Data Protection in Heterogeneous Distributed Systems: A Smart Meter Example

Prachi Kumari, Florian Kelbert, Alexander Pretschner
Karlsruhe Institute of Technology, Germany
{kumari, kelbert, pretschner}@kit.edu

Abstract: Usage control is concerned with how data is used after access has been granted. Enforcement mechanisms have been implemented for distributed systems like web based social networks (WBSN) at various levels of abstraction. We extend data usage control to heterogeneous distributed systems by implementing a policy enforcement mechanism for a smart meter connected to a WBSN. The idea is to provide users an opportunity to share their energy usage and other related data within their social group while maintaining control over further usage of that data. The implementation borrows from an existing usage control framework for a common web browser.

1 Introduction

Smart meters are energy (and gas and water consumption) monitoring tools, introduced to record and display real time usage data with the goal to bring down both energy consumption and the costs. By use of smart meters, users can track the amount of energy (and its cost) utilized by different devices over different time points/spans in a day. Using information provided by these smart meters, users can make better decisions regarding the choice of buying devices or operating them at particular times [BHM+11]. Combined with various data storage and interpretation tools, a smart meter can be transformed into an energy information system. A well-known initiative in this direction is the Google Powermeter [GP11, REU11]. We take this energy awareness initiative to the next step where the user can not only see the different interpretations of his energy usage, but can also share this data with his friends and others in his social network.

Connecting a smart meter to a WBSN provides interesting applications of energy usage data. For example, it can show a user a comparison of his energy usage and related spending with that of his friends in a graphical form like an avatar (*"his avatar is greener than mine!"*). Also, combining a popular and engaging application with energy management would increase the frequency of user's interactions with the energy information. The idea is simple: let the technology integrate systems to help users conserve energy.

However, sharing energy usage data in a WBSN can raise serious privacy and data protection concerns [PRI11, TRU11, Pen11]. Smart meters collect far more information than traditional meters: precise energy usage ranging from per second to per hour in a day. Also, smart meters are envisaged to control the home appliances for monitoring and load balancing, e.g., a smart meter can turn off a washing machine if the load is too high or the

energy is expensive during a particular time of day to restart it later. In sum, a smart meter produces and can have access to much more information than mere readings. This means that connecting a smart meter to the Internet and publishing all the data it has, can be problematic for security, privacy, social, legal and political reasons. Many data protection issues need to be addressed before such a system can be acceptable and become a norm; e.g. ownership of data, purpose of data collection, persistence, processing and deletion of collected data and so on. The challenge therefore is to design and build privacy-aware applications that can control and protect all this data while enabling the user to enjoy all the benefits of the smart meter - social network link. This is the goal of this work.

Relevant privacy issues are (1) misuse and theft of energy data from the profiles by other WBSN users; and (2) the access, storage, processing and usage of energy data by the WBSN and other related service providers. We have addressed the first set of issues in earlier work: we presented a social network application SCUTA which generates and sends usage control policies along with requested web page to the client side where the policy is enforced at three levels of abstraction: the web browser, the windowing system and the operating system [KPPK11,LP11]. In this paper we focus on the second set of privacy issues which consider the WBSN and associated service providers as potentially malicious users of data. To limit the scope, we consider the energy providers as well as the reading and billing service providers as trusted. However, from a general data protection perspective, they are not different from other service providers and there is no conceptual difference in implementing data protection mechanisms at their end as well.

As a proof of concept, we implemented a prototype that connects a smart meter simulation to SCUTA [SCU11]. Its interface is identical to a real smart metering system; we use a simulation rather than the actual implementation because of the flexibility this provides in "generating" energy consumptions. The prototype consists of policy enforcement points at every location in the system except the smart meter and the meter reader's domain ("energy domain" in Figure 1). The prototype is work in progress.

Problem. The problem that we tackle is the enforcement of data protection requirements in heterogeneous distributed systems; in particular, a smart meter connected to a WBSN. We consider privacy concerns that are a consequence of storing energy usage data outside the energy domain as well as sharing that data with other WBSN users who might misuse it. The problem generalizes to data protection if multiple applications – in the domains of both business and embedded IT – are connected to share data across different domains.

Solution. We introduce usage control mechanisms at every location outside the energy domain. These mechanisms intercept every request to data access and allow the flow of data only if a proof of existence of a similar mechanism at the other end is provided. A second usage control mechanism is implemented in the WBSN system that takes care of controlling misuse of the data when it is shared on the social network web page. This is an instantiation of our previous work on the topic. Protection of data after it has been downloaded by other users is not the subject of this paper; this is done in [LP11,KPPK11].

Contribution. Firstly, we propose an architecture for data protection in a heterogeneous distributed system while maintaining control over further distribution and usage of data. Secondly, by means of a prototype and security analysis, we provide insights into the

limitations and the assumptions and conditions under which a certain level of security guarantees in such a heterogeneous distributed system can be provided.

