Elektrotechnik & Informationstechnik (2020) 137/1: 33–37. https://doi.org/10.1007/s00502-019-00779-4

ORIGINALARBEIT

# Enhancing privacy in smart energy systems

D. Engel

The mission to move from fossil to renewable energy sources is accompanied and enabled by the digitalization of our energy systems. With the introduction of information and communication technologies, the widespread integration of distributed, renewable sources, even in the distribution grid, are enabled. New use cases such as fast EV charging, local energy communities and dynamic energy tariffs are also enabled. However, this move toward digitalization also increases the exposure of the energy systems for cybercrime and raises concerns regarding the privacy of personal data. In this article, we address the issue of privacy in smart energy systems and give an overview of current methods to enhance privacy.

Keywords: privacy; data protection; energy systems

***Verbesserung der Privatsphäre in intelligenten Energiesystemen.***

*Die Energiewende weg von fossilen und hin zu erneuerbaren Energieträgern wird von der Digitalisierung unserer Energiesysteme begleitet und ermöglicht. Durch den Einsatz von Informations- und Kommunikationstechnologien wird die umfassende Einspeisung durch erneuerbare und dezentrale Energiequellen auch im Verteilnetz ermöglicht. Neue Anwendungsfälle wie das schnelle Laden von Elektroautos, gemeinschaftliche Erzeugungsanlagen und dynamische Energietarife werden dadurch realisierbar. Neben allen Vorteilen macht die Digitalisierung Energiesysteme aber auch verwundbarer gegen Cyber-Kriminalität und es bestehen Bedenken, was den Schutz persönlicher Daten betrifft. In diesem Artikel werden die Themen Privatsphäre und Schutz persönlicher Daten näher beleuchtet und aktuelle Methoden zum Schutz der Privatsphäre diskutiert.*

*Schlüsselwörter: Privatsphäre; Datenschutz; Energiesysteme*

Received September 16, 2019, accepted October 23, 2019, published online December 17, 2019


## 1. Introduction

The term "smart grids" is used to describe the next-generation energy systems – digitized systems of systems that are an important enabler for turning from fossil energy sources to renewable energy sources. Smart grids employ state-of-the-art information and communication technology to control generation, distribution and consumption of energy. With smart grids the power network organization moves from a hierarchical to a decentralized structure and communication flow moves from largely uni-directional to bi-directional. Compared to traditional power networks, significantly more data is acquired, transmitted and made available to different stakeholders in fine granularity, sometimes in near real-time.

One of the most important goals of smart grids is the accommodation of environmentally sustainable energy sources. Traditional, non-renewable energy sources can be controlled with a hierarchical network structure, with energy sources and energy sinks at opposing levels of the hierarchy. Many types of renewable energy sources, such as photovoltaics or wind power, generate power at the distribution level. In order to integrate a high number of these renewable sources to produce in bulk quantities, an evolution of the network infrastructure and the intense use of information and communication technologies, even in the distribution grid, become necessary.

A significant portion of (potential) end-users at this point in time are wary about possible disadvantages of the new smart grid technology, like the uncertainty regarding the level of privacy and possible security breaches [1, 2]. Apart from privacy and security concerns, end-users are skeptical regarding possible benefits of smart grids as a new technology, such as cost savings [2]. End-users have difficulties understanding the level of control they can exert in a smart grid environment [3].

It is valid to diagnose a severe lack of trust towards smart grids on the end-user level. If this lack of trust were to persist, it would prevent many important features of the smart grid: dynamic energy tariffs [4], distributed energy management, adaptive load balancing, e-mobility, private renewable energy sources and the usage of smart grid infrastructure for other areas, such as home automation or local energy communities.

In order to establish the needed degree of trust in the end-user domain, providing a visible level of both, security and privacy, are imperative. In addition, a further component is necessary, namely: user control. In order to alleviate concerns of a lack in benefits (especially on a personal level) a sufficient degree of understanding of possible interaction is required. Correspondingly, user interaction needs to be reflected accurately on the system side.

