# Smart meter security: a survey

Ross Anderson, *Cambridge University* Shailendra Fuloria, *Cambridge University*

***Abstract*—Europe's smart metering initiative may be the largest engineering project ever undertaken in the region; it is significantly larger than the Channel Tunnel. The European Parliament mandated the replacement of electricity meters with new 'smart' meters by 2022, except in Member States who certify this year that it would be uneconomic. This project could cost over $100 billion, and will involve non-trivial engineering challenges, a number of which touch on security and privacy issues. In fact, it is a fascinating case study in security economics: systems are much harder to protect when incentives conflict, and smart metering exposes perverse incentives galore.**

**Nonpayment is a major concern for the utilities, whose main goal is to move defaulting customers to prepayment remotely, rather than having to roll a truck. But prior experience from countries with widespread prepayment metering suggests that it may increase technical fraud. Second, fine-grained energy consumption data reveal a lot of information about house occupants' behaviour, leading to serious privacy concerns. Third, the industry is worried that over-regulation could significantly increase the cost of the project, following negative experiences of regulatory mechanisms in smart grid projects to modernise transmission and distribution networks. Fourth, there is growing concern that centrally controllable electricity meters could be vulnerable to attack by a state-level or substate adversary. Fifth, there are serious conflicts of interest between the energy retailers who will operate the meters in most countries, the customers, and governments, which may undermine the goals of the project and which may be made worse by myopic architectural choices. Finally, the lack of a viable framework for communication between smart meters and appliances in the home will not merely lead to lack of interoperability, but could thwart competition and is likely to frustrate one of the main project goals: that future smart grids can provide demand response by tailoring the demand for energy rapidly to supply fluctuations. Without demand response, much less of our energy can come from fluctuating sources such as wind and solar. If we want to maximise the use of renewables, we will need a more incentive-compatible system architecture, and we discuss some possible first steps.**

***Index Terms*—Smart grids, smart meters, security.**

## I. Introduction

THE US Congress decided to modernise its electricity transmission and distribution network via the Energy Independence and Security Act of 2007. The American Recovery and Reinvestment Act followed this up by allocating several billion dollars for the construction of the new 'smart grid'. The European Union's response in 2009 was a Directive requiring all Member States to conduct an economic assessment of smart metering; states who find it to be beneficial must ensure full rollout by the year 2022, with 80% implementation by 2020 [4].

Ross Anderson is professor of security engineering at the Computer Laboratory, University of Cambridge, UK. email: Ross.Anderson@cl.cam.ac.uk.

Shailendra Fuloria is a PhD student at the Computer Laboratory, University of Cambridge, UK. email: Shailendra.Fuloria@cl.cam.ac.uk.

Manuscript received September 15, 2011; revised .

The current electricity infrastructure in most countries emerged in the 1930s as local generation and distribution facilities were merged into national or regional power grids. Electricity is produced by a small number of large generators, fed into a high-voltage transmission grid that transports it over long distances, then stepped down at substations into medium-voltage distribution networks until it finally reaches the customer's homes and businesses. The meter at the customer premises records consumption and the customer is billed once per billing cycle.

Smart meters are supposed to help transform the delivery network into a two-way information system which can signal price changes to the customer; the customer in turn will be able to set rules so that heavy-load appliances such as cars and dishwashers work when the electricity is cheapest. This 'demand response' will help cope with a growing number of fluctuating energy sources such as solar and wind. Even before home automation supports this at scale, it is hoped that being able to charge customers by the half-hour rather than on a simple day / night tariff will shift demand from the evening peak. Peak demand shaving will help governments meet energy security goals and will also save utilities money, as customers on day-night tariffs are typically paying less then the wholesale cost of energy during the peak.

