TCM, hierarchies of classifier collections formed the basis of permissions processing, and permissions design. Also inheritance of permissions within classifier collection hierarchies was specified using permission types. In this paper, hierarchies of classifier values, with permissions inheritance always assumed, replaces classifier collection hierarchies. This is a major difference and simplification between TCM2 and the TCM. Also the TCM has no concept of permission-triggered messages.

Regarding emergency access to data, the Break-Glass approach [5] provides emergency accounts giving access to normally restricted data. The difficulties of such an approach are discussed in [6], which integrates a break glass approach into access control software; emergency level access is supported. These emergency levels are similar to the 'deny levels' concept in TCM2.

A large research development in RBAC can be described under the term parameterized RBAC. Part of this work involves using external (sometimes called contextual, environmental) information to control the processing of roles, and therefore provides additional functionality over standard RBAC, including what could be described as an override capability [2, 19]. The TCM2 model provides aspects of external parameter handling as part of its basic model and design framework (in that classifiers can represent external parameters). This approach is similar to that advocated in [7], which prefers the use of 'role attributes' to the use of external policy-enforcing systems (where this is possible).

Recently, investigations into Attribute Based Access Control, or ABAC, have been carried out, to address the inflexibility to change of RBAC models, and authorization models to be used for distributed applications [4, 8, 9, 12]. Access decisions are based on attributes that the user can be proved to have. In ABAC, different parties must reach trust agreements over attribute definitions, which can be more straightforward than agreeing consistent role definitions. ABAC provides good support for context, such as time of day. ABAC has been sometimes referred to as Policy Based Access Control or Claims Based Access Control. ABAC research, particularly focusing on attribute integrity and security, has been referred to as the 'grand challenge', and the future direction of authorization model development [17]. Applications in messaging and cryptography are described in [13, 21], and consistency and fault detection in rule structures is reported in [11].

XACML is an extensively developed and implemented ABAC approach, for which the underlying model has similarities with TCM2. XACML subjects, actions, and resources (corresponding to TCM2 users, operations, and protected objects) have attributes, on which authorization decisions are made. A comprehensive architecture involving PDPs, PEPs is defined for this. There is provision for extensions to be

written into an XACML application, which could be used in an implementation of TCM2.

TCM2 has additional concepts, namely Levels of Access, and overrides. A significant difference between TMC2 and XACML appears to be in simplicity of use. TCM2 very simply facilitates the modeling and use of authorization concepts, such as hierarchically-structured attribute values, inheritance of permissions. An industrial strength TMC2 implementation would use full relational database, with efficient management of large volumes of data and permissions, and direct database programming of permissions processing, which is essentially simple. An efficiency study for large XACML applications is reported in [16].

There are potential difficulties for permissions review/risk exposure for ABAC—potentially large numbers of rules, and their processing, must be considered. Reference [10] proposes a combination of ABAC and RBAC, in which the permissions available to a user are the intersection of permissions provided by RBAC active roles and ABAC rules. The TCM2 model extends the ABAC approach in that classifiers (which can represent ABAC attributes) are defined for operations and protected objects, in addition to users. Note that there is no direct TCM2 equivalent to RBAC permissions, which are used in the presentation of ABAC models. A recent approach to combining RBAC and ABAC was presented in [14]; TCM2 permissions can be designed to directly implement RBAC authorization.

6 Conclusions

We have described an ABAC permissions structure which directly supports fine-grained authorization, overrides, and highly-targeted messages produced during permissions execution. A formal specification of our model has been developed using the B-Method [3, 18], which is too detailed to be covered in this paper. As far as we are aware, no other model provides all this functionality in a simple and straightforward way. The functionality enables the support of the interactive development of permissions, during which permissions review ("who can see what") and deny/override schemes can be explored and demonstrated. It has been our experience that this feedback engenders trust in the authorization system on the part of non-technical end users.

We have provided a detailed healthcare records authorization scenario which demonstrates the modeling power of our approach, and we have briefly described the feedback and messages provided to the end user to promote trust. Throughout the development of the TCM and TCM2 models, close collaboration with the England healthcare authorities (the NHS) has taken place, and the ideas have contributed to the current authorization scheme mandated by the NHS [20], and to its previous versions.

Acknowledgment. The author wishes to thank Tony Howitt, Professor Mike Lockyer, Professor Michael Thick and Steve Dunne for advice and contributions. The work was supported in part by grants and contracts from the England NHS National Programme for IT, particularly as part of the ERDIP and HRI Programmes (2000−2006).

References

1. ANSI 2012, American National Standard for Information Technology: Role Based Access Control, ANSI INCITS 359-2012. www.incits.org (2012)
2. Bacon, J., Moody, K., Yao, W.: A model of OASIS role-based access control and its support for active security. ACM Trans. Inf. Syst. Secur. **5**(4), 492–540 (2002)
3. B-Method: www.methode-b.com (2013)
4. Blaze, M., Feigenbaum, J., Ioannidis, J.: The KeyNote Trust Management System Version 2. IETF RFC 2704. http://www1.cs.columbia.edu/~angelos/Papers/rfc2704.txt (1999)
5. BREAK-GLASS (SPC): Break-glass: an approach to granting emergency access to healthcare systems. White paper, joint NEMA/COCIR/JIRA Security and Privacy Committee (2004)
6. Brucker, A.D., Petritsch, H.: Extending access control models with break-glass. In: Proceedings of 2009 ACM Symposium on Access Control Models and Technologies (2009)
7. Goh, C., Baldwin, A.: Towards a more complete model of role. In: Proceedings of Third ACM Workshop on Role-Based Access Control (1998)
8. Karp, A.H., Haury, H., Davis, M.H.: From ABAC to ZBAC: the evolution of access control models. Tech. Report HPL-2009-30, HP Labs (2009)
9. Hu, V.C., Ferraiolo, D., Kuhn, R., et al.: Guide to Attribute based Access Control (ABAC) Definition and Considerations (Draft). NIST Spec. Publ. 800-162. http://csrc.nist.gov/publications/drafts/800-162/sp800_162_draft.pdf (2013)
10. Huang, J., Nicol, D.M., Bobba, R., Huh, J.H.: A framework integrating attribute-based policies into role-based access control. In: SACMAT '12, Newark, New Jersey, USA (2012)
11. Kuhn, D.R.: Vulnerability hierarchies in access control configurations. In: 4th Symposium on Configuration Analytics and Automation. IEEE (2011)
12. Kuhn, D.R., Coyne, E.J., Weil, T.R.: Adding attributes to role-based access control. IEEE Comput. **43**(6), 79–81 (2010)
13. Li, J., et al.: Attribute-based signature and its applications. In: ASIACCS '10, Beijing, China, 13–16 April (2010)
14. Longstaff, J.J., Lockyer, M.A., Nicholas, J.: The tees confidentiality model: an authorization model for identities and roles. In: Proceedings of Eighth ACM Symposium on Access Control Models and Technologies (2003)
15. Longstaff, J.J., Lockyer, M.A., Howitt, A.: Functionality and implementation issues for complex authorization models. IEE Proc. Softw. Special Issue (on Role Based Access Control) **153**(1), 7−15 (2006) ISSN 1462-5970
16. Ros, S.P., Lischka, M., Marmol, F.G.: Graph-based XACML evaluation. In: SACMAT '12, Newark, New Jersey, 20–22 June (2012)
17. Sandhu, R.: The authorization leap from rights to attributes: maturation or chaos? In: SACMAT '12, Newark, New Jersey (2012)
18. Schneider, S.: The B-Method: An Introduction. Palgrave, Basingstoke (2001)
19. Stermbeck, M., Neuman, G.: An integrated approach to engineer and enforce context constraints in RBAC environments. ACM Trans. Inf. Syst. Secur. **7**(3), 392–427 (2004)
20. UK NHS: Care Records Guarantee. http://www.nigb.nhs.uk/pubs/nhscrg.pdf (2011)
21. Yu, S., et al.: Attribute based data sharing with attribute revocation. In: ASIACCS'10, Beijing, China, 13–16 April (2010)

Security and Privacy Policy

Coordination of Trust and Security Project Clustering

Jim Clarke[1(✉)], Paul Malone[1], and Catherine Bodeau-Pean[2]

[1]Waterford Institute of Technology—Telecommunications Software and Systems Group, Waterford, Ireland
{jclarke, pmalone}@tssg.org
[2]ONYAX-CBPO, Paris, France
catherine.bodeau-pean@wanadoo.fr

Abstract. The DG Connect Unit H4 Coordination and Support Actions and Networks of Excellence took part in two conference sessions during the Cyber Security and Privacy EU Forum (CSP 2013) to collectively address their roles, and, in particular, how they might work together within a Project Cluster framework to the advantage of the research and innovation projects and to the programme as a whole, and particularly in the context of significant recent EU initiatives concerning Cyber Security Policy and a Network Information Security Platform. The morning session examined goals and timescales of the projects; the afternoon session looked in further detail at options and possibilities for the structure and modus operandi for a project cluster, ways forward towards a NIS Platform, and extending participation, influence, and effect to projects outside the immediate ICT trust and security community.

Keywords: Cyber security policy · Trust · Privacy · Information security · Coordination · Project clusters

1 Introduction

In response to foreseen needs for the security of the digital infrastructure and information that is so vital to all aspects of the lives and livelihoods of its citizens, there is significant action by the EU, with emphasis on a Cyber Security Policy and directive [1], and related initiatives including the establishment of a Network Information Security (NIS) Platform [2].

The Trust and Security (T&S) Coordination Action (CA) SecCord – *Security and Trust Coordination and Enhanced Collaboration*)[1] – is responsible for managing the annual CSP Conference in line with the formal objectives and commitments in its Description of Work,[2] and for running the two conference sessions –*Track* 14– reported here.

[1] http://www.seccord.eu/
[2] "Description of Work" forms Annex 1 of the Grant Agreement of a FP project.

M. Felici (Ed.): CSP EU FORUM 2013, CCIS 182, pp. 141–152, 2013.
DOI: 10.1007/978-3-642-41205-9_12,

The purpose of the Track 14 workshop was to look at the current *Coordination and Support Actions* (CSAs) and *Networks of Excellence* (NoEs) of DG Connect Unit H4 – Trust and Security, and, in particular, to explore how they can work together for maximum benefit to the research and innovation projects and to the programme as a whole. This has two linked components: how the CSAs and NoEs can work in concert, and to what ends; and how the Trust and Security research and innovation projects can collaborate and support each other through forming project clusters.

This paper provides an overview of the workshop, and examines its recommendations and goals for future action.

Project Clustering. The concept of bringing projects together into clusters goes back to the early days of the Framework Programme – known then as Concertation – with the objective of projects achieving more together collectively or in focussed groups rather than as individual entities. A cluster is drawn from projects with shared interests; it comes together to look at common problems and issues, provide mutual benefit and insights, reduce overlap, and help leverage of results and outcomes. Clustering of T&S projects had (re)started already with the recent EFFECTS+ CA,[3] and with specific interest groups such as PRIMCLUSTER, the in-built clusters of the NoEs, and the Working Groups of earlier projects. The objective of SecCord is to further develop the clustering process and its effectiveness, and, in so doing, further the goals of the above Cybersecurity policy and NIS initiatives.

At a minimum, a project cluster should provide for a recognizable identity, a strategic roadmap for research, a repository for results, and channels for dissemination. The clusters themselves should be further brought together to provide a coordinated set of results and outputs that contribute to the EU cyber security policy and strategy. This might be in the form of a high-level Network Information Security Cluster cooperation mechanism, established at European Union level, to allow for information exchange and could form an integral component of the proposed NIS Platform, whose main purpose is to assist with implementing the measures set out in the NIS Directive, e.g. to simplify incident reporting, ensure its convergent and harmonised application across the EU, and provide input to the secure ICT R&I agenda [3].

