Monitoring and Metering

Chapter 12

VICTOR HANNA

Introduction

- Many secure systems are concerned with monitoring and metering the environment.
- Electronic systems that use cryptography and tamper-resistance are rapidly displacing older mechanical systems.
- Many metering systems are much more exposed physically.

Prepayment Meters

Prepayment Meters

- Systems where the user pays in one place for a token
  - magic number, cardboard ticket , rechargeable smartcard
- For example
  - electricity meter
  - Photocopiers
  - washing machine
  - transport tickets
- The main protection goal in these systems is to prevent the stored-value tokens being duplicated or forged.

Prepayment electricity meter

- They were coin-operated, but the costs collection led to develop token-based meters.
- The customer goes to a shop and buys a token, which may be a smartcard, or a disposable cardboard ticket
- Most tokens say something like ‘meter 12345 — dispense 50KWh of electricity!’

Security requirements

- Tokens should not be easy to forge.
- tokens should not work in the wrong meter, or in the right meter twice.
- One strategy is to make tokens tamper-resistant, by using smartcard chips of some kind or another.
- Another strategy tie each token to a unique meter, make each token unique using serial numbers or random numbers.

How the System Works

- The original system had a single vending machine for each neighborhood.
- But many people commute long distances from home, so they are never at home during business hours, so we had to support multiple retailers.

How the System Works

- Vending machines were stolen and used to sell tokens in competition with the utility.
- The countermeasure to maintain a credit balance in the tamper resistant security processor that also protects vend keys and foreign meter keys.

What Goes Wrong

- The only evidence of how much electricity has been sold resides in the vending equipment itself.
- 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.
- Fall in voltage from 220 to 180 volts, then a particular make of meter went to maximum credit.
- Allowed refunds, but a copy of the refunded token could still be used
- Remembered only the last token serial number entered.

The Tachograph

- These are devices used to monitor truck drivers' speed and working hours.
- 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.

The Tachograph

- First let's look at the old analogue system, which is still used in most trucks on Europe's roads.
- The chart is loaded into the tachograph, which is part of the vehicle's speedometer. It turns slowly on a turntable inside the instrument and a speed history is inscribed by a fine stylus connected to the speedometer.
- If it's digital, you must have a driver card plugged into it. the card and the vehicle unit both keep records.