However, smart meters also raise several serious security issues:

1) The industry is most concerned with the risk of widespread fraud if a security vulnerability is industrialised. If meter readings can be manipulated, whether by returning false readings from credit meters or forging authorisation messages to prepayment meters, this could lead to substantial losses.
2) Privacy activists are concerned at the amount of sensitive personal information that could be disclosed about households to principals able to access fine-grained consumption data.
3) Equipment suppliers argue that the move towards smart grids has led to excessive technical regulation, especially in the USA, which has pushed up equipment costs for little or no benefit. This leads to pessimism about the prospect for fixing security by mandating standards centrally.
4) The presence of a remote off switch in all electricity meters can lead to strategic vulnerability: a capable adversary could switch off the lights using a cyber attack rather than having to physically bomb power stations or transformers.
5) There are severe conflicts of interest: the main goal of governments is to cut energy use, which they hope to achieve by making energy use more salient to consumers, while in most countries the meters will be

controlled by energy retailers who want to maximise sales and who depend on confusion pricing. Meanwhile the competition authorities should worry about whether giving energy retailers vast amounts of data on customers will adversely impact competition via increased lock-in.

6) While over-regulation is a challenge, the lack of universal standards for communications between meters and appliances will prevent the benefits of demand reduction being realised, as well as reducing interoperability and competition generally. In fact many countries cannot even decide on the architecture for hooking up appliances to meters.

The rest of the paper is organised as follows. In section II, we provide a brief history of electricity fraud and show how it is a concern even today; in sections III, IV and V, we discuss challenges from privacy, strategic vulnerabilities and over-regulation. Section VI discusses the conflict of interests; section VII discusses architectural challenges; we discuss architectural options in section VIII, and finally in sections IX and X suggest architecture solutions for smart meters and home area networks.

## II. Security economics of fraud

Edison had the vision to develop electricity for the mass market, extending it from specialised applications like arc lighting into peoples' homes. In the early years, it was not a necessity but a status symbol. Utilities charged exorbitant rates – almost $5/kWh in today's terms – and exploited local monopolies wherever they could. Metering technology was primitive; after a lightning strike, meters were often demagnetised and started running faster. Utilities quietly chose not to repair them. Soon the customers began to realise that they were being ripped off, and the economic climate during the Depression further motivated unhappy customers to seek ways to cheat their utility. The 1930s saw a wave of fraud cases [7], [8], [11].

The industry responded by installing feeder meters that record the electricity supplied to a few dozen houses so it can be balanced against individual consumption; the National Electric Code was modified to have the meter installed outside the customer's house where utility staff could easily read it and inspect it for tampering; anti-tampering mechanisms included wired lead seals; and electricity theft was made a criminal offence. As for consumer protection – against unreliable meters and the bigger threat of monopolistic behaviour by the utilities – regulation was introduced; the view emerged that electricity could be most efficiently distributed as a regulated local monopoly.

The face of the metering industry was changed in the nineties by digital technology as a number of countries introduced prepayment meters based on cryptographic credit control. Prepayment meters had previously been used largely in rented accommodation and were operated by coins; coin collection was expensive, and meters were vulnerable to theft. The new meters would accept an encrypted command to dispense a certain quantity of energy. The UK acquired over a million such meters by the early 1990s, but the biggest project was in South Africa, which, with the end of apartheid embarked on an ambitious project to electrify more than 2 million homes within 5 years. Prepayment was the natural choice, given that many poor households lived in informal accommodation without a postal address – let alone a credit rating. It was found that prepayment meters reduced the overall cost of payment collection from about 10% to about 5% of the turnover. They started to be introduced in prosperous suburbs too, and South Africa now has 4 million prepayment customers.

The South African project is a particularly interesting reference point as the security problems were publicly documented [1]. Quite apart from the technical issues, the security economics was complex. There were several mutually conflicting parties – Eskom (the state-owned generation and transmission system), local electricity distributors, token vending agents, customers and equipment vendors. Many of these tried to defraud the others. Over time, people discovered interesting vulnerabilities in meters and vending systems; for example, customers in Soweto noticed that the meters would set themselves to maximum credit if the voltage fell to 160-180V. The meters had been designed in the UK and just not been tested for a brown-out. The utilities discovered the fraud only when the customers started throwing chains over the 11kV feeders to credit their meters. Customers were always trying to hack the token and refund systems; vending staff were trying to defraud the bookkeeping systems or even steal the token vending machines. One lesson was that none of the principals could be entirely trusted!

