Looking at IEEE SmartGridComm 2017 from a Security and Privacy Perspective

www.esat.kuleuven.be/cosic/looking-ieee-smartgridcomm-2017-security-privacy-perspective/

November 7, 2017

The IEEE International Conference on Smart Grid Communications (SmartGridComm) is a flagship conference in the Smart Grid (SG) domain. This year there were three sessions on "Cyber Security" (16 out of 92 papers) and a whole day workshop on "Safety, Privacy & Cyber Security". It is good to see that the community is paying attention to the risks associated with remotely monitoring the electricity grid. Unfortunately, proper attention to privacy risks is still missing (only 2 out of 16 papers).

[Slightly off topic] Windows XP is still in use in critical systems!!!

Our trip to Dresden started off with some worries as right before boarding the plane we noticed that **Windows XP is still being used in critical systems**. However, luckily for us, no hackers were interested in our flight, so we made it to Dresden safely. 🙂

In Dresden, we had the chance to attend a variety of interesting talks and discussions. Below we give an overview of the most important take-home messages in terms of security and privacy.

Blockchain is the hype, but don't forget the main goal of the SG…

As expected, **blockchain is a hype in SG too**: everyone is talking about it. Although, undoubtedly, it has attractive properties, such as accountability and verifiability, **blockchain technology is not a magic box that solves everything**. For example, it fails to protect users' privacy as each user transaction is registered in a (public) ledger. This makes user de-anonymisation possible by analysing their transactions. More importantly, we should not forget **the main goal of the SG: increased sustainability & efficiency** throughout the entire electricity generation/transportation/consumption process. A local electricity trading solution based on blockchain technology that uses the proof-of-work concept (requiring many trial-and-error iterations) does not make much sense. In simpler words, **validating a single transaction of a few KWh of electricity between neighbours should not require an electricity consumption of hundreds of KWh[1]**.

Cyber-physical security is not the same as cyber-security…

Prof. Bruno Sinopoli stressed that **cyber-physical security is not the same as cyber-security**. Existing countermeasures in cyber-security are useful, but not sufficient to provide cyber-physical security due to the following three main reasons. (i) **Cyber-physical security is mainly a matter of graceful degradation**. The system should keep working on an acceptable level, even when it is under attack. Cyber-physical security is not just about keeping the attackers out of your system, but rather about detecting them once they are in and recovering to a normal state of operation. (ii) **The underlying physical dynamics of the system are essential**. If attackers have physical access to the sensors, they can influence the measurements even if the overlying network infrastructure is perfectly secure. One can manipulate the environment such that sensors report ‘wrong’ data, making such attacks extremely difficult to protect against. (iii) **Updating and patching is much more difficult in a cyber-physical system** because it should be done while the system is in operation. Furthermore, it is infeasible to find countermeasures against each attack. Hence, **countermeasures should defend against classes of attacks rather than focus on individual attacks**.

Compliance with regulations does not guarantee security…

Three speakers from Siemens and Omnetric talked about standards and regulations relevant to SG privacy and (cyber-) security. As expected, the GDPR, the NIS directive, the NIST cybersecurity framework, ISO 27001 and NERC CIP were all mentioned. The speakers argued that to the three pillars of security (people, processes and technology) a fourth one, namely regulatory requirements, should be added. They argued that regulatory requirements are a key driver for security and privacy. Nevertheless, they strongly emphasised that **being compliant with regulations does not guarantee security**. More than being compliant, it is important to embrace the intent of the regulations. As most of the regulations are actually based on the same best practices, embracing these best practices and the reasoning behind them is definitely a step in the right direction. Interestingly, they also remarked that **being fully secure also does not guarantee compliance with regulations**, so companies should be working on both.

Encryption is not always the solution…

One talk, “Encryption in ICS networks: a Blessing or a Curse?”, elicited a lot of discussion as the presenter argued that encryption can negatively affect the security of Industrial Control Systems (ICS) and raise the cost of troubleshooting and recovery. The presenter pointed out that encryption would not have stopped any of the known major attacks on the SG: Stuxnet, Dragonfly 1.0 & 2.0, and BlackEnergy. More generally, he argued that (i) the endpoints are actually the weakest points, (ii) one cannot do proper network monitoring for anomalies if end-to-end encryption is deployed, and (iii) key management and properly implemented encryption are never trivial.

For everyone with a crypto background, it is obvious that for example integrity and availability cannot be achieved simply by using encryption. Whether or not confidentiality is necessary depends on the specific use-case, and it is something that should be carefully considered and weighed against the cost. However, it is vital to convey the following message to utilities and DSOs – **blanket encryption is not the solution for everything**! Despite some confusion in terminology, we liked this talk as it conveyed a very important message to industry.