Organization. §2 presents related work. §3 introduces one example use case our system can handle and describes the prototype's design. Section §4 presents a security analysis, assumptions and limitations. The paper concludes with possible refinements in §5.

2 Related work

This paper addresses the enforcement of data protection policies in a heterogeneous distributed system. These policies can and must be enforced at different layers of abstraction in the system. Among others, this has, for various policy languages [Ian08, XRM04, AHK+03, Ope08, ZPPPS04, HPB+08, DDLS95, W3C05], been done at the operating system level [HP09], at the X11 level [PBH+09], for Java [DJLP09, IDC07], .NET [DJM+09] and machine languages [ES99, YSD+09]; at the level of an enterprise service bus [GNC10, NPD11]; for dedicated applications such as the Internet Explorer [EKK+07] or in the context of digital rights management [Ado10, Mic10, PHS+08]. The reason for this variety of enforcement mechanisms is that the *data* that has to be protected comes in different *representations*: as network packets, as attributes in an object, as window content, etc. In principle, all these representations eventually boil down to some representation in memory, but it turns out to be more convenient and simpler to perform protection at higher levels of abstraction. In this paper, we use existing data usage control enforcement mechanisms from previous work to enforce data protection policies in a heterogeneous [KPPK11, LP11].

Using smart meter data for creating awareness about energy consumption is not a new idea. Two well-known initiatives in this direction are the Google Powermeter [GP11] and the GE smart energy interface [GE11]. In Finland, the government has initiated projects combining smart meters, social networks and cloud computing [Abe11, Fin11]. Ensuring that multiple applications from different domains work together with adequate data protection is a difficult task and although data protection for smart meters and grids has been the topic of research [EK10, BSU10, JJK10, RD10], so far focus has been on securely collecting data from the smart meters. To the best of our knowledge, there is no publicly available work that enforces data protection policies for further usage of the collected data.

3 The Proposed Framework

To connect a smart meter to a WBSN, we extended the WBSN application SCUTA [SCU11] to include a 'smart energy' component. If the user of the smart meter wants to share his energy usage data on his WBSN profile, he needs to access this component provided on his profile page. The smart energy system provides many interesting applications of smart meter data, including: users can publish their absolute energy usage over a period of time; users can share their overall energy usage in a visual format like an avatar which changes face and color (red, yellow, green) according to energy usage; users can compare their

energy usage with that of others in their social group; users can see how energy usage at different times of the day affects total costs and they can learn how they should move their energy consumption patterns to minimize the costs; users can post ideas/suggestions about the efficient usage of energy and share with all; users can get useful information and advertisements customized according to their energy needs.

The remainder of this paper focuses on data protection in the system described above.

3.1 A Use Case

Consider a WBSN scenario where Alice shares her smart meter data with her social group. Alice wants no other user to be able to copy and store her meter readings for further usage. Alice also wants that third parties like the advertisement providers may only temporarily store her readings and the valid purpose must only be to serve advertisements. In a usual connection between a smart meter and WBSN, without a data protection mechanism, it is not possible for Alice to achieve this desired level of control over her data. Later, we will show how our solution helps Alice.

3.2 Requirements

We consider two attackers: the potentially malicious end users of WBSN and other services as well as potentially malicious service providers. Thus we have two types of user requirements for data protection. The first category concerns controlling the usage of data downloaded and rendered at the end users' machines. An example requirement is to inhibit copy, save, print and other actions on data. These requirements have been taken from [KPPK11]. The second category relates to the collection, storage, further distribution and usage of data at the service providers' end. Requirements in this category include the following. The list is not complete; we quote a few interesting requirements to clarify the kind of requirements we are interested in:

- Meter data should be collected by the WBSN every t seconds;
- At the WBSN server, meter data should be aggregated every N hours;
- Energy usage should be displayed without time, location and device information;
- Meter data should not be stored for more than three months, i.e. if data is older than three months, delete it;
- All energy data should be deleted if the user deletes his profile at the WBSN;
- Whenever energy data flows out of the WBSN domain, the event should be logged;
- Third parties like advertisement service providers should only be able to process the data for their stated purposes, they should not permanently store any energy data.