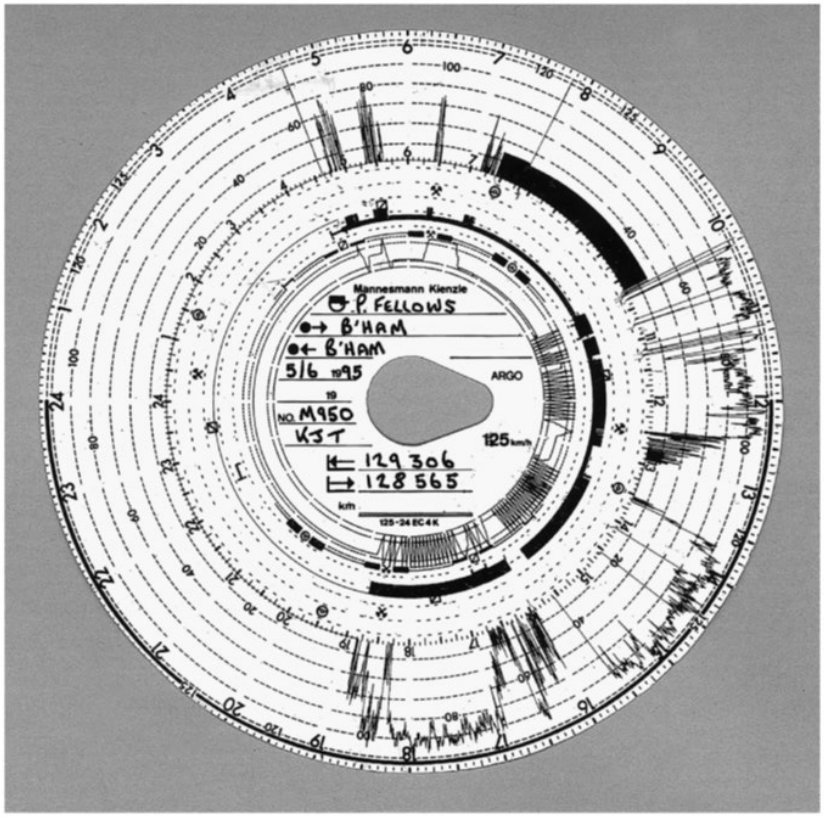


Figure 12.3: A tachograph chart

What Goes Wrong

procedural weaknesses

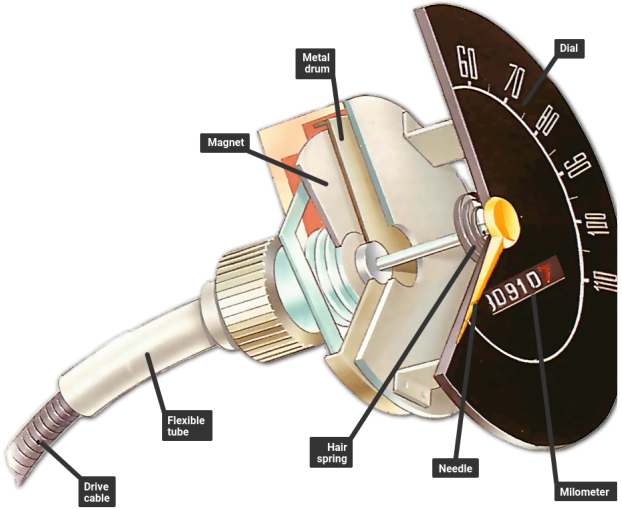
- About 70% of offences do not involve tampering but exploit procedural weaknesses.
- For example
- As the distance is about 500 miles and the journey takes about 10 hours — which is illegal for a single driver to do every day. (should have four drivers)
- So two drivers who meet at an intermediate point, change trucks, and insert new paper charts into the tachographs.
- This (widespread) practice, of swapping vehicles halfway through the working day, is called *ghosting*.

procedural weaknesses

- Simpler frauds include setting the clock wrongly.
- Recording the start point as a village with a very common name, If stopped, the driver can claim he started from nearby.

Tampering with the Supply

- About 20% of the total fraud involves tampering with the supply to the tachograph instrument.
- Old-fashioned tachographs used a rotating wire cable that was hard to fiddle with.

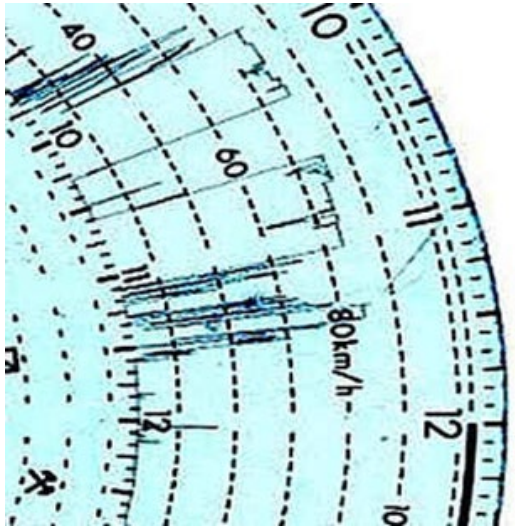


Tampering with the Supply

- More recent analogue tachographs are ‘electronic’, in that they use electric cables rather than rotating wire, which sends electrical impulses as the prop shaft rotates. This has made fiddling much easier!

Tampering with the Supply

- Attack is to unscrew the sensor about a tenth of an inch, which causes the impulses to cease, as if the vehicle were stationary.
- Drivers short out the cable or replace the tachograph fuse with a blown one.
- Power supply interruption.