Structure of This Paper. After this introduction, Sect. 2 outlines the current position, with some of the obstacles to successful clustering and possible ameliorations, with some areas of clustering activity to be explored; Sect. 3 gives a brief account of the workshop itself; Sect. 4 discusses the findings and proposals by the workshop; and Sect. 5 gives our conclusions and principle recommended actions.

2 Current Position

A fundamental problem for participation in clustering has sometimes been a reluctance of projects to allocate resources that may prejudice the achievement of their formal objectives of the Description of Work (DOW); a way forward may be to earmark certain

[3] http://www.effectsplus.eu/

resources in the Grant Agreements of the projects, or to allocate funds to the clustering process to facilitate participation by projects. This concept should be investigated, both for current running projects and new projects currently in negotiations.

Three areas of clustering are identified:

1. Trust and Security Project Clusters as currently envisaged in the SecCord Description of Work, building on the earlier clustering activities of EFFECT-S + and developing the clusters to open up to other relevant domains, and, in particular, legal, social, economics, and health. SecCord already has the task to examine further mapping and alignment to achieve these extended goals. Other objectives are: to build on the topics where there are European strengths; to build up in areas seen to offer future opportunities, avoiding the waste of gaps and overlaps, and to jointly provide significant leverage and benefits.
2. Networking and Coordination Cluster for Trust and Security (CSAs and NoEs): the cluster management or coordination of this is also envisaged as a SecCord responsibility. The CSAs should collaborate amongst themselves to actively support the clustering activities. A similar model should be developed for bringing the R&I and NoE projects together and integrating activities and results, and also to add value, possibly using a similar structure to the earlier cooperation of the Future Internet Support Actions (see FISA[4]).
3. At the time of the workshop, the NIS Cluster was yet to be defined in terms of its structure and relationships, but is seen as a super-cluster that gathers, coordinates, and delivers material specifically for the NIS Platform. The success of the NIS Platform will call not only for strong moral support from European industry and commerce, but also for their active contribution and participation in the instruments of the platform. The way to tie-in and to incentivise participation of these communities effectively without overlaps is of utmost importance to the success and impact of clusters.

The first of these is already operational: the CSP conference, of which these two sessions were a part, also hosted trust and security R&I project cluster activities of SecCord.

The second can move forward from these two meetings to decide the details of its responsibilities and modus operandi answering the question posed above, and in general,

> *how best to work together for maximum benefit to the research and innovation projects and to the programme as a whole?*

The third –*NIS cluster*– although outside the scope of these meetings, it is envisaged that its operation will almost certainly involve the other two clustering processes.

The main outcome of the morning session was the presentation of the projects' objectives, expected results and mapping of timelines, and the examination of potential commonalities and specialties of the projects. A number of these were identified from the participating partners as shown in the table given below.

[4] http://fisa.future-internet.eu/index.php/Main_Page

A further analysis of this data was undertaken in the afternoon meeting, with follow up actions for the participants.[5]

A number of topics resonated throughout the presentations of the morning session as ways of increasing impact, principally:

Research roadmaps: an activity for several projects; therefore, we should examine how work can be aligned and coordinated;
Focus on excellence: focus on areas where the EU has recognised leadership and competitive advantage: e.g. cryptography, biometrics, smart card and smart grid, etc.;
Sharing information: clusters should maintain visibility and accessibility of project results and insights for longer, so they do not simply disappear at the end of a project;
Learning lessons: using the cluster to gather lessons learned (good and bad) from projects, which are usually never captured anywhere;
Risk management: bringing together projects involved in developing multi stakeholder approaches to risk management for trust, security and privacy.

3 Workshop Sessions

All the current CSAs and NoEs, together with the recently completed ECRYPT II NoE, took part in two sessions during CSPF 2013. The CSP Track 14 session was part of the general workshop agenda. It consisted mainly of presentations of the goals and timescales of the CSAs and the projects' answers to questions looking at current objectives, outputs, planned events and interactions, relation to current European policies for cyber security, and possible structure for a NIS Platform and ways that the CSAs and NoEs – and the research and innovation projects – might participate and contribute. The presentation details, answers to the questions, together with the commonalities and niche specialties of the CSAs that were examined were captured in a comprehensive CSP Forum 2013 *Track14* report [4, 5].

The purpose of the follow-on afternoon meeting between the CSAs, the NoEs, and DG CNCT Unit H4 was to look in further detail at options and possibilities for the structure and modus operandi of project clustering, and ways forward towards a NIS Platform. A number of desirable clustering attributes were identified. These include extending their participation, influence, and effect to projects outside the immediate ICT trust and security community, particularly those concerned with legal, economic, health, and social focus, where there is an inherent need for security of information and infrastructure. Not least is the requirement for continuity of the project clusters so that the legacy and achievement of projects is not immediately lost on their completion; one of the difficulties has arisen from the batch profile of a particular Call for Proposals, so that work from earlier calls, e.g. FP7 Call 1 with its Identity Management objectives, say, seems all but forgotten by the time of later calls, although results and issues are still valid and valuable.

[5] The full slide sets of the speakers are available from http://www.cspforum.eu/uploads/14_NetworkingCoordination.zip

3.1 Agenda Track 14 Workshop

The purpose of the morning clustering session was

1. to identify requirements for clustering to ensure a well-coordinated approach for the industrial cyber security strategy in the EU and beyond;
2. for CSAs and NoEs to present their core objectives, specialty areas of coverage, synergy with other projects, and relation to current major EC actions;
3. to identify common interests and potential synergies that can be exploited to set up a coordinated approach for clustering;
4. to discuss and gather feedback from participants on where the CSAs/NoEs can potentially support the setup of NIS platform.

In order to maintain focus, the projects were given a structured template in which they presented their coverage areas and specialties, in terms of: objectives, challenges, timeline; outputs, and synergy with other projects; relation to current major European Commission policy actions; and vision of NIS Technology platform infrastructure. The table below summarises the identified *commonalities* and *specialties* of projects.

This presented material and subsequent discussions provided valuable input to the follow-up meeting held in the afternoon.

3.2 Follow-Up Meeting

The purpose of the afternoon session was to explore some of the functional and operational requirements of project clusters, particularly concerning cluster-coordination, and possible need to support NIS – or other future *targeted* initiatives. The main outputs are discussed in Sect. 4 below, and listed in full in the Appendix. Discussion between the projects and EU representative arrived at a recommended framework for clusters.

General Coordination Cluster. The functionality of the cluster (in common with other envisaged clusters) –and hence *deliverables*– would concern:

– *policy support* for cyber security and information protection;
– *cluster dissemination*: cluster website, cluster book, cluster identity, spreading excellence;
– *conference and event planning*: thematic tracks for publication, joint conferences and workshops;
– *research roadmap*: strategic research agenda, cyber security innovation plan, standardization plan.

NIS Cluster Functional Structure. The basic framework of the NIS support cluster would provide: cluster secretariat; cluster coordination; EU contacts and liaison; activity coordination; three expert Working Groups (currently being established).

This might be set up as a specific ad hoc structure, or could be sourced from one or more of the available members of the General Coordination Cluster. The cluster activities could lead on to a more extended European Technology Platform (ETP).

Table of project commonalities and specialties	NESSoS	STREWS	CIRRUS	ATTPS	FIRE	SysSec	CYSPA	ECRYPT II	BIC	SECCORD
Cloud computing – security certification, internationalisation, standards	☑	☑	☑	☑	☑				☑	
Research agendas	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Web services security road-map		☑								
Dissemination expertise	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Participatory methods e.g. running Advisory Boards, Working groups, Clusters	☑	☑		☑	☑	☑	☑		☑	☑
Establishment of platforms/ infrastructures for cooperation	☑			☑	☑	☑	☑		☑	☑
Repository/platform for dissemination/sharing information		☑	☑	☑	☑	☑			☑	☑
Enabling technologies e.g. Cryptography	☑			☑		☑		☑		
Services and software engineering security	☑	☑	☑							
Building International cooperation (INCO) via road mapping and models									☑	
INCO in terms of involvement of non EU countries		☑	☑	☑	☑	☑		☑	☑	
Policy analysis and support (e.g. for H2020, cybersecurity, NIS platform, …)	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Education: summer-schools etc.	☑					☑		☑		
Linkages with industry and industrial sectors	☑	☑		☑	☑	☑		☑		☑

4 Workshop Recommendations and Proposals

The workshop arrived at a number of findings or proposals for future action regarding Trust and Security project clustering. These are given in full in [4], but included here for completeness as an Appendix. Below we attempt to summarise and consolidate them into a small number of groups, and discuss briefly the implications arising. The conclusions and overall recommendations and goals are then given in Sect. 5.

4.1 Overview of Grouping of Recommendations

The workshop recommendations can be allocated into four inter-linking groups outlined below.

Membership: the conditions and qualifications of membership, and the challenges of ensuring involvement by all (H4) T&S projects, and extending participation to the wider community of framework projects and beyond.

New work items, content, and cluster initiatives: the nature, content and priorities of the work to be undertaken by the project clusters.

Organisational and administrative: mainly about possible evolution of EU procedure to formally support the formation and operation of *project clusters*.

Cluster operations: how the clusters should be organised – and organise themselves – to undertake collaborative work and to contribute to collective activities, such as, currently, the annual CSP conference, and, in the future, shaping the programme and policy, and inputs to the NIS initiative.

4.2 Disposition and Discussion of Workshop Recommendations

This section looks at the groups of recommendations and seeks to provide pointers to future action. The assumption is that Project Clustering can and should be beneficial:

– the underlying questions concern *what*? and *how*?

MEM – Membership
(items labelled MEM in Appendix)
Membership of T&S clusters should be free of charge, in that there should be no direct joining or contributory participation charges; however, clustering activities do not come for free, and there needs to be either funding allocated in project budgets (in Grant Agreements), or there should be some form of centrally allocated budget, possibly channelled through a nominated project. Currently, the cost of participation is generally 'found' from some squeeze or underspend within existing project budgets. (see also *ORG*, below).

Cluster participation should be extended by invitation to all projects with an interest, dependency, or commitment, relating to trust and security. The more obvious fields would include health and welfare, economics, legal, societal, infrastructures (physical services, transport and communications, and underlying administrations, etc.), some of which come under the Security Research programme.[6]

Work Items, Workplan, Content
(items labelled NWI in Appendix)
There are four principal aspects to the work of the clusters: *technical cooperation and collaboration*; *dissemination and communication*; *community building*; and *contribution to cyber-security policy and planning*. In addition there may be, from time to time, special assignments from the Commission.

The scope and content of the technical work should be decided by the cluster participants taking into account their own interests together with the needs of the overall EU [cyber] trust and security programme and initiatives.

There is an urgent need to get the clusters active, following an inclusive plan. The intention is for the NoEs and CSAs to form a sort of *programme committee*, chaired by SecCord. In general, the work should build on EU strengths in areas such as cryptography, smart card, embedded systems, biometry, privacy, but recognizing the projects own commitments. The clusters could also provide a lookout, monitoring

[6] http://cordis.europa.eu/fp7/security/

gaps or weaknesses, and giving warnings of technical or economic vulnerabilities, as many projects are committed to this type of activity anyway.

