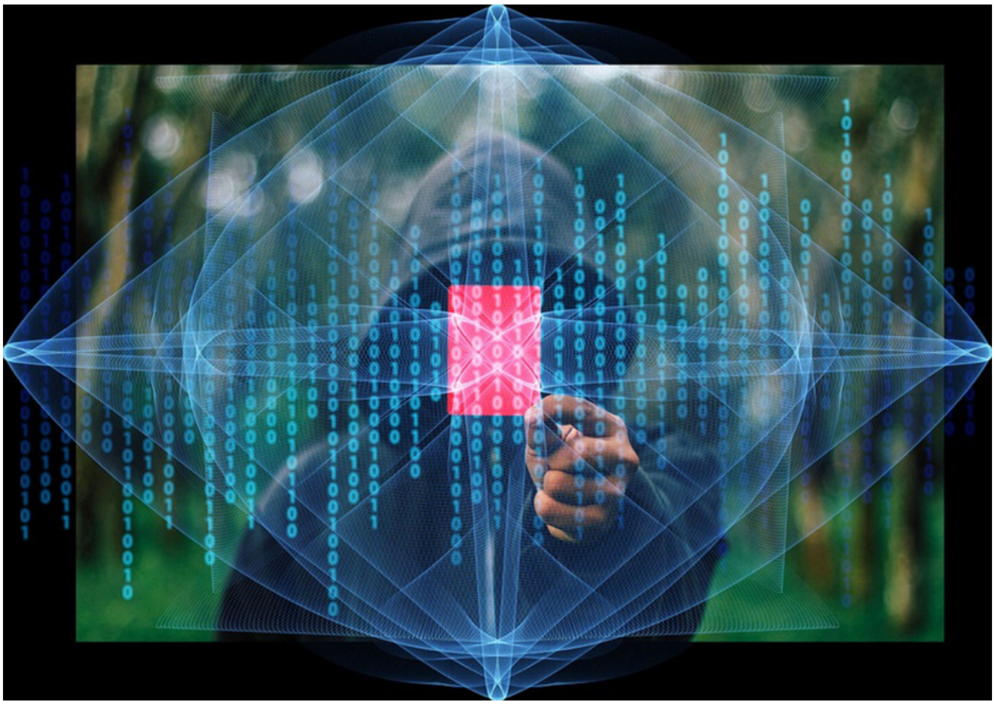
Electric cars: Policy

Lecture notes: Lecture 4.3

Data exchange

The data exchange that comes with EV charging invades the users' *privacy* and is therefore subject to legal obligations of *personal data protection*. The intensity of data exchange and therewith the risk of potential privacy breaches, increases if the charging process is subject to demand response schemes that provide flexibility to the electric power system. In order to benefit from low electricity tariffs during off-peak times and avoid high tariffs during times of peak demand, the electric vehicle user has to indicate personal preferences for when his vehicle must be ready for use. As car use times are a strong indicator for personal routines, the user must be able to trust the flexibility provider, an aggregator or any other intermediate between himself and the power system, to secure his privacy.



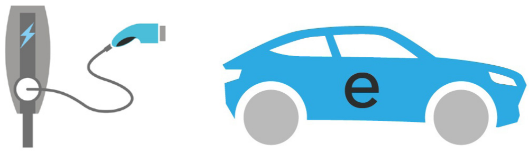
This course material is licensed under a Creative Commons Attibution-NonCommercial-ShareAlike 4.0 License.

Given the digital communications between the electric vehicle, the electricity distribution network operator, the energy service provider or other providers of charging services, the data exchange and communications scheme is vulnerable for any kind of *cyberattack*, *hacks* and *data manipulation*. That is also the case for the electric vehicle as such, which is often described as a ‘computer on wheels’, and the risks will only be aggravated for autonomous vehicles. It is evident that cybersecurity breaches in electric vehicles can have far more dramatic consequences than only privacy breaches.

Protocols

Already many of the parties in the field are working on safe and secure communication protocols. However, establishing such protocols is not easy, as the interconnected e-mobility and energy system involves many different actors. *Minimum requirements* are therefore set which much be adhered to by all parties, such as the authentication process of each charging session through a *cryptographic key*. Meanwhile, it is important that the protocols used remain open and relatively easy for new players to implement, so that a tradeoff must be made.

Interoperability between countries is also important, as electricity networks and markets are connected across national borders, especially in the European context. The European Network for Cyber Security has therefore taken a frontrunner role in setting minimum requirements for smart charging transactions. Implementation might be taking some time, however, since not all European countries use the same set of protocols for operating charging stations.



This course material is licensed under a Creative Commons Attibution-NonCommercial-ShareAlike 4.0 License.

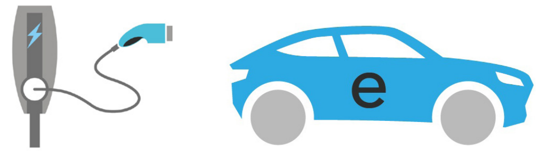
Trade-offs

The privacy and cybersecurity risks that come with the use of electric vehicles will be balanced by the user with the *private benefits* to be gained. These may be immaterial, such as a cleaner conscience for not polluting the air while driving, or material, in terms of cost savings by participating in demand response schemes, which allow the electric vehicle user to reap part of the value of flexibility services provided to the grid. Each user will weigh the various costs and benefits differently in deciding whether or not to buy an electric vehicle, and how to use it.

Unfortunately, many apps and other cases of internet-based services show that most citizens are hardly aware of the privacy they give up, or the risk of privacy breaches they expose themselves to. Especially if they are rewarded with free services or substantial discounts, many consumers seem to be willing to provide personal details, trusting the other party that the data will be handled in a secure manner.

Policy options

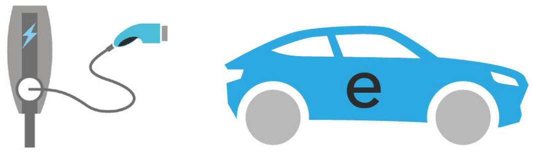
As a policy maker it is not easy to intervene in the exchange of data between an individual consumer and a company. Limiting these exchanges could bring a penalty in limiting the flexibility volume that electric vehicles could provide to support the operation of the electricity grid. Government could, however, impose certain *boundaries* on the exchange of personal data and define requirements for how, where and how long the data is stored. Furthermore, government can stage *campaigns* to raise awareness with consumers of the data they provide and the risks involved, for instance, with respect to the data that electric vehicle owners



This course material is licensed under a Creative Commons Attibution-NonCommercial-ShareAlike 4.0 License.

provide to the aggregator. As a default, aggregators should not be allowed to share personal data with other parties unless the client has given explicit consent.

In view of the cybersecurity risks and vulnerabilities involved in coupling electric vehicles as flexibility providers with the electricity grid, aggregators should be *transparent* about where, for how long and how securely they store our data. They should be transparent about the possible threats and explicitly and immediately report cybersecurity breaches and data leaks. Consumers are thus in a better position to weigh the pros and cons of participating in smart charging schemes, and to include cybersecurity performance in the choice for one aggregator or another.



This course material is licensed under a Creative Commons Attibution-NonCommercial-ShareAlike 4.0 License.