To enforce the aforementioned requirements in the distributed system, we introduce usage control policy specification and enforcement points at several locations. In the following,

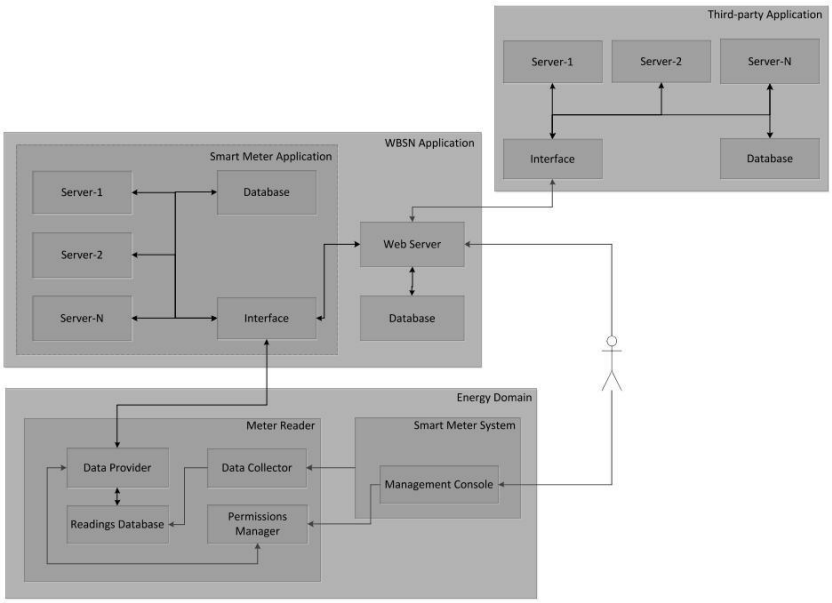

Figure 1: The Proposed Architecture

we present the proposed architecture of the prototype.

3.3 Design

Figure 1 shows the proposed architecture. Meter readings are forwarded to and stored in the meter reader's database for billing and other purposes. These entities are trusted; we collectively call them the *Energy Domain*. The meter reader provides stored readings to various data interpretation services to help users understand different semantics of their energy usage. Data usage control policies are specified at the management console in the smart meter system and the data provider component in the meter reader.

The Smart Meter Application handles collection, storage, processing and forwarding of meter readings from the meter reader to WBSN and other third party service providers. Data is sent out of the energy domain only in response to a request. Before sending data outside its domain, the meter reader seeks proof of an existing usage control mechanism at the requester's end. Data is forwarded to the requester along with usage control policies. To make sure that the policies are enforced at every location in the distributed system, the following requirements must be implemented:

1. Data can be forwarded to another location only if a usage control mechanism is present at the receiving end;

2. Policies can only be strengthened before being forwarded [PSSW09];

3. All policies received with data must be re-attached to the data before it leaves the sender's system.

We call the respective process *conditional forwarding*.

Thus, as data flows through various locations, checks for ensuring the existence and integrity of usage control mechanisms are done recursively throughout the complete system. For example, before the Smart Meter Application forwards meter readings to be displayed at the end user's profile page, it performs a mechanism check for the WBSN Application which in turn does a similar check if it forwards readings to a third-party like advertisement provider for rendering advertisements on the user's profile page.

Energy Domain *Smart Meter System (SMS).* This is the complete set of hardware and software installed inside a smart meter user's home. The user can control distribution of meter readings by editing the default policies provided by the meter reader using the Management Console.

To share energy usage data in the WBSN, the user must (a) register to use the 'smart energy' tool at the WBSN server and provide his smart meter ID; and (b) provide a digitally signed confirmation about his agreement on releasing the data to the WBSN application. The user can also specify policies that put constraints on the collection and further distribution of energy data, e.g., the frequency of data collection, deletion of data after a certain time period etc. These policies are specified using templates and they override the default policies specified by the meter reader while releasing data to external service providers.

Meter Reader. This is the set of components responsible for meter reading services at the energy provider's end. Data Collector represents the logic and the connection between the individual smart meters and the Readings Database. Permissions Manager takes care of checking the authenticity of signed permissions. If the external service provider requests meter readings by presenting the signed permission provided by the smart meter user, the Data Provider queries the Permissions Manager and depending upon the response, it forwards the meter readings along with policies to the requester, or denies the request.

Smart Meter Application (SMA) This component provides smart meter data storage and interpretation services to the WBSN. These services can be provided by a third party or can be a part of the WBSN application. That is why it is shown by dotted lines in Figure 1.

SMA servers. The SMA provides a number of services like requesting/receiving meter readings from the meter reader's database, saving the readings to SMA database, processing stored readings to generate avatars, graphs etc. and forwarding them (including raw data) to the social network web server. All these functionalities are provided by the various servers (Server-1 to N in Figure 1) via the smart meter application interface.