Dissemination and communication activities are addressed mainly under *Cluster operations*, below, about events and communication channels, however, it is suggested that a component of technical collaboration would be producing forward-looking research white-papers on challenges and achievements.

Community building has two dimensions: strengthening the cohesion within the clusters; and extending visibility and awareness within the programme and externally to other EU entities, and into Member States. This extension has always been a problem: the annual CSP conference does provide a platform to a potentially wider audience, but getting beyond the *usual suspects* does remain a challenge. The Commission should be able to provide support with contacts and active participation.

As an input to policy and future planning, CSAs have had a tradition of producing roadmaps that contribute to the forward *Strategic Research Agenda*. The clusters provide a valuable mechanism for coordinating and integrating this work, with further opportunities for mechanisms for searches, *views*, digests. The above white papers, particularly the *kite-flyers*, can also add value here.

Organisational and Administrative – Mainly EU Procedure

(items labelled ORG in Appendix)

Two main points were made concerning the role of the Commission, and more particularly Unit H4, responsible for trust and security.

The first concerns the material support for clustering, and its formal recognition and funding. The participation in clustering is actively encouraged by Unit H4; however, other than some budget in the CSAs to cover organisational matters, there has been no R&I project budget nor work package commitment formally allocated to cluster participation to date. The question is raised whether there can be any revision to current DoWs, and whether future Grant Agreements should make provision (automatically) for cluster participation.

The second point concerns active participation in, and support of project clustering by the Commission. Unit H4 is already active in promoting the importance of ICT trust and security: that the programme as a whole – and its participants –should be as much cyber-security aware as it is cyber-aware. However, it is suggested that universal cluster membership should be mandated as strongly as possible, and that optimum use should be made of current CSAs and NoEs by ensuring full collaboration – again by strong encouragement where brute force may not be actually possible. Future provision for clustering should recognise the need for appropriate coverage by CSAs, with the possibility for flexible movement of responsibilities between them.

As noted earlier, it would be most helpful for the Commission to provide the contacts and introductions to beyond the immediate area of cyber Trust and Security.

Cluster Operations and Support

(items labelled OPS in Appendix)

The main topics here concern dissemination and communication, and their channels; and activities supporting other project cluster operations. These include activities and responsibilities that may already fall naturally within the remit of existing CSAs (see

Table given above), but could be extended and strengthened through their further collaboration and cooperation.

Dissemination concerns the sharing and publication of content arising from the cluster projects: their results and ideas – as individual projects, and from cluster collaborations. One aspect is communication with the immediate Trust & Security (technical) community; the second is communication with other research bodies and industry, and with the policy and decision makers of the EU and *current/future/planned* initiatives such as H2020, NIS, and Directives.

The channels that project clustering can provide are a common website (*Cyber Security and Privacy*, say, as already established for the CSP conference), and cluster workshops and conferences.

The website should provide communal cluster and individual projects spaces to provide not only access and visibility to the CVs and prospectuses of projects and participants, their results and achievements, and cluster event news and reports, but also to provide for sharing of more speculative ideas and challenges (*kite-flying*, as above). Ideally, the whole set of information could be seen as a structured, searchable library of Trust and Security news, concepts, technical outcomes and policy contributions (such as roadmaps). It could also provide a valuable directory to other sources of news, events, and information. The cluster could also make use of other social media outlets, as appropriate, e.g. LinkedIn Group, Twitter, …

Cluster workshops and conferences should address big-picture *themes* and concepts as well as specialist, detailed-picture *topics*. Successful events of these sorts have, of course, been held previously, but a coordinated cluster approach should be able to add further value to the quality of content and communication of outcomes.

For example, an annual publication could go beyond this set of CSP conference proceedings (as here, that could provide a valuable foundation and approach); it may need to extend beyond a single volume if it were to incorporate leading results and discussions from the Trust and Security community.

An ongoing challenge for cluster dissemination and communication is how to reach out to those *outside* the Trust & Security community itself, not least to the areas of the programme that have inherent or implied Trust & Security issues or dependencies (e.g., health, transport, legal, economic, infrastructure, as in *Membership*, above). The challenge of getting them to actively participate – with presumably limited funding, scope, and direct references in their DOWs – is, of course, something that needs to be overcome and would need direct support from their constituent funding authority and project officers.

Activities supporting other project cluster operations mainly concern planning and coordination: the management of cluster events; establishment and maintenance of a work programme; integration of, for instance, the roadmapping work of individual projects, and creating a unified structure with identifiable scope, commonalities, overlaps, and gaps.

5 Conclusions and Goals

The longer term continuation and extension of Trust & Security project clustering is seen as potentially beneficial and effective if structured correctly: for the individual projects; and for the trust and security aspects of the Framework Programme.

Immediate next steps should be

- to start building the cluster community, including addressing the administrative, scope, promotion, and structure questions to address the challenges as outlined for existing, new and future projects;
- to build web presence and visibility;
- to compile the CSPF book – selected proceedings including this paper to share with a wider audience (published summer time 2013);
- to generate a calendar overview of relevant events.

Acknowledgements. The participating projects are supported within the portfolio of the European Commission's DG-CNECT Unit H.4, Trust and Security;
http://cordis.europa.eu/fp7/ict/security/home_en.html
SecCord is supported under Grant Agreement No. 316622.

Appendix – Workshop Recommendations

(MEM) – membership; (NWI) – new work items, content, initiatives;
(ORG) – organisational; administrative; (OPS) – cluster operations

R1. Membership of the Trust and Security Project Clusters should be open to all Framework Programme projects; those outside Trust & Security itself that have inherent or implied Trust & Security issues would be most welcome (e.g., health, transport, legal, economic, infrastructure, …). (MEM)

R2. Membership of clusters should be free; a project will coordinate the cluster activities and, if necessary, Descriptions of Work (DOWs) should be examined and changed if necessary to align a project's tasks with the responsibilities taken up in the cluster.
Note: The SecCord (CA) project already has such cluster coordination responsibilities in its objectives; it could act as a "contact point" for the cluster community. (MEM)

R3. The cluster of CSAs/NoEs should make a start on areas that are more concerned with community building (e.g. conferences, workshops, research roadmaps …).
Note: Assistance from the Commission will be needed to provide contact points and short descriptions of all projects, especially those in new Calls. (NWI)

R4. The Unit H4 Trust and Security should be take part in the cluster activities, and should strongly encourage its projects to play an active role in the clusters. (NWI)

R5. In order to provide continuity through H2020 (and even beyond), clusters should have a span beyond a set of projects arising from a single call; responsibilities in the clusters and allocations of activities may change over this lifespan, partners in newly-funded projects taking over tasks from completing projects. (ORG)
R6. The Commission should also consider the need for specific cluster-supporting project(s) when drafting future calls. (ORG)
R7. Cluster priorities should be the responsibility of the cluster-members themselves, but taking full account of the requirements of such as the Cyber Security Strategy, the NIS platform, the societal pillar in H2020, etc. (NWI)
R8. There should be provision for rotation of certain periodic responsibilities to lessen the burden on some projects e.g., hosting meetings, organizing sessions, specific work activities required. (ORG)
R9. The appropriate stakeholders (people/projects/initiatives) should be brought together to begin scoping cluster activities, to get active membership, and to gain agreement on who does what and when. There should be draft plan for 2013 cluster activities, with allocated responsibilities, available for the next cluster meeting. (NWI)
R10. Earlier and current cluster models should be reviewed, e.g. Effectsplus, SecurIST, PRIMCLUSTER, GEANT, IN-HOME, etc., to see how they have been organized, their benefits and/or problems encountered. (ORG)
R11. Clustering should be supported by all Trustworthy ICT projects. A number of coordination and support activities in the security domain already have some associated cluster activity that they should look with a view to taking on further clustering responsibilities. (ORG)
R12. The clusters should build activity streams around EU strength areas: e.g. cryptography, smart card, embedded systems, biometry, privacy, and others. (OPS)
R13. The cluster should examine benefits and possibilities for collaboration on utilising summer schools of the projects. (OPS)
R14. Similarly, the cluster should look at possibilities for theme-based conferences/workshops: a continuous effort in order to share data, capitalizing in the "scale effect" of a big cluster for small companies could be provided. (NWI)
R15. The cluster should encourage white papers, to be made available in a central featured repository (as in BIC), in which authors are invited to submit articles via the projects, keeping in mind that the basic data sometimes comes in a fairly rough format and the responsible project compiles into a nice glossy format for publication. (OPS)
R16. The clusters should be used as a vehicle to promote the trust and security message and promote it as a central consideration for all projects. The audience is our community, including the European Commission, research, industry, policy, decision makers (and eventually NIS platform). (OPS)

R17. There would ideally be an annual book from the clusters. (possibly along the lines of this CSP Forum volume; another example was the yearly FIA book). The annual trust and security book should take care to support the identity of the trust and security clusters (of course, it also links in the Future Internet, telecommunication, mobile, smart grid, and many other topics, but the competence of the trust and security community should be the dominant contributor. (OPS)

R18. Each project that is a member of the Trust and Security cluster should put an executive summary on-line on the cluster web platform. The choice for the web platform has not yet been made but the CSP forum would be a candidate. There should be formal agreement from all projects to communicate their public deliverables to the cluster website; the cluster website should be a collaboration platform that offers broad functionality to the cluster members (e.g. to upload deliverables themselves, to update entries in the cluster agenda, to release news items, …). (OPS)

R19. Research agendas/roadmaps should be catalogued. (OPS)

R20. There should be a directory or atlas of roadmaps, taking into account the diversity of the various topics. They could use the rendezvous concept, where the roadmaps have been analysed and points of contact determined so that matters may be coordinated along technology (or other) lines. (OPS)

References

1. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS – Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
2. 2013/0027 (COD) Proposal for a directive of the European parliament and of the council concerning measures to ensure a high common level of network and information security across the Union (e.g.,) http://www.europarl.europa.eu/oeil/popups/summary.do?id=1247517&t=d&l=en
3. Minutes of the NIS Platform Kick-off meeting held 17th June 2013 in Brussels
4. NoE & CSA Clustering Report – CSP EU Forum 2013. http://www.cspforum.eu/uploads/CSP_Track14_Report.pdf
5. Track 14 presentation material: Networking and Coordination cluster of CSAs in Trust and Security; Chair: Jim Clarke, Waterford Institute of Technology (TSSG); within Presentations Day 2. http://www.cspforum.eu/2013/programme/presentations-day-2

Electronic Identity Adoption: Online Survey

Hugo Kerschot and Jiri Bouchal(✉)

IS-practice, Brussels, Belgium
jiri.bouchal@is-practice.eu,
info@is-practice.eu, www.is-practice.eu

Abstract. SSEDIC (Scoping the Single European Digital Identity Community), a thematic network funded under the European Commission CIP ICT PSP program, conducted an online survey on the use of electronic identity (eID) in 2012. The fundamental goal of the survey was to collect the information on the use of electronic identity by the wider European public and its opinions on eID regulation, use, and privacy issues. The 2012 eID Adoption Survey is a continuation of the 2011 eID Adoption Survey conducted by SSEDIC. Compared to the 2011 survey, which was aimed at eID experts, the 2012 iteration of the survey was modified in order to make the survey comprehensive for non-experts and to reach for a wider public. At the same time, the approach and structure of the survey as well as the user profile was similar, which allows the comparison of the results up to a certain level. This paper summarizes the major findings of the survey according to the research topics: use of electronic identity, use of e-signature, opinions on eID regulation and policy, privacy issues, eID federation, and secure electronic document exchange.