Who cares about privacy?

There were several talks, for example "Automated Classification of Appliances Using Elliptical Fourier Descriptors", on how to do Non-Intrusive Load Monitoring (NILM) – identifying which appliances a household is using at any point in time based only on the fine-grained total consumption data of the household. Although it might be useful in some use-cases, **NILM is extremely privacy-invasive if the fine-grained consumption data leave the household**. Thus, it would be interesting to study NILM from a privacy angle. We see two different approaches: (i) apply privacy-friendly machine learning techniques to NILM, or (ii) make NILM more efficient so it can run locally, e.g., on smart meters. There are already promising results for the second approach, cf "An Innovative Cost-Effective Smart Meter with embedded Non-Intrusive Load Monitoring".

Unsurprisingly, the comparison with Facebook once again came up during discussions; some quotes: "Who cares about privacy? … Our generation already shares lots of personal data via Facebook". It is very important to stress that, despite the fact that many of us disclose personal information on Facebook, **we have a choice on what information and when to disclose**! Of course, we are all aware that companies like Facebook try to collect as much personal data as possible, even without a proper user consent, cf an earlier COSIC post "Preserving Privacy in Belgium".

In the SG context, if any entity (e.g., supplier, grid operator, third party) has access to individual users' high resolution consumption data (e.g., every 15 minutes[2]) by default, the comparison with Facebook does not hold. An equivalent would be a social network where, by default, everyone has an account and everyone's status is automatically updated every 15 minutes with exactly what they have done in the previous 15 minutes regardless of users' opinion. We hope that nobody wants to live in such a world. Our view is the following: **give users the option to choose from various levels of privacy protection** and **have a maximum level of privacy protection by default**

Protecting users' privacy by load flattening using residential batteries

Fortunately, there were a couple of talks on **protecting users' privacy by using residential batteries to flatten out the load profile of users**, thus making it difficult for adversaries to infer users' actions from the load profiles. The advantage of this approach is that even the utility or the grid operator (the legitimate receivers of the metering data) cannot infer sensitive information about the household from the received consumption data. Moreover, load flattening has also the added advantage that the consumption data the utility (or grid operator) receives is the actual pattern of the electricity the household has taken off the grid; no noise is added; none of the data points are suppressed nor are the data rounded. The disadvantage, of course, is that the household must possess a residential battery, which at this point in time is not very common.

In the first talk, "Optimal demand-side management for joint privacy-cost optimization with energy storage", Giulio Giaconi introduced piecewise flattening of load profile and elaborated on the impact of battery capacity, the possibility to sell electricity to the grid and the trade-off between cost and privacy leakage. In the second talk, "Smart meter privacy via the trap-door channel", Miguel Arrieta explained how to measure privacy leakage by using mutual information. In this research the battery is equivalent to a trapdoor channel, where the output is a permutation of the input (electricity consumption) which is considered stochastic. This provides an information-theoretic upper bound on the information leakage rate. Note that **load flattening might actually be a desirable property even for the utility (the grid operator)** as it makes demand more predictable, thus simplifying forecasting.

In conclusion, **protecting users' privacy using load flattening systems is a promising approach**. One may wonder how this will work using batteries of electric vehicles, which impose additional constraints such as mobility and users' preferences. Perhaps an interesting research topic…

Guess who won the student video competition…

During the gala dinner we had a very pleasant surprise – our video, "Secure and Privacy-friendly Local Electricity Trading", had won the student video competition. In this video we show our vision for a secure and privacy-friendly local electricity trading market, which we already wrote about in our previous post. You can also check our work on the topic: "A Local Electricity Trading Market: Security Analysis" and "An MPC-based Privacy-preserving Protocol for a Local Electricity Trading Market".

We were very happy to see that the SmartGridComm organisers appreciated our vision and gave us the chance to share it with so many people! We also made some good friends at the conference – all interested in SG privacy issues. No surprises here. 🙂

Aout the authors

Sara Cleemput and Mustafa A. Mustafa are researchers at COSIC. They primarily work on designing secure and privacy-friendly solutions for various smart grid use-cases.

References

[1] According to Digiconomist, at the time of writing this post, the average amount of electricity consumed per bitcoin transaction (which uses proof-of-work concept) was 211 KWh. [2] According to "Data Mining and Privacy of Personal Behaviour Types in Smart Grid", 15 minute electricity consumption data resolution still poses significant privacy risks.