Connecting SMA to Meter Reader. Figures 2 and 3 show the steps that connect an SMA to the Meter Reader. Alice registers with the smart energy component in the WBSN ap-

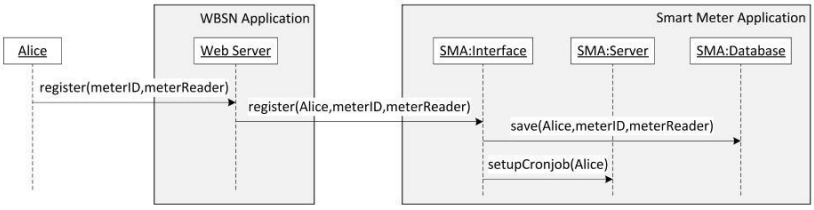

Figure 2: Registration Process

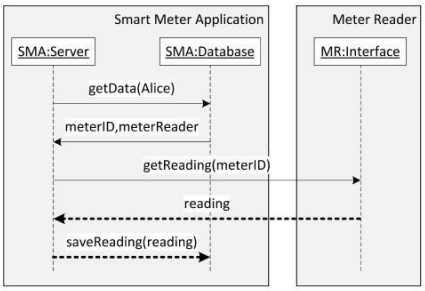

Figure 3: Connecting SMA to Meter Reader

plication. This component stores the details of registration in the SMA database. The registration data is then used by the responsible SMA server to start fetch data from the meter reader at regular intervals. Usage-controlled data is sent only after getting a confirmation about the existence and integrity of the requester. Details of this process are shown in Figure 4. The sender's policy enforcement and policy management component (PEMC) intercepts the send event and asks the receiver to show a proof of usage control mechanism (UCM) which is taken care of at the receiver's end by the receiver's PEMC [NHP11]. Consequently the sending process is aborted or continued by attaching a policy to the data and forwarding them together to the receiver. If the receiver's PEMC gets the data and policy together, it detaches the policy from data and deploys it while forwarding the data to the component that initiated the request for data at this end.

Other Third-party Applications Other third party applications (e.g., a service providing customized advertisements) get access to smart meter data through the WBSN application which first requests readings from the smart meter application and then forwards them to the third party service provider.

An Example Scenario. Figure 5 shows one example scenario where Bob accesses Alice's 'smart energy' page at the WBSN. While the avatar shown at this page is generated using Alice's meter readings, advertisements are served using Bob's energy consumption pattern. This complete scenario shows how different components of the proposed framework interact with each other and how the resulting data flow is controlled (note the bold dotted lines representing the *usage controlled data forwarding* as per Figure 4).

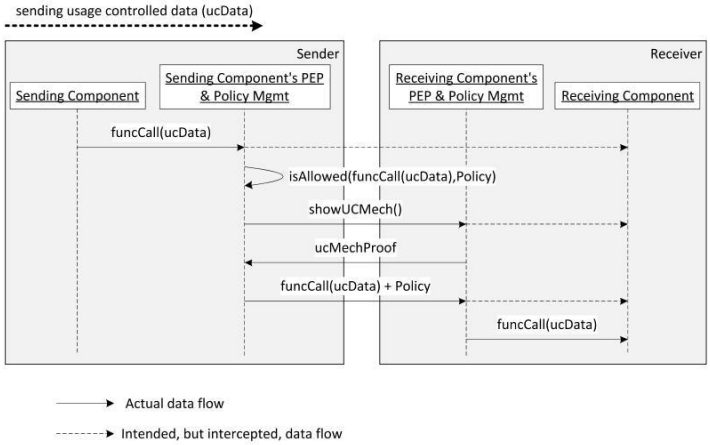

Figure 4: Forwarding Usage Controlled Data

3.4 Revisiting the use case

In our example in §3.1, Alice wants no other user to be able to copy and store her meter readings for further usage if she shares them on her WBSN profile. For this, she can specify usage control policies in the SCUTA web interface. These policies are then enforced at the other users' machines by the policy enforcement point BRUCE, as explained in [KPPK11, LP11].

Alice also wants third parties like the advertisement providers to only temporarily store her readings and that the only valid purpose is to serve advertisements. For this, she can use our proposed system to edit the policy templates and specify policies at the management console of the smart meter system. This policy can be formally expressed in OSL [HPB+08] as:

$(Decl, \{$
$(AdvertisementProvider, \underline{permitonlyevname}(\{storeTemporary, process, serveAd\}, \{(object, readings)\})),$
$(AdvertisementProvider, \underline{permitonlyparam}(\{serveAd\}, purpose, storeTemporary, \{(object, readings)\}))$
$\})$

Various policy enforcement and management components in our system ensure that this policy is enforced throughout. One basic assumption is that the requirement of conditional data forwarding (mentioned at the beginning of this section) is enforced every time there is a request for meter readings.

While the policy is specified by Alice, the latter requirements are hard coded at the Data Provider's side. With conditional data forwarding, the policies are sent to the third party advertisement provider via the WBSN application. Depending on the chosen implementation mechanism [MAS10], an attempt to permanently store readings inside the advertisement provider's infrastructure is inhibited, modified, or executed and logged.