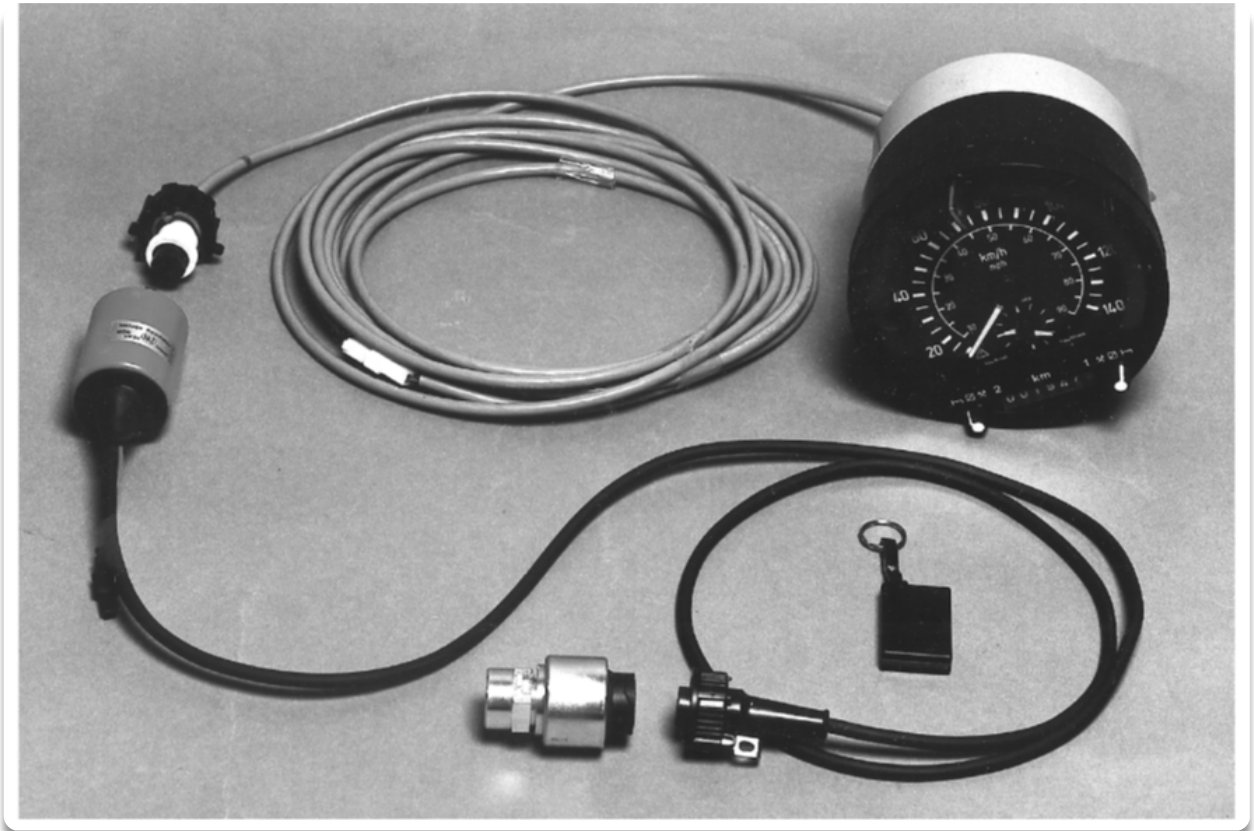
Tampering with the Instrument

- 6% of offences is 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.

High-Tech Attacks

- The plastic cylinder on the left of the photo is marked Voltage Regulator, is certainly not a voltage regulator.



High-Tech Attacks

- 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 and a fourth causes the device to return to proper operation.

The Digital Tachograph

- The European Union took the initiative to design a unified electronic tachograph system to replace the existing paper-based charts with smartcards.
- Each driver can now get a ‘driver card’ that contains a record of his driving hours over the last 28 days.
- Every new vehicle has a vehicle unit that can hold a year’s history.

The Digital Tachograph

- There are two further types of credential: workshop cards used by mechanics to calibrate devices, and control cards used by law enforcement officers to read them out at the roadside.
- Was not clear how going digital will help combat the procedural frauds that make up 70% of the current total.
- So the driver card has only 32K of memory and can only contain a limited number of alarm events.
- The choice of a smartcard rather than a memory card was probably the most critical wrong decision in the whole program.

Problems

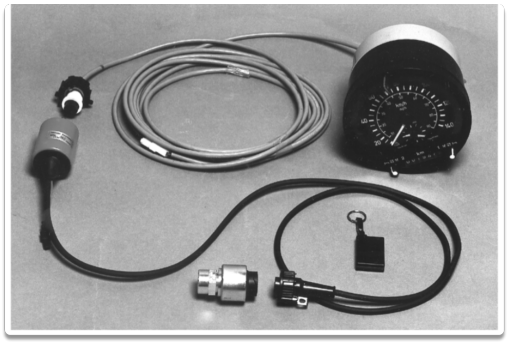
- So the move from analogue to digital isn't always an improvement.
- Many drivers have more than one driver card.
  - One source of cards is to borrow them from drivers who use them only occasionally.
  - Second source is that many drivers have more than one address.
- A truck driver can easily destroy his smartcard by feeding it with mains electricity. Under the regulations he is allowed to drive for 15 days while waiting for a replacement.

Other Problems

- Some of the cards in the system are very powerful. They can be used to erase evidence of wrongdoing.
- If any police card, or workshop card, can be used to erase evidence of a crime, then what's to stop a corrupt mechanic or policeman in Sicily or in Romania
- 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 and10th become unreadable.
- Villains might physically reverse-engineer a card, extracting its master key and enabling a powerful workshop or police card to be forged.
- Some countries have therefore gone to minimize the number of workshop cards that fall into bad hands.

frustrate the use of interrupters

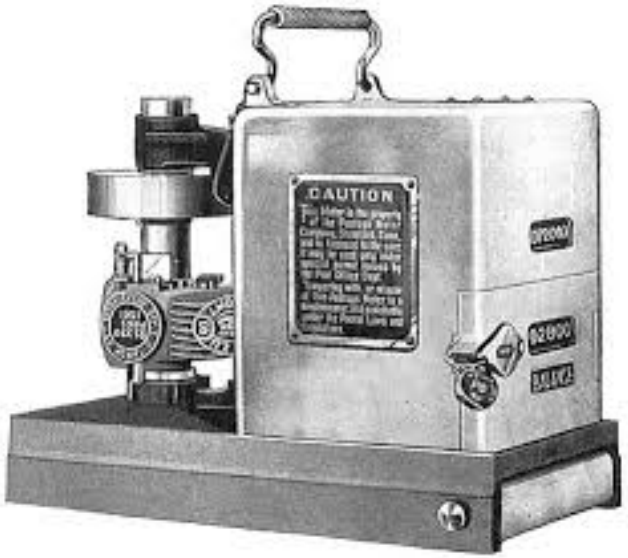
- All digital tachographs had to encrypt the pulse train from the gearbox sensor to the vehicle unit.
- A ‘newborn’ vehicle unit can recognize as its owner the first gearbox sensor that sends it a secret key.
- The sensor does this on power-up. As soon as this key is received, the vehicle unit is no longer a newborn.
- 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,

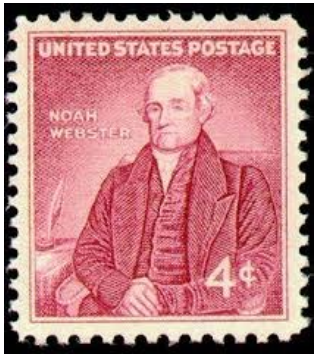


Postage Meters

- 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.

