PRIVACY ISSUES IN SMART BUILDINGS BY EXAMPLES IN SMART METERING

Stephan CEJKA
Siemens AG – Austria
stephan.cejka@siemens.com

Felix KNORR
Siemens AG – Austria
felix.knorr@siemens.com

Florian KINTZLER
Siemens AG – Austria
florian.kintzler@siemens.com

ABSTRACT

Main goals of building automation are to optimize costs and to reduce energy consumption. For these tasks, high amounts of data are collected, including data directly related to an individual inhabitant. Such data usage possibly infringes the privacy of a person, thus compromises on their collection and processing need to be found. In this paper, we enumerate possible solutions to privacy issues in the Smart Building domain. Tightly connected are privacy issues introduced by Smart Meters, currently being rolled out in many member states of the European Union, including households not being part of a Smart Building. As their privacy issues have been heavily discussed in the literature, they serve as the main example for described privacy-preserving solutions.

INTRODUCTION

The overall objective in the building automation domain is to increase the comfort of users and inhabitants [1]; safety and security regarding privacy and confidentiality of their data are further requirements. Cost optimization and energy reduction are often inversely related to the inhabitants' comfort [2]. Savings in this area, however, have a high impact as buildings account for ~40% of the overall energy consumption in the U.S. [3]. Generating energy through PV systems and utilizing a battery system for temporary energy storage allows for cost optimization; in addition their installation costs are constantly decreasing. Systems for heating, ventilation, and air conditioning (HVAC) and for lighting can exceed 70% of a building's total energy consumption [4]. Effectively controlling those systems by utilizing occupancy information could save up to 40% of energy [5]. Occupancy has traditionally been detected using sensors or video cameras; newer non-intrusive approaches include using mobile phones' GPS information [6], evaluating computer network traffic [7] or utilizing the power meter data [8]. This is problematic in terms of privacy if data is transmitted outside of the customer's sphere. Nevertheless, use cases based on these sensed data are manifold; it is possible, for example, to detect the best operating time for devices, to reveal still running appliances without anyone being present [9], to generate recommendations about individual energy reduction [10], or to identify failing appliances earlier on detecting unexpected behavior [11].

PERSONAL DATA IN THE SMART BUILDING DOMAIN

The required information used in the introductory example could directly or indirectly be associated with a user. In EU jurisdictions, data are legally defined as personal data if they relate to an identified or at least identifiable person, imposing legal restrictions on how to use them [12]. For optimization purposes, various types of data are collected and processed in a Smart Building. Relevance of privacy regulations in this area is strongly inferred by the type of the building as privacy will be a more important aspect in residential buildings than in office blocks or hotels. However, if rooms are exclusively used by a small number of people, privacy regulations need to be applied.

Revolutions in energy grids - the 'Smart Grid' - include the introduction of Smart Metering. 'Smart Meters' are increasingly rolled out into customers' houses all over the world, including customers not living in a Smart Building. The introduction of Smart Meters to a stipulated percentage of households is postulated in the EU Directive 2009/72/EG, whereof the customer should primarily profit from higher energy efficiency and incentives to improve its behaviors, e.g., by providing historical data on a web page. However, the directive did not contain any regulations on privacy. This was heavily criticized such that the Austrian national implementation law was amended in 2013 to address data protection and privacy [13]. Meanwhile, the European Commission issued its Recommendation 2012/148/EU, extensively dealing with data protection and data security of Smart Meters; it is - as a recommendation, however - not legally binding. In 2014, 200000 Smart Meters were already rolled out in Austria [14]; operators are now legally obligated to equip 95% of their customers until 2022 (this deadline was already extended from previously 2019).