Users need to be informed of what choices can be made (user information), how these choices influence smart grid processes (functional transparency), what data items at what granularity need to be disclosed for this purpose (user-managed privacy) and that processes and data transfer are operated in a secure way (traceable security). On all items, systemic feedback to the user needs to be provided consistently in order to raise user awareness and ultimately create a level of user trust that allows meaningful interaction.

At the Salzburg University of Applied Sciences, a research center has been established to address these issues. In 2013, the "Josef Ressel Center for User-Centric Smart Grid Privacy, Security and Con-

**Engel, Dominik,** Center for Secure Energy Informatics, Salzburg University of Applied Sciences, Urstein Sued 1, A-5412 Urstein/Salzburg, Austria
(E-mail: dominik.engel@fh-salzburg.ac.at)

trol" was founded. Since 2018 the scope of the research center has been broadened under the new name "Center for Secure Energy Informatics". The goal of the methods developed at the research center is enabling trust in the smart grid end-user domain, by improving existing approaches and developing new mechanisms to establish secure, private and informed – i.e., trusted – user interaction with smart grid technology. The fundamental question addressed is: How can a sustainable level of trust by the users be established the various entities (applications, processes, data protocols, and interfaces) of the smart grid user domain, in order to foster participation and acceptance on the side of the users?

The main focus is on methods that safeguard end-user data, both in terms of preserving end-user privacy in face of potentially curios or malicious insiders and providing security to fend off outside attackers. Apart from privacy and security, general methods for data handling, such as compression, are discussed. Furthermore, the important topic of user control is introduced, i.e., methods that aim at a two-fold benefit: incentivizing users to participate in smart grid optimization schemes and allowing informed interaction with the new technology. Both, of course, under the assumption that appropriate methods for preserving privacy and providing security are in place.

Overall, the research at the center aims at enabling user acceptance of smart grid technologies by providing methods for the important fields of privacy, security and user control. In this paper, we give an overview of selected published research results in the area of smart grid privacy. Note that this paper does not present original research, but is intended as a summary of research results. We will focus on smart meter privacy as a an example for the research performed at the center.

## 2. Related work

Overviews of privacy issues and privacy enhancing are given by [5–7]. There is a number of contributions that deal with technological approaches to end-user privacy in general, for an overview see [8]. In the context of smart grid privacy, a major part of current proposals is focused on smart metering and the load profiles generated by smart meters.

It has been argued, that approaches relying on policy alone, may prove inadequate to provide a sufficient level privacy and that technological methods that enforce privacy by virtue of "strength of mechanism" need to be employed [9]. Indeed, a number of such technological approaches have been suggested to remedy the (perceived) loss in privacy and still enable smart metering functionality on a broad basis. In the following, we give a brief overview of these contributions, closely based on own work published in [10]. More detailed surveys can be found in [5–7, 9, 11].

The only approach that is widely used in the real world at this point in time, is *anonymization or pseudonymization* of smart metering data. Consumption data and the personal data are split and stored separately. Methods for de-anonymization are a major threat for these types of approaches. It has been shown that even after anonymization or pseudonymization, data items can still be attributed to the individual that originated them. Jawurek et al. [12] show that de-anonymization can also be done in the smart grid user domain. This structural traceability is a problem for schemes that rely on anonymization or pseudonymization only without the use of additional encryption.

*Simple aggregation* tries to hide data related to individuals by aggregating over a number of house-holds, e.g., all households in a neighborhood are network (NAN). For example, Bohli et al. [13] propose a privacy scheme in which high resolution smart meter readings are aggregated at NAN level and only the aggregate is sent to the utility. They introduce two solutions both with and with-out involvement of trusted third parties.

