Who controls the off switch?

Ross Anderson
Computer Laboratory
15 JJ Thomson Avenue
Cambridge University, England
Ross.Anderson@cl.cam.ac.uk

Shailendra Fuloria
Computer Laboratory
JJ Thomson Avenue
Cambridge University, England
Shailendra.Fuloria@cl.cam.ac.uk

***Abstract*—We're about to acquire a significant new cyber-vulnerability. The world's energy utilities are starting to install hundreds of millions of 'smart meters' which contain a remote off switch. Its main purpose is to ensure that customers who default on their payments can be switched remotely to a prepay tariff; secondary purposes include supporting interruptible tariffs and implementing rolling power cuts at times of supply shortage.**

The off switch creates information security problems of a kind, and on a scale, that the energy companies have not had to face before. From the viewpoint of a cyber attacker – whether a hostile government agency, a terrorist organisation or even a militant environmental group – the ideal attack on a target country is to interrupt its citizens' electricity supply. This is the cyber equivalent of a nuclear strike; when electricity stops, then pretty soon everything else does too. Until now, the only plausible ways to do that involved attacks on critical generation, transmission and distribution assets, which are increasingly well defended.

Smart meters change the game. The combination of commands that will cause meters to interrupt the supply, of applets and software upgrades that run in the meters, and of cryptographic keys that are used to authenticate these commands and software changes, create a new strategic vulnerability, which we discuss in this paper.

I. Introduction

Both the USA and Europe are introducing smart meters on a huge scale. The construction of a smart grid became US policy with the Energy Independence and Security Act of 2007, and President Obama allocated $4.5bn to its development as the headline measure when he signed the American Recovery and Reinvestment Act [12]: it is considered "key to national efforts to further energy independence and curb greenhouse gas emissions" [15] (which describes the total spending as $11bn). The European Parliament followed with a 2009 law mandating smart metering by 2022 [8].

Traditional electricity (and gas) meters measure energy use on either a simple tariff or a two-part (day and night) basis. Smart meters provide much more fine-grained control; a typical device supports half-hourly measurement, so that a utility can charge different rates for night, day, shoulder and peak periods. Some of the business case for smart metering comes from the prospect of peak demand shaving. However, a feature of even more interest to energy retailers is that the supply can be interrupted remotely. At present, customers who fall into arrears are typically fitted with prepayment meters, but this can be an expensive process involving court orders, home visits and in some areas physical risk to staff. Once all meters are 'smart' they will be support both credit and prepayment tariffs; defaulting customers will simply be cut off remotely and told to buy units online or from a local shop in future.

There has also been growing concern about the potential vulnerability of power grids and other critical infrastructure to cyber attack. Electricity generation and distribution is arguably the most critical of all; when it stops, so, in short order, does everything else. Blackouts following ice storms, hurricanes and the like are usually resolved within a few days, but a longer loss of service causes an almost complete economic shutdown. For example, a six-week failure of the power supply to the central business district of Auckland, New Zealand, in 1996 led to 60,000 of the 74,000 employees having to work from home or from relocated offices, while most of the area's 6,000 apartment dwellers moved out for the duration [9]. And perhaps the worst terrorist 'near miss' in recent history was an IRA attempt in 1996 to blow up transformers at three of the big substations that supply London [11]. This failed because a senior IRA commander was a British agent; had it been successful it would have wrecked electricity supplies to much of London for many months, blacking out millions of people and businesses responsible for maybe a third of Britain's GDP. Finally, attacks on electricity transmission and distribution have been a standard US tactic in wars from Serbia to Iraq. (In fact, the Iraq insurgency after 2003 was fuelled by delays in restoring the power supply, which left millions of Iraqis sweltering in the summer heat with no air conditioning.)