Accounting and demand planning require reading out the power consumption. Traditionally, Ferraris meters have usually been read out only annually. The accumulated consumption of the household and the average distribution of energy consumption (i.e., load profile) through a day were the only information that system operator and energy vendor knew for deducting expected energy requirements. By using Smart Meters, it is technically possible and in some cases even legally or regulatory specified to read-out consumption values more often. However, there is a big difference in perspective of privacy, if a consumption of 2500 kWh within one year, or in contrast a consumption of 0.5 kWh within 15

minutes is known.
Short read-out intervals allow for significant insights into private homes and their residents' habits. The first value does not divulge when energy has been consumed. No inferences on customer's behavior can be concluded; therefore privacy concerns do not occur in this setting. However, for the latter value it is evident that the inhabitant was at home during this interval, it may even be possible to find out which appliances were used by detecting characteristic power consumption patterns [15,16]. Increasing the interval obviously increases the amount of data, and the potential infringement into privacy increases too. It was shown, that using an interval of only 0.5 Hz, even the consumed TV program could be identified [17]. A read-out of 15 minutes can still be sufficient to identify some appliances [18]. Fewer read-outs could at least identify sleep and absence phases, still problematic if such data is available for example to robbers. Obviously, data measured by Smart Meters can directly be related to an inhabitant and hence are – by definition – personal data. Individual profiles can be derived, which intrude into the inhabitants' privacy. Reports on user behavior could be generated, for example, for targeted advertising [19], to identify health problems [20], or for landlords and insurance to detect prohibited behavior in flats [21].
Privacy issues in Smart Metering have thus heavily been addressed in the literature. In previous work, we investigated approaches to privacy and possible infringements into fundamental rights, as well as the legal perspective of privacy in Smart Metering in Austria [22]. Preliminary results were presented as poster [23]. Some of the approaches listed in this paper can be mapped to other personal data arising in the building.
However, the customer is now able to estimate consumption and costs during the year and to set measures for their reduction. Furthermore, data collected by Smart Meters can be used to optimize future energy demand from the grid (i.e., Short Term Load Forecasting) [24]. Economic studies do not agree yet, whether significant savings are reasonable (cf. pro for Austria [25], contra for Germany [26]). From the customer perspective, it will mainly depend on who will finally pay for their introduction – the customer himself or the system operator. It will also depend on whether the customer is ready to change his behaviors, for example, by utilizing dynamic pricing and shifting activation of devices with high energy consumption to cheaper times.

COUNTERMEASURES FOR PRIVACY INFRINGEMENTS

The right of protection of personal data is included in the European Convention on Human Rights (ECHR) and in the EU Charter of Fundamental Rights. They postulate a right to respect one's private and family life, his home, and his correspondence. Doubts about the compliance of Smart Meters with the ECHR delayed their introduction in the Netherlands for two years [27]. In May 2018, the new EU General Data Protection Regulation (GDPR) replaced national data protection acts of member states and introduced significant sanctions for wrongful usage of personal data. According to the Recommendation 2012/148/EU, the finding of technical and legal solutions for using smart metering systems is critical and necessary; it requires that 'fundamental rights and freedoms of individuals are respected'.

Privacy by Design

Privacy by design is a concept, taking data privacy into account from the beginning and throughout the whole product's lifecycle. The Recommendation terms it as 'conceptual data privacy', imposing the implementation of data privacy and information security attributes before the product's launch and usage on both the technical and the organizational levels. The concept has then also been included into the GDPR.

Data Protection Proposals

To solve the data protection issue, identified proposals from the literature in the Smart Metering domain are investigated (summarized in Fig. 1), some of which have also been addressed in the Recommendation and in national acts. Some of these approaches can also be used for other arising data in the Smart Building.

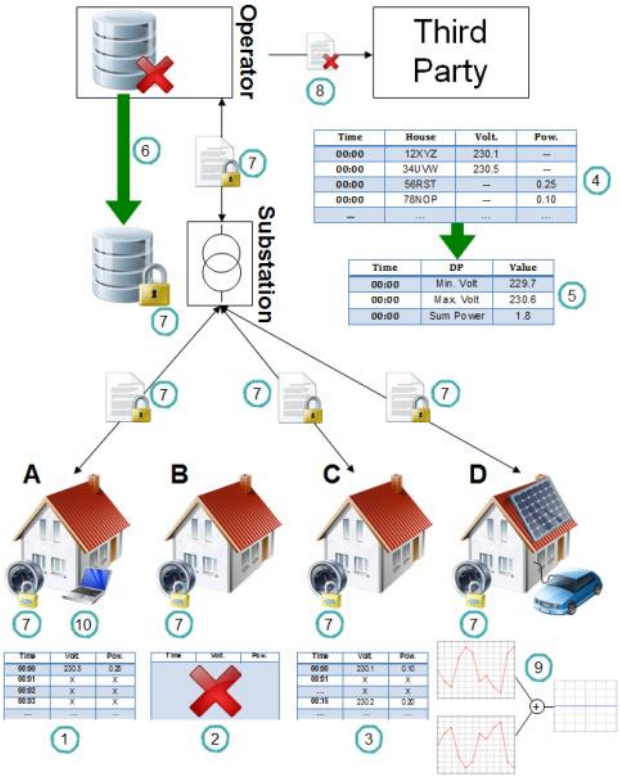

Figure 1: Overview of the investigated privacy enhancing technologies

1. Data Minimization

Any processing of personal data needs to be necessary and proportionally. Thus, the collection of personal data should be limited to those necessary to fulfill the contract. In the observed domain, this can mainly be achieved by reading out personal data rarer. A good compromise is nevertheless necessary as the grid operator relies on short-time feedback on the status of the grid.

2. Opt-Out

Every end user should decide whether he wants to get a Smart Meter or not. The EU and national acts, however, require a certain percentage of households to be equipped with Smart Meters. It is therefore not intended that customers explicitly opt-in for a Smart Meter installation. In 2017 – following numerous critics – Austrian law was amended such that an opt-out is now permitted.

3. Explicit Opt-In

Proposals suggest an opt-in (at least) for using extended Smart Meter functions: In Austria, it is required by law to read out Smart Meter values once per day. Literature suggests that a more frequent readout as required by dynamic tariffs shall require an explicit opt-in. This proposal was incorporated into Austrian law, as the use of quarter-hour readings are permitted only by an explicit consent. For the current Austrian legal situation, it is necessary to obtain an explicit and voluntary declaration of consent of every participating user for the use of personal data not included or exceeding the special Smart Metering privacy regulations [28]. Not agreeing people must not be prevented to live in a Smart Building, but their data cannot be used for individual optimization. In consequence, the profit for those people will be limited.

4. Data Anonymization

Data are anonymized if all identifying elements have been eliminated, i.e., it is not possible by using reasonable efforts to re-identify the person concerned. In pseudonymized data all identifiers are encrypted; in contrast to anonymized data, they still count as personal data [12]. As far as possible it should always be sought to get along with anonymized or pseudonymized data only [18]. Even though the grid operator needs to know the status of the network timely (i.e., high-frequency meter data), there is no need to know the connection between data and the end user [29]. For billing purposes, the end user necessarily needs to be identified; however, it is not necessary to transmit that information using such a high interval (i.e., low-frequency meter data).

5. Data Aggregation

To get information about the grid status, it is often not necessary to collect individual information from all households. Usually, aggregated data combining more than one measuring point is sufficient, e.g., minimum and maximum voltage levels, the sum of the consumed power, or the sum of the current flow from a transformation substation.

6. Minimal and Local Data Storage

Data should be kept only as long and as detailed as required for the objective they have been collected for. Furthermore, data should be retained in a local place only, without a transmission to the operator's database or central systems if the data is not necessarily required there - most types of Smart Building data will usually fall into this category. Privacy and cost efficiency needs to be weighed, since costs can be reduced when having access to all building service systems in a centralized monitoring and control center [30]. For Smart Meter data, a transfer is usually desirable since the grid operator is interested in the current grid state. A full view on the grid including central storage of the collected individual consumption data on the operator's site is however not necessary when using automated secondary substations that react on grid problems by themselves (cf. [31]), e.g., by automatically controlling the transformer level on demand [32]. There are also approaches that even move the procedure of factorization into the customer's sphere, only requiring transmitting accumulated energy costs (e.g., [33]).

7. Data Security and Technical Data Protection

Communication to the outside of the customer's sphere has to be protected against unauthorized access, interception and modification. This can be achieved by mechanical locks, by installing the meters in protected areas, and by utilizing encryption and authentication [21]. By Austrian law, all data needs to be removed from the Smart Meter device after 60 days and it needs to be prevented that tenants can access any data of earlier inhabitants. Since today's encryption algorithms may be deprecated in the future while meters may be in use for decades, algorithms need to be changeable by software updates [34]. A role concept should restrict the access of personal data that legally left the customer's sphere at authorized parties, for example, employees shall only be able to access data if they are required to [28]. Every access (i.e., local database readouts, data exports, remote maintenance) needs to be logged.

8. Data Sovereignty and Earmarking

The end user shall decide what his data is used for. Authorized people shall use personal data only for the defined objectives; they must not link data with those of other sources and they must not pass them over to third parties. All accesses of third parties (e.g., landlords, insurances, or employers) shall only be allowed with an explicit permission by the end user. Austrian privacy law for Smart Meters even denies the use of such data in administrative or civil courts – but not in criminal trials [13].

9. Data Obfuscation

The proposals usually require the grid operator to implement new protocols or to upgrade infrastructure. In

comparison, this approach only involves the customer trying to mask the usage by changing its consumption curve. Generally, load hiding techniques can be divided into battery-based load hiding (BLH) and load-based load hiding (LLH) [35,36].
Using BLH, the battery storage is charged or discharged strategically to flatten the curve, such that it is not possible to find out when the end user was at home or used a device. The battery is charged when the actual demand is below a target, and discharged when the demand is above to keep the resulting demand as near as possible to a leveled target line (Fig. 2). In result, the overall consumption remains the same.

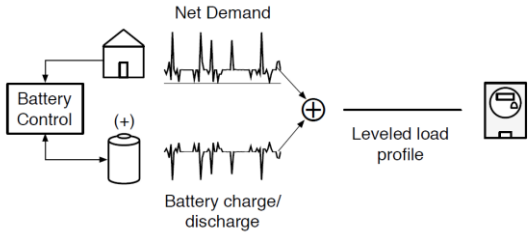

Figure 2: A BLH approach [35]

Using LLH, controllable appliances with high energy consumption that are not user-driven, for example, water boilers, are utilized. Noises are added to the consumption curve by randomly turning the device on and off (Fig. 3). Furthermore, a PV system could feed modified current into the grid [37], but it requires standby resources for such demands, and thus cannot work as efficient as it would be able to. When using "Simulating Appliance Load Signatures" [37], the use of an appliance is simulated – in result, the same energy is required as by using the real device. Both latterly described approaches are thus of scientific nature only and are in our opinion not suitable for the market.

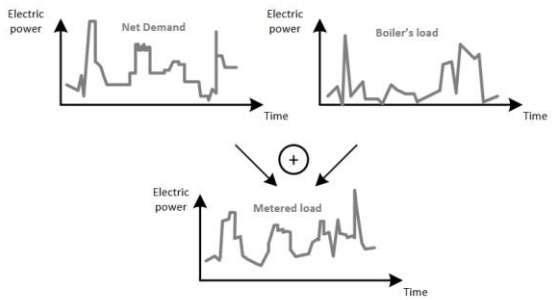

Figure 3: An LLH approach [36]

10. Data Control and Customer Incentive

As of the legal acts, Smart Meter systems are primarily introduced to enhance energy efficiency and energy consumption control of customers. EU acts state that transparent and objective access to consumption data is an important aspect. Thus, customers are entitled to receive information about their energy consumption as an incentive to save energy. Consequently, a system is necessary that enables the end user to monitor his data and to see immediate effects (i.e., money savings) by changing his habits. Legal acts do not deny a more frequent recording of data as required by some functions in the Smart Buildings if those data are not transmitted to the household's outside. The customer shall be able to check the correctness of the values for a suitable time and to erase those values afterwards. The most obvious way to enable such accesses is by using a website, complying with the latest safety standards and data protection regulations. This means that the web portal needs to use authentication and an encrypted connection. Direct access for third parties is not allowed, keeping it the end users' choice to pass on his data.

OUTLOOK AND CONCLUSION

The transition to intelligent buildings introduces a high amount of data that can directly be related to their inhabitants. Of various types of collected data, energy consumption data have mainly been served as example since privacy issues in Smart Metering have been heavily addressed in the literature. Using those data, however, also needs to be viewed from another perspective as processing and combination of different types of data are used for the optimization of energy costs and to improve the comfort of inhabitants. Austrian studies have shown that critics on Smart Meters mainly originate from people that do not yet have one installed; people already being equipped with one predominantly see their installation positively [14]. It is not yet clear whether and how Smart Meters will influence the overall energy consumption. Economic studies have not been consistent in whether there are reasonable economic savings possible.
Besides Smart Meters, data generated by various sensors (e.g., door sensors, room air quality sensors) can also allow detecting occupancy. Further research on privacy in these fields, as well as legal activities, will necessarily be required in future. Some of the approaches addressed in this paper will also be applicable for those other types of personal data.
European Union member states still show differences in their level of personal data protection. The European Commission addressed these discrepancies and proposed a new regime for data protection effective since May 2018. The General Data Protection Regulation (GDPR) is directly applicable in all member states to unify data protection in the Union. Inevitably, the new act has impacts on whether and how to handle personal data, including in the Smart Building context.

ACKNOWLEDGEMENTS

The presented work is conducted in the framework of the joint programming initiative ERA-Net Smart Grids Plus, with support from the European Union's Horizon 2020 research and innovation programme. On national level, the work was funded and supported by the Austrian Climate and Energy Fund (KLIEN, ref. 857570).

REFERENCES

[1] D. Dietrich, et al, 2010, "Communication and Computation in Buildings: A Short Introduction and Overview", *IEEE Trans. Industrial Electronics*, vol. 57, 3577-3584.

[2] Z. Ylmaz, 2007, "Evaluation of energy efficient design strategies for different climatic zones: Comparison of thermal performance of buildings in temperate-humid and hot-dry climate", *Energy and Buildings*, vol. 39, 306-316.

[3] U.S. Department of Energy, 2011, "Buildings Energy Data Book".

[4] K. Saurav, et al, 2016, "Minimizing Energy Costs of Commercial Buildings in Developing Countries", *IEEE SmartGridComm*, 655-660.

[5] T. A. Nguyen, et al, 2013, "Energy intelligent buildings based on user activity: A survey", *Energy and Buildings*, vol. 56, 244-257.

[6] J. Krumm, et al, 2011, "Learning time-based presence probabilities", *Pervasive Comp.*, 79-96.

[7] R. Melfi, et al, 2011, "Measuring building occupancy using existing network infrastructure", *Green Computing Conference and Workshops*, 1-8.

[8] G. Tang, et al, 2015, "The meter tells you are at home! non-intrusive occupancy detection via load curve data", *IEEE SmartGridComm*, 897-902.

[9] S. Nagar, et al, 2016, "SMOME: A Framework for Evaluating the Costs and Benefits of Instrumentation in Smart Home Systems", *IEEE SmartGridComm*, 134-139.

[10] T. Hosoe, et al, 2016, "Automated Generation Method of Recommendation for Effective Energy Utilization as a HEMS Service", *IEEE SmartGridComm*, 74-79.

[11] A. Reinhardt, et al, 2016, "Detecting Anomalous Electrical Appliance Behavior based on Motif Transition Likelihood Matrices," *IEEE SmartGridComm*, 704-709.

[12] European Union Agency for Fundamental Rights and Council of Europe, 2014, "Handbook on European data protection law".

[13] R. Knyrim, et al, 2013, "Smart Metering NEU - die Änderungen durch die ElWOG-Novelle 2013", *ecolex*, 1123-1126.

[14] K. Bernhardt, "Smart Metering – ein "nicht" technischer Blickwinkel", *e & i*, vol. 131, 193-194.

[15] V. Abeykoon, et al, 2016, "Real Time Identification of Electrical Devices through Power Consumption Pattern Detection", *Micro & Nano Conf.*

[16] R. Streubel, et al, 2012, "Identification of electrical appliances via analysis of power consumption", *UPEC*, 1-6.

[17] U. Greveler, et al, 2012, "Multimedia content identification through smart meter power usage profiles", *Computers, Privacy and Data Protection*.

[18] T. Jeske, 2011, "Datenschutzfreundliches Smart Metering", *Datenschutz und Datensicherheit*, 530.

[19] F. Skopik, 2012, "Security Is Not Enough! On Privacy Challenges in Smart Grids", *Journal of Smart Grid and Clean Energy*, 7-14.

[20] A. Molina-Markham, et al, 2010, "Private Memoirs of a Smart Meter", *ACM BuildSys*, 61-66.

[21] S. Renner, 2011, "Smart Metering und Datenschutz in Österreich", *Datenschutz u. Datensicherheit*, 524.

[22] S. Cejka, 2017, "Vorschläge für Datenschutz und Privatsphäre bei Smart Metern und deren Umsetzung im österreichischen Recht", *Jusletter IT*.

[23] S. Cejka, et al, 2017, "Privacy Enhancing Technologies – Privacy Issues in the Smart Building Domain", *Poster Session at the Symposium on Innovative Smart Grid Cybersecurity Solutions*.

[24] C. Gerwig, 2015, "Short term load forecasting for residential buildings - an extensive literature review," *KES-IDT*, 181-193.

[25] PricewaterhouseCoopers, 2010, "Studie zur Analyse der Kosten-Nutzen einer österreichweiten Einführung von Smart Metering".

[26] Ernst & Young, 2013, "Cost-benefit analysis for the comprehensive use of smart metering".

[27] C. Cuijpers, et al, 2013, "Smart metering and privacy in europe: Lessons from the dutch case", *Europ. Data Protection: Coming of Age*, 269-293.

[28] B. Richter, et al, 2016, "Praxisprojekt "Seestadt Aspern": datenschutzkonforme Forschung für die Energiezukunft", *Dako*, 52-55.

[29] C. Efthymiou, et al, 2010, "Smart grid privacy via anonymization of smart metering data", *IEEE SmartGridComm*, 238-243.

[30] W. Kastner, et al, 2005, "Communication systems for building automation and control", *Proceedings of the IEEE*, vol. 93, 1178-1203.

[31] M. Faschang, et al, 2017, "Provisioning, deployment, and operation of smart grid applications on substation level", *Computer Science - Research and Development*, vol. 32, 117-130.

[32] S. Cejka, et al, 2018, "Operation of Modular Smart Grid Applications Interacting through a Distributed Middleware", *OJBD*, vol. 4, 14-29.

[33] C.-I. Fan, et al, 2013, "Design and implementation of privacy preserving billing protocol for smart grid", *Journal of Supercomputing*, vol. 66, 841-862.

[34] H. Khurana, et al, "Smart-Grid Security Issues", *IEEE Security and Privacy*, vol. 8, 81-85.

[35] S. McLaughlin, et al, 2011, "Protecting consumer privacy from electric load monitoring", *ACM Computer and Communications Security*, 87-98.

[36] D. Egarter, et al, 2014, "Load hiding of household's power demand", *IEEE SmartGridComm*, 854-859.

[37] A. Reinhardt, et al, 2015, "Worried about privacy? Let your PV converter cover your electricity consumption fingerprints", *IEEE SmartGridComm*, 25-30.