It was found that moving customers from credit to prepayment meters reduced household energy use by about 10%, a factor that was helpful in South Africa, which suffered a supply crisis over the last ten years. The same effect has been noted in Northern Ireland, which has a majority of prepayment meters, as well as in Russia and Brazil. The energy price suddenly becomes salient when people can no longer pay for electricity painlessly by monthly direct debit, but have to go to a vending station and either use their ATM card or hand over cash. Even prosperous people to whom the cost was of no real consequence would suddenly pay attention to how much they used.

Prepayment is nonetheless of interest to investor-owned utilities, because of debt management. When a credit customer fails to pay their bill, the routine is to get a court order and send a team to replace their meter with a prepayment one. This is expensive, and the utilities want smart meters mainly so that they can turn any meter into a prepayment one remotely. Normally, they would prefer that prosperous customers should continue on credit plans so that consumption does not become salient. A state-owned utility mindful of energy saving, carbon targets and supply security might well make prepayment the default.

So there may be a downside for utilities in smart meters, in that at a time of supply crunch, the state might compel everyone to move to prepayment, drastically reducing sales. There is a further downside in that a vulnerability might be industrialised, allowing customers to top up their meters at

will. Experience from the South African project suggests that this will happen more than once. Fixing a bug once a large number of devices have already been rolled out is expensive; in the Soweto case, 55,000 meters had to be physically replaced. Replacing 100 million smart meters in Europe would cost perhaps $20bn and take five years. There can also be potential strategic risks from nation-state adversaries (or even activist groups) which we'll discuss later in section IV.

## III. Privacy

Smart meters in Europe will typically record energy consumption by half-hour periods, and the fine granularity of the consumption record raises privacy concerns. Researchers have shown that it is possible to extract personal information about people living in a household by analysing meter data [6], [9].The spikes in the energy trace can often be mapped to appliances such as electric showers and cookers; by noting the time and size of the spikes, an observer can deduce how many people there are in a house, when they get up, when they eat and when they go to bed. This information could be valuable not only to Google and home appliance vendors, but to burglars and maybe even divorce lawyers.

Before we can enforce access control rules, clarity is needed on who actually owns the meter data. The energy companies believed that they should, since they owned the meter and were liable for any inaccurate billing from it. After pressure from privacy and consumer groups, some EU countries are moving towards the view that the customer shall own the data and the utility would not be able to share that data with any other party without consent. The tussle at the moment is about the granularity of the data that the customer must pass on to its supplier. Needless to say, the suppliers want everything – 48 meter readings per day – while privacy groups argue that the supplier should get only enough to calculate the bill. Thus, for example, if the tariff is 30p from 6pm till 9pm, 3p from midnight to 6am and 8p otherwise, and the customer is billed monthly, the utility should be sent only the monthly totals for these three tariff bands in a single digitally-signed message from the meter. The UK government is currently consulting on this, and has indicated a preference for the customer handing over enough data for billing, and also to other parties like the distribution network operator (DNO), which is interested in maintaining the quality of supply, and to the regulator. Such a privacy policy might be expressed as having the customer handing over only enough data for regulated functions – but the devil is in the detail as always. Should theft management be a regulated function? What about debt management? Data use by distribution network operators? For wholesale hedging? We will have to see how utility lobbying wears down ministers' resolve.

Such tussles take place against a backdrop of European human-rights, privacy and data protection law. Section 8 of the European Convention on Human Rights declares that European citizens have the right to respect for the privacy of their family life. This has got in the way of a number of centralised data-collection initiatives by various governments across Europe. In April 2009, the Dutch First Chamber declined to approve a smart metering bill on these grounds. The bill had proposed a mandatory rollout – any customer who refused to have a smart meter could be prosecuted. There were also serious objections on the proposals to collect fine-grained energy data and maintain it centrally.

Cases like this raise interesting questions on the relationship between the citizen and the state. What happens when the state's environmental preferences are stronger than those of many of its citizens, and it wants them to change their lifestyles more than they do? The previous UK Government talked about giving each customer a carbon ration card [10]. While this is no longer policy, we should not ignore the possibility of coercive policies in the future, for which smart meters could provide a perfect platform. The family on each street falling furthest short of government energy-saving targets might have its electricity cut off in the evening peak as a punishment; it might even be publicly stigmatised to add social pressure to physical discomfort.