Due to the inherent link between load data resolution and privacy, splitting the load data into a variety of *different resolutions*, each associated with different authorization levels, has been proposed by a number of contributions. For example, the anonymization scheme proposed by Efthymiou and Kalogridis [14] is based on two different resolutions: a low resolution that can be used for billing purposes, and a high resolution that allows further investigation. This scheme employs a trusted third party escrow service. In our own work, we propose wavelet-based multi-resolution privacy (e.g., [15]).

*Masking* relates to approaches which add numerical artifacts, e.g., random sequences to the original load data to obfuscate individual contributions. The added artifacts are constructed in such a way that they cancel each other out upon aggregation. The aggregator can therefore combine the data values of all participant to create an accurate aggregation, but cannot gain access to individual contribution. For example, Kursawe et al. [16] propose such an aggregation protocol, which compared to other approaches has the advantage of relatively low computational complexity. Defend and Kursawe [17] further improve on this idea. Danezis et al. [18] present another low-overhead protocol for aggregation of smart meter data, which puts minimal computational demands on the smart meter hardware.

*Differential privacy*, as Dwork [19, p. 1] puts it, roughly speaking, "ensures that (almost, and quantifiably) no risk is incurred by joining a statistical database". Adding or removing an item from the database will not (or only to a very limited degree) affect the result of statistical computations. This is commonly achieved by the distributed generation of noise which is added to the individual data contribution. Shi et al. [20] propose a scheme for adding random noise to time series data using a symmetric geometric distribution. An advantage of this scheme is that the participants need not trust each other, nor rely on a trusted aggregator. As another example, Ács and Castelluccia [21] obscure individual data sets by adding Laplacian noise, which is jointly generated by the participants. Apart from the obvious drawback that the data is no longer exact after differential privacy is applied, data pollution by malicious participants is another issue with this approach [20].

*Secure Signal Processing* (SSP) refers to the possibility to perform certain computations, such as aggregation in the encrypted domain. A commonly employed mechanism in SSP is additively homomorphic encryption, which allows some specific manipulations of the ciphertext to be reflected in the plaintext domain. For example, Li et al. [22] propose an overlay network in a tree-like topology and the use of a Paillier cryptosystem. Garcia and Jacobs [23] combine secret sharing with a Paillier cryptosystem to add flexibility in the aggregation (at the expense of additional computational complexity). Erkin and Tsudik [24] extend the idea of homomorphic encryption of smart meter readings by splitting the module into random shares, which, in combination with a modified Pailler cryptosystem, allows flexible spatial and temporal aggregation for different use cases, such as billing or network monitoring. In our own work, we propose the combination of SSP with multi-resolution methods to increase customer privacy choices [25, 26].

## 3. Results on smart meter privacy from the center of secure energy informatics in Salzburg

The primary goal of the methods proposed at the research center is to improve existing approaches and develop new mechanisms to establish secure, private and informed – i.e., trusted – user interaction with smart grid technology. Results have been published in a

number of peer-reviewed journal publications as well as a number of publications in conference proceedings. In the following, the contribution of the publications in the area of smart meter privacy are summarized briefly and put into context to each other.

Smart metering has been in the focus of the discussion on privacy issues in smart grids. This discussion has been led without taking the resolution of the underlying data into account, also in the academic discourse. In two papers [27, 28], we have presented a formal analysis on the impact of resolution on smart meter privacy.

In [27], we analyse the impact of resolution on a the first step of non-intrusive load monitoring (NILM), i.e., the identification of individual appliances in a household load profile. We show that decreasing resolution has an impact mainly on recall (rather than on precision) in NILM.

In [28], we extend on the previously presented NILM results and discuss the influence of load profile resolution on the degree of extractable personal information. The intuitive claim that lowering the resolution will increase privacy has been studied systematically. We show that this is indeed the case and that a dyadic series of decreasing resolutions is suitable for providing a series of privacy levels to the end-user. Although this paper was published after our work on wavelet-based smart meter privacy, it provides the formal basis for the utility of this approach. As an aside, we also investigated how well owners of swimming pools could be detected in an energy consumption set in [29].

