On the Security of Digital Tachographs *

Ross Anderson
Cambridge University Computer Laboratory
Pembroke Street, Cambridge CB2 3QG
rja14@cl.cam.ac.uk

Executive Summary

Tachographs are used in most heavy vehicles in Europe to control drivers' hours, and for secondary purposes ranging from accident investigation to the detection of fraud. Their effectiveness is under threat from increasing levels of sophisticated fraud and manipulation. We examine this in the context of recent EU proposals to move to smartcard-based tachograph systems, which are aimed at cutting fraud and improving the level of enforcement generally. We conclude that the proposed new regime will be extremely vulnerable to the wholesale forgery of smartcards and to system-level manipulation; it has the potential to lead to a large-scale breakdown in control. We then sketch some potential solutions.

1 Introduction

Vehicle accidents where the most likely cause was the driver falling asleep at the wheel account for about 16% of the total on all UK roads, and about 23% on motorways in one study [13]; for 10% and 25% in a second [24]; and 10–30% according to a third source [22]. Death or serious injury is significantly more likely than in other types of accident, probably because of the greater speed on impact [29]. Consistent figures have been reported from the USA, Germany, Israel and Sweden [13]. By comparison, vehicle accidents where alcohol is a significant contributory factor range from 3.1% in the UK through 4.9% in Sweden and 9.5% in Germany to 14.1% in Finland [31].

Heavy commercial vehicles are a particular problem as they can do much more damage in a crash. Although they are involved in only 6% of serious accidents, these include 16% of fatal accidents [4].

In Europe, the principal control on the hours worked by heavy vehicle drivers is the tachograph — a device fitted behind the speedometer which logs the vehicle's speed, distance and mode of work on a waxed paper chart, in the centre of which the driver must write his name, starting location, vehicle number, date and odometer reading before starting his journey. Tachograph use is mandatory for most heavy trucks in the European Union, and about half the bus and coach fleet. Drivers must carry their charts for the current week and the last driving day of the previous week; older charts must be stored at the employer's premises until they are one year old.

Although the system was introduced to control drivers' working hours, it has since acquired a number of other uses. The police find tachograph charts helpful in investigating accidents and other offences, including drug smuggling and unlicensed toxic waste dumping, while many operators use them to prevent theft of fuel by drivers (which can amount to 5,000 ECU per vehicle per year otherwise) [27]. Almost a third of tachograph charts are already scanned by fleet operators or bureaux and fed into fleet management systems for this purpose; the operators at least would welcome digital tachographs. However, safety remains the main purpose of the system.

Driving heavy vehicles is a dangerous job, even with a model employer. Shell Petroleum reports 50 deaths per 100 million duty hours for drivers, against 2.7 deaths per 100 million duty hours in the rest of a relatively hazardous industry. There are many less perfect employers: a union poll reveals that 40% of employed drivers had been asked to exceed their duty hours in the previous month, while self employed drivers are even worse violators [22].

The UK with tight enforcement has proportionally fewer fatal accidents involving heavy vehicles than any other member state [22], despite UK drivers' average working week being longer than the average for other EU countries [12]. This suggests that enforcement of driving time is more important than controls on total work time.

About 50 fatalities a year result from sleep-related accidents involving heavy vehicles in Britain [4]; perhaps half of these might be prevented by draconian enforcement of driving hours regulations, while the

*This paper reports research funded by the Department of the Environment, Transport and the Regions during 1997–98.

total might be doubled by a breakdown in control. In countries with lax enforcement, the prospective gains should be higher and the potential losses lower. In total, a uniformly high level of control might save the EU several hundred lives a year and a sum in the high hundreds of millions of ECUs, while a breakdown might have additional human and economic costs on the same scale.

Although these are only order-of-magnitude figures and more detailed research would be useful, there are clear safety and social interests in enforcing driving hours regulations, as well as a competitive issue for law-abiding drivers and companies.

2 Tachograph Tampering and Fraud

There is therefore great concern at a growing wave of tachograph fraud and tampering, by which both drivers' hours and speed regulations are flouted on a large scale. Most of this fraud is motivated by economic pressures on vehicle operators, and might be reduced by better tachograph systems.

Good security engineering requires a detailed understanding of threats. We therefore list here the main techniques used at present for tachograph fraud and tampering. Our figures for their relative prevalence come from a recent survey by the UK Vehicle Inspectorate of convictions for tachograph offences [10]: the sample size was 1060, made up of 854 convictions of drivers and 206 convictions of operators.

1. Most offences that result in conviction do not involve tampering but exploit procedural weaknesses. These accounted for 68% of driver and 71% of operator convictions.

    - A very common fraud is 'ghosting' — manipulating tachograph charts so that there appear to be more drivers than there actually are. 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; the distance is about 800km and the journey takes about 10 hours which is illegal for a single driver to do on a daily basis.

      The standard fiddle is to have two drivers, who meet en route at Penrith, change trucks, and insert new paper charts into the tachographs. The driver who had come from Southampton now returns with the vehicle from Dundee. When stopped and asked for his charts, he would show the current chart from Penrith to Southampton, the previous day's for the leg from Southampton to Penrith, the day before's for Penrith to Southampton, and so on. In this way he would 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 widespread [23].

    - Much casual deceit involves very simple manipulation, such as altering the clock to simulate a rest period, inserting a fresh tachograph chart and hiding the old one, forging a chart by hand (perhaps with the help of compasses or bottle tops) or even driving with no chart at all and hoping to produce an old one by sleight-of-hand if stopped [32]. These tricks are likely to be detected if the vehicle is stopped by an alert officer; they are often used when a normally honest driver is delayed and is under pressure to deliver a load rather than take an unscheduled break.