## IV. Strategic Vulnerabilities

As we discussed earlier, utilities want central control over meters so they can deal with non-paying customers by moving them to a prepayment tariff by flicking a switch, rather than by getting a court order and then rolling a truck. however a centralised metering system with a remote off switch in every meter opens up new strategic vulnerabilities on a scale that energy companies have not faced before [3]. Modern societies are absolutely dependent on electric power; when it goes off, pretty soon almost all economic activity ceases.

In time of conflict, nation states often try to switch off an enemy's electricity using air power if they have it; even better would be a remote computer exploit. This need not involve access to the keys used by utility to sign commands to its meters; there are potentially many critical components, from software upgrade mechanisms to tariff setting and billing, that might be exploited in service-denial attacks. Modern smart meters can support as many as 200 instructions, interactions between which may give rise to API attacks. Meters may also run multiple applets, leading to software security issues. The transfer of cryptographic key material when a customer changes their electricity supplier may involve complex cryptographic protocols. All such mechanisms have the potential to expose a nation to a 'cyber-nuke' that would reduce its population to destitution. Yet utilities have no experience of defending themselves against capable motivated cyber-adversaries.

Recovery from such an attack would be painful. As a matter of national survival, the government would probably authorise any electrician or other competent person to short-circuit dead meters. Utility contractors might need to spend a year or more visiting every house to rekey or replace them. Even this would involve a massive recruitment campaign; current utility and contractor staff are not reckoned to be sufficient to replace all meters with smart meters by 2022. What arrangements might be made to resolve billing disputes in the meantime is anyone's guess.

The capable adversaries could be anyone – as well as state level actors, they might be environmental activists or

even organised crime. Chinese hackers are claimed to have reconnoitred the US electricity grid, possibly in order to identify systemic vulnerabilities that could be exploited. The Stuxnet malware is claimed to have been designed to stop the Iranian nuclear enrichment program, and to be capable of modification to attack other infrastructure targets [12]. The hazard created by the possibility of cyber-attacks can only be mitigated by a serious effort to design security into the system architecture right from the beginning.

## V. Overregulation

Yet attempts to do this so far have been less effective than one might have hoped, and have brought growing resistance from industry. The potential cybersecurity problem was realised about ten years ago when utilities started using the Internet for communications that had previously run on closed networks using proprietary protocols. These protocols have almost nothing in the way of authentication, and so once devices move on to open IP networks they become vulnerable. Anyone who knows the IP address of a sensor can read it, and similarly anyone who knows the address of an actuator can operate it. What's more, the protocol implementations can be fragile, so that a security engineer cannot even scan a network for fear of bringing down the plant it controls. Yet IP networks are so much cheaper than the proprietary networks that preceded them that a lot of control systems have moved anyway – and not just utilities but transport and even factory automation.

It was realised in the late 1990s that the information part of the electricity infrastructure was increasingly exposed to the security threats common to the IT community. The rapid growth of the security-industrial complex following 9/11 led to anxiety about cyber-threats to national infrastructure and attempts to bolt security mechanisms to the existing networks and protocols, without a proper design exercise. Numerous standards committees and regulators have fought to stake out turf in control systems security. In the world of electric power, the most influential players are often US government bodies (DHS, DoE, FERC and NERC) and NIST, although the IEC also plays a role.

NERC-CIP imposed heavy fines on utilities that failed to identify and report the protection mechanisms for their critical assets, and insisted that all critical assets have cybersecurity measures by 2009. This led to moral hazard as utilities responded by making their critical assets non-critical. For example, a generating plant with a black-start capability (the ability to start up in the absence of power from the grid) is considered critical, as we must have enough of them to restart the grid after a cascade failure. So owners of coal-fired power stations got rid of their diesel generators and thus made their assets non-critical – at the cost of making the U.S. electricity grid more fragile.

A second example comes from attitudes to technical security standards. The IT business has developed rapidly and has an entrepreneurial approach to standards; firms hack systems together and, if they succeed in the marketplace, they try to get some of the key aspects of their platform adopted formally as a standard. As a result there are often several standards to choose from, and claims of compliance are made lightly. The utility industry's approach is entirely different. This is a mature industry whose players are extremely wary of lock-in; which operates billion-dollar assets with lifetimes of decades; and where equipment malfunction can kill people. Power engineers adopt standards with religious sincerity and test products for strict compliance. Standards are now being promoted without any thought as to whether they add any value except possibly to their promoters. As a result, the recent adoption of a range of information security standards by NIST and the IEC has the potential to be a major train wreck.