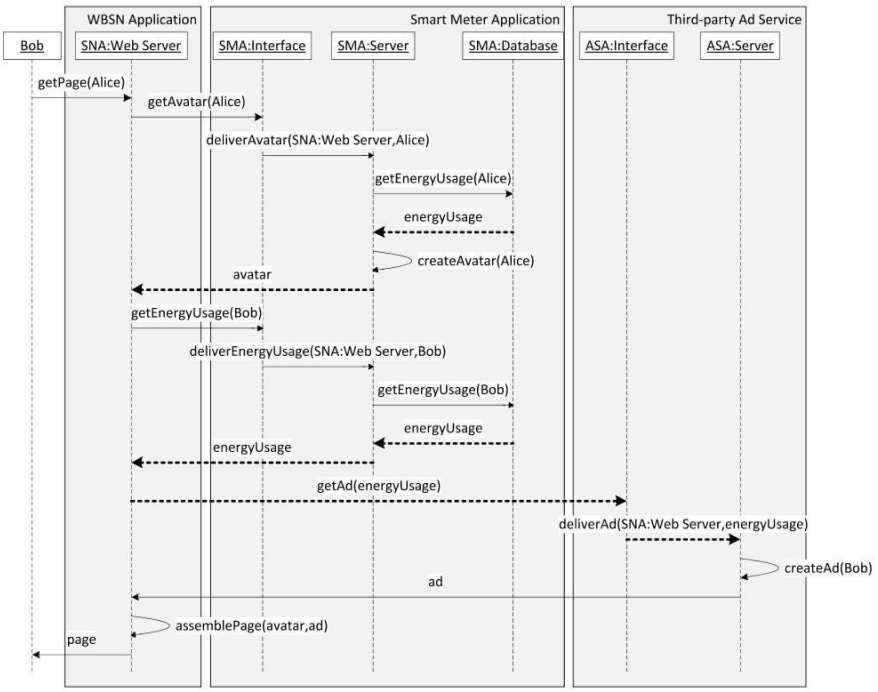

Figure 5: An Example Scenario

4 Security analysis

Our proposed architecture guarantees that the user's energy usage data is not redistributed and reused in an uncontrolled way once it has been released by the meter reader. However, certain assumptions must hold true for this.

Assumptions. One of our main assumptions is that all systems maintaining usage controlled data are always online. Since we are working on making the enforcement mechanisms tamper-proof (see below), they will enforce usage control requirements while the system is offline and potentially report usage control violations asynchronously once the system goes online again.

We also assume that all network connections are secure. Assuming this, Man-in-the-middle and similar attacks, whether active or passive, are not possible. Such secure connections can be achieved using IPSec [KS05], tcpcrypt [BHH+10] or virtual private networks. TLS [DR08] is not an option, since we want our architecture to be as little intrusive as possible and be independent of concrete applications and their support for TLS.

Moreover, we consider all the hardware and software used in our scenario to be free of vulnerabilities. If some hardware, the underlying operating system or the enforcement mechanisms are vulnerable, this could give an unexpected attack surface for any attacker from the outside.

Policy Enforcement. To correctly enforce usage control policies, we need to make sure that (a) policy specification and enforcement mechanisms exist and they are not circumvented or tampered with and (b) the implemented policies actually enforce the policy specified by the end user. Securing such a usage control infrastructure can and has been done [NPD11]; the remote attestation part is the subject of future work. In terms of checking whether or not a policy is indeed enforced by a specific mechanism, formal techniques have been developed earlier [PRSW09]. In sum, the components of the solution to this problem exist but need to be integrated.

For the first case, we need to trust one particular component inside each system that makes sure that all the other components that are built upon it are secure. Considering a computer system where the user does not have root privileges, this component can be the operating system. If the user has full access, even to the hardware, this problem boils down to the usage of trusted computing hardware.

We plan to integrate the BonaFides system [NHP11], which we have developed in earlier work, into our architecture. BonaFides tackles the problem of malicious system administrators in virtualized infrastructures and allows for trusted computing by measuring crucial system files. These measurements are then sent to and checked by a trusted verifier at regular time intervals. Since the systems of the WBSN and the third-party application providers are most likely to be virtualized, BonaFides can help to make the enforcement mechanisms secure.

Moreover, certificates signed by a certificate authority allow for the secure authentication of data requesters. Using certificates, detective enforcement mechanisms at the WBSN, the SMA and third-party applications may be sufficient, since the data provider already knows the receiver through the certificate. The securely authenticated data requester may then be held responsible whenever he uses usage controlled data in an unauthorized way.

Guarantees. Since we focus on privacy issues of a smart meter connected to a WBSN, our main concern is about the end user Alice who registers for the smart energy tool provided by the WBSN. While Alice wants to share her energy usage data and use additional third-party services, she also wants to keep full control over all copies of her data by tracking, and possibly constraining, the flow and usage of data throughout the overall architecture. With our approach of recursively checking for usage control mechanisms, we achieve a reliable data flow tracking across different systems and domains. Controlling the usage of Alice's data within each single system is then accomplished at the different layers of each system [LP11], each layer implementing a PMEC.