    - More sophisticated procedural frauds include 'forgetting' to write the date on the chart centre field, representing a hitch-hiker as a co-driver, using a chart for a 140 km/h tachograph in a 125 km/h device, filling completely fictitious centre field details, and representing the start point of the journey as an obscure or commonly named village, in order to make geographical distance tracing as hard as possible for enforcement officers [23] — for example there are 17 villages in Spain called 'La Hoya'. As with ghosting, such tricks often involve collusion with the operator. Often, when the operator is ordered to produce charts and supporting documents such as pay records, weighbridge slips, ferry tickets etc., his office will conveniently burn down.

2. The next largest category of fraud involves tampering with the supply to the tachograph instrument, including interference with the power and impulse supply, cables and seals. Offences involving electronic tachographs amounted for 23% of driver convictions and 18% of operator convictions; offences involving the older mechanical instruments added another 2% and 3% respectively.

    - Such frauds often involve collusion with fitters. Electronic tachographs get their input from a sensor in the gearbox, which sends electrical impulses as the prop shaft rotates, and a common attack is to unscrew it about

2mm. This 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 kept by workshops rather than by individual fitters complicates prosecution.

- Some determined offenders fit a switch into the cable so that the input can be drawn either from the real gearbox sensor or from an additional sensor that is mounted under the driver's seat rather than being rotated by the gearbox [23]. At least one operator has had all its vehicles wired to interrupt impulses on demand.
- However the two most common techniques are very simple: to insert an earthing wire into the cable, thus shorting out the impulses, and to replace the tachograph fuse with a blown one. The incidence of the former attack has been reduced recently by a switch to armoured cables [1], but blown fuses continue to provide a plausible excuse [23].

3. The third category of fraud is tampering with the tachograph head itself (the unit mounted behind the speedometer). 4% of driver offences, and 5% of operator offences, are ascribed to this kind of abuse of the older mechanical tachographs, with a further 1% and 2% respectively booked for attacks on the newer electronic devices.

   Most tachograph head tampering involves miscalibration, which is often performed with insider assistance. Tachograph heads contain potentiometers or switches with which the radius of the road wheels can be set, thus translating impulses into distance and impulse rates into speed. Corrupt fitters often set these to indicate some 90% of the actual road speed. Drivers may also break seals and change the calibration directly [25], and steam cleaning often destroys seals anyway thus providing a good excuse. In some cases, drivers have broken seals and repaired them invisibly [11, 23]. The current seals are easy for skilled persons to defeat, and their knowledge is spreading rapidly [16]. Work needs to be done urgently in this area.

   The remaining attacks tend to exploit vulnerabilities discovered by chance, knowledge of which spreads more rapidly among drivers than among policemen. They include:

   - in many devices, one can bend the styli that write on the chart and thus falsify the recorded speed [25];
   - one device can be caused to register zero speed by inserting a piece of wire into the tachograph head. This shorts the circuitry to earth without breaking the seal. In another device, an earth wire can similarly be inserted into a sealed cable joint. These wires can be pulled out in a second if the vehicle is stopped by police [25];
   - the earlier electronic tachographs had the power for the impulse generators and head motors wired through the ignition circuit to minimise battery drain, while the clock and lighting circuits come directly from the battery. However diesel engines once started can run with the ignition off, in which case the device is frozen. If the driver turns off the ignition before moving off, all three traces will indicate a vehicle at rest;
   - in some of the following generation of electronic tachographs, the clock and the chart table motors operated at different voltages, so the device could be frozen by reducing the supply voltage. In one model, the overspeed warning light helpfully came on at just the right voltage [23];
   - with some models, one could wire up a flasher unit to interrupt the supply voltage and thus reduce the rate at which the chart table turned;
   - when features to detect supply voltage interruption were introduced [2], implementation was poor. In one device, an alarm causes the speed stylus to strike downwards, which has no effect if the vehicle is stationary when power is resumed [23]. In all currently manufactured tachographs, the undervoltage alarm can be suppressed by connecting two generally unused terminals together;
   - with one model, the driver can press down on the centre of the speedometer plastic and prevent the needle from moving when he accelerates from (say) 30 to 60 km/h. As the assembly is driven by a stepper motor, both the speedometer and the underlying tachograph will register 30km/h less than

[1] Commission Regulation 2470/95

[2] as a result of Commission Regulation 3314/90

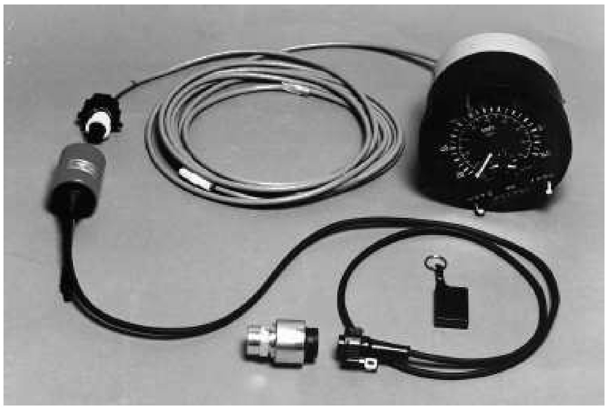

Figure 1: A tachograph with an interruptor controlled by the driver using a radio key fob.

the true speed until this speed next drops below 30km/h.

4. The state of the tampering art is the radio controlled interruptor device depicted in figure 1. This is a red plastic cylinder bearing the inscription 'Voltage Regulator — Made in Japan' but which is actually inserted into the tachograph cable and controlled by the driver from the cab 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 become inactive so that the tachograph and speed limiter return at once to proper operation. Such devices are extremely hard to find as they can be hidden at many different places in the truck's cable harness; miniature versions are even found inside the tachograph head itself. Police officers who stop a speeding truck equipped with such a device, and cannot find it, have difficulty getting a conviction as the sealed and apparently correctly calibrated tachograph contradicts the evidence from their radar or camera.

   Only six convictions — five driver and one operator — fall into the category of 'Radio controlled devices etc' but intelligence suggests that their use is becoming widespread; the lack of convictions is due to the difficulty of detection. In fact, tampering offences in general are most frequently detected by procedural rather than technical controls — it being impossible to drive from Dundee to Southampton (say) in 600 km.

As with many of the so-called 'victimless' crimes that are usually detected only by enforcement action, hard figures on the extent of tachograph manipulation are not readily available. In any case the extent and methods of fraud vary by country. In countries with poor enforcement, drivers may simply not use charts at all (industry sources named two member states with negligible chart sales).

However, the consensus of informed people in the UK is that maybe 5–10% of drivers are persistent offenders and about half offend occasionally. The persistent offenders tend to be associated with certain operators, some 20–40% of whose vehicles turn out to have signs of past tampering when examined closely at inspection stations. These signs include seal defects, calibration faults and suspiciously loose wiring [34]. The significance of this is that well funded attempts to defeat future tamper proofing systems can be anticipated; one operator with over a dozen tachograph convictions has over 500 trucks.

Tachograph tampering brings secondary safety hazards, in that most heavy vehicles must now be fitted with speed limiters, which are usually driven from the tachograph head. So drivers who wish to exceed the speed limit may tamper with the tachograph, and drivers who tamper are tempted to speed as well. Speed limiter tampering is even more widespread than tachograph tampering (as drivers can also attack the limiter, and the cable between it and the tacho head, in various ways). Unfortunately, the introduction of limiters has caused some truck makers to de-rate tyres and other systems, making speeding significantly more hazardous.

One might think that as vehicle systems become more integrated, using standards such as CAN-BUS, tampering would decrease because unauthorised modifications to systems can have a side-effect on safety. Experience shows that this hope is vain. One truck ran its antilock braking system from the same circuit as the tachograph, so that a driver who replaced the fuse with a blown one would disable his ABS. Many drivers still replaced the fuse; the same happened when speed limiters were powered from this circuit.

It might also be thought that the situation has been improving over time, with more recent tachographs being more resistant to tampering. This is not the case; the move from mechanical to electronic equipment led to a tenfold rise in convictions for tampering with the supply. Older devices used rotating wire cables and an attempt to physically jam the odometer caused gear teeth to strip or the cable to shear; the move to electrical impulses was a large setback for enforcers as it enabled odometer jamming (which in turn made other frauds harder to detect), while cable earthing and then interruptors opened up a whole new set of attacks.

Attempted improvements just made the frauds more complex and difficult to detect [23]; it also took time for enforcers to identify new fraud techniques and devise control strategies.

It is now generally agreed that the cable from the sensor to the tacho head should be protected by cryptography. But there is still no agreement about how, and it is unclear how unique crypto keys can be loaded safely into the sensor and the head when the fitters are in the pay of the attacker. (In fact, one supplier has proposed loading the same crypto key into every sensor unit.)

It may be thought that the problems are primarily technical, and that the combination of cryptography, better seals and improved tamper resistance generally would cut the incidence of fraud. Experienced enforcement officers disagree, and hold that the main problem is getting the right enforcement priorities in place. In some countries, as noted above, enforcement is almost non-existent. The EU has set a target of 1% of charts to be inspected, but this is ignored by some governments. Even this relatively low target reflects the level of enforcement that current tachographs can deliver without the cooperation of fleet operators in scanning charts. Enhancing enforcement without greatly increasing costs is another justification for the proposed change.

In the UK, the EU target is exceeded, but fines are low (typically £50 for hours exceeded or failing to produce a chart, and £200 for falsification). As there is no central reporting from magistrates' courts, repeat offenders get away with it. (This problem is being worked on.) Meanwhile, a police priority is to increase the number of specialist enforcement officers [22]. Other problems include the many classes of vehicle exempted from the regulations (such as trucks in the utilities and other industries that were state-owned when Britain joined the EU) [6].

A further set of problems comes from the EU member states' different operational models. For example, in the UK much of the enforcement is done by roadside checks, while in the Netherlands it is mostly at operator premises. In addition, a variety of computer systems have been developed to support enforcement, and there are also the fleet management systems described above. The actual tachograph is thus a component of many different information and operational systems.

3 The Tachosmart Project

This is the background to the emerging consensus in Europe for action at the Community level to improve the dependability of drivers' hours recording [8, 32].

The EU tachograph market is dominated by two companies, VDO Kienzle of Germany and TVI of Britain, with about 75% and 25% respectively of an equipment market worth about 100 MECU per annum. Sales made by analysis bureaux, fitters, calibrators, suppliers of consumables and spare cables, etc., make up the total tachograph market value to some 300–400 MECU per annum — significantly less then the annual economic cost of sleep related accidents.

So a change to the system can be justified by enforcement considerations, and the EU has funded a 'Tachosmart' project to develop a more tamper resistant electronic replacement for the current chart-based systems. There have been three phases so far, and Tachosmart 3 resulted in prototype devices built by manufacturers in five different member states [30].

The prototypes use a smartcard rather than a chart to personalise the equipment. The main design change that this forces is that the vehicle speed history must now be kept in the vehicle unit's memory. The cards used in the prototype have 8K EEPROM of which a little over 5K is available for driver record keeping; production cards are planned to have twice as much memory. However, paper charts keep speed history with a resolution, under microscopic examination, of 1 second — equivalent to a capacity of several tens of kilobytes per chart. Recording 28 days' (or even 14 days') driving activity on a commodity smartcard is thus out of the question. So a smartcard based tachograph must either have auxiliary memory, store a compressed record, or both.

3.1 The draft council regulation

Prior to 1997, there were several years of disagreement between member states as to the best way to introduce digital tachographs. The main argument was whether to move to a fully digital system in one leap or migrate via an interim solution in which the paper chart would be retained but augmented with a smartcard. A majority of member states preferred the former, more radical approach. Another problem was that insufficient research and development was being done in the absence of an indication from the EU of the type of instrument that would be required. A draft regulation agreed in 1997 [8] sought to break this deadlock by making a clear statement that fully digital tachographs would be required and calling for a specification to be prepared as soon as possible. At the UK's request, the regulation makes type approval conditional on security of the system as a whole. This study is directly concerned with that requirement.

The draft regulations severely constrain the system design in three ways. Firstly, it is left to the discretion of member states whether operators should be required to download drivers' hours data, whether to their own systems or to a bureau, so that they would be available at a central point for inspection. Secondly, member states were not able to agree that operators should be compelled to retrofit digital systems, so analogue and digital systems will coexist for a long period (perhaps 15 years). Thirdly, the use of secure means of recording vehicle location (such as GPS units in tamper-resistant enclosures) is left as an option for member states, rather than being mandated across the EU.

3.2 The proposed solution

The proposed solution is that a memory in the vehicle unit will retain 365 days' drivers' hours data, plus a speed history for the last 24 hours. The driver card will have memory for 28 days' driving hours, but no speed history. There will also be cards for the vehicle operator, vehicle inspectors, calibration stations and fitters which will give differing kinds of access to the data in the vehicle unit. The vehicle operator, for example, will be able to download complete data for integration into his fleet management system. Some of the interfaces, including those between the various types of card and the vehicle units, will be standardised across the EU to allow interoperation.

In the prototype systems, the impulses are generated as before in a gearbox sensor, and passed to the vehicle unit (the means of protecting the impulses from tampering are left to the manufacturer). They are converted in the vehicle unit into a speed history which is retained in memory for 24 hours and may be downloaded using an operator or inspector card. The vehicle unit can also store more alarms than the card; typically 10–25 of each type. It will normally hold one or two cards, which in normal operation will be drivers' cards. It will then associate driver's and if appropriate co-driver's hours to them in its internal log. A much compressed history of drivers and hours will be kept for 365 days.

Cards (of whatever type) are authenticated to the tachograph by a bidirectional challenge-response using keys that are common throughout the system; data exchanges between tachographs and the cards carried by drivers and inspectors are claimed by the security specification to employ digital signatures [9]. However, the specification of the card contents does not contain enough room for signature keys [17, 18]. We conclude that, as often in the smartcard industry, 'digital signature' or 'data signature' actually means a message authentication code computed using a common secret. This leaves it unclear how signatures are to be verified in the software of external systems, and how the system will interact with the digital signature laws already introduced by Germany and Italy, and being developed by other member states.

Key material is loaded into drivers' cards by a national card issuing authority. The vehicle units are manufactured with embedded secret keys that are common throughout the system, and every time they are calibrated, new signature keys and certificates are loaded from a calibration card using the common secret for authentication. The protocols used are not specified in sufficient detail for close analysis.

In theory, the driver's card is retained in the instrument during driving (though ensuring this is harder than it looks), and at the end of the trip it is updated with a signed record of working hours plus the last three alarms (overspeeds, tampering events, etc) if any. The card can retain up to 28 days' records, depending on driving conditions.

At any time, an inspector can request a print-out from the vehicle unit in one of two ways. If he has a control card, he can obtain a signed copy of the contents of the tachograph memory transmitted to a lap-top over a serial link [19]; if not, the driver can print out appropriate data from the vehicle unit's memory and hand it to the inspector.

3.3 Anticipated problems

The simultaneous operation of vehicle fleets with paper charts and driver cards is expected to lead to serious enforcement problems. In cases involving ghosting, it is predicted that the operator will have one new vehicle that uses a card and an older one that uses charts. (This is expected to raise the price of older vehicles and depress new vehicle sales — an effect already seen with previous changes in regulations, not just for tachographs but also for speed limiters and emissions.)

Conscientious operators' fleet management systems will enable downloaded digital tachograph data to be merged with data from scanned analogue charts, fuel purchases, drivers' overtime etc. But, as noted above, there is no EU requirement for such systems. Some countries might consider making them mandatory at the national level, with controls mirroring those proposed for cryptographic systems in general [5] in that large companies would be trusted to run their own systems while the smaller operators would have to use an approved bureau service. This would extend the current system whereby the workshops of large, trusted operators may be approved as tachograph fitters while small operators must use third parties.

In countries where downloading is not mandated, the theory is that drivers would take paper printouts from any digital tachographs they used and keep them along with the paper charts from any analogue devices. This would make enforcement harder; the printouts from the Tachosmart prototype systems are much easier to forge than charts are. It is also unclear how operators could discharge their legal duty to maintain records of drivers' hours [8], as the vehicle units containing this information could be distributed all over Europe and beyond.

There will be serious consequences for competition and the internal market. From July 1998, the EU will have unrestricted cabotage — drivers from one member state will be able to carry goods in another state. The current wide variation in tachograph enforcement does not pose a competitive issue so long as the primary control is carried in the vehicle. However, if digital tachographs move the primary control to the computer system of the vehicle operator or his bureau, and this control is only effective in some countries, then drivers from other countries will have a competitive advantage which will exert downward pressure on the quality of control everywhere. This will be further complicated by the fact that there are vehicle operators with depots in (say) Belgium and Holland, and who operate a given vehicle out of both of them depending on the day of the week; there are also operators who share vehicles. Even more serious problems may come from non-EU vehicles. The proposals are silent on how the control factors, from card issue onwards, will be managed in that case.

The second set of anticipated problems comes from the loss of detailed redundant data. At present, fraud and accident investigation depends on comparing the speed and distance traces against the claimed journey end points and against other documents such as delivery notes and ferry tickets. In the digital system, speed history will be retained in the vehicle unit for only 24 hours, and if not downloaded will be lost; while journey end points will only be logged at the granularity of a region, as a keyboard to enter the names of towns would be expensive.

It is not clear how the inspector is to do his job in a digital environment. The detailed, redundant data on the chart often provides inspectors with grounds for suspicion to justify a detailed examination. However digital systems either indicate a violation or do not. Thus while the older analogue systems degrade gracefully under attack, digital systems fail abruptly. For example, the lack of journey end point data will remove the main current method of detecting tampering attacks. This means that a much higher level of tamper resistance is needed in the digital environment, to which we will return below. As for the use of additional inputs, the draft regulations permit countries to require inputs from GPS for domestic vehicle, if they wish ([8] article 15 clause 5a). However the Tachosmart standards do not support this — although there may be an interface port for GPS, which may be used if a manufacturer wishes to design a system that utilises a GPS receiver mandated by an individual member state, it appears that instruments available on general sale in the Community will not support GPS, which would make its use by individual member states difficult in a number of ways. Quite apart from single market issues, it would appear that GPS units carried by visiting vehicles would not be connected to the tachograph but carried as separate equipment; in that case, many of their enforcement benefits will be lost and the visiting vehicles would have a competitive advantage.

The third problem set concerns reliability. Smartcards started out as bank cards, designed to be used several times a week in cash machines; when they are used heavily in applications such as building access control and transport ticketing — and especially in grimy environments — common models experience failure rates of up to 7% per annum. This is not compatible with the expected 5 year card lifetime and 10,000 hour mean-time-to-failure [17], and would be a serious burden on companies and workshops given that cards are to be issued centrally with replacement taking as much as two weeks [20].

An unreliable system will facilitate such simple frauds by drivers and operators that it could bring the system into disrepute. By destroying the card (e.g. by applying mains electricity) a driver can eliminate a problematic record, and under the regulations he will be allowed to drive for 15 days without a card. Such card-destruction attacks have been perpetrated on bank smartcard systems in the UK, France and elsewhere; by forcing the system back on less secure stand-in procedures many avenues of abuse are opened up. One UK bank has had to open a specialist laboratory to examine failed smartcards presented by customers.

Other reliability issues impinging on security include the failure rate of printers in a commercial vehicle environment.

Many of these objections can be overcome by changes to the details of the specification. However there is a much more fundamental problem with the Tachosmart concept and that is the belief that smartcards are tamper-proof.

3.4 Smartcard Security Issues

The draft regulations state that 'the total system, including the connections to the speed and distance sensor, must be tamperproof' ([8] p 27). This cannot be achieved given the card technology currently available in Europe.

For years, smartcard vendors claimed that their products were tamperproof, or as nearly so as made no difference. In the last few years, this claim has been demolished by a large number of attacks on pay-TV and on other systems.

The state of the tampering art is constantly evolving. A number of historical attacks are described in [2], together with the techniques used by pirates in 1994-96. The state of the art in early 1998 is more advanced; professional pirates now use microscopes fitted with lasers and microprobes to extract card data quite rapidly. One technique is to fit a probe to the line that controls the instruction latch, and use this to prevent new instructions being loaded from the bus. Now when the card is clocked there will be no jump instructions, and all the words in memory will appear on the bus in sequential order. A second microprobe is then used to recover the memory contents from one bus line at a time.

The laser is used to remove the passivation layer from the card surface over the feature to be probed; this avoids removing the whole layer, which may set off an alarm in some card designs. It also creates a depression in which the microprobe will lie stably.

The cost of the laboratory equipment needed to perform this attack is about 150,000 ECU, though second-hand equipment is much cheaper. The equipment is also available at many university laboratories, and at least one EU university teaches chipcard breaking techniques to undergraduates as part of their course work [3].

The effect of attacks, carried out both by students and by professional pirates, has been to force pay-TV operators such as BSkyB to change their entire card base about once a year, moving each time to a new technology of card with ever more expensive tamper resistance mechanisms. To date, the pirates have managed to keep up; an example of the Sky series 9 card, opened with hand tools and yet still functional, can be seen in figure 2.

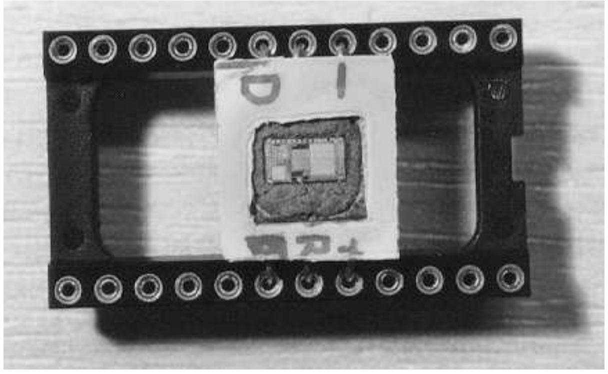

Figure 2: A Sky-9 smartcard processor prepared for microprobing attacks and still fully functional.

The arms race between attackers and defenders is expensive; for example, the technology supplier to BSkyB has seen its research department grow from 60 to 200 people over the past four years, while at a recent trial of a card forger, BSkyB claimed that forgery has cost them £30m [15]. Yet there is still no real breakthrough in tamper prevention, and senior scientists at some large semiconductor makers expect none, for reasons discussed in [2].

Attacks have mostly taken place on systems where universal secrets are stored in cards, and where the compromise of these secrets can enable cards to be forged and sold for mass use (such as pay-TV). They have not been widespread on cards that store only individual secrets and where forgery can bring only limited benefits (such as GSM SIM cards).

The system prototyped in the Tachosmart 3 project falls squarely into the former category. The workshop, operator and inspector cards contain only common secrets and so we expect that they will be rapidly duplicated and sold through the channels currently used to market interruptors (such as ferry terminals and transport cafes). The workshop card will enable alterations to be made to tachograph parameters. The calibration cards, if required after such changes (the specification is vague), contain a list of keys plus a common secret for authentication. These cards will also be duplicated as they will allow speed limits to be changed.

The workshop card can clear the tachograph memory and the calibration card can then be used to re-load keys. If a forged calibration card were used for initialisation of the device in the first place, then the original keys could be re-loaded thus causing an embarrassing record to vanish without trace.

If, as appears in [17, 18], the 'data signatures' do not really use asymmetric cryptography but message authentication codes (MACs) computed with shared secrets, then once these common secrets become known, the system will be completely broken. Pirates will be able to manufacture any type of card and forge any type of record.

We will now look at the likely effects of attacks.

3.5 What will go wrong

If we now work down the four categories of fraud which we analysed in section 2, we can get a overall picture of the likely effect of introducing the proposed technology in its present form.

1. The initial attraction of the smartcard-based digital tachograph was that it might stop ghosting which together with other chart manipulations amounts for most UK convictions.

   However, this would only be the case if (a) digital devices were tamperproof (b) cards could not be forged or duplicated and (c) the entire EU vehicle park were retrofitted with digital devices. None of these is likely to be the case. Retrofitting a vehicle with a tachograph other than of the original type is expensive, as it involves custom engineering; one vendor reported 19 replacement sales last year against 20,000 units repaired. Yet in the absence of retrofit or download, ghosting will be easy even without system penetration; the operator will just use one digital and one analogue truck.

   Attacks involving simple manipulation will become much easier as drivers will be able to cause tachograph malfunctions in many ways (mains electricity in the card, electrical contact failure, sand in the printer, ...). The digital tachograph is much like a burglar alarm in that the attacker only has to destroy confidence in it, by making it appear to be unreliable, in order to defeat it. The lessons from attacks on digital burglar alarms [26] should be studied carefully.

   Frauds in which the operator colludes with drivers and covers up for them by destroying records in the event of an investigation will become more common if record destruction involves only a 'disk crash' on a PC rather than burning down part of the premises as at present. In addition, we expect that the larger rogue operators will invest in manipulating cards. If operators are allowed to keep records on paper, the printouts from vehicle units will be easy to forge, and this may be the method of choice for one-man operators if downloading is not compulsory.

2. Attacks on the sensor seal are not tackled by the proposals, and although new systems are supposed to protect the signalling, this is left to individual vendors with no standards being set. The one unit we examined sent conventional unprotected pulses plus a second channel of encrypted pulses. The latter is used by the tachograph, but only the former is available to the speed limiter. So an interruptor could still be fitted between the tacho head and the limiter.

   The simultaneous entry into the market of several new vendors with no experience of the industry will be an aggravating factor. Reliability generally will fall, as will inspector's level of experience with the equipment in use. So old tricks (such as replacing the tachograph fuse with a blown one) will gain a new lease of life.

3. As noted above it seems that tachograph calibration may be tampered with given workshop cards, which contain only shared secrets and so should be widely forged. At present, intentional miscalibration can be proved if the setting within the instrument differs from that recorded on the plate, and the seal is intact; it is unclear what evidence could be extracted from the new digital system.

   More generally, attacks on computer security systems involve the opportunistic exploitation of implementation defects, and these are more prevalent in new systems [1]. The introduction of digital tachographs will be no different: vehicle inspectors report increased tampering attempts whenever new technologies are introduced.

4. Finally, there will be a number of new avenues of attack which will appeal to the underground workshops that currently make their money from interruptors. One obvious target is the vehicle unit itself. The proposed regulations are silent on the anti-tampering mechanisms and standard of testing required here; but the move from an analogue tachograph to a digital one raises the possibility that tachographs' program code could be modified, or circuit boards substituted, or totally bogus devices manufactured which would conform with the regulations in all externally visible ways but contain extra features for the driver or operator. Criminals have already used altered or completely bogus cash machines and point-of-sale terminals in bank card fraud; bogus digital tachographs are to be expected.

The hope has been expressed that testing under the ITSEC programme will ensure that the equipment is fit for purpose. This may be the case eventually, but at present the institutions participating in ITSEC are oriented to evaluating military computer systems for NATO use. An early attempt to produce ITSEC testing criteria for smartcard-based systems yielded a document which emphasises the secrecy of the chip design [28] — a relatively pointless goal given that attackers can buy microscopes. Much more convincing test criteria have been developed by VISA [35].

In conclusion, the Tachosmart proposals do not address most of the existing fraud problems effectively, and do not tackle the important ones at all.

4 What can be done?

The security industry's view of how to use devices such as smartcards has evolved over the past few years. While 7–8 years ago the vendors' tamper-proofness claims were widely accepted at face value, by 2–3 years ago engineers had split into two camps. The first, which dominated thinking in the pay-TV companies and in Mondex, was that chips could ultimately be made sufficiently tamper-resistant. The second, which was prevalent in VISA, Intel and elsewhere, was that tamper-proof devices did not and would never exist; so systems had to be engineered to detect and recover from attacks.

These views have converged over the last year or two. The current consensus is that tamper-resistance can add value if used intelligently, but one must expect it to fail eventually and build in security recovery features from the beginning. Examples of systems now being built that incorporate both tamper resistance and security recovery mechanisms are:

- the next generation of US postal meters combines a highly tamper resistant processor in the meter with a two-dimensional barcode on the indicia that it generates. The barcode contains in digitally signed form the zipcodes of the sender and the recipient, the date and the postage amount. Mail samples can be automatically scanned at various points in the delivery system to detect various frauds [33];
- the new digital broadcast set-top box contains a smartcard, as with the current satellite TV systems, but also a slot for a PCMCIA card. This enables a complete replacement of all the descrambling and decoding circuitry in the event of a catastrophic compromise;
- Mondex is moving from common-secret to public-key cryptography, investing in anti-tampering research, and simultaneously implementing a system to detect fraud by reconciling a sample of transactions. In the event of a penetration, the card base can be rapidly moved to the next generation of protection mechanisms.

It is likely that future digital tachographs will include mechanisms such as these. If they are not present in the initial deployment, then escalating fraud levels will force their adoption later. This will be much more expensive and may involve several years of chaos before control can be restored.

Possible components of the technical architecture might include:

1. The tachograph should have a slot for a larger form factor card, as with the PCMCIA card used in the new digital broadcast systems but rugged enough for vehicle use, so that future system upgrades do not involve replacing the whole vehicle unit. In the meantime, this slot could hold either a 'driver's log book' containing 365 days' detailed driving history, or a GPS receiver, if required by any national regulations. In this way, different national approaches to enforcement could be accommodated without creating competitive downward presure on standards or adversely affecting the single market;
2. The cards used by drivers, operators, workshops and calibration stations should be furnished with high quality security printing features such as kinegrams, alias band structures and optically variable inks, combined with tamper-evidence features such as laminates and reactive inks to make chip replacement difficult. They should also have full public key capability and be as tamper resistant as achievable in mass market products (at present this would mean a chip like the Thomson ST16CF54);
3. the paper record printed by the tachograph should carry a 2-D barcode or glyph with a digitally signed version of the hours data;
4. The processor of the digital tachograph itself should be as difficult to penetrate as is economic using available technology. It should also be capable of public key cryptography;
5. a serious effort should be made at the Community level to develop and deploy better physical sealing technology;
6. there should be carefully thought out support for secure downloading to fleet management and other administrative systems, and these systems themselves should be subject to certification.

Even if agreement on downloading cannot yet be secured, it is prudent to encourage and support the large number of reputable operators who derive business benefit from it;

7. consideration should be given to the likely administrative problems, such as what sanctions might be applied to card issuers (e.g. in non-EU countries) who negligently issue duplicate cards.

The emphasis placed on the above control mechanisms could be varied according to national requirements. However, it is most important not to let the design be technology driven, as was the case with the Tachosmart project up till now.

Two or three models of enforcement need to be elaborated, which take account not just of whether downloading will be mandatory but whether there are other inputs (from GPS, GSM, number plate recognition systems, document inspection and so on). Once each member state has adopted one of them, the business issues (such as cabotage) should be explored. This, together with a detailed threat model (as set out in this document and in [10, 11, 23, 25]) will enable us to develop a system security policy. Only then should a detailed functional specification be written on the basis of the security policy and the actual capabilities of available equipment. We cannot stress too strongly that security is a systems property and not than something that can be achieved automatically by incorporating 'security' components such as smartcards in poorly designed systems.

The additional costs of doing the security engineering properly will be much less than the cost of replacing the entire card base once a year, as has happened with BSkyB. With approximately 7 million drivers in Europe covered by the regulations, and with replacement cards costing perhaps 10 ECU, annual replacement could cost about 70 MECU per annum, plus perhaps an annual re-engineering cost of 5 MECU. An extra 50 ECU per vehicle for a highly tamper resistant vehicle unit processor, applied to 500,000 tachograph sales annually, would cost only 25 MECU. In this case, there would be a one-off engineering cost of perhaps 10 MECU to ensure that the job is done properly.

It is worth noting that even with a good design, changeover costs will be significant; the recent introduction of armoured tachograph cable cost many millions of ECU as there were thousands of trucks with the wrong cable in the supply chain. For this reason too, it would be foolish to skimp on the engineering work needed to get the specification right.

Finally, we would strongly recommend that a technology change to a safety critical system, which is as complex as the change proposed, should not be introduced without a proper pilot. A suitable place for a pilot might be one of the peripheral member states with a small vehicle park.

5 Conclusions

The admirable objective of EU Council was to 'put an end to the most common abuses of the present system' ([8] p 4). We cannot see how that objective will be met if the proposed technology is fielded as proposed in the year 2000 (and given the disruption that the millennium date problem is expected to cause to systems generally, this is a totally unrealistic choice of deadline). The current prototype technology does not address the most common abuses, and those that it does try to tackle are not dealt with effectively. Very little attention has been paid to potential new abuses.

We expect that the introduction of the proposed equipment would ensure that much fraud will become almost impossible to detect, and that the regulations will fall into disrepute. The cost of such a failure could amount to many hundreds of additional traffic fatalities, and billions of ECU, before control could be restored. If this is to be prevented, the specification and timescale of the project will need a careful rethink.

Acknowledgements: A number of people provided valuable background information including Peter Dean, Department of Transport; Jean-Philippe Lelièvre, ERTICO; Gregory Clough, UCL; John Martin, Hampshire Constabulary; Gary Geldart, Vehicle Inspectorate; Jim McCallum, Marks and Spencer; Dick Edmonds, R & G Consultancy Services; Peter Needham and Nick Rendle, Lucas Kienzle; and Frank Clish of TVI. Roger Needham of Microsoft Research and Markus Kuhn of Cambridge University provided a sounding board as this analysis was developed.

References

[1] RJ Anderson, "Why Cryptosystems Fail", in *Proceedings of the 1st ACM Conference on Computer and Communications Security* (November 1993) pp 215–227

[2] RJ Anderson, MG Kuhn, "Tamper Resistance — a Cautionary Note", in *The Second USENIX Workshop on Electronic Commerce Proceedings* (Nov 1996) pp 1–11

[3] E Bovenlander, invited talk on smartcard security, Eurocrypt 97

[4] *Stats 19 database*, Department of the Environment, Transport and the Regions

[5] *'Licensing of Trusted Third Parties for the Provision of Encryption Services'*, Department of Trade and Industry, March 1997

[6] EU Regulation 3820/85 (drivers' hours rules)

[7] *'Council Regulation (EEC) no 3821/85 of 20 December 1985 on recording equipment in road transport'* No L 370/8, 31/12/85

[8] *'Draft Council Regulation Amending Council Regulation (EEC) no 3821/85 and Council Directive 88/599/EEC on Recording Equipment in Road Transport'*, EU, The Council, Interinstitutional file no 94/0187 (SYN), 2 July 1997

[9] *Euraxiat — Security Analysis*, March 1997

[10] "False Records: Analogue Tachographs", G Geldart, Vehicle Inspectorate, 22nd January 1998

[11] Hampshire police training video

[12] "Driver sleepiness — an economic perspective", D Higginbotham, at *Falling Asleep at the Wheel*, Loughborough University 18–19/11/96

[13] "Sleep related vehicle accidents", JA Horne, LA Reyner, in *British Medical Journal* v 310 (4/3/95) pp 565–567

[14] "Falling Asleep at the Wheel", J Horne, L Reyner, preprint, 29/2/96; distributed at *Falling Asleep at the Wheel*, Loughborough University 18–19/11/96

[15] "Ex-radio chief 'masterminded' TV cards scam", NDS v Carey et al., reported in *Irish Independent 17/2/98*

[16] "Vulnerability Assessment of Security Seals", RG Johnson, ARE Garcia, in *Journal of Security Administration* v 20 no 1 (June 97) pp 15–27

[17] *'Driver Card 16kByte version 00.01.01'*, 24/11/97

[18] *'Workshop, Control and Company Card version 00.01.01'*, 24/11/97

[19] *'External Interface version 00.01.01'*, 25/11/97

[20] *'Card Issuing version 00.02.00'*, 25/11/97

[21] O Kocar, "Hardwaresicherheit von Mikrochips in Chipkarten", in *Datenschutz und Datensicherheit* v 20 no 7 (July 96) pp 421–424

[22] "Falling Asleep at the Wheel", JS Martin, report on conference of the same name, Loughborough University 18–19/11/96

[23] "Principal frauds used on the current tachographs", J Martin, UK response to ERTICO consultation document on tachograph falsification

[24] *'Driver sleeplessness as a factor in car and HGV accidents'*, G Maycock, UK Transport Research Laboratory report 169 (1995)

[25] *'Principales fraudes partant atteinte à l'intégrité du chronotachygraphe'*, Ministère de l'Équipement, des Transports et du Tourisme, Direction des Transports Terrestres, Sous-direction des transports routiers, bureau R3 (France)

[26] "Denial of Service: An Example", RM Needham, in *Communications of the ACM* v 37 no 11 (Nov 94) pp 42–46

[27] "Spying tags could stop fuel fraud", N Nuttall, in *The Times* (Interface Section) 28/1/98 p 7

[28] *'Common Criteria for IT Security Evaluation — Smartcard Integrated Circuit Protection Profile'*, registered at the French Certification Body under the number PP/9704; Motorola, Philips, Siemens, SGS-Thomson, Texas Instruments, October 1997.

[29] "Driver sleepiness as a causal factor in accidents on the M180/A180 in South Humberside: A Preliminary Analysis", L Reyner, at *Falling Asleep at the Wheel*, Loughborough University 18–19/11/96

[30] *'Tachosmart 3 Digital Tachograph — Final report'*, Thomson CSF, 1996

[31] "Ministers unveil plans to toughen drink-drive laws", in *The Times* 2/2/98 p 2

[32] "Commission wants black box, smart cards to enforce road safety", A Torres, Reuters news item 0804 (2/9/94)

[33] "Cryptographic Postage Indicia", JD Tygar, BS Yee, N Heintze, in *ASIAN 96* (Springer-Verlag LNCS v 1179) pp 378–391; also available from `http://www.cs.cmu.edu/afs/cs.cmu.edu/user/tygar/www/recommend.html`

[34] *'A Report on the Fitment of Tachograph Interruptors'*, 10/8/95, Vehicle Inspectorate, Wighill Lane, Walton, Wetherby, West Yorkshire

[35] *'Integrated Circuit Chip Card — Security Guidelines Summary for IC Chip Design, Operating System and Application Design, Implementation Verification'* v 2.1, 4/11/97