For example, IEC 62351 suggested that the all GOOSE/SMV communication between Intelligent Electronic Devices (IEDs) on the local area network of a substation be digitally signed. Yet computing and verifying a digital signature on commodity hardware takes tens of milliseconds, while GOOSE messages have a latency requirement of at most 4 milliseconds [5]. In this case even the equipment vendors cried enough; industry told the standards body that compliance was just not possible. The standard's working group is now debating alternate mechanisms using message authentication codes. However a security engineer would stop and ask why we need to authenticate communications between IEDs in the same substation bay! Anyone with physical access to the LAN to wiretap the traffic will have physical access to the IEDs and could operate them manually.

Such episodes raise significant concerns about the capacity of both national and international regulators and standards bodies to do anything particularly effective about the cyber threat to control systems. If critical assets are to be protected, we had better see to it that the asset owners have sufficient incentive to do the protection themselves. This brings us to the topic of conflict of interests.

## VI. Conflict of Interests

In the USA as well as in the UK and a significant number of other EU Member States, energy retailers buy electricity from a wholesale market where prices vary greatly by time of day: in the UK power is bought and sold in half-hour slots. But customers' billing granularity is half a day rather than half an hour: they are typically on a flat tariff or have day and night rates. So when the price of electricity peaks during the late afternoon (in hot regions) or early evening (in colder ones), the suppliers lose a lot of money.

So there is a strong incentive for them to shave peak demand. In this their incentives are aligned with governments, who want to minimise reliance on coal and gas-fired plant during peak hours. Their incentives are not aligned with all users, many of whom want to consume at the peak. However, governments are also interested in reducing overall demand, which energy companies resist as they rely on sales volumes; governments also want to promote demand response, about which many retailers are at best ambivalent. So peak demand shaving is the one smart meter project goal on which all big industry players can agree.

Cutting overall demand is much harder. It exposes severe conflicts of interest where governments wish to use smart

meters to make reduce overall demand by making energy use more salient to customers. Yet the user interface is controlled by the energy companies whose profits depend on increasing sales volume and whose retail business models largely depend on confusion pricing. They are oligopolists in a market with some price competition, high fixed costs for suppliers and low switching costs for customers, so (like banks or phone companies) they bombard customers with special offers of new tariffs that give good introductory rates but then rapidly become more expensive. There have been serious tussles recently in the UK between the regulator and the retailers over price transparency, while Germany attempted to foster the growth of independent energy service companies which supply meters to customers and advise them of the best tariff available from retailers (that has been frustrated by the energy retailers buying up the service companies – something that happened in the UK too even though the service companies have less power.) So long as the big energy retailers control the user interface, a reasonable person may doubt that smart meters will ever reduce overall demand.

## VII. Architectural differences across Europe

It appears that most EU Member States will roll out smart meters by 2022, or at least undertake to try. But there is significant variability in these countries' motivation, market structure, and even their definition of what counts as a smart meter.

Italy has been the leader where Enel, the dominant utility, launched its 'Telegestore' project and has now rolled out more than 32 million so-called smart meters. These devices use narrow-band Power Line Communication (PLC) to pass on consumption data to data concentrators owned by Echelon, which then push data to Enel's enterprise servers. The meters are primarily for debt management through prepayment, and some dispute that they are really 'smart', although they do have features to support demand response and provide the customer with time-of-use tariff plans.

The adoption of smart meters and the smart grid in Germany is linked to the national policy to gradually phase out existing nuclear power stations (which has been accelerated since Fukushima) and replace them with renewables. The Energiegesetz (Energy Law) set a goal to generate at least 30% of total generation through renewables by 2020. There are plans to integrate 25GW of wind power into the infrastructure in the next 20 years. The Energiegesetz entitles every customer to choose a 'meter point operator', essentially an energy service company that gets an annual fee for installing and maintaining a meter and can also sell the customer energy management services. This was a bold attempt to introduce competition into the market, but it was disliked by equipment vendors as they sold fewer smart meters than in more centralised regimes, and (as noted above) it has been subverted by energy retailers buying up the service companies.