Usage control policies can be enforced in both preventive and detective ways. End users who visit Alice's smart energy page, would prefer preventive usage control enforcement than being spotted upon wrong usage of data and face penalties. Moreover, if a data consumer proves the existence of preventive usage control mechanisms, there is not necessarily the need for the data provider to know the identity of the data consumer.

On the other hand, WBSN, SMA, or third-party application providers would prefer to prove the existence of detective enforcement mechanisms and additionally prove their identity to the data provider using certificates. This is because these providers run complex computer systems and because they do not want to lose control over their systems

by deploying a more restrictive preventive usage control mechanisms. Instead, detective enforcement mechanisms can help the system administrators to comply with the policies, e.g. by raising an alarm whenever a restricted usage is attempted and asking the administrator for a decision. Assuming that the identity of the data recipient has been correctly proven before he gets usage controlled data, he may face penalties for illegal usages.

Our architecture focuses on controlling energy usage data. In addition, one would also like to protect other sensitive data like meter IDs or users' personal information. Moreover, WBSN, SMA, and third-party application providers have a legitimate interest in getting valid, authentic, and correct energy usage data in order to offer valuable and interesting services. Although we do not consider these aspects in this paper, guarantees of that kind can be provided using the same infrastructure that protects the energy usage data.

Attack scenarios. For the scope of this paper, we consider the scenarios in which WBSN, SMA, or third-party application providers are malicious. The scenario where end user Bob, who accesses Alice's smart energy page, is malicious, is investigated in related and ongoing work [KPPK11].

The SMA may ask the meter reader for the energy usage data of users who did not opt-in for the smart energy tool. Clearly, the meter reader must not reveal energy usage data upon such a request. Countermeasures can be implemented using pre-shared secrets and/or certificates. Using certificates, the user could give a signed permission, that allows for the collection of his energy usage data, to the SMA (via the WBSN). The validity of the permission is then checked by the meter reader. Going one step further and assuming that the SMA is outside the domain of the WBSN, an additional delegation mechanism becomes necessary.

WBSN, SMA, and third-party applications providers may try to circumvent, switch off, or tamper with the usage control mechanisms once the the usage controlled data has been received. Therefore we need to make sure that usage controlled data cannot be accessed if usage control mechanisms do not exist or if they are tampered with. This can be achieved by encrypting the usage controlled data and assuring that only untampared usage control mechanisms can decrypt the data. However, this is rather hard to achieve, since providers will have full control over their systems including hardware access and administrative permissions and may therefore circumvent the mechanisms just one level below. Therefore we plan to integrate trusted computing mechanisms and the BonaFides system [NHP11] in order to tackle this problem.

Since we consider the network connections between the different systems as secure and the software as free of vulnerabilities, there is no (technical) attack surface for attackers from the outside. Of course, an attacker could still break the system using social engineering, phishing or faking certificates. However, we do not consider such attacks here.

Limitations. We do not consider the scenario in which Alice wants to change the policy of some data that has already been released and distributed. This is because our architecture does not provide mechanisms to attach policies to data that has already been released. These issues are subject of ongoing work that we will incorporate into the proposed architecture later. Another crucial point is the integrity and authenticity of Alice's data and the results of processing this data. Our architecture does not deal with the problem of wrong

calculations on Alice's data, e.g. if the SMA serves wrong or misleading avatars or energy usage graphs, therefore violating the integrity of Alice's data. Yet, such a behaviour would result in a bad reputation of the service and user's opting-out from the service.

For the energy domain, we did not performa a security analysis since we consider this part of the proposed architecture as trusted. Whether the services inside the energy domain (e.g. billing) can be trusted, and if not, what can be the requirements in that case, is the subject of ongoing work [Pee11]. In this paper, we assume that the smart meter and the meter reader must always be trusted by all stakeholders. If not, we believe that protecting energy usage data within the energy domain is conceptually the same as what we have presented in this work. As a starting point, we implemented traditional access control mechanisms at the Data Collector in order to check whether a requesting component is allowed to get the usage controlled data it has been asking for. Moreover, before releasing energy usage data, the Data Collector requests for a proof of usage control mechanisms and therefore kicks off the recursive check for usage control mechanisms.

Also, we do not look into security analysis at the end user's system where the web page containing sensitive usage controlled data is rendered in a web browser. This has already been investigated in previous work [KPPK11].

5 Conclusions and future work

In this paper, we presented an architecture for enforcing data protection in a heterogeneous distributed system comprising of a smart meter connected to a WBSN. Our initiative is similar to Google Powermeter [GP11,REU11] except that (i) our solution is comparatively easier to use as the smart meter end user need not upload his data, he only needs to give his consent and can be oblivious of how the WBSN gets the data; and (ii) we enforce data protection to prevent the abuse of this data by malicious entities.

We presented a framework that connects multiple applications to share data among themselves and enforces data protection policies in the resulting distributed system. We have also performed a security analysis of our proposed framework and discussed limitations to data protection in such a heterogeneous distributed system.