Keywords: Electronic identity · Adoption · Internet use · Survey · Online survey · SSEDIC · eID · Thematic network

1 Introduction

SSEDIC, a thematic network funded under the European Commission CIP ICT PSP program,[1] conducted an online survey on the use of electronic identity (eID) in 2012. The fundamental goal of the survey was to collect the information on the use of electronic identity by the European wider public and its opinions on eID regulation, use, and privacy issues.

The Year 2 eID Adoption Survey is a continuation of the Year 1 eID Adoption Survey conducted by SSEDIC in November 2011. Compared to the 2011 survey, which was aimed at eID experts. The SSEDIC 2011 expert survey was conducted to learn about the attitudes of eID experts towards electronic identity and the related security, privacy and usability aspects in the context of both their professional and

[1] SSEDIC is the EU project funded under the ICT PSP Call 4. Within SSEDIC, more than 70 eID related organisations work together to prepare the agenda for a Single European Digital Identity Community as envisaged by the Digital Agenda in its Key Action 16.

M. Felici (Ed.): CSP EU FORUM 2013, CCIS 182, pp. 153–164, 2013.
DOI: 10.1007/978-3-642-41205-9_13,

private activities. The experts were also asked about their opinions regarding a European framework for eID-based services. This survey is to be considered as the first step in a longer term monitoring process.[2]

This paper summarizes the major findings of the survey according to the research topics: use of electronic identity, use of E-Signature, opinions on eID regulation and policy, privacy issues, eID Federation, and secure electronic document exchange. The full text of the survey report is available at the SSEDIC website.[3]

2 Sample Composition

Respondents were targeted via different networks in IT, consultancy, public sector, university sector etc. The survey was distributed via social networks (including SSEDIC LinkedIn group) and via networks and mailing lists of the SSEDIC partners and associate partners as well as via several projects' and organisations' newsletters. The survey was also promoted at the European Commission DG Connect website.

SSEDIC distribution efforts and mass mailing to thousands of e-mail addresses resulted in 1000 respondents completing the whole survey between October and December 2012. Thanks to the successful mass-mailing campaigns of Spanish SSEDIC partners distributing the survey, 383 respondents were Spanish residents. To prevent their overrepresentation for the analysis of the answers, the weight of Spanish residents' responses was reduced from 4 to 1 (from 383 to 96 respondents). Therefore a theoretical sample of 713 Internet users (N = 713) was defined for the analysis of the survey.

The survey sample reached for the survey does not have scientifically representative ambition; as such a goal was not within the "budget-reach" of the SSEDIC project. Since the input for the study was collected by distributing an "open link" towards the professional and personal networks of the SSEDIC members and via a few mass-mailing actions of professional databases, the sample mostly consists of a relatively highly educated, Internet-savvy universe and Internet professionals with an in-depth experience with the tools they were questioned about.

The majority of 85 % respondents are EU residents, are male (72 %) and received higher education (90 %). Compared to the 2011 expert survey, the 2012 survey attracted more women and slightly more respondents with lower education. More than half of the respondents were aged between 35 and 54 years. The group of participants younger than 34 years was slightly larger than the one of 55+. The professional background of respondents was various. Some domains of expertise (like IT industry - hardware, software, and services) were stronger represented in the sample.

2.1 Internet Use Profile

The respondents were profiled according to the frequency of their Internet access, devices used, and the motivation for Internet use. Vast majority of respondents use the

[2] Year 1 survey report is available at the SSEDIC website: http://www.eidssedic.eu/images/stories/pdf/SSEDIC%20D2.3.1%20eID%20Adoption%20Survey%20Y1%20v1.1.pdf

[3] http://www.eid-ssedic.eu/index.php?option=com_content&view=article&id=104&Itemid=100101

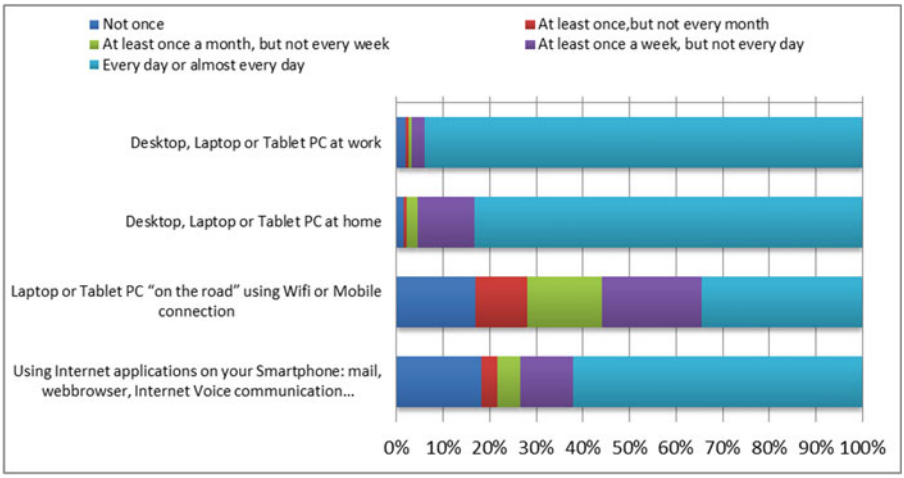

Fig. 1. Internet access frequency and devices used

Internet every day or almost every day, either at work (94 %) or at home (83 %). More than 55 % of participants use their laptop or tablet PC to access the Internet "on the road" on daily or weekly basis. More interestingly, almost 75 % of respondent do the same thing using their smartphone (62 % on daily basis). The significant uptake of smartphones compared to "mobile" laptops and tablet PCs is quite obvious (Fig. 1).

The respondents were also asked about the purposes they use the Internet and frequency of use for each of these purposes. 95 % use the Internet on daily basis for professional purposes such as checking e-mail or searching information. Social networks are visited by almost 60 % of users on daily or weekly basis (34 % daily). Approximately the same amount of respondents, with only a little lower frequency, uses the Internet regularly to administer their bank account via the Internet banking. Most of the people do that on weekly rather than on daily basis. Half of the respondents use the Internet daily or weekly to watch online videos or TV, listen to online music or radio streaming, download movies or music etc. Active participation at discussions and blogs, posting opinions at news websites, Twitter etc. and making for phone or webcam video calls is the daily or weekly activity for 30 % of respondents. Almost 60 % of respondents access the Internet to do their online shopping at least once a month. Quite surprisingly, only 5 % of respondents do not purchase goods or services online at all. The use of online auction sites as eBay is considerably lower.

3 Use of Electronic Identity

In this part of the survey, the participants were asked what types of online credentials they use to identify themselves on the Internet and the frequency of use of these credentials. The results show that the most frequently used credentials are the traditional and relatively weak user ID/password based credentials mostly obtained to create an email account, to become a member of a social network or to purchase goods

or services online. Users seem prefer to have a username indicating their real name rather than the anonymous one when using social networks and email. Username/password credential connected to a card (e.g. bank payment card or smart card used for public transportation) with the personal information verified by a 3rd party is also very common as it is used by 76 % of respondents. Hardware devices (including code-generating tokens, SIM card mobile devices, and card readers with PIN verification) are usually obtained for eBanking. An interesting finding is the one-year progress in the use of SIMcard/Mobile related eID's. Compared to the 2011 the expert survey, three times more respondents indicated to use these credentials on daily basis in 2012. Respondents rarely use more sophisticated identification methods based on PKI, hardware devices, and biometrics. The use of PKI infrastructures (allowing to sign documents electronically with eSignature) is mostly connected to the official government issued eIDs. Surprisingly large majority of users buy goods or services online from other countries (75 %) and make online money transfers to other EU member state via online banking, PayPal etc. (51 %).

The most frequent reasons for not possessing or hardly using listed eID credentials are no need to use these tools, doubts about their security, and lack of trust in the issuers.

3.1 Comparison with 2011 Expert Survey Results

The frequency of use of the credentials is similar. However, several differences can be found. The eID experts prefers anonymous username, by 17 percentage points (pp), when accessing websites and social networks rather then the username indicating their real identity (which is the preference for wider public according to the 2012 results).

The eID experts also use more frequently, by approx. 10 pp the more sophisticated identification methods such as a card in combination with card reader and PIN protection and eID in combination with one-time password generated by a token. On the other hand, username and password connected to a card (smart cards) was indicated to be used more frequently by almost 20 pp in the 2012 survey. Also the eID combined with SIM card mobile device is used more frequently (by 10 pp) by respondents of the 2012 survey. For more details on the comparison (see Fig. 2).

3.2 Reasons for not Using Some eIDs Types

The respondents were asked about the reasons for not using the eID credentials, which they previously described as not possessing or hardly using. The most common reason for not possessing or hardly using the listed types of eID credentials was no need to use these tools. In case of username/password eID credentials, 15–25 % of non-users do not believe these tools are technically secure. It is interesting to point out that in case of username/password indicating the real identity of the users (by real name, address, date of birth etc.), one-third of non-users selected that they do not trust the issuers of these tools. In the case of more sophisticated eIDs (eID embedded in public register – PKI, eID in combination with one-time password generated by a token, or biometric information supported eID), 15–20 % of the respondents were not aware of the existence of these tools.

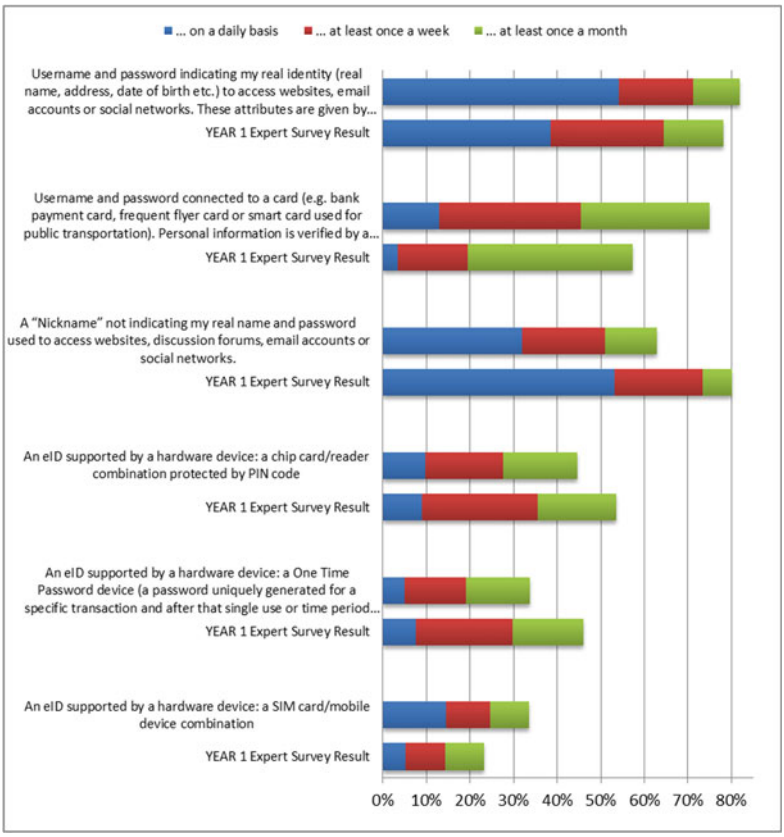

Fig. 2. Credentials used - comparison with 2011 (N = 713 for 2012 results)