The UK has opted for a centralised architecture in which the government will license a monopoly Data Communications Company (DCC) to control all 52 million electricity and gas meters in the country (uniquely, Britain is mandating smart gas meters too). The idea is that the DCC will provide a control point from which data will be passed to energy retailers, DNOs, the regulator, service companies and customers, as appropriate. It is also supposed to help keep down the costs of customer switching between retailers so as to protect market competition. There are serious concerns though about whether the government is capable of setting up a complex information system that will communicate with multiple types of device in tens of millions of households in eighteen months (April 2013 – September 2014) as called for in the project plan. This is an extremely short timescale, and large government IT projects have a long history of lateness and failure.

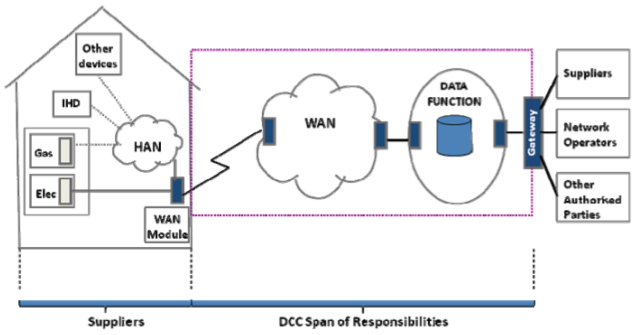


Fig. 1. UK's centralised smart metering architecture

A further architectural consideration is how one might control appliances in the home depending on the price of electricity. The idea behind demand response is that when the wind blows in Germany, the price of energy will fall, so customers in Belgium will wash their clothes, heat their water tanks and charge their cars. So appliances on a Home Area Network (HAN) must be able to communicate with the smart meter, or with the market, or with something. What's involved?

One of the arguments for a central switch such as Britain's proposed DCC is that, to promote competition, UK policy mandates that the customer be able to switch energy suppliers seamlessly without having to change the meter. So every energy supplier has to manage a fleet of all types of meter, which would make a free-for-all move to smart meters more expensive and perhaps increase the utilities' lock-in. The DCC is supposed to make this more manageable.

But this leads to the question of how the DCC will interact with the HAN. If I buy a new energy-saving washing machine, with a red button for 'wash it now' and a green button for 'wash it later when it's cheaper', do I have to register this with the government database for it to work? If I set up a startup company to manufacture such devices, do I have to persuade the government's programmers to accommodate my new invention, and perhaps hire lobbyists to lunch members of parliament to put pressure on the minister to tell them to get on with it?

## VIII. Architecture options

If the preferred architecture is one like Italy where a regulated monopoly controls most of the metering, the next

architecture decision is where appliances should be controlled. In some US systems this is done by the utility, which can switch heavy loads such as airconditioners directly at times of peak demand. As well as providing control signals, such systems typically provide the customer with a web interface to manage energy use. In a less centralised architecture, the meter would receive tariff updates from the utility, and respond with aggregate energy use for each price band in the previous billing period. The billing periods might initially be monthly, though with the introduction of demand response there would be more frequent messaging to deal with peak events. The customer might involve a third party for energy management. Centralised systems may pass over 1Mb/day of data between the meter and the utility; while the less centralised approach might involve only a few Kb per month.

Britain pioneered retail electricity market competition in the 1980s, and there are now six energy majors competing for domestic business. Customers can switch at will, and choose between a great variety of tariffs. Many other countries in Europe have followed Britain's lead. A more complex ecosystem like this might support energy service companies which advise customers on how to save energy, creating a new vector of competition with the energy retailers. Such companies in Germany and the UK have tended to operate central websites that monitor their customers' energy use and let them manage it; they get the large volumes of fine-grained consumption data and get to control high-load customer appliances, while the energy retailers only get aggregate meter readings. We remarked above that such firms have been vulnerable to takeover by the big retailers.

The third architecture option may be that currently planned in the UK, and on which the European Commission is looking with some favour. This is a centralised platform that will read meters and relay information to customers, energy retailers, energy service companies, distribution network operators and others in accordance with ministerial decisions. This architecture begs the question of where appliance control will reside.