So modern societies absolutely require a dependable electricity supply, and this supply is becoming computerised like everything else. Over the last ten years, control system engineers have begun to realise that moving from closed, proprietary networks to open IP networks may save money but it can certainly open up vulnerabilities. The protocols commonly used in industrial control don't come with authentication, so in principle anyone who can talk to a sensor can read it, and anyone who can talk to an actuator can operate it. Over the last few years, control-systems security has received attention, with engineers developing ways for the energy industry to protect the central generation, transmission and distribution assets. In the USA, the North American Electricity Reliability Council (NERC) ordered utilities to secure critical assets by 2009, or face fines. The Energy Independence and Security Act of 2007 had already given NIST "primary responsibility to coordinate development of a framework that includes protocols and model

standards for information management to achieve interoperability of smart grid devices and systems", and NIST's 'Framework and Roadmap for Smart Grid Interoperability Standards' [15] sets out to identify existing standards relevant for the smart grid in the first phase, then identify gaps and establish priorities to devise new standards to fill them

So far so good. This paper argues that it will not be enough to protect the grid if an attacker can send a command to millions of homes instructing their meters to permanently switch off the supply. How can we ensure that remote control does not become a remote vulnerability? In this paper we start to discuss the options.

II. Background

Electricity supply is rapidly becoming more complex and variable. The USA may move from 3,000 utilities with 30,000 generators in 2004 to over 200,000 generators in 2014 and ultimately to millions of generators as individuals operate wind and solar assets and sell the surplus to the grid. Many renewable power sources are variable; while tidal power is predictable, solar power is less so and wind power much less so.

So it is becoming ever more important to improve demand response. Electricity demand peaks in the early evening; in many markets, utilities lose money then as their regulated prices to consumers are lower than open market prices. The business pressure for peak demand shaving has led to mechanisms that enable consumers to adapt usage and may also control major loads. For example, Southern California Edison offers its customers a discount if they consent to have their air-conditioners switched off for 40 minutes in the hour during peak demand [17]. In Hungary each household has two power meters, one for appliances under the customer's complete control and the second for water and space heating. The customer gets eight hours' cheap heat a day, but the timing is under the control of the utility. And a future with millions of electric vehicles will dramatically increase the opportunity for demand modulation; motorists will program their cars to recharge when electricity is cheap.

A. Metering

At present a typical electricity meter offers only two rates – a cheap rate for night-time and a standard rate for the day.But wholesale electricity prices vary by the hour, half-hour or quarter-hour, depending on the market. A dislocation between wholesale and retail prices can have serious effects; in California such a dislocation caused serious power shortages [19], and more generally it will be difficult to alter consumer behaviour in the direction of energy savings unless consumers are more exposed to market prices than at present. This has led to smart metering initiatives in both the USA and Europe that aim at metering end use of energy with the same time resolution as in wholesale markets – in the UK, by 48 half-hour segments each day. Europe has now passed a law requiring all Member States to introduce smart meters, with 80% adoption by 2020 and 100% by 2022 [8].

Most users will not want to look at their meter to check the current price before deciding whether to operate appliances, so the customer will be provided with an automatic means of setting energy policy and having appliances turned on and off. Proposed smart meter standards thus envisage that meters will have not only the traditional metrology component, but also data communications to both the utility and the home. The meter will get from the utility data on energy prices, both current and future (in the UK, for example, power is auctioned and prices set each day for the following day's 48 half-hour slots). Finally, there will be a control function operated by the customer to monitor usage and set energy policy. Some of this control function may be dispersed to appliances; for example, a dishwasher of the future may have two start buttons, a red one saying 'do it now' and a green one saying 'do it when it's cheap'. But some of it will be automated.

One big policy question is where. If control lies with the energy company, there will be issues with data volumes, and with privacy [14]. Studies in [10], [13] show that it is possible to identify some of the appliances in use through load monitoring. So it might be possible to deduce facts about the customers' lifestyle – when they eat, which TV programs they watch, and when they take a shower. The Dutch courts have already found fine-grained central data collection by smart meters to be an unacceptable infringement of citizens' privacy and security, following opposition by the Dutch consumers' association [6]. 'Smart meter security' has so far focussed on these privacy issues, plus to a lesser extent on the possibility of fraud. In this paper, however, we're concerned with denial-of-service attacks. Our main focus is not whether the customer's air-conditioner can be switched on and off by an attacker (though that would certainly be a nuisance) but whether her electricity supply supply can be.

B. Prepayment

Prepayment meters are very widely used in less developed countries and for low-income customers in developed countries (for a description of existing prepayment metering systems, see [3]). In Europe, at least, access to utilities is considered to be a human right; defaulters cannot be cut off but merely moved to a prepayment tariff. At present, this is an expensive and often difficult process involving court orders, home visits, and in some neighbourhoods the possibility of threats or violence to energy company staff. Smart meters will fix this, as they can be switched remotely from credit to prepayment tariffs. Remote switch-off and switch-on can also help in places like university towns where short property rentals mean frequently changing customers. Such revenue protection concerns can be as strong a selling point as peak demand shaving for energy companies. The country with the greatest density of smart meters is Italy, where the utility ENEL has installed over 30 million of them; there, switching defaulters to prepay became easy, leading to large operational cost savings.

Non-payment isn't the only reason for a remote switch-off to be authorised. While smart meters in the USA are

owned and controlled by the utility, Britain's Department of Energy and Climate Change (DECC) has decided that meter communications will be centralised at a government head-end and then relayed to the utilities [16]. DECC will be able to monitor use, set targets, and even enforce power cuts on a per-household basis. It's also envisaged that Britain may face a supply crunch after 2016, after a number of old coal and nuclear stations come to the end of their design lives; it may be argued that fine-grained central control will enable any required power cuts could be organised with greater fairness. (At present, households on the same feeders as essential services such as doctors' surgeries and police stations would escape their share of darkness.) It hasn't escaped people's attention that this mechanism could be used to enforce energy savings: families who failed to meet a government savings target might be blacked out in the early evening as a punishment. While there is no immediate threat of this, its future possibility is likely to make many people uneasy. Thus the control of the off switch may in some countries carry a political charge as well as being a matter of revenue protection, peak load shedding and national security.

In a country with less central control, power cuts could still be an issue. If demand management is left to the energy companies, then smart meters should lead to significant time-of-day price variation. At present, UK retail energy prices might be 7p at night and 11p during the day; wholesale prices are more like 5p night, 10p day and 15p peak (typical US prices involve similar numbers of cents). In the one country (Japan) where three-times price variation is already transmitted to end customers, they have started to invest in batteries. And once many customers have batteries, the energy companies will probably start offering interruptible tariffs to retail users as well as industrial ones. Customers who need a high-quality supply will pay for it; those who can tolerate a daily two-hour interruption will pay less. Power cuts won't black out a whole neighbourhood any more, but just those premises with customers on particular tariffs. There will be even more incentives to arbitrage, to cheat, and to hack.

III. Attacks

One nightmare scenario is that a country installs tens of millions of smart meters, controlled from a single head-end, and without a proper design exercise to identify and prevent possible attacks[1]. In due course an attacker takes over the head-end and sends a message to all meters instructing them to interrupt the supply. The interruption is made permanent by (for example) also sending out a commend to meters to change their crypto keys to some new value that may be known only to the attacker (or not known at all). The blackout hits tens of millions of households; resumption is slow as electricians – and householders – physically connect jump-leads across their meters. Millions of homes are left without power for days and in some cases for weeks; people die of hypothermia, from failure of medical equipment, or from electrocution as they handle live mains without the necessary training. The energy industry's revenue model is wrecked by the destruction of the metering infrastructure, and replacing tens of millions of meters takes years. Economic activity is disrupted; energy company CEOs are sacked, and government ministers resign.

As for what sort of organisation or individual might launch such an attack, we know that Chinese state bodies and their auxiliaries have done extensive reconnaissance of Western energy networks [18], and the techniques they used to take over machines in the Dalai Lama's private office during the Peking Olympics have been documented [4]. So it is quite possible that a nation state might launch such an attack during a time of international tension. A second possibility is a terrorist organisation. A third possibility could be environmental activists; many idealistic young people are concerned with global warming and the failure of the Copenhagen climate talks, and some have already clashed violently with police at the sites of proposed new power stations. A further possibility is a criminal, who switches off a number of an energy company's meters and threatens widespread havoc unless a ransom is paid. This criminal might be an outsider, perhaps an online crime gang, or simply a disgruntled former employee.

Yet another angle is the possibility of criminal energy theft; even with existing prepayment meter systems, there have been cases where criminals managed to steal a token vending station and set up selling energy tokens at a discount [3]. If the off switch is not secure, criminals might switch prepay meters back to being credit meters. For this reason, we can't just solve the service-denial problem by giving everyone an emergency 'on' switch.

IV. Metering Architecture

In what follows we'll discuss a likely metering architecture. Britain is a good working example, having pioneered the regulatory regime now being spread to other European countries [7]. Britain has six major energy suppliers who buy electricity in wholesale markets, transmit it over a shared distribution network, and sell it to retail customers. Customers have the right to switch supplier; when this happens, ownership of the customer's meter passes from the old supplier to the new one. There are three main meter suppliers and thus three main product lines of electricity meter (as well as a further three families of gas meter). It is policy that new companies should be able to enter the market and compete both as energy suppliers and as meter vendors.

A. Control mechanisms

The communications between the meter and the head-end will be protected using cryptography. The details of the protocols are still being worked on; for gas meters, at least, it seems likely that public-key operations will be used only for initial key establishment, perhaps when a meter passes from one energy company to another, and thereafter shared keys will

[1]This is what's presently happening in the UK, where even meter vendor technical staff and the Royal Academy of Engineering were excluded from meetings to settle the specification of the smart metering programme.

be used to authenticate messages[2]. There is no such constraint on electricity meters.

Let's assume without loss of generality that when an energy supplier wants to move the customer to prepayment mode. It sends a signed encrypted message to the meter containing a shared key that will be used to switch the meter off and on again. In standard protocol notation, if the energy supplier's public signature verification key is $KES1$, its private signature key is $KES1^{-1}$ and the meter's public encryption key is $KM1$, we have

$$ES1 \longrightarrow M1 : \{ES1, M1, Kppm\}_{KES1^{-1}}$$

Thereafter the energy supplier would send switch-off messages, and switch-back-on messages, authenticated using Kppm:

$$ES1 \longrightarrow M1 : \{OFF\}_{Kppm}$$

$$ES1 \longrightarrow M1 : \{ON, 100kWh\}_{Kppm}$$

We note in passing that it would be prudent for regulators to demand that the meter notify the user of a proposed move to a prepayment tariff and observe a time delay of say fourteen days. That would not only be good service practice but also ensure that a service-denial attack that used the prepayment facility would become obvious some days before it would actually take effect. It is also common practice for prepayment meters to have a 'reserve tank' facility whereby a customer can get an 'empty' meter to deliver an extra 20kWh or so by pressing a red button, to tide things over until she can buy more credit.

There would remain, however, three problems. First, there are likely to be other switch-off commands, e.g. for the purposes of load-shedding during a supply crunch. Perhaps these won't require fourteen days' notice for deployment; in a time of scarcity a set of switch-off keys might be universally deployed already. There may also be commands that are functionally equivalent to switch-off commands, such as a command to change the tariff to a very high value that would rapidly exhaust the available credit. Second, if you do detect a service-denial attack in progress, what do you do about it? And third, how do you recover from a compromise of the energy company signing key $KES1$?

B. Shared control

Engineers who design nuclear command and control systems have come up with a number of mechanisms for shared control. It is not sufficient to have the nuclear firing codes carried around in a briefcase by one of the President's aides; that leaves the prospect that a decapitation attack could leave the arsenal intact but useless. So there are mechanisms to pass command rapidly to the President's successors in office; and in the chaos of war, some sets of weapons can be used on the authority of various combinations of more junior officers and officials. The mechanisms are described, for example, in [2].

In the smart metering application, we are faced with the dual problem. How do we ensure that, in the event of attack, meters that have been turned off by an attacker can be turned back on again? Suppose for example that an environmental activist has hacked the control system of energy company 1 and now controls $KES1$. He has sent, or threatens to send, switch-off messages to the meters of its four million customers. What should the company, or the regulator, or the industry, or the government, do?

Applying the shared-control approach, we might initially suggest that each meter have baked into it the public signature-verification keys of each of the six energy companies. Thus if any company's key become compromised, its customers could simply register with one of the others, who would send each new customer's meter a signed message informing it of its new control relationship and authorising it to supply electricity. That would have the advantage of aligning incentives; a company that lost its key would lose all or at least many of its customers.

But things are not quite so straightforward in practice. If the second company's key $KES2$ can be used to take over the first company's meters in the event that the first company's key is compromised, in order to recover from an attack, then what is to stop the same mechanism being used to spread an attack in the event that it's $KES2$ which is compromised rather than $KES1$? One possibility is to break symmetry by requiring more than one company to cooperate to take over a meter; another option is a combination of a company plus the regulator. Such mechanisms can also provide rate control; for example, the regulator might embed her key in equipment that would normally allow only a few thousand account takeovers per day.

Another possible approach is key backup. Microsoft, for example, installs a default signature verification key in Windows, so that PCs can authenticate software updates and the like; there's also a backup verification key, whose corresponding signing key is kept offline in a vault. If the regular signing key is compromised, the backup key can be used to override it. But this may not be enough. Our environmental activist perhaps got a job at the energy company rather than simply hacking its control system and stealing the key. What then?

However, using a static set of company signing keys would not be sufficient. First, as a matter of policy, there should be free entry to the energy market, and baking incumbents' keys into meters would preclude this. So how should we add new energy companies, and remove companies that have failed (whether due to key compromise, or due to bankruptcy or takeover)?

C. PKI approaches

This gets us into the field of public-key infrastructure (PKI). Perhaps the regulator on each country signs the energy companies' keys, and the meters contain the regulator's verification key so that they can check these certificates. In this way, the

[2]The constraint is energy; gas meters must function for 15 years on a single AA battery and so use very low-power processors, which might take a minute to perform an elliptic curve encryption or signature.

regulator can add new energy companies or keys as needed, and remove keys if they're compromised or if an energy company ceases trading.

A second possibility, inspired by the shared-control research tradition, is that any three energy companies might be able to admit a new member to their club, by signing the new entrant's key. However, they have no commercial incentive to do so, and would presumably drag their heels. There is also the problem of what happens if all the energy companies' keys are compromised simultaneously.

An alternative approach is for the meter vendors to perform this function: each vendor embeds its own verification key in its own meter and then signs the keys of the energy companies operating in that market. The alert reader at this point will of course ask: what happens if the hackers get the regulator's key, or the meter vendor's key? (This is one of the ways in which all the suppliers' keys could be compromised at once – via false certificates signed by a compromised vendor key.) Of course, a prudent authority will bake in not one key but two, as Microsoft did; and it may be prudent for a regulator's key to act as backup to a vendor's key. Of course the chain has to stop somewhere, but there are some interesting questions. One of these is liability. Will the meter vendors be keen to assume the responsibility? For that matter, will the regulator be as keen to control everything if it acquires liability along with power?

D. Software upgrades

One strong argument in favour of vendors providing the root key for their meters is that they need to embed a signature verification key in their meters anyway for software upgrades. Upgrades are a requirement, as the metering infrastructure is being built out before the specification is settled. A typical meter has a central metrology unit that's calibrated in the factory and cannot be upgraded; this provides read-only access to a database of the last six months' readings to an executive unit which is upgradeable and which communicates both with the head-end and with domestic devices. This unit is different in different national markets (because of differing communications methods and standards); it also contains the cryptography. In addition, the executive unit may contain a virtual machine to execute applets that implement a particular tariff. These applets will also be signed; they will be smaller, and may be changed much more frequently, than the platform software itself.

The denial-of-service hazards here are legion. It's been known for software upgrades to disable computers, and while an ISP can recover from 100 bricked routers by having technicians spend a few hours reflashing and rebooting them, an equivalent problem with 8 million electricity meters would have catastrophic consequences. A lot of thought will have to go into procedures for testing, backup, rollback, key recovery and manual override. Software attacks or just failures might affect applets as well as the platform software; if a new tariff applet gets into an infinite loop, how will the customer – or the energy company – recover?

E. Possible application architecture

It's not clear that the applets used to implement tariffs need a full programming language such as java, with the attendant risks of infinite loops and other unpredictable behaviour. One possibility is to develop a restricted tariff description language which limits the damage that can be done by error or malice. At present, a typical meter consists of a factory-sealed tamper-resistant metrology unit which exports a database of half-hourly energy usage readings for the previous six months. The tariff is a sum of nonlinear functions computed on these data, for example "15p per kWh from 6pm to 9pm weekdays up to a 2kW limit, then 50p per kWh". This is computed in a separate communications unit sealed by the energy company; the engine outputs not just tariff readings but also usage readings for balancing by the distributor. The tariff and usage readings must be consistent and not misleading from the viewpoint of both customer and distributor. The design of such a language is not trivial, but we believe it is doable [5].

The second aspect of the application architecture that bears on the meter's security against service-denial attacks relates to active demand management. The move to variable and fluctuating energy sources makes it necessary for energy companies to manage demand more actively. One interesting discovery is that in Japan, where the time-of-day price variation is now a factor of three in retail as in wholesale electricity markets, households are installing batteries so they can buy electricity at night when it's much cheaper. Smart meters should bring retail and wholesale prices into rough alignment, so we can expect to see domestic power storage systems becoming common all across Europe. Then energy companies will surely offer households the interruptible tariffs that they currently sell to businesses such as cement factories. If the wind falls in Yorkshire and clouds cover the sun at the solar-thermal plants in Spain, the companies will shed load by telling cement factories to switch off their kilns and domestic customers to switch in their batteries.

The key observation here is that load-shedding should not involve compulsory remote switch-off. If it does, households and businesses will need their backup power supplies to be engineered to the standards of the uninterruptible power supplies used in data centres, which would be expensive. So rather than saying '13 Acacia Avenue, we're cutting you off at 8pm for two hours', the company should say '13 Acacia Avenue, we're invoking the interruptible tariff clause and putting your rate up from 15p/kWh to 150p/kWh for two hours starting at 8pm.' This way, householders can use the main supply as a backup to their backup supplies, which in turn can be much cheaper. In addition, the opportunity for an attacker to abuse the remote off switch is largely removed.

F. Possible key architecture

The next issue is how the key infrastructure might work. As a starter, we suggest that each meter vendor embed two signature verification keys in each meter they ship: their own vendor key KVi plus a vendor backup key KBi which would be different for each jurisdiction. In normal times, the

vendor will provide a set of certificates enabling its meters to identify and use the energy companies' keys as well as to authenticate genuine software changes. If the vendor's signing key is compromised, the vendor backup key is used to certify such of the energy companies's keys as are still useable, and to certify a new vendor key once the vendor has recovered from the compromise.

The management of backup keys is not straightforward; designers really need to consider the problems identified during the debate on key escrow in the 1990s [1]. There will have to be a robust governance arrangement – perhaps the backup key will be kept in a bank vault, and made available only on application by the energy regulator to a court; and there will also have to be a sound design and extensive testing of the implementations. This will have to take account of all the abuse cases we can think of. What happens, for example, if an attacker who compromises a vendor key falsely certifies an extra energy company key under his control? And what if the attacker gets a nation's gas meters to perform thousands of public-key cryptographic operations until their batteries run flat? Designing crypto protocols to resist resource exhaustion attacks is non-trivial. So we strongly recommend that both the design and the test plan be published and subjected to open peer review, so that the maximum number of eyeballs can be brought to bear and the probability of missing a significant attack can be made as low as possible.

The role of the standards body may vary by country. In the UK, it is a requirement that all of the energy companies be able to work with all the types of meter, so that customers can continue to move easily from one supplier to another. Since the Electricity Directive, the same will apply more or less in other European countries, as energy markets are opened up. Thus in Europe the standards bodies might eventually specify the control and recovery mechanisms. We are slightly sceptical about this; if there are in effect eighteen different systems (each being a combination of a meter platform and an energy company's application) then the resulting diversity might help limit the scope of errors and attacks. In the USA, with its tradition of local monopolies regulated as to price and service level, perhaps the regulator will be less intrusive. However in both continents we would hope to see regulators and standards bodies insisting that vendors and energy companies make a safety case for the systems they propose to deploy; this safety case should include detailed analysis of all possible service-denial attacks, together with the mechanisms designed to mitigate them and recover from them.

V. Conclusions

Electricity and gas supplies might be disrupted on a massive scale by failures of smart meters, whether as a result of cyber-attack or simply from software errors. The introduction of hundreds of millions of these meters in North America and Europe over the next ten years, each containing a remotely commanded off switch, remote software upgrade and complex functionality, creates a shocking vulnerability. An attacker who takes over the control facility or who takes over the meters directly could create widespread blackouts; a software bug could do the same.

Regulators such as NIST and Ofgem have started to recognise this problem. There are no agreed solutions as yet; in this paper we've discussed the options. Possible strategies include shared control, as used in nuclear command and control; backup keys as used in Microsoft Windows; rate-limiting mechanisms to bound the scale of an attack; and local-override features to mitigate its effects. It's important that these issues are discussed now, before large-scale roll-out creates large-scale vulnerabilities in too many utility areas (and indeed national markets). We commend the problem to NIST's standardisation process and to European regulators.

Acknowledgement

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

References

[1] H Abelson et al., "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption" in *World Wide Web Journal* v 2 no 3 (Summer 1997) pp 241–257

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

[3] 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

[4] R Anderson, S Nagaraja, *'The snooping dragon: social-malware surveillance of the Tibetan movement'*, University of Cambridge technical report UCAM-CL-TR-746, March 2009

[5] R Anderson, S Fuloria, "On the security economics of electricity metering", *Workshop on the Economics of Information Security* (2010), at http://www.cl.cam.ac.uk/~rja14/Papers/meters-weis.pdf

[6] C Cuipers, BJ Koops, "Het wetsvoorstel 'slimme meters': een privacy-toets op basis van art. 8 EVRM", Universiteit van Tilburg 2008

[7] Department of Energy and Climate Change, *'Towards a smarter future'*, at http://www.decc.gov.uk/en/content/cms/consultations/smart_metering/smart_metering.aspx

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

[9] P Gutmann, "Auckland's Power Outage, or Auckland – Your Y2K Test Site", at www.cs.auckland.ac.nz/~pgut001/misc/mercury.txt

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

[11] W Hope, "Britain Convicts 6 of Plot to Black Out London", New York Times, July 3 1997

[12] M LaMonica, "Obama signs stimulus plan, touts clean energy", CNN, Feb 7 2009, at http://news.cnet.com/8301-11128_3-10165605-54.html

[13] 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

[14] MA Lisowich, S Wicker, "Privacy Concerns in Upcoming Residential and Commercial Demand-Response Systems", in *IEEE Proceedings on Power Systems* v 1 no 1 (Mar 2008)

[15] NIST, *Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft)*, Sep 2009

[16] Office of Gas and Electricity Maarkets, "Smart Metering", at http://www.ofgem.gov.uk/e-serve/sm/Pages/sm.aspx

[17] Southern California Edison: "Rebates and Savings", at http://www.sce.com/residential/rebates-savings/rebates-savings.htm

[18] *'2008 REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION'*, 110th Congress, Nov 2008

[19] FA Wolak, "Diagnosing the California Electricity Crisis", The Energy Foundation (2003); at www.ef.org/documents/CA_crisis_Wolak.pdf