In terms of methods for privacy enhancement in smart metering, our contributions focus on the idea of lowering the resolution of the available data, providing a wavelet-based data representation, that integrates all resolutions in a single bitstream without data expansion and providing conditional access combined with hierarchical key management.

In [30], the initial idea of wavelet-based data representation of load profiles is proposed. We have shown that the wavelet transform is a suitable tool to provide the aforementioned dyadic decreases in resolution, as each iterative application of the wavelet transform effectively halves the resolution. A first proof-of-concept implementation is presented and evaluated on inexpensive hardware (a *Beagleboard* embedded computing platform in this case).

The idea of multi-resolution representation is elaborated in [31]. Two wavelet filters are investigated for this purpose: the simple Haar Wavelet and the LeGall 5/3 Wavelet. We show that while the integer-based LeGall 5/3 Wavelet is faster, due to the necessary border handling and the ensuing errors, it is not a possible choice. The Haar Wavelet is well suited for application, as it is also fast in application and provides lossless transformation in practice. Furthermore, we discuss the fact that the original sum is preserved over multiple wavelet decomposition, which is an important property for use-cases such as billing (which also has to work at the lowest resolution). The performance of the approach is evaluated at the example of an extended prototypical implementation. It is shown that the performance these environments offer is sufficient for use in the field.

We show that our approach can be combined with additively homomorphic encryption to provide additional degrees of freedom in [25]. Formal proof is given that wavelets are fully compatible with additively homomorphic encryption in the context of a Paillier cryptosystem [32]. A proof-of-concept implementation is presented and the high computational demands are discussed.

Privacy-aware data representations need to be secured for access by authorized parties. In order to facilitate secured, authorized access, different keys need to be provided for different privacy levels. For example, for multi-resolution load profile data, a different key is required for each resolution. For this setup, in [33] we propose a hierarchical key scheme, based on previous work by Lamport [34]. In order to limit the number of keys a user needs to handle, a hierarchical key generation scheme is used. With this key scheme it is ensured that a user who has the key for the highest resolution can derive all necessary sub-keys to the lower resolutions (which are, of course, needed to reconstruct the highest resolution)

In [15], all of the components for wavelet-based multi-resolution data representation in Smart Metering are integrated into system of a whole. The underlying protocols are presented and discussed in detail, as well as the different communication paths from Smart Meter to distribution system operator, energy provider or another third party. The degrees of freedom are addressed, e.g., the alternatives to run the protocols with or without a data concentrator. For the first time, a comprehensive and detailed security and privacy analysis is conducted, including the basic security assumptions, different attacker models and the discussion of privacy properties from an information-theoretic point of view.

Based on the idea of multi-resolution data representation in smart metering, we explore the options to combine the previously proposed wavelet-based representation with other privacy enhancing technologies (PETs) in [26]. The paper discusses the applicability of multi-resolution methods to three PETs: masking protocols, differential privacy and secure aggregation.

We found that in literature, the presentation of PETs for the energy domain is very heterogeneous, especially when it comes to privacy analysis. We therefore teamed up with colleagues from Koç University to make the concept of game-based privacy proofs viable for energy consumption protocols. The results and the formal framework are presented in [35].

Privacy measures try to assess the amount of information contained in data. While the previously discussed papers tried to assess privacy from a model-based view, there were also some ideas to come up with an entropy-like measure for privacy. While exploring options in this direction, we found that the compressibility (which, of course, is related with entropy) of load profiles had not been studied systematically before. Therefore, in [36], an approach for compression of load data is proposed, that is based on ideas for compression of multimedia data. It is shown that the approach is lightweight on the side of the smart meter and that it is resumable, which is an important property if a smart meter loses connectivity for a period of time.