If a government opts for central control of appliances, there will be complaints about 'Big Brother' as well as serious practical problems. The government would presumably manage help-desks to register all customer appliances, and (as noted above) an entrepreneur who comes up with a new energy-saving appliance might have to lobby for years to get the government's programmers to support it. (The UK government was originally keen on central control but has become less so as these consequences have been spelled out.)

The second possibility might be to locate control in the meter. However, this would entail reprogramming the meter regularly to accommodate new appliance types, and would create the same kind of barriers to innovation as a new appliance vendor would have to persuade three meter vendors to support it and many utilities to roll out the necessary upgrades. In the case of smart gas meters, this causes a serious problem as they have to run for ten years on a single penlight battery; each software upgrade costs the equivalent of a year's battery life. (Again, the meter vendors originally liked the idea of controlling appliances but have cooled noticeably as the consequences have become clear.)

Some industry leaders hope that appliance control will reside in the home controller – typically a device in the hallway that communicates with the meter and displays usage data to the customer. However, most of these devices are manufactured for a few Euros, and as they are battery operated they cannot realistically maintain 24/7 communications with dozens of appliances, let alone host a website for the customer to manage his home. The controllers that are designed with such a capability cost several hundred Euros and are meant for luxury rather than energy savings.

## IX. Possible way forward

One possible way forward is for each customer to have an 'Open Home Controller' (OHC), an open gateway that can connect the home area network to her electricity meter, her energy supplier, and if need be to others such as an energy service company of her choice. The OHC appears to be the missing piece of the architecture, and the Council of European Energy Regulators (CEER) has recently consulted on it. We will use their OHC terminology although the same device might be used to manage energy in small enterprises and commercial buildings.

The customer could use the OHC to set rules for her electrical appliances. It should empower the customer and help extend the benefits of smart metering from peak demand shaving to demand response. It should provide a platform for innovation with which appliance vendors, ESCOs, energy retailers and others could interact.

The next question is what sort of framework might be used to develop the OHC. Our suggestion is to look to the Apache Software Foundation for a model. Apache was put together by a number of firms to create an open web server, and the OHC is essentially a web server. Although it interfaces with meters, washing machines and car chargers rather than with electronic shopping databases, content delivery systems and card payment mechanisms, it will serve up web pages to the user and act on the commands she enters.

A key problem facing an OHC project is managing intellectual property in an industrial collaboration. If the OHC is to interface with (say) white goods from Samsung, then Samsung will want its engineers to write the device drivers or communications modules to do this properly. However if the OHC software is hosted on (say) home router hardware provided by Cisco, then Cisco will be wary of accepting code from Samsung for fear of a future demand for royalties on the intellectual property in Samsung's code. The exact same problem arose in the mid-1990s with the early web servers and has been solved by the Apache license, under which contributors agree to a project agree not to sue users for infringing any of their intellectual property thereby. The Apache framework also incorporates a lot of experience about the governance of such collaborations.

To be more concrete, our suggestion is that the OHC be a software suite that can run on any suitable platform – a meter, a network gateway, a home router or even a central server farm, whether operated by an energy retailer, and energy service company or a government. It would communicate with the

home area network and also give the customer a web interface to manage usage. It would be communally maintained by the industry – Itron will write the device drivers for it to speak to Itron meters, LG will write the communications libraries needed to talk to LG appliances, car makers will write the code needed to control vehicle charging, and so on. An open platform can help create an ecosystem in which innovation can thrive and all can benefit: appliance vendors can ensure their new products will interoperate with what their customers have already, market makers can experiment with new demand-response tariffs on which appliances will act, and the energy companies, who maintain meters, will have most of the software engineering done for them.

The OHC might support scripting with which energy companies can implement tariff description languages, and energy services firms can provide management routines. These firms have found that local management is important: many users' internet connectivity isn't anything like reliable enough for 24x7 control of critical domestic appliances. A local OHC can not only increase dependability but also assuage many of the privacy worries, as the user might keep the fine-grained power trace under her control and upload only the aggregated data need for billing.