As a proof of concept, we have implemented a prototype in the context of connecting a smart meter to a WBSN. By means of a use case, we explained the user requirements and showed that our system (i) provides interfaces for the end user to express data protection policies and (ii) enforces these policies both at the service providers infrastructure and the end users' machines.

This work is a first step towards the development of a full-fledged heterogeneous usage-controlled system that brings together multiple applications like smart meters, video surveillance systems, location-based services and social networks, etc. Such systems offer many useful applications and open a new domain of research for application and data security.

Acknowledgment This work was supported by Fraunhofer Gesellschaft Internal Programs, Attract 692166.

References

[Abe11] John C Abell. Linking Smart Meters and Social Networks, June 2011. http://www.wired.com/epicenter/2010/05/linking-smart-meters-and-social-networks/.

[Ado10] Adobe. LiveCycle Rights Management ES. http://www.adobe.com/products/livecycle/rightsmanagement/indepth.html, August 2010.

[AHK+03] P. Ashley, S. Hada, G. Karjoth, C. Powers, and M. Schunter. Enterprise Privacy Authorization Language (EPAL 1.2). IBM Technical Report, 2003. http://www.zurich.ibm.com/security/enterprise-privacy/epal/Specification/.

[BHH+10] A. Bittau, M. Hamburg, M. Handley, D. Mazieres, and D. Boneh. The case for ubiquitous transport-level encryption. In *USENIX Security Symposium*, 2010.

[BHM+11] B. Beckert, D. Hofheinz, J. Müller-Quade, A. Pretschner, and G. Snelting. Software Security in Virtualized Infrastructures – The Smart Meter Example. *it-information technology*, 53(3):142–150, 2011.

[BSU10] J.-M. Bohli, C. Sorge, and O. Ugus. A Privacy Model for Smart Metering. In *Communications Workshops (ICC), 2010 IEEE International Conference on*, pages 1 –5, may 2010.

[DDLS95] N. Damianou, N. Dulay, E. Lupu, and M. Sloman. The Ponder Policy Specification Language. In *Proc. Workshop on Policies for Distributed Systems and Networks*, pages 18–39, 1995.

[DJLP09] M. Dam, B. Jacobs, A. Lundblad, and F. Piessens. Security Monitor Inlining for Multithreaded Java. In *Proc. ECOOP*, pages pp. 546–569, 2009.

[DJM+09] L. Desmet, W. Joosen, F. Massacci, K. Naliuka, P. Philippaerts, F. Piessens, and D. Vanoverberghe. The S3MS.NET Run Time Monitor: Tool Demonstration. *ENTCS*, 253(5):153–159, 2009.

[DR08] T. Dierks and E. Rescorla. IETF RFC 5246: The transport layer security (tls) protocol. *The Internet Engineering Task Force*, 2008.

[EK10] C. Efthymiou and G. Kalogridis. Smart Grid Privacy via Anonymization of Smart Metering Data. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 238 –243, oct. 2010.

[EKK+07] M. Egele, C. Kruegel, E. Kirda, H. Yin, and D. Song. Dynamic Spyware Analysis. In *Proceedings of USENIX Annual Technical Conference*, June 2007.

[ES99] U. Erlingsson and F. Schneider. SASI enforcement of security policies: A retrospective. In *Proc. New Security Paradigms Workshop*, pages 87–95, 1999.

[Fin11] Finland to Connect Smart Meters to Social Networks, June 2011. http://theenergycollective.com/taylenpeterson/30622/finland-connect-smart-meters-social-networks.

[GE11] GE to introduce smart energy interface, June 2011. http://www.smartmeters.com/the-news/760-ge-to-introduce-smart-energy-interface.html.

[GNC10] G. Gheorghe, S. Neuhaus, and B. Crispo. xESB: An Enterprise Service Bus for Access and Usage Control Policy Enforcement. In *Proc. Annual IFIP WG 11.11 International Conference on Trust Management*, 2010.

[GP11] Google Powermeter, May 2011. http://www.google.com/powermeter/about/.

[HP09] M. Harvan and A. Pretschner. State-based Usage Control Enforcement with Data Flow Tracking using System Call Interposition. In *Proc. 3rd Intl. Conf. on Network and System Security*, pages 373–380, 2009.

[HPB+08] M. Hilty, A. Pretschner, D. Basin, C. Schaefer, and T. Walter. A Policy Language for Distributed Usage Control. In *Proc. ESORICS*, pages 531–546, 2008.

[Ian08] R. Iannella. Open Digital Rights Language v1.1, 2008. http://odrl.net/1.1/ODRL-11.pdf.

[IDC07] I. Ion, B. Dragovic, and B. Crispo. Extending the Java Virtual Machine to Enforce Fine-Grained Security Policies in Mobile Devices. In *Proc. Annual Computer Security Applications Conference*, pages 233–242. IEEE Computer Society, 2007.