4 e-Signatures

In this section, the respondents were asked about their possession of an eSignature, whether the signature is qualified, for what purposes they use it and what tools do they use to sign documents electronically. If the same question was asked in the Y1 eID expert survey, the results are compared. All 713 respondents were asked whether they have an electronic signature with a public key certificate that can be used in the context of their private or professional life. More than half of the survey participants replied positively. 43 % do not possess the eSignature. 74 % of the eSignature holders indicated that their signature is qualified. The results are again very similar to the Y1 survey where 73 % of respondents replied that their signature was qualified. As far as the purposes of the eSignature possession are concerned, its usage seems to be quite limited mostly to signing declarations for public services (58 % of respondents). The other purposes of eSignature use out of the scope of public services with a more commercial purpose, like signing a registered mail, invoices, contracts, etc. do not see

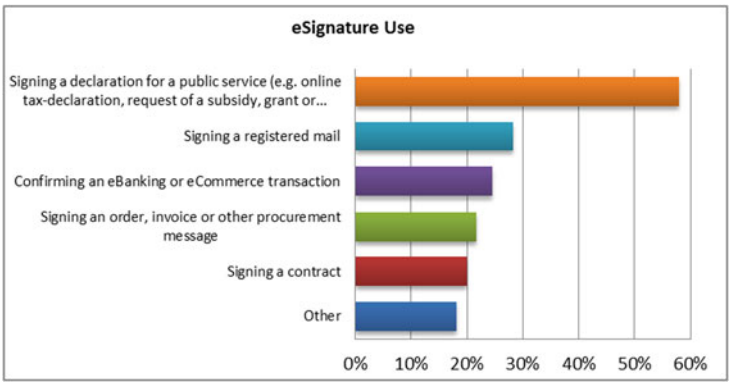

Fig. 3. Use of eSignature (N = 371)

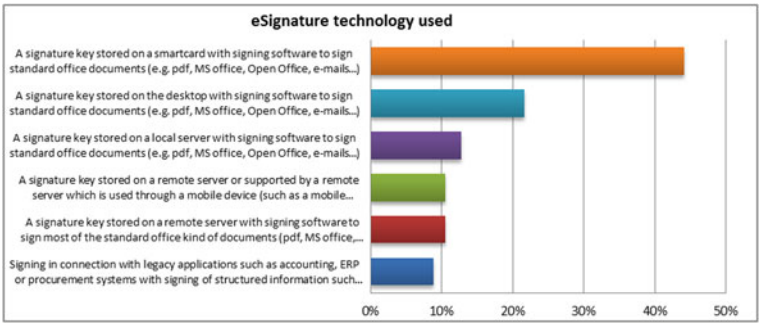

Fig. 4. eSignature technology (N = 371)

similar levels of uptake as public services (selected only by 20–30 % of respondents). These results are again very similar to the ones of Y1 expert survey (Fig. 3).

By the very similar results as in the last year, the survey confirms that the technology predominantly used by the eSignature holders is smartcard based (44 % sign digital documents with a signature key stored on a smartcard). 22 % of respondents use a signature key stored on desktop. Other types of the eSignature infrastructures (i.e. SMS, signatures stored on local or remote servers, etc.) are much less frequently employed (Fig. 4).

5 Opinions on Electronic Identity Regulation

In this survey section, we investigated the respondents' opinion on issues related to eID regulation, federation of eIDs and cross-sector use of eID, privacy, cross-border use of eID when purchasing goods and services online, and making online money transfers. To explore the respondents' personal view, we presented them with several statements and explicitly asked them to provide their personal opinions.

5.1 eID Regulation at the European and National Level

Respondents were asked about their opinion on the need of the European-level regulation of eID. The exact wording of the question was: *"Should European regulation fix a minimum level of quality requirements for electronic identities in order to ensure that all electronic identities will be accepted by public authorities in all other member states?"* 78 % of respondents think that establishing a minimum level of eID quality requirements in order to ensure all eIDs are accepted by public authorities in all member states (MS) is a task to be done by the EU. Only 7 % think each MS should address it separately and 6 % would leave this task to the private sector.

The next question asked respondents whether they think that new EU proposals for eIDs, eSignatures etc. (if approved) would help to improve take-up and usage of eIDs and digital signatures. More than half of respondents replied that the EU proposals would really help and another 27 % think they may marginally help. Only 9 % of participants do not expect the new EU proposals to help to improve take-up of eIDs and eSignatures.

The respondents were also requested to provide their opinion on the following question: *"Should the governments of all EU member states ensure that their citizens have access to trustworthy electronic identities that can be used cross-border, i.e. to access online eGOVERNMENT services in other EU countries?"* In this case too, the positive answer dominated. 67 % of respondents think that it is absolutely necessary to have eIDs that can be used to access eGovernment services in other MS. 16 % think this is not a core task of the government. 7 % would prefer to maintain separated eIDs in each MS. Only a minor percentage of respondents (2 %) would leave this task to private sector.

The next question demanded an opinion on a similar issue, however related to the use of eIDs to access online services of the private sector in other MS. In line with previous answers, most of the respondents (55 %) think that it is an absolutely necessary task for governments to ensure that their citizens have access to trustworthy electronic identities that can be used cross-border, i.e. to access online PRIVATE services in other EU countries. 26 % think this is not necessary since it is not a core task of the government. Compared to the previous question, we can see a shift of 10 % of respondents from the "absolutely necessary" option towards the answer "not necessarily, this is not a core task of the government". The percentage of respondents that would leave this task to the private sector is also remarkably higher (10 % compared to 2 % in the case of eGovernment services).

6 eID Federation and Privacy Issues

6.1 Federation and Cross-Sector Use of eID

This section of report addresses the respondents' opinions on issues such as eID federation and eID use across multiple sectors. Some private Internet companies (like Facebook, Google etc.) make it possible to use their user/password to login to other (3rd party) services (electronic identity federation). The respondents were asked whether they use eID federation, as well as for the motivation to (not) use such

service. More than half of the respondents indicated that they do not use eID federation. The motivation for most of them for not using eID federation is that they do not want to provide information about what service they use to another company. Only 6 % of respondents are not aware of the existence of eID federation. 45 % of survey participants use eID federation. Quite surprisingly, only 10 % replied that they use eID federation because it makes a login easier. Two similar groups of respondents (17–18 %) use federation rarely or only when they foresee a possible benefit of sharing their eID between both services.

When we cross-check this result with the profiles of the respondents we see that the age-category −34, males and higher educated respondents are more in favour for federation then elders, women and respondents with a lower degree of education. Taking into account the answers to the previous question, it may seem odd that most of the respondents expect future positive effects of the use of private sector's payments and eIDs for other services, including e-government services (e.g. using bank credentials for non-banking services such as tax declarations or online shopping). The use of private sector's payments and eIDs for other services is the only way forward according to 23 % of respondents, 44 % replied it can have positive effects, and only 25 % do not consider such development to be a good idea. It seems that the respondents would support eID federation if they can foresee positive effects and use cases that would make their online transactions easier. Nevertheless, they are not willing to provide more information about themselves to a 3rd party then necessary. These conclusions are in line with the findings on privacy protection issues described on the following section.

6.2 Privacy Issues

The respondents were asked two questions concerning privacy protection issues. There are a lot of companies (Facebook, Google, banks, supermarkets, etc.) which are not formally in the business of providing reliable electronic identities but which nonetheless hold a significant amount of identity information about citizens that they can release to other service providers. The respondents were asked whether specific rules on the privacy of persons and the integrity of personal information should be required for these service providers. The clear majority of 82 % respondents think that a specific regulation and control of such companies holding a significant amount of identity information is necessary. Only 11 % of participants consider the existing general privacy protection rules to be sufficient.

In addition, most of the respondents think that, in certain circumstances, there should be a legally protected explicit right to online anonymity ensuring that no one can be identified in an online transaction. For 34 % of participants, anonymous access should be the rule and for another 27 %, the anonymity is preferable in certain circumstances. According to 28 % of respondents, the right to anonymity should be conditional and should be revoked when criminal acts are involved.

6.3 Comparison with 2011 Expert Survey Results

Most findings regarding eID federation and privacy are in line with the privacy recommendation of eID experts in the SSEDIC Y1 survey. 90 % of the experts support the principle of minimum disclosure according to which

- the service provider should be obliged to declare the minimum number of attributes needed
- it should be unlawful for a service provider in any country to request more attributes than the
- minimum requirement necessary to establish identity,
- the user should be able to provide more attributes than the required minimum if he/she chooses so.

Regarding multiple identities, the experts also recommended:

- A user should be able to have multiple digital identities.
- A user should be able to have digital identities with partially fictitious information (e.g. pseudonyms).
- A user should be able to have digital identities with entirely fictitious information (e.g. personas or avatars).
- At the request of law enforcement agencies, identity providers should assist in linking multiple identities (including their respective unique identifiers) together.

Expert also agreed at a certain level that actions using Digital Identities should be traceable by law enforcement agencies.

7 Secure Electronic Document Exchange and Digital Identity

Only financial managers and professionals responsible for invoicing and payments who electronically exchange sensitive documents as part of their professional activities (respondents who indicated to be occupied with financial operations) were questioned in this section of the survey. We investigated types of documents that are exchanged securely, communication solutions used, and problems encountered. 133 respondents were asked whether (as part of their professional activities) they exchange sensitive electronic documents (e.g. invoices and purchase orders) with other business partners, financial institutions, administration etc. via the Internet. 88 % replied positively and were asked the other questions following in this section.

7.1 Types of Documents Exchanged

The electronic exchange of sensitive documents between business partners is rather common practice among the survey respondents. Sensitive documents most frequently exchanged with business partners via the Internet are invoices (77 % of respondents), followed by contracts and purchase orders (both 66 %) and B2B payment notices (49 %). Under the "other documents" option, the respondents mentioned technical

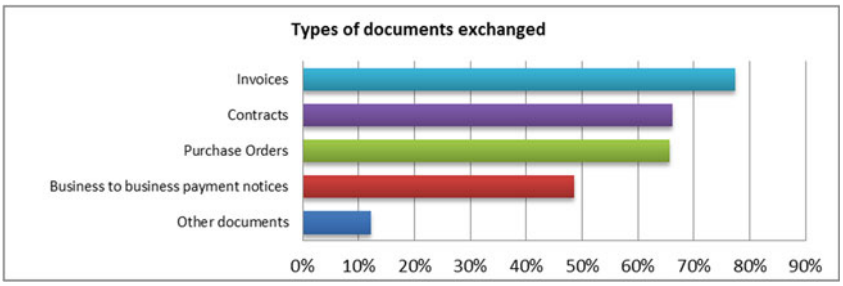

Fig. 5. Types of sensitive documents exchanged (N = 116)

specifications, rapports, sensitive client information, attestations, presentations or other confidential information (Fig. 5).

7.2 Technical Solutions

To exchange these electronic documents, the respondents mostly use regular e-mail (77 %). Web portals are preferred by 39 %. A secured e-mail system is used by only 35 % of respondents. As other solutions, the respondents use AS2 (Applicability Statement 2), cloud storage services (e.g. Dropbox), encryption of attached files, extranet, password-protected pdfs, remote desktop protocol, Webex, electronic data interchange (EDI), special file transfer environment or encrypted documents within regular email.

7.3 Problems Encountered

More than half of respondents have not encountered any problems when receiving or transmitting sensitive electronic documents. Within the remaining 49 % who have encountered some problems, the most common trouble was related to spam and spam filtering (29 % of all respondents replying to this question), followed by poor traceability, unclear status of transaction, and problems with sender identification (18 %). Problems with delivery denial by recipient were faced by 11 %. Delivery to the wrong recipient was a problem encountered by 9 %. Among the other problems, the respondents mentioned a poor acceptance of eSignatures, lack of interoperable tools, blocking by receiver's firewall, uncertainty about the delivery to recipient, nonexistence of a "standardized" way of communicating securely, or the capacity of the recipient's mailbox.