There is one small problem though. The BSI (the German federal office for information security) has issued a 'protection profile for the gateway of a smart metering system' which specifies that the gateway should be a trusted system, sufficiently hardened to be able to fully mediate communications between the utility and the meter, with a hardware security module containing keys to sign meter readings and with all its software upgrades subject to stringent evaluation. This means that it cannot be an open platform to support innovation; it may even make it too expensive to deploy at scale.

Instead, we believe that the meter readings should be signed in the meter and transmitted unaltered by the gateway to the utility. This way, the gateway does not have to be trusted by the utility; it merely advises the customer of his energy use and lets him control local appliances in response to online price signals. Of course, the home gateway must not be a mechanism whereby an attacker can 'turn off the lights'; but rather than weaponising the gateway hardware and software, we should simply provide for a manual override. If a gang, a terrorist group or even a hostile state writes malware that causes millions of people's home gateways to switch off appliances, they should be able to physically switch off the gateway until the vendor can ship an upgrade. Making it a non-critical component will make it much less of a target.

## X. Conclusion

Smart metering is the largest engineering project ever undertaken in Europe. The costs in the UK are currently estimated at £11bn but seem likely to overrun, so it appears likely that the cost of replacing all electricity meters in all 27 Member States will exceed $100bn. Yet very little attention has been paid to the significant security and privacy problems. Will EU citizens suffer privacy invasion if our household energy use patterns become widely available? More brutally, could an attacker switch off the lights?

The biggest question, though, is whether the project will work at all, in the sense of bringing enough energy savings to pay for itself. As things are planned at present, the proposed architecture leads to conflicts of interest; while smart meters might lead to some peak demand shaving via half-hourly billing, it does not look like they can deliver demand response on the scale needed to accommodate future large-scale deployment of renewables such as wind and solar.

We argue that the missing architectural link is the development of an open home gateway which will enable the home network to talk to the market so that, for example, if the windmills are turning in Germany, a household in Belgium can turn on their washing machine and start to charge their car. The best way to develop this would be using the Apache model to make the gateway am open platform for innovation. Yet that will be less likely to happen if the home gateway is required to be a 'secure' device, as the German government argues; we argue that the security should be end-to-end (meter to utility) instead. It may seem a paradox, but in order to secure Europe's electricity supply over the next thirty years, one of the key components may need to be less secure so it can be more open and our electricity supply can be more dependable.

## Acknowledgment

The second author's research is funded by ABB. The contents of this article do not necessarily express the views of ABB.

## References

[1] R Anderson, SJ Bezuidenhoudt, 'On the Reliability of Electronic Payment Systems' in *IEEE Transactions on Software Engineering* vol 22 no 5 (May 1996) pp 294–301, at http://www.cl.cam.ac.uk/~rja14/Papers/prepay-meters.pdf

[2] R Anderson, *'Security Engineering – A Guide to building Dependable Distributed Systems'*, Second edition, Wiley 2008

[3] R Anderson, S Fuloria, "Who controls the off switch?" in *IEEE conference on Smart Grid Communications*, NIST, Maryland, USA, Oct 2010

[4] European Parliament and Council, *'Directive 2009/72/EC concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC'*

[5] S Fuloria, R Anderson, K McGrath, K Hansen, F Alvarez, 'The Protection of Substation Communications' in *SCADA Security Scientific Symposium*, Miami, USA, Jan 2010

[6] GW Hart, "Nonintrusive Appliance Load Monitoring," in *Proceedings of the IEEE*, Dec 1992 pp 1870–1891

[7] Los Angeles Times archive, 'Rancher Pleads Guilt in Theft of Electricity', Oct 30, 1931.

[8] The Montreal Gazette, 'Electricity theft charged in court', Mar 22, 1934.

[9] C Laughman, K Lee, R Cox, S Shaw, S Leeb, L Norford, P Armstrong, "Power Signature Analysis" in *IEEE Power and Energy Magazine* March/April 2003 pp 56–63

[10] P Wintour, "Miliband plans carbon trading 'credit cards' for everyone", in *The Guardian* Dec 11 2006; at http://www.guardian.co.uk/politics/2006/dec/11/uk.greenpolitics

[11] The Palm Beach Post, 'Theft of electricity is charged in court', Jan 18, 1933.

[12] Nicolas Falliere et. al, 'W32.Stuxnet Dossier', *Symantec Corporate Publication*, 2010 at http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf