**Chapter 14**

**Monitoring and Metering**

**Management is that for which there is no algorithm. Where there is**

**an algorithm, it’s administration.**

– ROGER NEEDHAM

**The market is not an invention of capitalism. It has existed for**

**centuries. It is an invention of civilization.**

– MIKHAIL GORBACHEV

**14.1** **Introduction**

In addition to the burglar alarms we discussed in the last chapter, your home will  
 likely have a number of other monitoring devices: utility meters, baby monitors,  
 smoke detectors, exercise equipment, health trackers and connected appliances.  
 You may also buy value online for some metering systems, from a prepayment  
 utility meter in your home through prepaid postage labels. An increasing num-  
 ber of systems are concerned with monitoring and metering human activities  
 and indeed the natural environment too. They go back a long way. James

Watt, the steam engine pioneer, didn’t just sell engines; he licensed his patents  
 using a sealed counter that measured the number of revolutions an engine had  
 made. His inspectors read these from time to time and billed the customer for  
 royalties.

Electronic systems that use cryptography and tamper-resistance have dis-

placed most of the older mechanical systems and opened up all sorts of new  
 applications. Ticketing is huge, from transport tickets through sports events to  
 coupons; my case study for ticketing is the prepayment meters used for gas and  
 electricity. Then I’ll turn to vehicle systems. The most familiar of these may be  
 taxi meters but as these are being replaced by phone apps, I’ll mainly discuss  
 tachographs – devices used in Europe and Australia to record the speed and  
 working hours of truck and coach drivers, and in the USA to record the comings  
 and goings of bank trucks. My third case study is the curfew tags used in the  
 USA to monitor criminal suspects before trial and in the UK for parolees after  
 release. My fourth is the electronic postage meters used to frank letters and

457

*14.2. PREPAYMENT METERS*

packages.

Many of these new applications follow the traditional IT industry mantra

of ‘ship it Tuesday and get it right by version 3’. We do have the beginnings  
 of general standards for IoT security, such as the draft ETSI standard EN 303  
 645 which lays out the usual motherhood-and-apple-pie stuff like no default  
 passwords, protecting crypto keys, updateable software, minimising the attack  
 surface and allowing users to delete personal information [640]. But turning  
 basic principles into good engineering takes effort, and we can learn a lot from  
 applications that have already gone through at least one iteration of attack and  
 defence. I hope the case studies in this chapter will give some of the needed  
 contextual insight.

You’ll recall that in order to defeat a burglar alarm it is sufficient to make

it appear unreliable. Meters add further subtleties.

When we discussed an alarm in a bank vault, we were largely concerned

with attacks on communications (though sensor defeats also matter). But many  
 metering systems are much more exposed physically. A taxi driver may want  
 the meter to read more miles or more minutes than were actually worked, so  
 may manipulate it into over-measuring. With tachographs, it’s the reverse: the  
 truck driver usually wants to drive above the speed limit, or work dangerously  
 long hours, so wants the tachograph to ignore some driving. Utility consumers  
 may want their meters to ignore some of the passing electricity or gas. Criminal  
 defendants and parolees may want to evade a curfew order. In such cases, the  
 subject of surveillance may cause the device to make false readings, or simply  
 to fail. There are also underground markets for exploits of various kinds.

Many metering and monitoring systems are also concerned with evidence.

An opponent could get an advantage either by manipulating communications  
 (such as by replaying old messages) or by falsely claiming that someone else  
 had done so. With postal franking systems, it’s not sufficient for the attacker to  
 cause a failure (as then he can’t post his letters). And we need to understand  
 the real threats. The post office is mostly concerned with stopping wholesale  
 fraud, such as crooked direct marketers who bribe postal employees to slip a  
 truckload of mail into the system. The system may look like it’s designed to  
 stop external fraud, but its real focus is internal.

**14.2** **Prepayment Meters**

There are many systems where the user pays in one place for a token – whether  
 a magic number, or a cardboard ticket with a magnetic strip, or an app that  
 displays a QR code, or even a rechargeable chip card – and uses the stored  
 value somewhere else. Examples include transport tickets, photocopier cards  
 in libraries, lift passes at ski resorts, and washing-machine tokens in university  
 halls of residence.

The main protection goal is usually to prevent the tokens being forged at

scale. Duplicating a single ticket is not too hard, and repeating a magic number  
 is easy. Such scams can be prevented if we make all the tokens unique and all  
 the devices online. But that makes things fragile; if people can’t get on the bus

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 458 | Ross Anderson |

*14.2. PREPAYMENT METERS*

in a mobile network black spot, or can’t use a ski lift or a washing machine if a  
 data centre is down, that can damage the business and cost real money. So the  
 replay and forgery detection must sometimes be done offline. But if we simply  
 encipher all our tokens using a universal master key, a villain could extract it  
 from a stolen terminal and set up in business selling tokens. What are our

options?

In most ticketing systems, procedural fraud is easy. A free rider can jump the

barrier at a subway station; an electricity meter can have a bypass switch wired  
 across it. But most people won’t cheat unless someone makes it seem easy and  
 safe by industrialising it. To maximise revenue, petty fraud should be at least  
 slightly inconvenient and – more importantly – there should be mechanisms to  
 prevent anyone forging tickets at scale.

The ﬁrst example I’ll discuss is the prepayment electricity meter. I chose

this because I was lucky enough to consult on a project to electrify three million  
 households in South Africa (a central election pledge made by Nelson Mandela  
 when he took power). This work is described in some detail in [93]. By December  
 2019, the STS speciﬁcation we developed was used in 68 million meters in 98  
 countries. Most of the lessons learned apply directly to other ticketing systems.

**14.2.1** **Utility metering**

Householders who can’t get credit buy gas and electricity services using pre-  
 payment meters (Figure 14.1). In the old days they were coin-operated, but  
 the costs of coin collection led vendors to develop token-based meters instead.  
 This technology was driven by less developed countries, and most notably by  
 South Africa, where it became a national priority to electrify the townships; as  
 many of the houses were informally constructed, and the owners did not even  
 have addresses (let alone credit ratings), prepayment was the only way to go.  
 Over 2 million meters were installed during Nelson Mandela’s term of office as  
 President, and there are now an estimated 10 million in use there. The largest  
 installation is 35 million in Indonesia, and they are common in in Africa, Asia  
 and Latin America, as well as in some developed countries; most meters in  
 Northern Ireland are prepayment. The typical developed country might have  
 about 10% of households using prepayment meters, because they’re on welfare  
 or have court judgments against them.

The customer goes to a shop and buys a token, which can be a card, a

cardboard ticket with a magnetic strip, or a 20-digit magic number. Most of  
 South Africa’s meters use a magic number. This is convenient for the customer,  
 as a ticket can be bought at a supermarket checkout, at an ATM, over the phone  
 or online.

The token is really just one or more instructions, encrypted using a key

unique to the meter, and saying something like ‘meter 12345 – dispense 50KWh  
 of electricity!’ The meter interrupts the supply when the credit runs out. Some  
 tokens have engineering functions too. Special tokens may be used to change  
 prices: if the power company charges different rates for the daytime and evening,  
 the meter may need updates on the relative prices and the times at which the  
 tariffs change.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 459 | Ross Anderson |

*14.2. PREPAYMENT METERS*

Of the UK’s electricity meters, about twice as many use smartcards as mag-

netic tickets. The former do not use the STS standard but are able to report  
 consumption patterns, tampering attempts and so on back to the power com-  
 pany. The magnetic-ticket and magic-number meters do not have such a back  
 channel. There is currently a project to replace all the meters in most EU

countries with *smart meters* which report readings and other data over a radio  
 link, and which can be set remotely into prepayment mode. Smart meters have  
 already been installed in other countries with mixed results. I’ll return to them  
 later.

Figure 14.1: – a prepayment electricity meter (Courtesy of Schlumberger)

Prepayment was the only way that less developed countries could electrify

millions of homes quickly. In the developed world, the main incentive was re-  
 ducing bad debts and other administrative costs. An added beneﬁt is energy  
 saving. In areas where most meters are prepaid, electricity consumption is up  
 to 10% lower, as its cost becomes more salient to the householder.

**14.2.2** **How the system works**

The security requirements for prepayment meters seem straightforward. Tokens  
 should not be easy to forge, while genuine tokens should not work in the wrong  
 meter, or in the right meter twice. The usual strategy is to tie each token to a  
 unique meter, so that someone can’t use the same magic number in two differ-  
 ent meters, and also make each token unique using serial numbers or random  
 numbers, so that the same token can’t be used twice in the same meter. But it  
 took a surprising amount of experience to develop this simple idea into a robust  
 system.

Each meter has a crypto key to authenticate its instructions from the vending

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 460 | Ross Anderson |

*14.2. PREPAYMENT METERS*

machine. Early systems had one for each neighbourhood, usually in a local store.  
 It had a vend key *KV* which is the master key for a neighborhood, and each  
 meter has a device key *KID* derived by encrypting its meter ID under the vend  
 key:

*KID* = *{ID}KV*

This is the same key diversiﬁcation technique described for parking lot ac-

cess devices in Chapter 4, and it works ﬁne where all the tokens are bought  
 locally. But real life is usually more complicated. In Britain, deregulation of the  
 electricity industry led to dozens of electricity companies who buy power from  
 generators and sell it onward to households through a common infrastructure,  
 so meters change ownership between multiple power companies with different  
 tariff structures. In South Africa, many people commute long distances, so they  
 want to buy tickets where they work. So we started with protocols to send a  
 customer meter key from the vending station that ‘owns’ the meter to another  
 station, and to pass sales data in the opposite direction for balancing and settle-  
 ment, somewhat like in ATM networks. In 2007 we introduced online vending;  
 a central server has a hardware security module with all the vend keys, so a  
 customer can buy a magic number over the Internet or via their mobile phone.  
 This server sells directly to seven million customers and also via about 10,000  
 online vend points such as ATMs and shops.

Statistical balancing is used to detect *non-technical losses*, that is, theft of

power through meter tampering or unauthorized connections to mains cables.  
 We compare the readings on a feeder meter, which might supply 30 houses, with  
 token sales to those houses. But customers hoard tickets and meter readers lie  
 about when they read the meter, so the discrepancy is a noisy signal. You can  
 use it as a source of leads for your investigation team, and as statistical check  
 on your bookkeeping systems, but that’s about it.

There were cases where vending machines were stolen and used to sell to-

kens in competition with the utility. Eliminating such a ‘ghost vendor’ generally  
 means changing the keys in all the local meters; there are a few stolen machines  
 still out there, operated by crime syndicates. The countermeasure was to main-  
 tain a credit balance in the vending machine’s security chip that also protects  
 vend keys and foreign meter keys. The balance is decremented with each sale  
 and only credited again when cash is banked; the operating company then sends  
 a magic number that reloads the chip with credit. So we have an accounting  
 system enforced by a value counter at the point of sale, rather than by ledger  
 data kept on servers at the utility. However, the strategic direction was central-  
 isation, to save the effort and expense of managing resellers, and operators have  
 replaced offline vending machines by online vending points that get their tokens  
 in real time from a central service.

**14.2.3** **What goes wrong**

As with burglar alarms, environmental robustness is critical. Apart from the  
 huge range of temperatures (as variable in South Africa as in the continental

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 461 | Ross Anderson |

*14.2. PREPAYMENT METERS*

United States) many areas have severe thunderstorms: the meter can be thought  
 of as a microprocessor with a 3-kilometer lightning conductor attached.

When meters were destroyed by lightning, the customers complained and got

credit for the value they said was still unused. So their next step was to poke live  
 mains wires into the meter to try to emulate the effects of the lightning. One  
 make of meter would give unlimited credit if the circuitry under the token slot  
 was destroyed, so service denial attacks worked well enough to become popular.

It was to get worse. Kids in Soweto observed that when there was a brown-

out – a fall in voltage from 220 to 180 volts – a particular make of meter went to  
 maximum credit. Soon they were throwing steel chains over the 11KV feeders  
 and crediting all the meters in the neighborhood. This bug wasn’t picked up  
 because brown-out testing hadn’t been speciﬁed. Developed-country environ-  
 mental standards were inadequate for use in Africa. The responsible company  
 almost went bust after 100,000 meters had to be pulled out and re-ROMmed.

There were numerous other bugs. One make of meter didn’t vend a speciﬁed

quantity of electricity, but so much worth of electricity at such-and-such a rate.  
 Vending staff discovered that the tariff could be set to a minute amount, and  
 the meter would operate almost for ever. Another allowed refunds, but a copy  
 of the refunded token could still be used. Another meter remembered only the  
 last token serial number entered, so by alternately entering duplicates of two  
 tokens it could be charged up indeﬁnitely.

As elsewhere, the real security breaches resulted from bugs and blunders that

were discovered by accident and exploited in quite opportunistic ways. Some of  
 the exploits scaled up and cost millions to ﬁx.

Other lessons learned, which we wrote up in [93], were:

*•* prepayment may be cheap and simple so long as you control the marketing  
 convenience stores, banks and supermarkets, it can become expensive,  
 complicated and risky;

*•* if you don’t get the security infrastructure right ﬁrst time, then changing  
 at distant shops, to support commuters;

*•* recycle technology if you can, as it’s likely to have fewer bugs. Much of

*•* use multiple experts. One expert alone can not usually span all the issues,

*•* you absolutely need prolonged ﬁeld testing. This is where many errors

The main lesson learned in the years after the initial deployment was to

design out scalable fraud, which meant centralisation. There are still procedural  
 exploits; for example, as any company can become a reseller, buying meters  
 and a vending station on the market, crooked ﬁrms can set up rogue meters  
 in community housing estates and direct the tenants to buy tokens from them

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 462 | Ross Anderson |

*14.2. PREPAYMENT METERS*

instead. So prepayment does not entirely abolish the need for good old-fashioned  
 audit, energy balancing and inspection – and neither does it entirely solve the  
 problems of local corruption or broader state capture in less developed countries.

What we learned ended up in the STS speciﬁcations that are now used by

dozens of manufacturers worldwide. One compromise did come back to bite  
 us, though. The date in the STS meters rolls over in 2024, which was the

distant future back in the early 1990s when we were doing the work1. Now that  
 there are 60 million meters in almost 100 countries, it’s going to cost utilities  
 hundreds of millions to give each customer a special key-change ticket to manage  
 the rollover. (The positive side of the key change is that the remaining ghost  
 vending machines will be ﬁnally put out of business.) So, when designing a new  
 system, please think of sustainability not just as ‘Will this system be OK for  
 the next 30 years?’ but ‘Will this be OK for the next 100 years?’ You may just  
 live long enough to be embarrassed!

**14.2.4** **Smart meters and smart grids**

In the early 2000s, the metering industry started selling the idea of a *smart me-*  
 *ter* – a meter with real-time communications to a central server so that it could  
 be read remotely. This had been patented as long ago as the 1970s but was de-  
 veloped into a broader concept involving not just billing, and prepayment if need  
 be, but ﬁne-grained pricing, power outage reporting and power quality moni-  
 toring. *Automatic meter reading* (AMR) was superseded by *advanced metering*  
 *infrastructure* (AMI); the latter has two-way communications, so commands can  
 be send to the meter remotely. Pricing can be complex, including both time-of-  
 day and demand-response tariffs. The beneﬁts sold to utilities included reduced  
 billing costs and easier debt collection. The case made to governments included  
 reducing peak demand and thus the number of power stations required. Mar-  
 keters talked about ‘smart grids’, talked excitedly of your meter being able to  
 control domestic appliances and to negotiate real-time tariffs with the market.  
 A more sober claim was that smart meters would pay for themselves by making  
 users more conscious of how much electricity they used, thus saving money. The  
 beneﬁt to the meter vendor was replacing a product that cost $15 and lasted  
 for 50 years with one that cost at least $50 and lasted for maybe 15.

There are many issues with smart metering. Researchers ﬁrst raised general

privacy concerns about ﬁne-grained consumption data going to utilities; if the  
 meter is set to monitor consumption by the minute or even by the second, the  
 utility can work out how many people are in the home, when they eat, when they  
 shower and when they sleep. This leads to direct concerns around predatory  
 marketing, and indirect concerns around third-party access – whether via law-  
 enforcement warrants, abuse of authorised access, or the perhaps inevitable  
 intrusion of the advertising ecosystem. This led to debates about the time

granularity of measurement, and how much data should be held in the meter

1We had to ﬁt everything into the 66 bits of a 20-digit token, and although we thought of

having an extra bit in the counter to get an extra 31 years, that would have meant a time  
 unit of 2 minutes rather than one, which would have made selling multiple tokens for a meter  
 at the same time tricky. But we did have the foresight to provide for resetting the counter on  
 key change.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 463 | Ross Anderson |

*14.2. PREPAYMENT METERS*

versus centrally. Then we noticed that putting a remotely commandable off  
 switch in all of a country’s homes creates a major cyber-war threat; if an enemy  
 can switch off your electricity supply they can quickly close down your economy,  
 or hold you to ransom [105]. This led to a scramble by the national-security  
 agencies. But perhaps the biggest bundle of issues was around the diverging  
 incentives of the various stakeholders. Utilities want to sell lots of energy, while  
 governments want to save it and to reduce peak demand. So who would win?

The pioneer was Italy, where the utility ENEL started installing smart me-

ters in 2001. Their main concern was power theft, particularly in southern Italy  
 where enforcement staff sent to disconnect non-paying customers were threat-  
 ened by gangsters. Smart meters enabled defaulters to be switched remotely to  
 a prepayment regime. This was seen as a success, and the lobbyists got to work.  
 The concept of a smart grid became US policy with the Energy Independence  
 and Security Act of 2007 and came forcefully to public attention when Presi-  
 dent Obama allocated $4.5bn to its development as the headline measure of the  
 American Recovery and Reinvestment Act; the European Parliament followed  
 with a 2009 law requiring member states to conduct an economic assessment of  
 smart metering by 2012, and if they found it beneﬁcial, mandate its use by 2022  
 (with 80% adoption by 2020) [652]. Many countries have now launched national  
 or regional smart meter programmes as have a number of U.S utilities, and we  
 have some experience of the successes (such as Spain) and failures (including  
 the UK and Ontario).

While US utilities tend to be regulated local monopolies, the European model

has competitive generation, regulated transmission and distribution monopolies,  
 and competitive retailers. Whether the meters belong to the distribution net-  
 work operator or the retailer is a matter of historical accident. It turned out  
 that where the distributor owned the meter, replacing all the meters with smart  
 meters was straightforward, as a contractor could do a whole street at a time,  
 and the meters could be connected to the utility via power-line communications  
 with the substation. In Spain, the utilities set up a buyers’ cartel and insisted  
 that every supplier’s meter would work with every other supplier’s headend, so  
 they got commodity hardware costing under e50 a meter.

However, in countries where the retailer owns the meter, things were not

so simple. There is a serious problem with incentives: if smart meters are

to pay for themselves by saving energy, then it makes no sense to put them  
 under the control of the retailer, which maximises its proﬁt by maximising  
 energy sales. Germany did an honest assessment, decided that smart meters  
 would be uneconomic, and abandoned the project. Britain unfortunately plowed  
 ahead. Its Department of Energy and Climate Change had already had economic  
 assessments in 2004, 2007 and 2008 which showed a negative return on the  
 investment. Undeterred, they stretched the assumptions about costs, beneﬁts,  
 electricity prices and interest rates, came up with a positive assessment in 2009,  
 and committed Britain to introducing smart meters not just for electricity but  
 for gas too [883].

Outside Europe, the same problems arose where meters were owned by mul-

tiple retailers. New Zealand made smart meters optional, calculating they would  
 be worthwhile only for large houses. In Ontario, as in Britain, the government  
 pressed on, leading to an expensive failure, documented in the 2014 Annual

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 464 | Ross Anderson |

*14.2. PREPAYMENT METERS*

Report of the Auditor General [1197]. The province dealt with 73 local distri-  
 bution companies by building a central system to collect all the meter readings  
 and making them available to retailers, as well as regulators. The goal of the  
 system, to cut peak demand, was not realised at all; the peak-to-trough price  
 variation that politicians were prepared to tolerate was not enough to change  
 behaviour. The Ontario cost-beneﬁt analysis that had been prepared in 2005 (a  
 year after ministers announced the project) turned out to have overestimated  
 beneﬁts as $600m when they were at most $88m, while costs ballooned to $2bn;  
 the largest retailer spent over $500 per meter on the devices and the systems to  
 support them. Overall, energy planning was so poor that the province ended up  
 selling surplus power to the USA, subsidising utilities in Michigan and in New  
 York State to the tune of billions of dollars.

In Britain, smart metering has evolved into what may be the largest ever

civilian project disaster. Successive governments (Labour, coalition and Conser-  
 vative) committed to rolling out smart meters by 2020 as nobody wanted to be  
 accused of not being ‘green’. To my way of thinking, wasting £20 billion without  
 saving any energy, and displacing better projects that could have yielded real  
 savings, was about as un-green as you can get. The project was gold-plated at  
 every level, with each home having up to four devices: smart meters for gas and  
 electricity, a home hub to connect them to a wireless network, and an in-home  
 display so the bill payer could track consumption. (The project started in 2009  
 just as people started to use smartphones but was too rigid to switch to using  
 apps instead.) Ministers followed the Ontario route of a central meter reading  
 server but nonetheless a UK householder who accepts a smart meter from one  
 vendor and then moves to a different supplier to save money usually has to sub-  
 mit manual readings thereafter. It took years to agree a national standard for a  
 second-generation meter and most of the deployed meter ﬂeet consists of older  
 incompatible models; the vendors fought for years to get their own patents in  
 there and the officials didn’t have the technical knowledge or political support  
 to bang heads together. Security mechanisms were retroﬁtted in a panic in the  
 mid-2010s once we pointed out that a hostile state could simply turn off British  
 households’ power at a time of tension [105]. Whistleblowers who threatened  
 to expose the project’s failure, and a likely cost increase from £11bn to £23bn,  
 were threatened with prison [919]. The National Audit Office then reported at  
 the end of 2018 that the project was falling materially short of expectations:  
 the plan had been to replace 80% of UK meters by the end of 2020, but only  
 12.5m had been done, with 39m yet to do [1391]. What’s more, 70% of the  
 meters lost functionality when customers switched supplier (as you have to do  
 annually to get decent prices). If government follows its declared strategy of  
 moving everyone to second-generation meters, all these old ones will have to be  
 replaced; according to a report from November 2019, only 2.3m of the meters  
 were the new ones. Cost savings are unlikely as the industry will have to support  
 good old-fashioned meters, several types of obsolete smart meter and the new  
 smart meters through the 2020s. As for energy savings, there’s no sign. (The  
 government could save a lot of energy if it used the meters to move everyone  
 to prepayment, but that’s not on the agenda, and could have been done with  
 much cheaper kit.) Nobody’s using the data for anything but billing. And now  
 officials just don’t want to know: in the words of the NAO report, “The Depart-  
 ment currently has no plans to continue engagement with consumers after the

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 465 | Ross Anderson |

*14.2. PREPAYMENT METERS*

rollout is complete.”

Two ﬁnal remarks on smart grids. While the meter makers were doing their

big marketing push in the late 2000s, there was breathless talk of meters helping  
 to stabilise the grid by creating demand response and improving measurement.  
 The scepticism expressed at the time by experienced power engineers has turned  
 out to be justiﬁed. Grids have indeed become more fragile as generation capac-  
 ity has moved from large spinning machines attached to the core transmission  
 network to hundreds of thousands of windmills and solar panels embedded in the  
 wider distribution systems. Recent large outages, such as in South Australia on  
 28 September 2016 and the UK on 9 August 2019, were cascade failures, caused  
 when a local issue (a storm in Australia, and a lightning strike in England)  
 caused a rate of change of frequency in excess of the safety limit, causing fur-  
 ther loads to be shed, resulting in undervoltage and further load shedding. A  
 complicating factor in each case is that now we have a lot of generation capacity  
 embedded on people’s rooftops, shedding load doesn’t work as well as it used to.  
 The takeaway is not that we need smart meters, even at the substation level,  
 but that we need more inertia in the system – which means buying batteries  
 or synchronous condensers. We also need to make the rest of the infrastructure  
 more tolerant of outages. Much of the political fury in Britain over the 2019  
 power cut came from London commuters being stuck in trains for hours. This  
 happened because 60 Siemens Desiro class trains tripped at 49Hz when they  
 should have tripped at 48.5Hz, and half of them would not restart because of a  
 software bug. Getting them going again required a visit from a technician with  
 a laptop2.

Demand response was also supposed to help with peak demand reduction.

Nowhere have smart meters helped. Many countries now have capacity mar-  
 kets where grid operators can buy extra megawatts, on timescales of seconds to  
 minutes, but these operate using dedicated systems. For example, data centre  
 operators who have standby diesel generators and have to run them for half an  
 hour a month to make sure they still work, are paid to start them when they’re  
 needed. In warmer countries, some people get discounts on their electricity bills  
 for allowing their air conditioners to be switched off for half an hour during  
 demand peaks. Eventually, the chargers for electric cars will contribute to this  
 too, once there are enough of them. But the equipment to do this is always  
 separate from the main utility meter; no entrepreneur starting a capacity com-  
 pany would want to get entangled with the regulated mess that is metering.  
 As for the smart meter marketing vision of your home hub negotiating energy  
 prices and turning off your cooker or water heater in response to a price surge,  
 that is remote from commercial reality. Firms that sell things like cookers and  
 heaters are indeed putting CPUs and communications in them, but they talk to  
 the ﬁrm’s own servers, not to other devices; and the idea that politicians would  
 allow retail prices to surge to match those on capacity markets is na¨ıve. All  
 that smart meters have achieved in Britain is to put a few tens of thousands of  
 meter readers out of work, at a cost to the bill payer of £20 billion. Ontario  
 was the same, but with one less trailing zero.

2UK trains and railway signals are not allowed to do over-the-air software upgrade because

of national security rules, as the railways are considered to be critical national infrastructure.  
 This also means that security patches take days to ship. Well done, MI5!

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 466 | Ross Anderson |

*14.3. TAXI METERS, TACHOGRAPHS AND TRUCK SPEED LIMITERS*

**14.2.5** **Ticketing fraud**

Transport ticketing is a larger application than utility metering, but I don’t  
 know of any serious and publicly available study of the failure modes of train,  
 bus and subway tickets. In the case of London, deregulation of the railways led  
 to problems with train companies manipulating ticket sales by booking them at  
 stations where they got a larger percentage of the takings; if you’re designing a  
 system that shares revenue between vendors, you should try to design out the  
 incentive for stakeholders to cheat. There was also a scare after the break of  
 Mifare Classic described in section 13.2.5; Transport for London scrambled to  
 add intrusion-detection systems to detect fraud.

One type of ticketing on which we do have some real fraud data is the airline

variety. During the 2010s, there emerged an ecosystem of fraudulently obtained  
 air tickets and of channels for reselling them. The tickets are obtained by a  
 variety of methods, ranging from compromised credit cards through dishonest  
 staff at airlines and travel agencies through stolen air miles and hacked book-  
 ing systems; the marketing channels include spam, affiliate marketing, sales to  
 migrant communities and sales to human traffickers. This is all documented  
 by Alice Hutchings [936, 937]. The key factors are that plane tickets, unlike  
 subway tickets, are sufficiently valuable for such an ecosystem to develop; and  
 that while some of the customers know they’re getting bogus tickets, enough of  
 them are simply suckers, so you can’t just arrest everyone who turns up for a  
 ﬂight with an invalid ticket.

I’ll now look at a class of applications where the attacks are more severe and

prolonged than on electricity meters. The threat model includes sensor manipu-  
 lation, service denial, accounting ﬁddles, procedural defeats and the corruption  
 of operating staff. This exemplary ﬁeld of study is vehicle monitoring systems.

**14.3** **Taxi meters, tachographs and truck speed**  
 **limiters**

A number of systems are designed to monitor and control vehicles. The most fa-  
 miliar is probably the odometer in your car. When buying a used car you’ll worry  
 whether the car has been *clocked*, that is, had its indicated mileage reduced. As  
 odometers became digital, clocking became a kind of computer fraud [391]. A  
 related problem is *chipping*, that is, replacing or reprogramming the engine con-  
 troller. This can be done for two basic reasons. First, the engine controller acts  
 as the server for the remote key-entry systems that protect most modern cars  
 from theft, as described in Chapter 4; so if you want to steal a car without steal-  
 ing the key, you might replace the controller in the street, or else tow the car  
 and replace or reprogram the controller later. Second, people reprogram their  
 cars’ engine controllers to make them go faster, and the manufacturers dislike  
 this because of the increased warranty claims from burned-out engines. So they  
 try to make the controllers more tamper resistant, or at least tamper-evident.  
 This arms race is described in [624].

Many vehicles now keep logs that are uploaded to the manufacturer during

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 467 | Ross Anderson |

*14.3. TAXI METERS, TACHOGRAPHS AND TRUCK SPEED LIMITERS*

servicing. General Motors started equipping some vehicles with black boxes to  
 record crash data in 1990. By the time the logging became public in 1999, some  
 six million vehicles had been instrumented, and the disclosure caused protests  
 from privacy activists [1938]. Indeed, there’s a whole conference, ESCAR, de-  
 voted to electronic security in cars. Vehicle security is becoming a hot topic  
 again in 2019 because of the growing interest in autonomous operation3.

Other vehicle monitoring systems are ﬁtted after manufacture, and the most

familiar may be the taxi meter. A taxi driver has an incentive to manipulate the  
 meter to show more miles travelled (or minutes waited) if he can get away with  
 it. There are various other kinds of ‘black box’ used to record the movement of  
 vehicles from aircraft through ﬁshing vessels to armored bank trucks, and their  
 operators have differing levels of motive for tampering with them. Insurers who  
 sell ‘pay-as-you-drive’ insurance to young and high-risk drivers demand that  
 they ﬁt black boxes with satellite navigation devices that let the insurer charge  
 a couple of pennies a mile for driving along a country road in the afternoon but  
 a couple of dollars a mile for evening driving in an inner city [1909]. Any young  
 man who wants to impress a lady by driving around town on a Saturday night  
 will have an incentive to beat the black box.

**14.3.1** **The tachograph**

The case study I’m going to use here is the tachograph. These devices are used  
 to monitor truck drivers’ speed and working hours; in Europe, the traditional  
 analogue devices were replaced by digital ones from 2006, and as a truck lasts  
 about ten years, most of the ﬂeet is now digital. This gives us some interesting  
 data on how such equipment works, and can fail; and it’s an example of how a  
 move to digital technology didn’t make things better. What was actually needed  
 wasn’t whizzy technology but more enforcement.

Vehicle accidents resulting from a driver falling asleep at the wheel cause

several times more accidents than drunkenness (20 percent versus 3 percent of  
 accidents in the UK, for example). Accidents involving trucks are more likely  
 to lead to fatal injuries because of the truck’s mass. So most countries regulate  
 truck drivers’ working hours. While these laws are enforced in the USA using  
 weigh stations and drivers’ log books, countries in Europe use tachographs that  
 record a 24-hour history of the vehicle’s speed. Until 2005–6, this was recorded  
 on a circular waxed paper chart (Figure 14.2); since then, digital tachographs  
 have been introduced and the old system has been largely phased out4.

First let’s look at the old analogue system as our baseline; it’s still in use by

old trucks and buses on Europe’s roads.

The analogue system uses a waxed paper chart that is loaded into the tacho-

graph, which is part of the vehicle’s speedometer/odometer unit. It turns slowly  
 on a turntable inside the instrument that turns once every 24 hours, and a speed  
 history is inscribed by a ﬁne stylus connected to the speedometer. With some

3Full disclosure: one of my research students is funded by Bosch.  
 4Vehicles registered since August 2004 in the UK had to have digital systems ﬁtted, driver

cards have been issued since June 2005 and the use of digital systems in new vehicles became  
 mandatory in August 2006; the dates vary slightly for other EU countries.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 468 | Ross Anderson |

*14.3. TAXI METERS, TACHOGRAPHS AND TRUCK SPEED LIMITERS*

Figure 14.2: – a tachograph chart

exceptions that needn’t concern us, it is an offence to drive a truck in Europe  
 unless you have a tachograph; if it’s analogue you must have a chart installed,  
 and have written on it your starting time and location. You must also keep sev-  
 eral days’ charts with you to establish that you’ve complied with the relevant  
 driving hours regulations (typically 8.5 hours per day with rules for rest breaks  
 per day and rest days per week). If it’s digital you have to have a driver card  
 plugged into it; the card and the vehicle unit both keep records.

European law also restricts trucks to 100 km/h (62 mph) on freeways and

less on other roads. This is enforced not just by police speed traps and the  
 tachograph record, but directly by a speed limiter that is also driven by the  
 tachograph. Tachograph charts are also used to investigate other offences, such  
 as unlicensed waste dumping, and by ﬂeet operators to detect fuel theft. So  
 there are lots of reasons why a truck driver might want to ﬁddle his tacho-  
 graph. Indeed, it’s a general principle in security engineering that one shouldn’t  
 aggregate targets. Forcing a truck driver to defeat his tachograph in order to  
 circumvent his speed limiter, and vice versa, was a design error – but one that’s  
 now too entrenched to change easily.

Most of what we have to say applies just as well to taxi meters and other

monitoring devices. While the truck driver wants his vehicle to appear to have  
 gone less distance, the taxi driver wants the opposite. This has little effect on  
 the actual tampering techniques.

**14.3.2** **What goes wrong**

According to a survey of 1060 convictions of drivers and operators done before  
 the introduction of the new digital system [64], the offences were distributed as  
 follows.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 469 | Ross Anderson |

*14.3. TAXI METERS, TACHOGRAPHS AND TRUCK SPEED LIMITERS*

**14.3.2.1** **How most tachograph manipulation is done**

About 70% of offences that result in conviction did not involve tampering but  
 exploited procedural weaknesses. For example, a company with premises in

Dundee and Southampton should have four drivers in order to operate one  
 vehicle per day in each direction, as the distance is about 500 miles and the  
 journey takes about 10 hours – which is illegal for a single driver to do every day.  
 The standard ﬁddle is to have two drivers who meet at an intermediate point  
 such as Penrith, change trucks, and insert new paper charts into the tachographs.  
 So the driver who had come from Southampton now returns home with the  
 vehicle from Dundee. When stopped and asked for his charts, he shows the  
 current chart from Penrith to Southampton, the previous day’s for Southampton  
 to Penrith, the day before’s for Penrith to Southampton, and so on. In this way  
 he can give the false impression that he spent every other night in Penrith and  
 was thus legal. This practice of swapping vehicles halfway through the working  
 day is called *ghosting*. It’s even harder to detect in mainland Europe, where a  
 driver might be operating out of a depot in France on Monday, in Belgium on  
 Tuesday and in Holland on Wednesday.

Simpler frauds included setting the clock wrongly, pretending that a hitch-

hiker is a relief driver, and recording the start point as a village with a very  
 common name – such as ‘Milton’ in England or ‘La Hoya’ in Spain. If stopped,  
 the driver can claim he started from a nearby Milton or La Hoya.

Such tricks often involve collusion between the driver and the operator.

When the operator is ordered to produce charts and supporting documents  
 such as pay records, weigh station slips and ferry tickets, his office may well  
 conveniently burn down. (It’s remarkable how many truck companies operate  
 out of cheap wooden sheds at a safe distance from the trucks in their yard.)

**14.3.2.2** **Tampering with the supply**

The next largest category of fraud, amounting to about 20% of the total, in-  
 volved tampering with the supply to the tachograph instrument, including in-  
 terference with the power and impulse supply, cables and seals.

The earliest tachographs used a rotating wire cable – as did the speedometers

in cars up until the early 1980s – that was hard to ﬁddle with; if you jammed  
 the truck’s odometer it was quite likely that you’d shear off the cable. More  
 recent analogue tachographs are ‘electronic’, in that they use electric cables  
 rather than rotating wire. The input comes from a sensor in the gearbox, which  
 sends electrical impulses as the prop shaft rotates. This has made ﬁddling much  
 easier! A common attack is to unscrew the sensor about a tenth of an inch,  
 which causes the impulses to cease, as if the vehicle were stationary. To prevent  
 this, sensors are ﬁxed in place with a wire and lead seal. Fitters are bribed  
 to wrap the wire anticlockwise rather than clockwise, which causes it to loosen  
 rather than break when the sensor is unscrewed. The fact that seals are issued  
 to workshops rather than to individual ﬁtters complicates prosecution.

But most of the ﬁddles are much simpler still. Drivers short out the cable

or replace the tachograph fuse with a blown one. (One manufacturer tried to

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 470 | Ross Anderson |

*14.3. TAXI METERS, TACHOGRAPHS AND TRUCK SPEED LIMITERS*

stop this trick by putting the truck’s anti-lock braking system on the same fuse.  
 Many drivers preferred to get home sooner than to drive a safe vehicle.) There’s  
 evidence of power-supply interruption on the chart in Figure 14.2: around 11  
 A.M., there are several places where the speed indicated in the outside trace  
 goes suddenly from zero to over 100 km/h. These indicate power interruptions,  
 except where there’s also a discontinuity in the distance trace. There, the unit  
 was open.

**14.3.2.3** **Tampering with the instrument**

The third category of fraud was tampering with the tachograph unit itself.  
 The typical offence in this category is miscalibration, usually done in cahoots  
 with the ﬁtter but sometimes by the driver defeating the seal on the device.  
 This amounted for some 6% of offences, but declined through the 1990s as the  
 introduction of digital communications made it easier to tamper with the cable  
 instead.

**14.3.2.4** **High-tech attacks**

The state of the tampering art at the time of the survey was the equipment in  
 Figure 14.3. The plastic cylinder on the left of the photo is marked ‘Voltage  
 Regulator — Made in Japan’ but is certainly not a voltage regulator. (It appears  
 to be made in Italy.) It is spliced into the tachograph cable and controlled by  
 the driver using the remote control key fob. A ﬁrst press causes the indicated  
 speed to drop by 10%, a second press causes a drop of 20%, a third press causes  
 it to fall to zero, and a fourth causes the device to return to proper operation.

This kind of device accounted for under 1% of convictions but its use was

believed to be much more widespread. It’s extremely hard to ﬁnd as it can  
 be hidden at many different places in the truck’s cable harness. Police officers  
 who stop a speeding truck equipped with such a device, and can’t ﬁnd it, have  
 difficulty getting a conviction: the sealed and apparently correctly calibrated  
 tachograph contradicts the evidence from their radar or camera.

**14.3.3** **Digital Tachographs**

The countermeasures taken against tachograph manipulation vary by country.  
 In Britain, trucks are stopped at the roadside for random checks by vehicle  
 inspectors, and suspect trucks may be shadowed across the country. In the

Netherlands, inspectors prefer to descend on a trucking company and audit their  
 delivery documents, drivers’ timesheets, fuel records etc. In Italy, data from the  
 toll booths on the freeways are used to prosecute drivers who’ve averaged more  
 than the speed limit (you can often see trucks parked just in front of Italian  
 toll booths). But drivers can arbitrage between the differing control regimes.  
 For example, a truck driver operating between France and Holland can keep his  
 documents at a depot in France where the Dutch vehicle inspectors can’t get at  
 them. The weakness in the UK system was that when a vehicle inspector stopped  
 a truck and found evidence of a violation, this would result in a prosecution some

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 471 | Ross Anderson |

*14.3. TAXI METERS, TACHOGRAPHS AND TRUCK SPEED LIMITERS*

Figure 14.3: – a tachograph with an interruptor controlled by the driver using  
 a radio key fob. (Courtesy of Hampshire Constabulary, England)

months later in the local magistrate’s court. Foreign drivers often just didn’t  
 appear.

So the European Union took the initiative to design a uniﬁed electronic

tachograph system to replace the existing paper-based charts with smartcards.  
 Each driver now has a driver card that contains a record of his driving hours  
 over the last 28 days. Every vehicle registered since 2006 has a vehicle unit that  
 can hold a year’s history. There are also workshop cards used by mechanics  
 to calibrate devices, and control cards used by law enforcement officers to read  
 them out at the roadside. In 1998, I was hired by the UK Department of Trans-  
 port to look at the new scheme and try to ﬁgure out what would go wrong.  
 After talking to a wide range of people from policemen and vehicle inspectors to  
 tachograph vendors and accident investigators, I wrote a report [64]. I revisited  
 the ﬁeld in 2007 when writing the second edition of this book; it was simulta-  
 neously pleasing and depressing to ﬁnd that I’d mostly predicted the problems  
 correctly. However a few interesting new twists also emerged. Finally, in 2020,  
 in the third edition, we can take a more mature view.

The main objection raised to the project was that it was not clear how going

digital would help combat the procedural frauds that made up 70% of the total.  
 Indeed, our pair of drivers ‘ghosting’ between Dundee and Southampton had  
 their lives made even easier. It took fourteen years – more than the lifetime of  
 a truck – to change over to the new system and meantime a crooked company  
 could run one new digital truck and one old analogue one. Each driver will now  
 have one chart and one card, with ﬁve hours a day on each, rather than two  
 charts which they might accidentally mix up when stopped. This turned out to  
 be well-founded. By 2008, some 20% of the vehicle ﬂeet had digital tachographs  
 – somewhat more than would be expected – which suggested that operators

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 472 | Ross Anderson |

*14.3. TAXI METERS, TACHOGRAPHS AND TRUCK SPEED LIMITERS*

may have been installing digital devices before they need to as they’re easier to  
 ﬁddle. In 2020, drivers have multiple cards.

Another objection was that enforcement would be made harder by the loss

of detailed speed and driving hours information. Back in 1998, the Germans  
 had wanted the driver card to be a memory device so it could contain detailed  
 records; the French insisted on a smartcard, thanks to lobbying from their smart-  
 card industry. So the driver card has limited memory, and can only contain a  
 limited number of alarm events.

**14.3.3.1** **System-level problems**

The response to the loss of ﬁne-grained data varies by country. Germany went  
 for an infrastructure of ﬂeet management systems that accept digital tachograph  
 data, digitized versions of the analog data from the existing paper charts, fuel  
 data, delivery data and even payroll, and reconcile them all to provide not just  
 management information for the trucking company but surveillance data for the  
 police. Britain has something similar, although it’s up to the police to decide  
 which companies to inspect; unless they do so, data on driving infringements  
 is only available to the employer. There are third-party service ﬁrms who will  
 analyse this for companies who are keen on saving time, or just demonstrating  
 compliance. Germany has also introduced a system of road pricing for heavy  
 goods vehicles that gives further inputs into ﬂeet management.

Britain has a network of automatic number plate reader (ANPR) cameras,

initially installed around London to make IRA bombing attacks harder; after  
 the Good Friday agreement in 1997 ended that threat, ANPR was not decom-  
 missioned but extended nationwide. That was justiﬁed on the basis of detecting  
 car tax evaders, but we then saw ANPR data adduced in more and more prose-  
 cutions, for everything from terrorism down to burglary. In the case of drivers’  
 hours enforcement, the strategy is to verify a sample of logged journeys against  
 the ANPR database; where discrepancies are found, the company’s operations  
 are then scrutinised more closely.

However, disagreements about privacy and about national economic interests

hindered EU-wide standardization. It’s up to individual countries whether they  
 require truck companies to download and analyze the data from their trucks.  
 And even among countries that require this, there’s still arbitrage. For example,  
 the German police are much more vigorous at enforcing drivers’ hours regula-  
 tions than their Italian counterparts. So, under the old analogue system, an  
 Italian driver who normally didn’t bother to put a chart in his machine did so  
 while driving over the Alps. Meanwhile, the driver of the German truck going  
 the other way took his chart out. The net effect was that all drivers in a given  
 country were subject to the same level of enforcement. But if the driving data  
 got uploaded from the Italian driver’s card and kept on a PC at a truck com-  
 pany in Rome then they were subject to Italian levels of enforcement (or even  
 less if the police in Rome didn’t care about accidents in Germany). The ﬁx  
 was extraterritoriality; an Italian truck driver stopped in Germany can now be  
 prosecuted there if he can’t show satisfactory records of his driving in Italy for  
 the week before he crossed the border.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 473 | Ross Anderson |

*14.3. TAXI METERS, TACHOGRAPHS AND TRUCK SPEED LIMITERS*

In the UK, foreign drivers who were stopped and ordered to appear at a

magistrates’ court often didn’t turn up. The real ﬁx turned out to be not

technological, but legal. In March 2018, Britain changed the law to allow spot  
 ﬁnes at the roadside. Previously, officers could only issue spot ﬁnes for ongoing  
 offences, rather than for offences visible in the truck or driver records. This  
 change led to a near-tenfold increase in ﬁnes [924].

**14.3.3.2** **Other problems**

Overall, the move from analogue to digital wasn’t an improvement. While com-  
 parative fraud statistics of digital and analogue devices have not been collected,  
 the view of officials is that while the initial detection of an unrealistic journey  
 remains much the same, the sophistication of digital defeat devices makes them  
 harder to ﬁnd [1726]. And there are other interesting problems with tachographs  
 becoming digital.

First, digital tachographs were the ﬁrst system that caused digital signatures

to turn up in court in large numbers. For years, security researchers have been  
 writing academic papers with punchlines like “the judge then raises X to the  
 power Y, ﬁnds it’s equal to Z, and sends Bob to jail.” The reality is different.  
 Judges found digital signatures difficult as they were presented as hexadecimal  
 strings on little tickets printed out from vehicle units, with no approved ap-  
 paratus for veriﬁcation. The police solved the problem by applying standard  
 procedures for “securing” evidence. When they raid a dodgy trucking company,  
 they image the PC’s disk drive and take copies on DVDs that are sealed in ev-  
 idence bags. One gets given to the defence and one kept for appeal. The paper  
 logs documenting the copying are available for Their Worships to inspect, along  
 with the printouts from the vehicle units.

Second, many drivers have more than one driver card. This is an offence

everywhere but that doesn’t stop it! Drivers borrow them from friends who  
 use them only occasionally – for example because they usually drive trucks  
 under 3.5 tonnes. And thanks to EU freedom of movement, drivers can easily  
 have more than one address: the Jean Moulin of Toulouse may also be Jean  
 Moulin of Antwerp. A database, Tachonet, was set up to try to catch duplicate  
 applications across European countries but it doesn’t seem to work very well.  
 For example, drivers may forget their middle name in one of their countries of  
 residence. From 2018 it was made mandatory for Member States to share data  
 with it.

Third, there are new kinds of service-denial attacks (as well as the tradi-

tional ones on gearbox sensors, fuses and so on). A truck driver can destroy his  
 smartcard by feeding it with mains electricity (even a truck’s 24 volts will do  
 ﬁne). Under the regulations he is allowed to drive for 15 days while waiting for  
 a replacement. As static electricity destroys maybe 1% of cards a year anyway,  
 it’s hard to prosecute drivers for doing this occasionally.

Fourth, I mentioned that the loss of detailed, redundant data on the tacho-

graph chart makes enforcement harder. In the old analogue days, experienced  
 vehicle inspectors had a ‘feel’ for when a chart isn’t right, but the analogue  
 trace was replaced by a binary signal saying either that the driver infringed the

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 474 | Ross Anderson |

*14.3. TAXI METERS, TACHOGRAPHS AND TRUCK SPEED LIMITERS*

regulations or that he didn’t. This spills over into other enforcement tasks; ana-  
 logue charts were often used to collect evidence of illegal toxic waste dumping,  
 for example, as the recorded speed history often gave an inspector a good idea  
 of the truck’s route.

Next, some of the cards in the system (notably the workshop cards used to set

up the instruments, and the control cards used by police and vehicle inspectors)  
 are very powerful. They can be used to erase evidence of wrongdoing. For

example, if you use a workshop card to wind back the clock in a vehicle unit  
 from 10th July to 8th July, then the entries for July 9th and 10th become  
 unreadable. Some countries have therefore gone to great lengths to minimise  
 the number of workshop cards that fall into bad hands. In the UK, for example,  
 truck mechanics have to pass a criminal records check to get one; yet this isn’t  
 foolproof as it’s often companies that get convicted, and the wealthy owners of  
 crooked truck-maintenance ﬁrms just set up new ﬁrms. There’s no company  
 licensing scheme, and although wrongdoers can be blacklisted from acting as  
 directors of licensed ﬁrms, crooks just hide behind nominee directors.

**14.3.3.3** **The resurrecting duckling, or TOFU**

There is one interesting spin-off from the world of tachographs. In the late

1990s, a European Union regulation decreed that, in order to frustrate the use  
 of interruptors of the kind shown in Figure 14.3, all digital tachographs had to  
 encrypt the pulse train from the gearbox sensor to the vehicle unit. As both  
 of these devices contain a microcontroller, and the data rate is fairly low, this  
 shouldn’t in theory have been a problem. But how on earth could we distribute  
 the keys? If we just set up a hotline that garages could call, it is likely to be  
 abused. There’s a long history of ﬁtters conspiring with truck drivers to defeat  
 the system, and of garage staff abusing helplines to get unlocking data for stolen  
 cars and even PIN codes for stolen car radios.

One solution is given by the *resurrecting duckling* security policy model,

more prosaically known as *trust on ﬁrst use*. This is named after the fact

that a duckling emerging from its egg will recognize as its mother the ﬁrst  
 moving object it sees that makes a sound: this is called imprinting. Similarly,  
 a ‘newborn’ vehicle unit, just removed from the shrink wrap, can recognize as  
 its owner the ﬁrst gearbox sensor that sends it a secret key. The sensor does  
 this on power-up. As soon as this key is received, the vehicle unit is no longer a  
 newborn and will stay faithful to the gearbox sensor for the rest of its ‘life’. If  
 the sensor fails and has to be replaced, a workshop card can be used to ‘kill’ the  
 vehicle unit’s key store and resurrect it as a newborn, whereupon it can imprint  
 on the new sensor. Each act of resurrection is indelibly logged in the vehicle  
 unit to make abuse harder. (This at least was the theory – the implementation  
 fell somewhat short in that in one unit the error code for sensor rekeying is the  
 same as the error code for a power outage.)

The resurrecting duckling model of key management was originally developed

to deal with the secure imprinting of a digital thermometer or other piece of  
 medical equipment to a doctor’s tablet or a bedside monitor [1819]. It is also  
 used in wireless LAN extenders; these devices typically use a protocol suite  
 called Homeplug AV to transmit data at 155Mb/s over the domestic power mains

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 475 | Ross Anderson |

*14.3. TAXI METERS, TACHOGRAPHS AND TRUCK SPEED LIMITERS*

from a unit plugged into your broadband hub to a remote unit on another ﬂoor.  
 In order to prevent your neighbours being able to use your wiﬁ, each virtual  
 network is encrypted with a key that’s set up the ﬁrst time you plug in an  
 extender [1437]. The idea is that when you plug something in, it should just  
 work; if it mates with the wrong network, you press a button and try again; in  
 extremis you can do the security manually by copying a key off the packaging  
 into any enrolled device that has a keyboard. As more and more devices with  
 constrained interfaces join the Internet of Things, such protocols will become  
 more widespread.

**14.3.4** **Sensor defeats and third generation devices**

However, even if the protocols can be secured, the sensors can still be attacked  
 directly. Since digital tachographs started shipping, the folks who brought you  
 the interruptor now have a new product: a black box containing electromagnets  
 and electronics to simulate a gearbox. The errant truck driver unscrews his  
 gearbox sensor and places it in this simulator, which comes with its own cable  
 and a sensor that he plugs into his actual gearbox. The system now operates  
 as before; on command it will either relay impulses faithfully, or discard them,  
 or ﬁlter some of them out. The dodgy pulse-train arrives at the tachograph as  
 before, but this time beautifully encrypted using triple-DES. Secure sensing is  
 harder than it looks!

This became such a nuisance that the EU passed a law in 2009 speciﬁcally

prohibiting, and requiring Member States to check for, “any device, or devices,  
 intended to destroy, suppress, manipulate or alter any data, or which is intended  
 to interfere with any part of the electronic data exchange between the component  
 parts of recording equipment, or which inhibits or alters the data in such ways  
 prior to encryption” [652]. It also upgraded the regulations to require that

vehicles registered from 2012 have the ‘third version tachograph’, which requires  
 an extra motion sensor as a countermeasure to sensor defeats

**14.3.5** **The fourth generation – smart tachographs**

In 2014 the regulations were updated to introduce the smart tachograph, which  
 is required in vehicles registered for the ﬁrst time as from 15 June 2019, and  
 adds:

*•* better security mechanisms to make fraud more difficult;

*•* a satellite navigation system, which will record the truck’s location at the  
 that;

*•* a radio link for a cop at the roadside to read tachograph data when the

By now, the reader might feel a certain cynicism about anything called

‘smart’. The regulations are a further move in the direction of pervasive enforce-  
 ment, but stop short of demanding that vehicle units keep detailed GPS history.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 476 | Ross Anderson |

*14.4. CURFEW TAGS: GPS AS POLICEMAN*

Privacy law in some countries would make that difficult; in egregious cases, such  
 as toxic waste dumping, the authorities can always subpoena the driver’s mo-  
 bile phone history5. Meanwhile, vendors offer ﬂeet management systems with  
 automatic infringement checking, assuring ﬁrms that this will minimise liability.  
 We will have to wait and see how this all works out.

But what might be the practicalities of requiring constant GPS monitoring?

We can get some insight from our next application.

**14.4** **Curfew tags: GPS as policeman**

My third case study of monitoring and metering is the curfew tags that criminal  
 suspects and paroled offenders wear on their ankles in order to constrain and  
 monitor their movements. Introduced in Britain in 1999, they are used to cut the  
 prison population. Most offenders are released after serving half their sentence  
 and spend some of their parole period under curfew, which typically means that  
 they must stay at home from 7pm to 7am. They wear a curfew tag on an ankle  
 bracelet which communicates with a home monitoring station. Others receive  
 community sentences instead of prison, with a curfew. Some 20,000 offenders  
 may be ‘on tag’ at any one time.

Curfew tags have spread to many other countries too. The more expensive

tags contain GPS chips and report the tag wearer’s location constantly to the  
 police. In Britain, these devices are worn by sex offenders whose curfews prohibit  
 them from going near schools, by persistent offenders in some police areas, and  
 by terrorism suspects. In France, they’re being introduced in domestic violence  
 cases [478]. In the USA, they’re offered to many suspects pre-trial as a condition  
 of bail (of whom the most famous may have been Harvey Weinstein). There,  
 the issue is that while the Federal government pays for its prisoners’ tags, 90%  
 of cases are raised by states and cities, which mostly force the tag wearer to  
 pay. Monitoring is dominated by two companies which typically charge $10

a day, with $350 up front. (When government pays, they only get $2–3 a

day.) So poor defendants get into debt, or get jailed for nonpayment. This is  
 short-sighted, as jail costs about $100 a day. Given that the USA has about a  
 million people awaiting trial in jail at any time, this is a policy issue with real  
 consequences; the number of tag wearers is over 125,000 and has been rising  
 since the First Step Act of 2018. Judges see monitoring orders as cost-free; they  
 issue them defensively, steadily widening the scope; two-thirds of tag wearers  
 are African-American; and unlike with bail, defendants don’t get their money  
 back if acquitted [1074].

In 2013–6, I was involved as an expert witness in a number of curfew-tag

cases. The ﬁrst, in 2013, involved a woman convicted of shoplifting who was  
 accused of tampering with her curfew tag as it indicated on several occasions  
 that she’d left home in the evening. Analysis of the logs relating to my de-  
 fendant’s case showed large numbers of false alarms; some of these had good  
 explanations (such as power cuts) but many didn’t. The overall picture was of

5All vehicles under 3.5 tons in Europe are required to have embedded phones for eCall

emergency service; this is unfortunately not mandatory for larger vehicles, no doubt because  
 of industry lobbying.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 477 | Ross Anderson |

*14.4. CURFEW TAGS: GPS AS POLICEMAN*

an unreliable technology surrounded by chaotic procedures and conﬂicts of inter-  
 est. The tagging contractor, Serco, not only supplied the tags and the back-end  
 systems, but the call centre and the interface to the court system. What’s more,  
 if you break your curfew, it isn’t the public prosecutor that takes you before  
 the magistrates, but the contractor – relying on expert evidence from one of its  
 subcontractors, who helped design the system. We asked the court for access  
 to the tag in the case, plus a set of tagging equipment for testing, the system  
 speciﬁcations, false alarm statistics and audit reports. The contractor promptly  
 replied that “although we continue to feel that the defendant is in breach of the  
 order, our attention has been drawn to a number of factors that would allow me  
 to properly discontinue proceedings in the public interest” [83].

Several months later, there was a case involving several men subject to ‘ter-

rorism prevention and investigation measures’ (TPIM) orders. These were a  
 measure introduced in 2011 that allows the UK government to impose curfews  
 on individuals believed to be a terrorist threat but against whom there is insuffi-  
 cient evidence to mount a prosecution; they have been controversial on human-  
 rights grounds. A number of individuals were served with orders restricting their  
 movements and ﬁtted with GPS tags to monitor compliance. These tags tended  
 to break off after about six months, whereupon the men were prosecuted for tag  
 tampering and imprisoned. As this was covered by a secrecy order, the pattern  
 only came to light when it was noticed by a London law ﬁrm that represented  
 three of them. Again, the government refused to expose any evidence to expert  
 examination, and the three men were acquitted, causing embarrassment to the  
 then Home Secretary, Theresa May [**?**]. A few days later, one of them evaded  
 surveillance by donning a niqab in a London mosque and leaving as a woman.  
 This caused outrage in the press [1904]. The following month, it turned out that  
 the two main UK curfew tag contractors – Serco and G4S – had been defrauding  
 the government at scale, by charging tag fees for offenders who had been ac-  
 quitted or who were in prison, abroad or dead, and that this had been going on  
 since the contracts started in 2005. They were stripped of their contracts and  
 the matter was referred to the Serious Fraud Office [1286]. Serco was eventually  
 ﬁned £19.2m in 2019 and ordered to pay £3.7m costs; its accountants, Deloitte,  
 were ﬁned £4.2m for audits they conducted of the tagging operation.

The dependability of curfew tags came to trial in 2014 in the case of yet

another terrorism suspect who was being held in immigration detention, accused  
 of tag tampering, which he denied. This time the government decided to risk  
 a trial. The suspect’s lawyers instructed me and a colleague at our Materials  
 Science department as experts. We formed the hypothesis that the stress of  
 wearing a heavy tag would lead to a fracture of the strap’s ﬁxing, particularly  
 for a devout Muslim who prayed ﬁve times a day. The court duly ordered that  
 the two of us, and a Saudi research student at our lab, be ﬁtted with GPS  
 tags, and we rigged up accelerometers and strain gauges to monitor the test.  
 While the student’s tag survived several days of prayer, my tag broke off when  
 I caught it on a radiator at home, and my colleague’s after he wore it while  
 playing football. The speciﬁcation called for the tag to withstand a 50kg pull,  
 and the operating company (which had taken over the business from G4S but  
 still used the same specialist subcontractors) claimed that the material from  
 which it was made was not liable to fatigue fractures. The government refused  
 however ‘for reasons of commercial conﬁdentiality’ to reveal what this material

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 478 | Ross Anderson |

*14.4. CURFEW TAGS: GPS AS POLICEMAN*

was. No matter; a test of a sliver from the broken ﬁxing lug revealed that it was  
 a polycarbonate that does indeed suffer fatigue fractures. The court ordered us  
 to hand back all our samples ‘to protect the contractor’s intellectual property’  
 but did not impose a secrecy order on our expert report, which can be found  
 at [85]. This suspect was also eventually freed by the court.

By 2015–6 GPS tags, from a new supplier, were being used by the Kent police

to monitor petty offenders. The supplier initially made inaccurate claims about  
 GPS accuracy (salesmen don’t like to admit anything is less than perfect), and  
 there were a couple of trials. This forced us to study the security and reliability  
 of GPS, or more generally GNSS (a term that includes not just the original US  
 service but the European Galileo system plus the Russian and Chinese offerings).  
 In such services, a constellation of satellites each broadcasts a very accurate time  
 signal, and a receiver seeing four or more of these can solve for its position and  
 time. In practice it takes more than that. First, the signal’s propagation depends  
 on conditions in the ionosphere, which are variable, leading to error unless this  
 can be calibrated against reference stations – a technique called augmentation,  
 which is used in aircraft navigation and can result in a precision of 2m. The  
 accuracy of consumer equipment is more like 10m on average, but it can be  
 signiﬁcantly worse, for several reasons.

First, if the visible satellites are clustered close together this dilutes the

precision, which may happen if only a few satellites are visible. In this case,  
 you can look up the resulting *dilution of precision* and use it to estimate the  
 error. (For the key ﬁxes in our ﬁrst case, only ﬁve satellites were visible and  
 the expected error was 45m; there are websites where you can look this up  
 as a function of location and time.) Second, many consumer devices (such

as phones) have *snap-to-ﬁt* software that automatically places the device on  
 the nearest road or path. Third, even larger errors can come from multipath  
 – typically when a signal reﬂected from a building competes with the direct  
 signal. The combination of multipath and snap-to-ﬁt is what causes your phone  
 or your navigator to jump from one street to another when driving or walking  
 through a town with tall buildings. Finally, there are various kinds of jamming,  
 ranging from barrage jamming that simply denies service to more sophisticated  
 strategies such as *meaconing* in which a decoy retransmits the radio spectrum  
 observed at another location, causing GPS equipment to believe it is at that  
 location instead. Until recently, GPS jamming was something governments did,  
 but the advent of low-cost software radios is starting to spread the fun. If I were  
 a gangster on tag, I could use meaconing to provide an alibi: it would tell the  
 police I’d been at home while I’d actually gone out and shot someone.

If you’re going to base a business on GPS, whether directly or by relying on

an underlying mapping service, it’s a good idea to understand not just the av-  
 erage error but the worst case, and the circumstances in which such outliers can  
 arise6. It’s possible to do better than commodity equipment, whether by using  
 professional equipment or by using clever signal processing. One of my post-  
 docs, Ramsey Faragher, did a startup (Focal Point Positioning) which applies  
 interferometry to successive GPS ﬁxes in order to increase accuracy and detect  
 both multipath and many kinds of jamming, supporting precision of about one

6You should employ at least one engineer who’s read up on the subject (such as via [1017])

and follows the relevant blogs (such as https://www.insidegnss.com.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 479 | Ross Anderson |

*14.5. POSTAGE METERS*

metre7.

At the organisational level, the court cases gave insight into how the tech-

nology was working its way into police practice. A signiﬁcant proportion of  
 burglaries are committed by ‘proliﬁc persistent offenders’ – typically men with  
 drug and alcohol problems with dozens of convictions for minor offences. (Our  
 ﬁrst case was of a man alleged to have snuck into someone’s kitchen and stolen  
 a bottle of wine from the fridge.) If police ﬁt their ‘frequent ﬂiers’ with curfew  
 tags, then when a burglary was reported they can simply look up to see if any  
 of them had been within 100 yards, and if so send a car to pick them up. This  
 may help the police drive down the crime statistics by locking up the frequent  
 ﬂiers for ever longer sentences; it might be less optimal socially if it ﬁlls up the  
 jails with men who should be on rehab or receiving psychiatric care – or if it  
 diverts attention from the more capable offenders.

**14.5** **Postage Meters**

My fourth case history of metering is the postage meter. Postage stamps were  
 introduced in Britain 1840 by Sir Rowland Hill to simplify charging for post,  
 and developed into a special currency that could be used for certain purposes,  
 from paying for postage to paying certain taxes and topping up the value of  
 postal money orders. Bulk users of the postal system started to ﬁnd stamps  
 unsatisfactory by the late 19th century, and the postage meter was invented in  
 1889 by Josef Baumann. Its ﬁrst commercial use was in Norway in 1903; in the  
 USA Arthur Pitney and Walter Bowes had a meter approved for use in 1920  
 and built a large business on it. Early postal meters were analogue, and would  
 print a stamp (known as an indicium) on a letter, or on a tape to stick on a  
 parcel. The indicium had a date so that old indicia couldn’t be peeled off and  
 reused. Each meter had a mechanical value counter, protected by a physical  
 seal; every so often you’d take your meter into the post office to be read and  
 reset. Fraud prevention relied on users taking their mail to the local post office,  
 which knew them; the clerk could check the date and the meter serial number.

In 1979, Pitney Bowes introduced a ‘reset-by-phone’ service, which enabled

ﬁrms to buy an extra $500 worth of credit over the phone; the implementation  
 involved a mechanical one-time pad, with the meter containing a tape with  
 successive recharge codes [477]. In 1981, this was upgraded to a DES-based  
 system that enabled a meter to be recharged with any sum of money. The

recharge codes were calculated in part from the value counter – so if the ﬁrm  
 lied about how much postage they’d used, they couldn’t recharge the device.  
 However, these meters still produced inked indicia.

In 1990, Jos´e Pastor of Pitney Bowes suggested replacing stamps and indicia

with printed digital signatures [1497]. This caught the attention of the US Postal  
 Service, which started a program to investigate whether cryptography could help  
 produce better postage meters. One concern was whether the availability of color  
 scanners and copiers would make stamps and indicia too easy to forge. A threat  
 analysis done for them by Doug Tygar, Bennett Yee and Nevin Heintze revealed  
 that the big problem was not so much the forging or copying of stamps, or even

7Full disclosure: I invested in the company.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 480 | Ross Anderson |

*14.5. POSTAGE METERS*

tampering with meters to get extra postage. It was bulk mailers corrupting  
 Postal Service employees so as to insert truckloads of junk mail into the system  
 without paying for them [1912]. As a bulk mailer on the ﬁddle would risk

arousing the suspicion of postal staff, there was a temptation to cut them in  
 on the deal; and then it was natural to forge a meter plate whose inducting  
 post office was elsewhere. By 1990 US Postal service losses were in nine ﬁgures,  
 and through the 1990s there were a number of high-proﬁle convictions of bulk  
 mailers who had manipulated their meters, getting away with millions of dollars  
 of free postage [265].

This led to a development programme for a meter using digital signatures,

generated by tamper-resistant processors in the postage meters. This was de-  
 veloped into an open standard available to multiple competing manufacturers.  
 The basic idea is that the indicium, which is machine-readable, contains both  
 the sender and recipient postal codes, the meter number, the date, the postage  
 rate, the amount of postage ever sold by the meter and the amount of credit  
 remaining in it, all protected with a digital signature. The private signature  
 key is kept in the meter’s processor while its corresponding public signature  
 veriﬁcation key is kept in a Postal Service directory, indexed by the meter se-  
 rial number. In this way, postal inspectors can sample mail in bulk at sorting  
 offices, checking that each item is not only franked but on a logical route from  
 its ostensible source to its destination.

The USA introduced the technology in 2000, with traditional suppliers such

as Pitney Bowes selling traditional meters while startups such as stamps.com  
 obtained licenses to generate indicia online so that customers could download  
 them and print them on their computers at home. Germany and the UK were  
 next in 2004 and Canada in 2006; other countries followed suit. By 2006, all  
 US postal facilities had the scanners needed to read the new indicia, of which  
 an example is illustrated in Figure 14.4 below.

Town Circle or Postmark

Licensing Post Office/Mailed From ZIP Code

|  |  |
| --- | --- |
| FIM Mark | Date of Mailing (as required) |

Postage Amount

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| |  | | --- | |  |   optional  advertising | MERRIFIELD VA 22180 | $0.32 | Rate Category |
| March 31, 1998 | FIRST-CLASS |
|  | |
| art area |

US POSTAGE DEVICE 12345678901234

Device ID

Two Dimensional Barcode

|  |  |
| --- | --- |
| •Licensing ZIP Code  •Destination ZIP Code  •Software ID  •Ascending Register  •Descending Register | •Signature Algorithm Flag•Digital Signature  •Device ID •Rate Category  •Date of Mailing •Reserve Field  •Postage •Version |

Figure 14.4: – one of the new formats for US postal meters (courtesy of Symbol  
 Technologies)

Such indicia can be produced by postage meters that are drop-in replace-

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 481 | Ross Anderson |

*14.5. POSTAGE METERS*

ments for the old-fashioned devices; you weigh a letter, frank it, and get billed at  
 the end of the month. You don’t have to take the meter in to be read though, as  
 that can be done over the Internet for a credit meter, while if you buy a prepay-  
 ment meter you replenish it by phoning a call centre and buying a magic number  
 with your credit card. This works in much the same way as the prepayment  
 electricity meters discussed earlier in this chapter.

Indicia can also be bought over the Internet by simply specifying the sender

and destination postal codes. This ‘online postage’ is aimed at small ﬁrms and  
 people working from home who don’t send enough mail for it to be worth their  
 while buying a meter. Both metered and online postage are cheaper than stamps  
 to distribute. It has also become possible to manage the system much better,  
 by tracking volumes and proﬁtability of mail down to local level. So, all told,  
 digital post offers more ﬂexibility to both users and postal services. But what  
 about security?

Postage meters are a slight extension of the utility metering model. There’s

a tamper-resistant processor, either in the meter itself, or attached to a web  
 server in the case of online postage; this has a value counter and a crypto key.  
 It dispenses value by creating indicia until the value counter is exhausted, then  
 requires replenishment from a control unit higher up in the chain. There are  
 some additional features in each case. Many postage meters include a ‘Clark-  
 Wilson’ feature whereby the value counter actually consists of two counters, an  
 Ascending Register (AR) containing the total value ever dispensed by the meter,  
 and a Descending Register (DR) indicating the remaining credit. The balancing  
 control is AR + DR = TS, the ‘total setting’, that is, the total of all the sales  
 made by or authorised for that device. If the balance fails, the meter locks up  
 and can only be accessed by inspectors.

The full threat model includes stolen postage meters, meters that have been

tampered with to provide free postage, genuine meters used by unauthorised  
 people, mail pieces with indicia of insufficient value to cover the weight and  
 service class, and straightforward copies of valid indicia. Various sampling and  
 other tests are used to control these risks. Subtleties include how you deal with  
 features like certiﬁed mail and reply mail. There are also national differences  
 on matters ranging from which authentication algorithms are used to what sort  
 of usage data the meters have to upload back to the postal service.

Once operators got real experience, the industry started to move away from

digital signatures to message authentication codes. Signatures appealed because  
 they were elegant; but in real life, signature veriﬁcation is expensive, and has  
 also turned out to be unnecessary. Equipment at major sorting offices must  
 process thousands of mail pieces a minute, and postal services usually verify  
 indicia as an offline batch operation. Forged mail pieces go through initially  
 and are only intercepted once a pattern of abuse emerges. Once veriﬁcation is  
 centralised, MACs make more sense than signatures; the central servers have  
 hardware security modules with master keys that are diversiﬁed to a MAC key  
 in each meter, just as with utility meters. It turns out that two-digit MACs are  
 enough to detect systematic abuse before it becomes signiﬁcant [477].

In many countries, the postal service contracts all the cryptography out to

the meter vendors. So indicia are veriﬁed only in the home postal system, as

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 482 | Ross Anderson |

*14.6. SUMMARY*

overseas systems will often use different vendors. We also see a diversity of

architectures. Canada, for example, uses both signatures and MACs on its

indicia. (And if you want to bribe a postal employee to let a few tons of junk  
 mail into the system, the place to do it is now at a border crossing.)

How stuff actually breaks in real life is – as always – instructive. In the

German post office’s ‘Stampit’ scheme, a user buys ‘smart pdf’ ﬁles that contact  
 the post office to say they’re being printed, without any interaction with the  
 user or her software. If the paper jams, or the printer is out of toner, then  
 tough. So users arrange to photocopy the stamp, or to copy it to a ﬁle from  
 which it can be printed again if need be. The UK system has learnt from this:  
 although a stamp is grey-listed when a user PC reports that it’s been printed,  
 the grey doesn’t turn to black until the stamp appears at the sorting office. The  
 difference in syntax is subtle: the German system tried to stop you printing the  
 stamp more than once, while the British system more realistically tries to stop  
 you using it more than once [884].

All told, moving to digital postal meters enabled much better control than

was possible in the old days, when postal inspectors had to refer to paper records  
 of mechanical meter readings. It also facilitates business models that extend  
 the service to many more customers and that also improve the post office’s cash  
 ﬂow and credit control. Unlike digital tachographs, digital postal meters have  
 brought real beneﬁts.

**14.6** **Summary**

Many security systems are concerned one way or another with monitoring or  
 metering some aspect of the environment. They range from utility meters to  
 taxi meters, tachographs, and postal meters. We’ll come across further metering  
 and payment systems in later chapters, such as the mechanisms used to stop  
 printer cartridges working once they have printed a certain number of pages.

Many monitoring, metering and payment systems have been redesigned as

the world moved from analogue to digital technology. Some of the redesigns  
 have been a success, and others less so. Digital prepayment electricity meters  
 have been a success, as they enable utility companies in the developing world  
 to sell power to hundreds of millions of people who don’t even have addresses,  
 let alone credit ratings. Digital tachographs have been less impressive; they just  
 do what the old analogue systems did, but less well. Their slow evolution was  
 perhaps inevitable given the many entrenched stakeholders and the lack of op-  
 portunity for a disruptive process change, as the goal was securing compliance  
 by a mature industry with existing safety law. Our third example, the curfew  
 tag, extends location monitoring from vehicles to human beings. It has sup-  
 ported some innovation, since technical offender monitoring is a new industry;  
 it also teaches us some of the limits of using GPS in large complex systems. Our  
 fourth example, the postage meter, did allow some competitive innovation and  
 has been a success.

As with burglar alarms, the protection of monitoring systems is tied up with

dependability. You have to think long and hard about what sort of service denial

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 483 | Ross Anderson |

*14.6. SUMMARY*

attacks are possible. Key management can be an issue, especially in low-cost  
 widely-distributed systems where you can’t provide a central key management  
 facility or hire enough trustworthy people. Systems may have to deal with

numerous mutually suspicious parties, and must often be implemented on the  
 cheapest possible hardware. Many of the monitoring devices are in the hands  
 of opponents. And there are all sorts of application-level subtleties that have to  
 be understood if you want your design to succeed.

**Research Problems**

There’s a lot of talk about the ‘Internet of Things’ but few concrete examples for  
 researchers to think about. Case studies such as those described here may help.  
 Although the mechanisms (and products) developed for payment networks can  
 be adapted (and are), much of the design work has to be redone and the end  
 result often has vulnerabilities. Metering applications are particularly useful  
 because of the pervasive mutual mistrust caused not just by competing com-  
 mercial entities but by the presence of dishonest staff at every level, as well as  
 dishonest customers; and the fact that most of the equipment is in the custody  
 of the attackers.

Again, there are questions for security economists and scholars of innovation.

Why did some digital transformations of existing metering systems work well  
 (utilities, postage) while others were less impressive (tachographs)? Why were  
 some disruptive, in that new entrants successfully challenged the previous in-  
 cumbent suppliers, while in other cases (such as postage) the existing suppliers  
 managed the transition to better digital systems and survived despite innovative  
 competition from dotcom startups?

**Further Reading**

Prepayment electricity meters are described in [93]. Tachographs are written  
 up in [64]; other papers relevant to transport appear in the annual ESCAR  
 conference on electronic security in cars. The early work on postal meters is  
 in [1912] and the US regulations can be found in [1320]. However the most  
 detailed exposition of postage meter security is a book by Gerrit Bleumer of  
 Francotyp-Postalia, which played a leading role in the program [265].

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 484 | Ross Anderson |