Respondents stated that they would increase their sensitive online communication if they had a secure electronic address linked to their company eID. The future potential for the take-up of eID and e-signature was identified in this domain (Fig. 6).

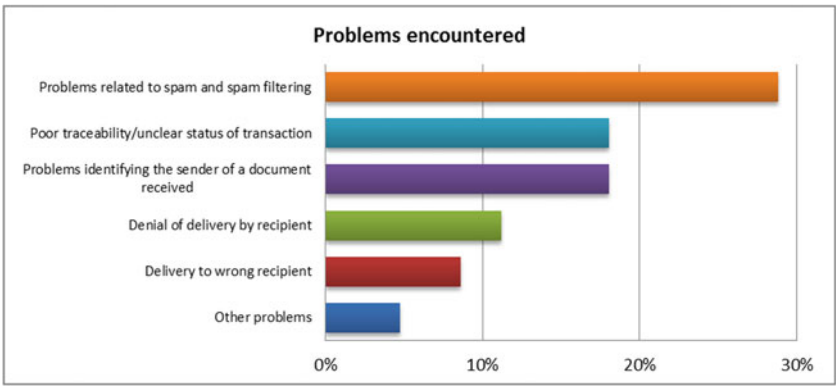

Fig. 6. Problems encountered (N = 116)

8 Conclusions

The SSEDIC consulted 1000 respondents residing mostly in the European countries in its 2012 eID adoption survey. Unlike the 2011 eID expert survey, the 2012 survey was designed to reach for a wider public (compared to 2011 survey), however the sample was still mostly composed of heavy Internet users and IT professionals familiar with the eID topics.

The survey produced valuable insights regarding the different types of **eID credentials used** by a wider public when proving the electronic identity on the Internet (including the frequency of their use, the way the credentials were obtained, and reasons for not using some types of eID credentials), **cross-border online use** of eID, **users opinions** on the necessity and goals of **eID regulation** at European as well as national level, on the **eID federation** and **privacy issues**, and secured **exchange of sensitive documents** via Internet.

The survey revealed that the **most frequently used** are the traditional and relatively weak **user ID/password** based credentials mostly obtained to create an email account or to become a member of a social network. Username/password credential connected to a **card** (e.g. bank payment card or smart card used for public transportation) is also very common as it is used by 76 % of respondents. The daily use of **SIM card/**Mobile related eID was indicated to be **three times higher** than registered one year ago. Surprisingly large majority of users **buy goods or services online from other countries** (75 %) and make online **money transfers** to other EU member state via online banking, PayPal etc. (51 %). Only half of the respondents possess an **electronic signature**. **A regular email** is the most used communication tool to exchange sensitive electronic documents. The respondents stressed the importance of **public sector involvement in eID regulation.** They indicated that the EU regulation is needed and expect positive impacts of new eID regulation resulting in wider eID use. Governments should ensure the acceptance of eID in other MS as well as both for public (eGovernment) and private (eBanking) services. The respondents are well aware of **privacy concerns** of Internet and eID use. They stressed the need for specific

privacy protection rules in the future. The respondents are **reluctant** to use the **eID federation,** as they are not willing to provide information about the service used to another company (3rd party) unless it is necessary.

The **findings of both SSEDIC surveys were consistent** and opinions of a general public confirmed the experts' recommendations of 2011 survey.

Anti-War Era: The Need for Proactive Cyber Security

Sven Herpig(✉)

University of Hull, Hull, UK
s.herpig@2008.hull.ac.uk

Abstract. Anti-war cyber warfare is not an oxymoron, it is reality. It describes actions taking place in a post-Cold War era which is defined by new strategies in the cyber domain. Those strategies mitigate conflicts through direct, non-lethal and *sub rosa* means. This paper argues that the international arena, with all its stakeholders, is entering a new era, creating an intense need for a holistic and proactive cyber security behaviour to counter the increasing number of hostile actions in the cyber domain. Proactive cyber security has to be steered by cooperating governments, and must involve the private and the public sector alike.

Keywords: Cyber security · Cyber warfare · Stuxnet · Tilded Platform · Multi-stakeholder · Anti-war · Cold war · Cyber espionage

1 Introduction

Fighting and warfare have always been part of the human society. Together with the evolution of the human being, technology progressed resulting in advanced warfare techniques starting with the infantry revolution around 1337 [1]. The latter dubbed 'revolution in military affairs' (RMA) reflects not only the genius of mankind but also its genuine drive to create even more destructive weapons [2]. While the peak of destructive potential and sophistication of weapons seemed to have been reached during the First World War, the Second World War taught us all a different lesson. The so-called 'Total War' will be remembered by historians for many of its superlatives and one particularly stands out: the development and use of the nuclear weapon – the most destructive weapon ever deployed. Even though nuclear powers have been engaged in several conflicts after 1945, none of them ever put a nuclear weapon to use – not even in the light of defeat. Some strategists of the Allied Forces even laid out the option of a 'limited war' in case the Soviet Union would dare to escalate the Cold War alongside the theoretical peak of destruction, the 'doomsday machine' [3, 4]. The Cold War turned out to revolve mainly around *sub rosa* activities and proxy conflicts. Many of the warfare operations which took place after the fall of the Soviet Union (e.g. anti-piracy and anti-terrorism missions) relied heavily on the use of special forces, thus moving even farther away from the notion of total war and completing the progression towards a time of limited warfare.

M. Felici (Ed.): CSP EU FORUM 2013, CCIS 182, pp. 165–176, 2013.
DOI: 10.1007/978-3-642-41205-9_14,

This article argues that the main powers in international politics are setting the stage for yet another transition towards a new period, the anti-war era. Anti-war is derived from the book with the same name written by Alvin and Heidi Toffler. It was originally thought of as a concept where 'Anti-Wars' include actions taken by politicians, and even by warriors themselves, to create conditions that deter or limit the extent of war' [5] which sees '… the transition from mass lethality to low-lethal or non-lethal weapons' enabling '… a peace-form for the future' [6]. This coincides to a certain degree with Derian's concept of a virtuous war, which he defines as '… the technical capability and ethical imperative to threaten and, if necessary, actualize violence from a distance -with no or minimal casualties' [7]. The world saw economically interwoven countries and a tendency to lower the use of force moving towards veiled warfare. It is one of the few tools which can be used to conduct actions against an adversary without necessarily sparking chaos in the international arena. Where Anti-War is the framework and espionage and sabotage are the core elements, cyber warfare cannot be far away. And indeed, it seems that cyber warfare is currently *en vogue*. The operation 'Olympic Games', commonly referred to only as 'Stuxnet' and its cousins, is the poster-boy of Anti-War cyber warfare. Various cyber weapons were developed to work together in order to infiltrate, analyse, sabotage and ultimately erase their traces [8–10]. Olympic Games hit Iran's centre of nuclear activity, a research and production facility which otherwise could have only been affected by a physical attack (e.g. a precise air strike). The latter would have caused the death of many people and might have destabilized this region even further. These are the situations – from the Iranian perspective – from which cyber warfare and proactive cyber security derive their *raisons d'être*. Information security and data security might have arguably been enough for businesses and government agencies to fend off hackers, hacktivists, crackers and criminal syndicates. It protected their data from computers going haywire and randomly deleting everything; or a competitor trying to steal useful information. In the Anti-War era where cyber warfare becomes the weapon of choice not only for activists and criminals but most especially for foreign military and intelligence services along with freelance mercenaries, proactive cyber security is desperately needed by both the public and private sector alike. Businesses, especially those considered vital by foreign nation-states, are being increasingly aimed at by sophisticated and targeted attacks which are backed by access to state resources [11]. This leaves the nation-state with a leading role in creating a strong and holistic national – and to a certain degree also international – proactive cyber security approach.

This paper first introduces the current state-of-the-art of cyber warfare and breaks it down in strategies that have been observed to be conducted in the cyber domain. The character and implementations of the strategic perspective on cyber warfare sets the stage for a comparison with the Cold War era. The comparison leads to the main contribution of this research: the conceptualization of Anti-War as a framework for cyber warfare efforts. Including the results of the case study on one of the elements of the operation 'Olympic Games' highlights consequently the need for proactive cyber security.

2 State-of-the-Art

2.1 Cyber Warfare Strategies

With the public discussion mainly revolving around 'deterrence', there are actually a number of strategies which can be applied to cyber warfare. Knowing the various options is vital because '[a] grand strategic vision of cyberspace can assist states in navigating the informational turbulence in which contemporary international politics appears to find itself. […] Cyberspace has its myriad of problems, but a true strategic sensibility demands that long-term interests prevail over short-term opportunism' [12]. Kuehl identifies a cyber strategy as 'the development and employment of strategic capabilities to operate in cyberspace, integrated and coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power in support of national security strategy' [13]. Starr sees it as 'the development and employment of capabilities to operate in cyberspace, integrated and coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power' [14]. While these authors refer to information warfare in general (also including propaganda, electromagnetic weapons etc.), cyber warfare is only a subcategory. Thus, cyber warfare strategy can be defined as 'the development and employment of cyber warfare operations, integrated and coordinated with other operational domains and forms of information warfare, to achieve or support the achievement of political objectives. Cyber warfare refers to the targeted use and hack of digital code by any individual, group, organization or state using digital networks and connected devices, which is directed against critical national, military or civilian information infrastructure in order to alter, destroy, disrupt or deny functionality with the ultimate aim to weaken and/or harm the targeted political unit' [15].

The cyber warfare strategies that are identified and analysed below are deduced from the literature on cyber warfare since its start in the 1990s. The research covers most literature on strategic cyber warfare and information warfare in order to derive a complete scale of potential strategies from it. It has to be kept in mind that the cyber warfare, especially its strategic applications, is a highly volatile research field and therefore subject to constant change. Cyber warfare strategies are stealthier and have an increased element of intelligence activities as compared to other kinds of warfare. Winkler suggests to '… look for Snakes, Not Dragons. Dragons are mythical beasts. Snakes are real and pervasive' [16]. Cyber warfare operations are pervasive. Thus, except from outright cyber war, all cyber warfare strategies are genuinely conducted as secret activities or how Libicki put it '… cyberwarfare *qua* warfare is soaked in intelligence' [17]. The following cyber warfare strategies have been identified:

- Going Dark
- Deterrence
- Sub Rosa
- Shashou Jian
- Cyber War

Going Dark. Going dark is not widely mentioned and even less addressed as a potential strategy. Mostly referred to as 'air-gapped networks', going dark reflects the disconnections of critical and vital networks from broader networks which are ultimately connected to the Internet. The strategic notion of this is still important as it would not be possible to implement it in any other domain as states are perennially connected in space, seas, and other domains. The main objective is to decrease the adversary's chances of realizing his objectives which he tries to achieve through the reliance on deterrence, *sub rosa*, *shashou jian* and/or cyber war strategies. 'Going dark' was implemented in Natanz.

Deterrence. Cyber deterrence as a strategy means that cyber warfare capabilities are deployed to deter any adversarial aggression regardless of the domain it takes place in. Cyber deterrence does not equate with only using cyber warfare means (e.g. air warfare) to deter cyber aggressions. Geers defines being caught up in a circle of cyber aggression and retaliation as 'mutually assured disruption' [18]. Cyber deterrence as a strategy can be applied on the basis of deterrence by punishment. This means that through cyber warfare costs are imposed, benefits are denied or incentives are given to the adversary in order to make him immediately stop his actions. Deterrence works only against adversaries who actually have something to lose in the cyber domain. This strategy is therefore restricted to nation-states with moderate to heavy reliance on information and communication technologies.

Sub Rosa. Extraction and disruption operations using networks and computer systems have been coined '*sub rosa* warfare' activities by Libicki. Subsequently, the *sub rosa* cyber warfare strategy 'has some aspects of intelligence operations, and some aspects of special operations – although it is neither. Notably, *sub rosa* warfare is almost impossible to conduct with tanks, much less nuclear weapons' [19]. Nation-states are aware of this strategy, as Gervais suggests when stating that '… anecdotal evidence suggests that cyber espionage is a familiar practice of state governments' [20]. Betz and Stevens even suggest that *sub rosa* cyber warfare is aspiring to be the most prevalent cyber warfare strategy as compared to strategies with a higher level of intensity [21]. The main objective is to create information dominance over adversaries and potential adversaries.

Shashou Jian. *Shashou jian* is Chinese for 'assassin's mace', a strategy which refers to the ability of striking the enemy decisively and stealthily (from behind) - making the fight fit the weapons [22, 23]. Incorporating this strategy into the cyber warfare framework is based on the evident Chinese use of *shashou jian* as a means to achieve its geo-strategic goals [24]. Sun Tzu describes this kind of strategy in his writings as relying on speed, stating that '… speed is the essence of war. Take advantage of the enemy's non-preparedness, travel by unexpected routes and strike him where he has taken no precautions' [25]. The main objective is to surgically take out adversary's centres of gravity to coerce the enemy. Libicki discusses three key roles that cyber warfare in general might play: 'It might cripple adversary capabilities quickly, if the adversary is caught by surprise. It can be used as a rapier in limited situations, thereby affording a temporary but potentially decisive military advantage. It can also inhibit

the adversary from using its system confidently' [26]. All of these goals can be achieved by the *shashou jian* strategy.

Cyber War. The main objective of cyber war is to supplement other kinds of warfare in order to support them in achieving their strategic and political objectives. At the same time, in terms of tools in foreign relations, cyber war offers a new layer of intensity (and escalation alike): cyber-to-cyber war. The new layer is located somewhere between economic sanctions, intelligence operations and actual use of physical violence. Schneier analyses the strategy of cyber war well when stating that '… and for there to be a cyberwar, there first needs to be a war' [27]. Libicki phrased it similarly arguing that '… operational cyberwar consists of wartime cyber attacks against military targets and military-related civilian targets' [28]. The intensity of cyber warfare is not limited in the framework of cyber war. As Libicki puts it: 'once something is called war, a victim's responsibility for the consequences of its acts dissipates' [29]. Compared to the other kinds of cyber warfare, escalation and along with it stealth play a minor role when open hostilities are already taking place.

2.2 Resemblances to the Cold War

Going dark is a rather simple and straightforward strategy. Critical devices which do not need to be connected to larger networks, especially the Internet, should not be connected. Also, in times of emergency, networks might be air-gapped temporarily to mitigate damage. The supplementary function of cyber warfare, as part of the cyber war strategy, has also been discussed – and most of the times been limited to it at length in academic literature.

The real potential of cyber warfare becomes apparent upon focusing on cyber deterrence, *sub rosa* warfare, *shashou jian* and the cyber-to-cyber war element of the cyber war strategy. Those strategies equip the nation-state with new options in international relations decision-making processes during times of conflict. The implementation of those strategies bears the potential of achieving political objectives without involving other domains. Not excluding the possibility of conflict-escalation, those strategies aim at preventing conflicts from turning violent or hot by solving them inside the cyber domain e.g. through decisive strikes. Bearing similarities to Cold War activities, the strategies add a whole new level to the traditional cloak & dagger – espionage and sabotage – game.

During the Cold War, nuclear weapons were the Sword of Damocles. Activities during the Cold War therefore aimed at limiting the sphere of influence of the opposed superpower without risking or using nuclear weapons, hence causing Armageddon. Somehow, the new cold war seems to take a step further. Cyber strategies are implemented in order to prevent conflicts from turning into a war or at least keeping them inside the cyber domain. Therefore, the strategies aim at preventing the use of conventional and nuclear forces, while allowing the different stakeholders to engage in a conflict to achieve their respective political aims. Sulek and Moran compared cyber warfare operations to the Cold War, stating that '… the cyber [war] as a Cold War analogy is ripe with similarities. The most obvious parallel between the Cyber and

Cold War eras is the central role of espionage. […] This appears to parallel efforts during the Cold War, where the Superpowers each invested resources into the creation and maintenance of rival spy networks. These networks were primarily designed to gather intelligence in an effort to gain a competitive advantage in diplomatic, economic, informational, and military confrontations' [29]. A heavy reliance on extraction (of information) operations gives a first clue of what Anti-War might look like. Sulek and Moran discuss another similarity between the Cold War and cyber warfare operations. According to them, '… the Cold War offers a powerful image, that of a protracted struggle between powers for political, military, and ideological supremacy. There are obvious similarities—the cat-and-mouse game of espionage that boils below the geopolitical surface; the proxy wars that may suddenly break out in cyberspace; and the importance of retaining technological superiority' [30]. Dipert paints a similar picture stating that '[…] what we are likely to see in the next years, perhaps decades, is something like the Cold War between the Allied Forces and the Soviet Union. The espionage 'cat and mouse games' of the Cold War are well known, and there was also extensive probing of each other's territorial defences, by the incursion of small numbers of air, sea, and ground forces, never giving sufficient reason to believe that a large-scale attack was imminent. What we are likely to see is the informal development of a similar 'equilibrium' in the accepted quantity and seriousness of cyberattacks' [31]. This 'cat-and-mouse game' can be played through the use of various cyber warfare strategies via cyberspace directly between the two or more adversaries.

Another indicator is important for the subsequent Anti-War debate. Janczewski and Colarik state that cyber-attacks often follow physical events, such as plane crashes [32], as manifested in the actions of the Honker Union in 2001. Dearth, Williamson and Stiennon state that cyber-attacks will most likely be responded to with cyber counter attacks rather than conventional retaliation [33, 34]. Anti-War therefore reflects a nation-state responding to internal political pressure by the adoption of cyber means or the support of allied stakeholders in a proxy war.

2.3 The Anti-War Concept

This new setting resembles very much like what Heidi and Alvin Toffler called 'Anti-War'. Toffler and Toffler describe Anti-War as 'actions taken by politicians, and even by warriors themselves, to create conditions that deter or limit the extent of war' [35]. They went further explaining how this could be implemented by stating that '… knowledge weapons alone, even including the use of the media, may never suffice to prevent war or to limit its spread. But the failure to develop systematic strategies for their use is inexcusable. Transparency, surveillance, weapons monitoring, the use of information technology, intelligence, interdiction of communication services, propaganda, the transition from mass lethality to low-lethal or non-lethal weapons, training, and education are all elements of a peace-form for the future' [36]. Anti-War therefore includes strategies which allow for political necessities as a response for a hostile action but stay below a potentially escalating threshold in order to prevent war by allowing to figuratively blow-off a certain amount of political steam, thus releasing tension out of a conflict, subsequently cooling it down. The Anti-War framework

however allows for direct contact of the opposing powers with a potential for but not a guarantee of escalation, depending on the level of communication and signalling. New opportunities come with new challenges. Apart from the signalling, Adams identified another problem, stating that the Cold War had rules and boundaries which are missing in cyber-aggressions, thus leading to a 'free-for-all, with more and more players hurrying to join scrimmage' [37]. Herein lies another difference between the Cold War period and the current developments. Due to the low costs of entry and the potentially asymmetrical advantage of cyber warfare, the cyber warfare arena portrays the world as a multi-stakeholder colosseum rather than a bi-stakeholder playing field. Even though different levels of resources are likely to result in different levels of sophistication for cyber attacks and cyber weapons, every nation-state – among other groups – can participate in the cyber struggle. Gross pinpoints the latter challenge, stating that '… much, perhaps most, information about cyber-conflict of all types is classified, which creates tremendous practical problems of communication' [38]. In addition to the complexity and frictions of cyber warfare discussed earlier, escalation cannot be excluded – especially because cyber warfare strategies tempt to bear comparatively high degree of intensity, based on Geers levels of intensity for strategic information warfare [39]. The Anti-War era is subsequently marked by

- a dominance of intelligence operations (according to the definition of cyber warfare);
- comparatively low rate of intended lethality of actions (if cyber warfare is an option);
- multi-stakeholderism with power centres (e.g. United States, China, Israel) and periphery (e.g. India, United Kingdom, Australia);
- international conflict resolution rather than conflict escalation;
- higher friction and complexity in terms of strategic challenges;
- a need for clear signalling and proper communication channels;
- affecting a geographical location (networks making up the Internet) which no stakeholder wants to see destroyed or crippled.

2.4 Weapon of the New Era: Tilded Platform

The name 'Tilded' is derived from the filenames of the malicious software used during the operation, which always includes a ~d (read: 'tilde d'). The Tilded Platform [40] which is part of the operation 'Olympic Games' and appears to be composed of Duqu, Stuxnet and Wiper. It can be regarded as the most prominent example to date of the new era. Assuming that the Anti-War era is all about keeping conflicts from turning into coercive use of traditional (physical) force, the activities carried out under the Tilded Platform operation should be compared to the more conventional option of a precision air strike against the target – Iranian nuclear research and production facility in Natanz. Sanger argues that Israeli bombing Iran would have had a unifying, polarizing effect (for the region) and might not have been very effective. As the facilities in Natanz would be difficult to hit and more secret facilities might exist to carry on any of those operations such as nuclear enrichment [41]. Additionally, Farwell and Rohozinski argue that '[…] a [conventional] strike poses risks. A single

strike might not succeed, and it is not clear how many over-flights Saudi Arabia or the United States might permit. Israel could sustain significant losses. Iran would hold the United States responsible, and could attack US installations and troops in Iraq, Afghanistan or elsewhere. It might disrupt the flow of oil out of the Gulf and oil prices could escalate. Air strikes might unite a currently divided Iran and enable Ahmadinejad and his allies to consolidate power' [42]. Geers supports this view of the possible impact of a conventional strike on the international relations arena, stating that '[…] Stuxnet may have been more effective than a conventional military attack and may have avoided a major international crisis over collateral damage' [43]. The strategic implication which can be derived from this discussion is that cyber warfare is now on the table as a viable military option to strike an adversary's centres of gravity – even as a stand-alone option – as opposed to conventional strikes. Estimates are seeing the nuclear programme setback estimated between 6 months to 18 months. Even though it is difficult to anticipate what damage and delay a conventional strike would have caused, the fact that cyber warfare had an impact with zero casualties on the attacker's side makes it an option for the future.