We extend the previous work on load data compression and data granularity in [37], where we explore the effect of data granularity on compression results. For this investigation we joined forces with Martin Ringwelski the main author of the only other algorithm specifically designed for load data compression. We investigate the properties of our algorithm compared to Ringwelski's approach. It turns out that depending on data resolution, one or the other may be preferable.

In discussion with the company partners of the Josef Ressel Research Center, it became evident that there is no clear view on the privacy relevance of different smart metering use cases and how this could be addressed by specific PETs. Such an account is also missing in literature. We address this issue in [38], where we aim at bridging the gap between privacy requirements of smart metering use cases and the features different PETs have to offer.

At the research center, data analytics has mainly been used to identify the leak of personal information from energy consumption data. In a joint project with the colleagues from Energy Institute in Linz, we broadened the scope to investigate dynamic network tariffs and their impact on different households. In [4], different

dynamic pricing schemes are discussed and their impact on socia-demographic groups is assessed.

## 4. Conclusion

In this paper, we gave an overview of the research done at the Center for Secure Energy Informatics at the Salzburg University of Applied Sciences. We mainly focused on our work in the field of privacy enhancing technologies in the energy domains. While investigating privacy issues, we also came across other research questions we found interesting, such as compression of load data or the socio-economic impact of dynamic network tariffs. The discussion of other research topics addressed by the center in the field of smart grid architecture and dependable system-of-systems engineering were out of the scope of this paper. A complete list of publications can be found at https://www.en-trust.at/publications.

## Acknowledgements

Open access funding provided by FH Salzburg – University of Applied Sciences. The financial support by the Austrian Federal Ministry of Digital and Economic Affairs and the Federal State of Salzburg is gratefully acknowledged. The input of the company partners Salzburg AG, Salzburg Wohnbau and Siemens is gratefully acknowledged.



### References

1. De, S. J., Metayer, D. L. (2016): Privacy harm analysis: a case study on smart grids. In 2016 IEEE security and privacy workshops (SPW) (pp. 58–65). New York: IEEE. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7527754.
2. Cuijpers, C., Koops, B.-J. (2013): Smart metering and privacy in Europe: lessons from the Dutch case. In S. Gutwirth, R. Leenes, P. de Hert, Y. Poullet (Eds.), European data protection: coming of age (pp. 269–293). Berlin: Springer.
3. Karg, L., Kleine-Hegermann, K., Wedler, M., Jahn, C. (2014): E-Energy Abschlussbericht – Ergebnisse und Erkenntnisse aus der Evaluation der sechs Leuchtturmprojekte. Bundesministerium für Wirtschaft und Technologie (German Federal Ministry for Economy and Technology), Tech. Rep, in German. [Online]. Available http://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/ab-gesamt-begleitforschung.pdf?_blob=publicationFile&v=4.
4. Azarova, V., Engel, D., Ferner, C., Kollmann, A., Reichl, J. (2018): Exploring the impact of network tariffs on household electricity expenditures using load profiles and socio-economic characteristics. Nat. Energy, 3, 317–325. https://doi.org/10.1038/s41560-018-0105-4.
5. Borges de Oliveira, F. (2017): On privacy-preserving protocols for smart metering systems. Berlin: Springer.
6. Finster, S., Baumgart, I. (2014): Privacy-aware smart metering: a survey. IEEE Commun. Surv. Tutor., 16(3), 1732–1745.
7. Lu, R. (2016): Privacy-enhancing aggregation techniques for smart grid communications. Berlin: Springer.
8. Iachello, G., Hong, J. (2007): End-user privacy in human-computer interaction. Found. Trends Hum.-Comput. Interact., 1(1), 1–137. [Online]. Available: http://dl.acm.org/citation.cfm?id=1324103.1324104.
9. Jawurek, M., Kerschbaum, F., Danezis, G. (2012): Privacy technologies for smart grids – a survey of options. Microsoft research, Tech. Rep.
10. Engel, D. (2013): Privacy-preserving smart metering: methods and applicability (invited talk). In Proceedings of the fourth workshop on communications for energy systems (pp. 9–16). Vienna, Austria: Austrian Electrotechnical Association. [Online]. Available: http://energyit.ict.tuwien.ac.at/index.php/de/events/87-comforen-2013-ergebnisse.
11. Erkin, Z., Troncoso-Pastoriza, J. R., Lagendijk, R. L., Perez-Gonzalez, F. (2013): Privacy-preserving data aggregation in smart metering systems: an overview. IEEE Signal Process. Mag., 30(2), 75–86.
12. Jawurek, M., Johns, M., Rieck, K. (2011): Smart metering de-pseudonymization. In Proceedings of the 27th annual computer security applications conference, ACSAC'11 (pp. 227–236). New York: ACM. [Online]. Available: http://doi.acm.org/10.1145/2076732.2076764.
13. Bohli, J.-M., Sorge, C., Ugus, O. (2010): A privacy model for smart metering. In 2010 IEEE international conference on communications workshops (ICC) (pp. 1–5).
14. Efthymiou, C., Kalogridis, G. (2010): Smart grid privacy via anonymization of smart metering data. In Proceedings of first IEEE international conference on smart grid communications, Gaithersburg, Maryland, USA (pp. 238–243).
15. Engel, D., Eibl, G. (2017): Wavelet-based multiresolution smart meter privacy. IEEE Trans. Smart Grid, 8(4), 1710–1721.
16. Kursawe, K., Danezis, G., Kohlweiss, M. (2011): Privacy-friendly aggregation for the smart grid. In Privacy enhanced technology symposium (pp. 175–191).
17. Defend, B., Kursawe, K. (2013): Implementation of privacy-friendly aggregation for the smart grid. In Proceedings of the first ACM workshop on smart energy grid security, SEGS'13 (pp. 65–74). [Online]. Available: http://dl.acm.org/citation.cfm?doid=2516930.2516936.
18. Danezis, G., Fournet, C., Kohlweiss, M., Zanella-Béguelin, S. (2013): Smart meter aggregation via secret-sharing. In Proceedings of the first ACM workshop on smart energy grid security, SEGS'13 (pp. 75–80). New York: ACM.
19. Dwork, C. (2008): Differential privacy: a survey of results. In M. Agrawal, D. Du, Z. Duan, A. Li (Eds.), Theory and applications of models of computation. Lecture notes in computer science (Vol. 4978, pp. 1–19). Berlin: Springer. https://doi.org/10.1007/978-3-540-79228-4_1.
20. Shi, E., Chow, R., Chan, T-h. H., Song, D., Rieffel, E. (2011): Privacy-preserving aggregation of time-series data. In Proc. NDSS symposium 2011.
21. Acs, G., Castelluccia, C. (2011): I have a DREAM! (DiffeRentially privatE smArt metering). In Proc. information hiding conference (pp. 118–132).
22. Li, F., Luo, B., Liu, P. (2010): Secure information aggregation for smart grids using homomorphic encryption. In Proceedings of first IEEE international conference on smart grid communications, Gaithersburg, Maryland, USA (pp. 327–332).
23. Garcia, F., Jacobs, B. (2011): Privacy-friendly energy-metering via homomorphic encryption. In J. Cuellar, J. Lopez, G. Barthe, A. Pretschner (Eds.), Security and trust management. Lecture notes in computer science (Vol. 6710, pp. 226–238). Berlin: Springer. https://doi.org/10.1007/978-3-642-22444-7_15.
24. Erkin, Z., Tsudik, G. (2012): Private computation of spatial and temporal power consumption with smart meters. In Proceedings of the 10th international conference on applied cryptography and network security, ACNS'12 (pp. 561–577). Berlin: Springer.
25. Engel, D., Eibl, G. (2013): Multi-resolution load curve representation with privacy-preserving aggregation. In Proceedings of IEEE innovative smart grid technologies, ISGT 2013 (pp. 1–5). Denmark: IEEE.
26. Knirsch, F., Eibl, G., Engel, D. (2017): Multi-resolution privacy-enhancing technologies for smart metering. EURASIP J. Inf. Secur., 2017(1), 6. https://doi.org/10.1186/s13635-017-0058-3.
27. Eibl, G., Engel, D. (2014): Influence of data granularity on nonintrusive appliance load monitoring. In Proceedings of the second ACM workshop on information hiding and multimedia security, IH&MMSec'14) (pp. 147–151). Austria: ACM. [Online]. Available: http://doi.acm.org/10.1145/2600918.2600920.
28. Eibl, G., Engel, D. (2015): Influence of data granularity on smart meter privacy. IEEE Trans. Smart Grid, 6(2), 930–939. https://doi.org/10.1109/TSG.2014.2376613.
29. Burkhart, S., Unterweger, A., Eibl, G., Engel, D. (2018): Detecting swimming pools in 15-minute load data. In IEEE international conference on trust, security and privacy in computing and communications 2018 (Vol. 8, pp. 1641–1655). New York: IEEE.
30. Engel, D. (2011): Conditional access smart meter privacy based on multi-resolution wavelet analysis. In Proceedings of the 4th international symposium on applied sciences in biomedical and communication technologies (pp. 45:1–45:5). New York: ACM. [Online]. Available: http://doi.acm.org/10.1145/2093698.2093743.
31. Engel, D. (2013): Wavelet-based load profile representation for smart meter privacy. In Proceedings IEEE PES innovative smart grid technologies, ISGT'13 (pp. 1–6). Washington: IEEE.
32. Paillier, P. (1999): Public-key cryptosystems based on composite degree residuosity classes. In J. Stern (Ed.), Advances in cryptology — EUROCRYPT'99: international conference on the theory and application of cryptographic techniques. Lecture notes in computer science Vol. 1592 Prague, Czech Republic, May 2–6 (pp. 223–238). Berlin: Springer.
33. Peer, C., Engel, D., Wicker, S. (2014): Hierarchical key management for multi-resolution load data representation. In Proceedings of 5th IEEE international conference on smart grid communications, SmartGridComm 2014 (pp. 926–932). Venice: IEEE.
34. Lamport, L. (1981): Password authentication with insecure communication. Commun. ACM, 24(11), 770–772. [Online]. Available: http://doi.acm.org/10.1145/358790.358797.
35. Unterweger, A., Taheri-Boshrooyeh, S., Eibl, G., Knirsch, F., Küpçü, A., Engel, D. (2019): Understanding game-based privacy proofs for energy consumption aggregation protocols. IEEE Trans. Smart Grid, 10(5), 5514–5523.
36. Unterweger, A., Engel, D. (2015): Resumable load data compression in smart grids. IEEE Trans. Smart Grid, 6(2), 919–929. https://doi.org/10.1109/TSG.2014.2364686.

37. Unterweger, A., Engel, D., Ringwelski, M. (2015): The effect of data granularity on load data compression. Energy Inform., 2015(9424), 69–80.

38. Eibl, G., Engel, D., Neureiter, C. (2015): Privacy-relevant smart metering use cases. In Proceedings of IEEE international conference on industrial technology, ICIT 2015 (pp. 1387–1392). Spain: IEEE.

## Author

**Dominik Engel**
is a professor at the Salzburg University of Applied Sciences in Austria, where he heads the Center for Secure Energy Informatics. He holds a PhD degree in Computer Science from the University of Salzburg and a venia docendi in Applied Informatics at the same university. Prior to joining Salzburg University of Applied Sciences, Dominik Engel was a researcher at the Universities of Bremen and Salzburg and product manager at Sony DADC, where he was responsible for video content security. His current research interests include smart grid privacy and security and technological methods for enhancing end-user trust. Dominik Engel has authored and co-authored a number of publications related to security and privacy in smart grids and is a member in various EU and national standardization committees in this area.