[JJK10] Marek Jawurek, Martin Johns, and Florian Kerschbaum. Plug-in privacy for Smart Metering billing. *CoRR*, abs/1012.2248, 2010.

[KPPK11] Prachi Kumari, Alexander Pretschner, Jonas Peschla, and Jens-Michael Kuhn. Distributed data usage control for web applications: a social network implementation. In *Proc. 1st ACM Conf. on Data and application security and privacy*, pages 85–96, 2011.

[KS05] S. Kent and K. Seo. IETF RFC 4301: Security Architecture for the Internet Protocol, 2005.

[LP11] Enrico Lovat and Alexander Pretschner. Data-centric Multi-layer Usage Control Enforcement: A Social Network Example. In *Proc. ACM Symposium on Access Control Models and Technologies*, 2011.

[MAS10] MASTER consortium. MASTER Deliverable 5.1.1: Security Enforcement Language. http://www.master-fp7.eu/, April 2010.

[Mic10] Microsoft. Windows Rights Management Services. http://www.microsoft.com/windowsserver2008/en/us/ad-rms-overview.aspx, 2010.

[NHP11] R. Neisse, D. Holling, and A. Pretschner. Implementing Trust in Cloud Infrastructures. In *To appear in Proc. 11th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, May 2011.

[NPD11] R. Neisse, A. Pretschner, and V. Di Giacomo. A Trustworthy Usage Control Enforcement Framework. In *Proc. 6th Intl. Conf. on Availability, Reliability and Security*, 2011. to appear.

[Ope08] Open Mobile Alliance. DRM Rights Expression Language V2.1, 2008. http://www.openmobilealliance.org/Technical/release_program/drm_v2_1.aspx.

[PBH+09] A. Pretschner, M. Buechler, M. Harvan, C. Schaefer, and T. Walter. Usage Control Enforcement with Data Flow Tracking for X11. In *Proc. 5th Intl. Workshop on Security and Trust Management*, pages 124–137, 2009.

[Pee11] Wenn die Waschmaschine mit dem Kraftwerk spricht. `http://www.kit.edu/besuchen/pi_2011_5908.php`, March 2011.

[Pen11] William Pentland. Why Smart People Are Suspicious of Smart Meters, May 2011. `http://blogs.forbes.com/williampentland/2010/12/10/why-smart-people-are-suspicious-of-smart-meters/`.

[PHS+08] A. Pretschner, M. Hilty, F. Schutz, C. Schaefer, and T. Walter. Usage Control Enforcement: Present and Future. *Security & Privacy, IEEE*, 6(4):44–53, 2008.

[PRI11] Smart Meters Raise Privacy Concerns, May 2011. `http://www.smartmeters.com/the-news/718--smart-meters-raise-privacy-concerns.html`.

[PRSW09] Alexander Pretschner, Judith Ruesch, Christian Schaefer, and Thomas Walter. Formal Analyses of Usage Control Policies. In *Availability, Reliability and Security, International Conference on*, pages 98–105, 2009.

[PSSW09] Alexander Pretschner, Florian Schütz, Christian Schaefer, and Thomas Walter. Policy Evolution in Distributed Usage Control. *Electr. Notes Theor. Comput. Sci.*, 244:109–123, 2009.

[RD10] Alfredo Rial and George Danezis. Privacy-preserving smart metering. Microsoft Research Technical Report, November 2010. `http://research.microsoft.com/pubs/141726/GridPrivacy.pdf`.

[REU11] Google pulls the plug on PowerMeter energy tool, June 2011. `http://www.reuters.com/article/2011/06/24/idUS112679473420110624/`.

[SCU11] SCUTA homepage, May 2011. `http://jenskuhn.eu/sns/`.

[TRU11] True cost of smart meters might include privacy and health, May 2011. `http://www.digitaljournal.com/article/296780`.

[W3C05] W3C. The Platform for Privacy Preferences 1.1 (P3P1.1) Specification, 2005. `http://www.w3.org/TR/2005/WD-P3P11-20050104/`.

[XRM04] Multimedia framework (MPEG-21) – Part 5: Rights Expression Language, 2004. ISO/IEC standard 21000-5:2004.

[YSD+09] B. Yee, D. Sehr, G. Dardyk, J. Chen, R. Muth, T. Ormandy, S. Okasaka, N. Narula, and N. Fullagar. Native Client: A Sandbox for Portable, Untrusted x86 Native Code. In *Proc IEEE Symposium on Security and Privacy*, pages 79–93, 2009.

[ZPPPS04] X. Zhang, J. Park, F. Parisi-Presicce, and R. Sandhu. A logical specification for usage control. In *SACMAT '04: Proceedings of the ninth ACM symposium on Access control models and technologies*, pages 1–10. ACM, 2004.