One of the key advantages which cyber warfare is supposed to have over other forms of warfare is the lack of collateral damage. In the case of the Tilded Platform, this issue is a tricky one. Stuxnet, the cyber weapon which actually did the most damage, was found on (mainly SCADA) computer systems around the world. There is also the rumour that due to an infection with Stuxnet, an Indian satellite has been destroyed. All of this '… creates a potentially serious risk of political blowback if the attacking parties are identified' [44]. However, an infection of systems with Stuxnet is not necessarily sustained damage at all. Gervais points this out, saying that '… while the Stuxnet worm did infect civilian industrial control systems around the world, the harmful effect was triggered only by the conditions present in Iran's nuclear program. The Stuxnet worm satisfies the criteria of distinction because the worm was designed for a specific military target – assuming the Natanz plant is not a civilian nuclear energy program – and it could not indiscriminately destroy civilian computer systems' [45]. So even though several systems which are not targeted got infected, no damage was done to those systems. None other than the Natanz incident was reported and traced back to Stuxnet. Other targets in Iran were reportedly hit by Wiper but those also appeared to be intended targets. So beyond the potential impact on the Indian satellite and the mere infection of systems, there seems to be no further collateral damage – and such damage was only economic in nature. It should however be kept in mind that cyber weapons such as Stuxnet are created with a high potential of functioning autonomously, especially when used in air-gapped systems. Healy therefore concludes that 'details on Olympic Games are difficult to come by but it appears Stuxnet was just such an exception, set loose with only algorithms – rather than a human – to tell it whether to unleash Hell' [46]. A programming bug could have changed that and might have had serious impact on industrial controls worldwide. No nation-state actor could be interested in carrying out cyber warfare activities resulting in the (temporary) break down of the worldwide Internet and connected systems. The potential collateral damage of cyber warfare therefore is immense. One has only to review emergency mitigation strategies which describe the outcome of day-long

black-outs. Even though the Tilded Platform had physical impact, it was non-lethal with no reported collateral damage or casualties at all.

Cyber warfare can make a strategic impact as stand-alone, physical, non-lethal option with low to none collateral damage and casualties. The activities were stealthy and aimed at achieving strategic goals while trying to avoid human casualties and especially further escalation leading to more physically destructive options and possibly war. The case of the Tilded Platform viably portrays the underlying Anti-War era.

3 Conclusions

As discussed, there is a certain notion that we find ourselves in an era that was described decades ago – an era that promotes the settlement of conflicts by warfare-like means but with much lower casualty and collateral damage levels than conventional or even nuclear warfare.

Having effective tools – or weapons – ready will likely result in a much lower likelihood of actually using them. If, as in the Natanz case, all other options are still left on the table afterwards and casualties are kept low, cyber warfare seems to be attractive and might virtually seduce decision-makers to their use whenever possible. In times like this, when the number of stakeholders participating in international cyber conflicts is constantly increasing and no end of hostilities seems likely, it is vital to step up the corresponding security measures, in this case: cyber security. Cyber security which aims at securing the nation's critical information infrastructure has to take a proactive approach – an approach which does not only rely entirely on research focused at defensive measures, trying to beat the attackers to it. Proactive cyber security bears a certain notion of 'offensive' research as well. This does not necessarily mean that cyber weapons should be developed but that the underlying research will be a necessity in order to further mitigate the impact of adversarial actions.

One way of doing so is to focus research on traps, the so-called honeypots and honeynets – either in a virtual/sandbox environment or as raw steel version. Their research, development and deployment allows the analysis of attack vectors and behaviours, therefore allowing an adaptation of the defensive measures in order to counter future attacks following those patterns. At the same time, research devoted at the more 'offensive' part of cyber warfare will allow *hardening* the systems even before attacks are noticed and analysed e.g. through honeypots. Finding a zero-day exploit before the adversary allows its correction before harm is done. In order to implement a holistic and sustainable cyber security paradigm to deal with this new reality, the Anti-War era, knowing offensive capabilities is crucial. This knowledge has to be created a priori to the potential attacks. In cyber security, being seconds too late can already make the difference between having an effective security in place and having none at all.

Approaches by international entities to address cyber security are well underway. The United Nations focusing on cyber arms control while the NATO fosters research on collective cyber security for its members. These works seem to be in the early stages. To efficiently implement proactive cyber security, a holistic national approach

– including private organizations, research institutes and academia – is crucial. In its essence, the cyber domain is different from other war fighting domains. Tanks positioned at an allied border can increase the security for said partner country. Translating this situation in the cyber domain would mean to allow allied IT security personnel access to another country's networks in order to protect them. This access could then also be abused to conduct *sub rosa* operations against the allied partner without him noticing. Thus, a holistic national paradigm towards proactive cyber security seems to be the most promising approach in the short-term. An international layer might be added in the future but postponing any activities until then would be dangerous and not advisable.

In summary, hostilities in cyberspace, involving private and public sectors, are likely to increase in number and intensity. The only way to deal with this is an international cooperation of national efforts, led by the governments and involving the private sector, through a proactive cyber security behaviour.

References

1. Krepinevich, A.F.: Cavalry to computer: the pattern of military revolutions. Natl. Interest **37** (1994). Foreign Affairs 30(13), p. 1
2. For an overview over the stages of RMA, see Krepinevich, A.F.: Cavalry to computer: the pattern of military revolutions. Natl. Interest **37** (1994). Foreign Affairs 30(13), p. 1
3. Kaplan, F.M.: The Wizards of Armageddon, pp. 195–200. Simon and Schuster, New York (1983)
4. Kahn, H.: On Thermonuclear War, pp. 114–152. Transaction Publishers, New Brunswick (2007)
5. Toffler, A., Toffler, H.: War and Anti-War Survival at the Dawn of the 21st Century, p. 4. Little Brown and Company, London (1993)
6. Toffler, A., Toffler, H.: War and Anti-War Survival at the Dawn of the 21st Century, p. 239. Little Brown and Company, London (1993)
7. Der Derian, J.: Virtuous war/virtual theory. Int. Affairs **76**(4), 771–788 (2000). Royal Institute of International Affairs, Blackwell Publishing, p. 772
8. Boldizsár, B., Pék, G., Buttyán, L., Félegyházi, M.: The cousins of Stuxnet: Duqu, Flame, and Gauss. Future Internet **4**(6), 971–1003 (2012)
9. Grauman, B.: Cyber-Security: The Vexed Question of Global Rules. Secure & Defence Agenda, Brussels (2012)
10. Falliere, N.; Murchu, L.O., Chien, E.: W32.Stuxnet Dossier. Version 1.3, Number 2010. Symantec Security Response (2010)
11. Examples for this kind of cyber operations are Ghostnet (1999), AURORA (2009) and the work of the APT/Comment Crew (2013)
12. Betz, D.J., Stevens, T.: Cyberspace and the State: Toward a Strategy for Cyber-power, p. 139. The International Institute for Strategic Studies, Routledge, New York (2011)
13. Kuehl, D.T.: From cyberspace to cyberpower: defining the problem. In: Kramer, F.D., Starr, S.H., Wentz, L.K. (eds.) Cyberpower and National Security, pp. 24–42. National Defense University, Washington D.C. (2009), p. 40

14. Starr, S.H.: Towards an evolving theory of cyberpower. In: Czosseck, C., Geers, K. (eds.) The Virtual Battlefield: Perspectives on Cyber-Warfare, pp. 18–52. IOS Press, Amsterdam (2006), p. 5
15. Definitions have been developed in the ongoing PhD research of the author which is conducted under the title 'Strategic Implications of Cyber Warfare for the Nation-State' at the University of Hull, United Kingdom
16. Winkler, I.: Zen and the Art of Information Security, p. 72. Rockland, Syngress (2007)
17. Libicki, M.C.: Cyberdeterrence and Cyberwar, p. 155. RAND Corporation, Santa Monica (2009)
18. Geers, K.: Strategic Cyber Security, p. 122. NATO Cooperative Cyber Defence Centre of Excellence, Talinn (2011)
19. Libicki, M.C.: Sub Rosa cyber war. In: Czosseck, C., Geers, K. (eds.) The Virtual Battlefield: Perspectives on Cyber-Warfare, pp. 53–65. IOS Press, Amsterdam (2009), pp. 1–2
20. Gervais, M.: Cyber Attacks and the Laws of War, p. 8. Yale University, Yale (2011)
21. Betz, D.J., Stevens, T.: Cyberspace and the State: Toward a Strategy for Cyber-power, pp. 81–82. The International Institute for Strategic Studies, Routledge, New York (2011)
22. Clarke, R.A., Knake, R.K.: Cyber War. The Next Threat to National Security and What to do About It, p. 51. Harper-Collins Publisher, New York (2010)
23. Navrozov, L.: Chinese Geostrategy: Assassin's Mace. Newsmax (2005)
24. Tzu, S.: The Art of War, p. 134. Oxford University Press, Oxford (1963)
25. Libicki, M.C.: Cyberdeterrence and Cyberwar, p. 142. RAND Corporation, Santa Monica (2009)
26. Schneier, B.: So-called Cyberattack Was Overblown. Schneier on Security (2009)
27. Libicki, M.C.: Cyberdeterrence and Cyberwar, p. 139. RAND Corporation, Santa Monica (2009)
28. Libicki, M.C.: Protecting the United States in cyberspace. In: Campen, A.D., Dearth, D.H., Goodden, T.R. (eds.) Cyberwar: Security, Strategy, and Conflict in the Information Age, pp. 91–105. AFCEA International Press, Fairfax (1996), pp. 104–105
29. Sulek, D., Moran, N.: What analogies can tell us about the future of cybersecurity. In: Czosseck, C., Geers, K. (eds.) The Virtual Battlefield: Perspectives on Cyber-Warfare, pp. 118–231. IOS Press, Amsterdam (2006), p. 8
30. Sulek, D., Moran, N.: What analogies can tell us about the future of cybersecurity. In: Czosseck, C., Geers, K. (eds.) The Virtual Battlefield: Perspectives on Cyber-Warfare, pp. 118–231. IOS Press, Amsterdam (2006), p. 9
31. Dipert, R.R.: The ethics of cyberwarfare. J. Military Ethics **9**(4), 384–410 (2010), p. 403
32. Janczewski, L.J., Colarik, A.M.: Cyber Warfare and Cyber Terrorism. Information Science Reference. IGI Global, Hershey (2008), p. xiv
33. Dearth, D.H., Williamson, C.A.: Information age/information war. In: Campen, A.D., Dearth, D.H., Goodden, T.R. (eds.) Cyberwar: Security, Strategy, and Conflict in the Information Age, pp. 14–29. AFCEA International Press, Fairfax (1996), p. 28
34. Stiennon, R.: Surviving Cyber War, p. 103. Plymouth, Government Institutes (2010)
35. Toffler, A., Toffler, H.: War and Anti-War: Survival at the Dawn of the 21st Century, p. 4. Little Brown and Company, London (1993)
36. Toffler, A., Toffler, H.: War and Anti-War: Survival at the Dawn of the 21st Century, p. 239. Little Brown and Company, London (1993)
37. Adams, J.: Virtual defense. Foreign Affairs **80**(3), 98–112 (May/June 2001). Council on Foreign Relations, p. 102
38. Vanity Fair, http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109

39. Geers, K.: Strategic Cyber Security, p. 26. NATO Cooperative Cyber Defence Centre of Excellence, Talinn (2011)
40. An in-depth research on this case study has been undertaken by the author for his current PhD research on the 'Strategic Implications of Cyber Warfare for the Nation-State'. For more details, especially on the technical details, inquire with the author
41. Sanger, D.E.: Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power, pp. 220–225. Crown Publishers, New York (2012)
42. Farwell, J.P., Rohozinski, R.: Stuxnet and the future of cyber war. Survival Global Polit. Strategy **53**(1), 23–40 (2011), p. 29
43. Geers, K.: Strategic Cyber Security, p. 13. NATO Cooperative Cyber Defence Centre of Excellence, Talinn (2011)
44. Farwell, J.P., Rohozinski, R.: Stuxnet and the future of cyber war. Survival Global Polit. Strategy **53**(1), 23–40 (2011), p. 35
45. Gervais, M.: Cyber Attacks and the Laws of War, p. 38. Yale University, Yale (2011)
46. Atlantic Council. http://www.acus.org/new_atlanticist/stuxnet-and-dawn-algorithmic-warfare

Author Index