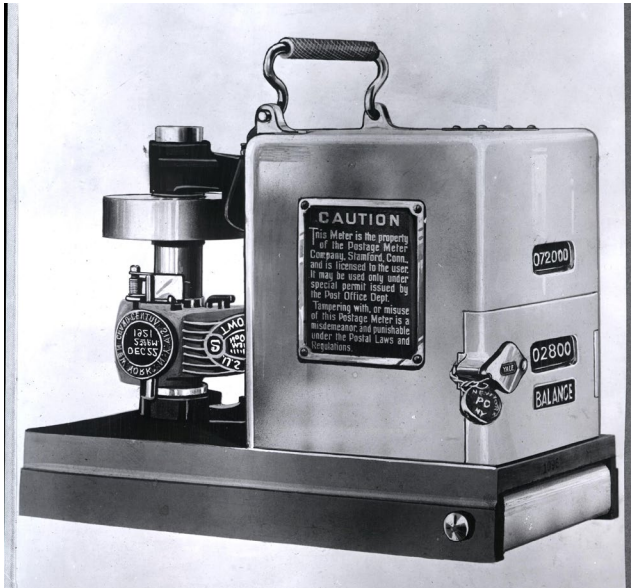
FIRST-CLASS
U.S. POSTAGE
PAID
LANCASTER, PA
PERMIT NO. 334





Postage Meters

- 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.
- In 1979, Pitney Bowes introduced a 'reset-by-phone' service, which enabled firms to buy an extra $500 worth of credit over the phone;

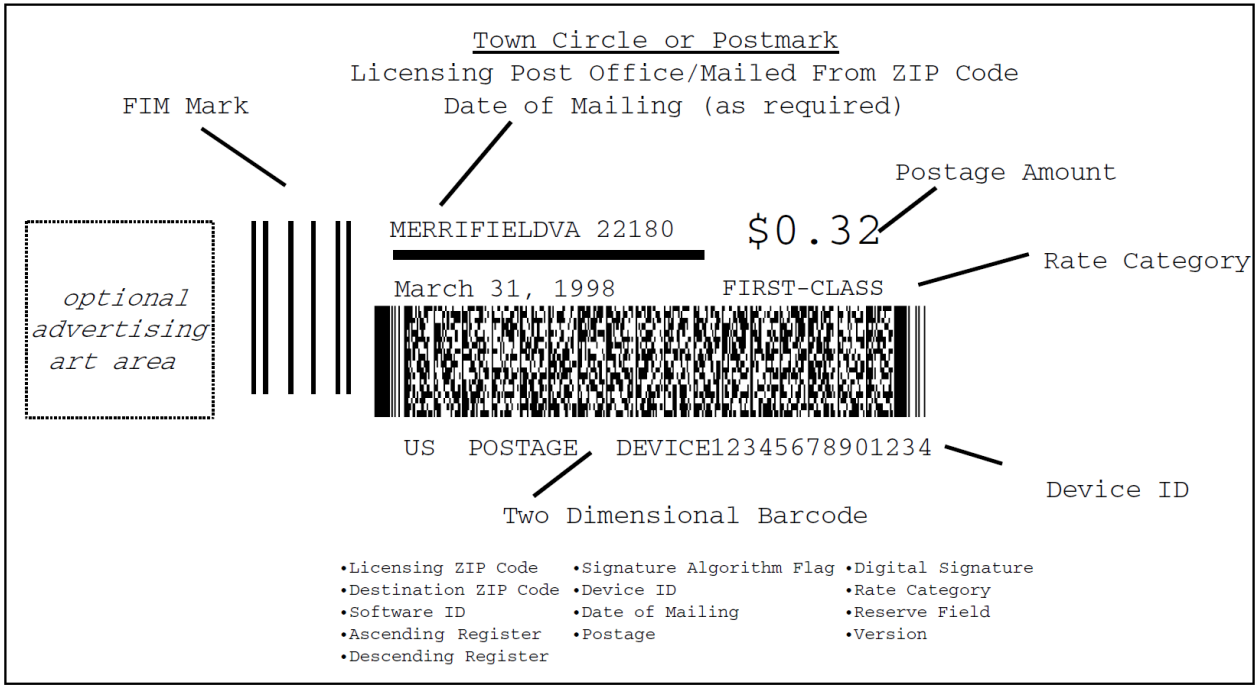


Postage Meters

- 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.

Postage Meters

- In 1990, suggested to replace stamps and indicia with digital marks protected by digital signatures.



Postage Meters

- One concern was whether the availability of color scanners and copiers would make stamps and indicia too easy to forge.
- the big problem was not so much the forging or copying of stamps, It was bulk mailers corrupting Postal Service employees to insert junk mail into the system without paying for them.
- This led to a development program to produce a design based on digital signatures, generated by tamper-resistant processors in the postage meters.

Postage Meters

- The basic idea is that the indicium, which is machine-readable, contains
  - the sender and recipient postal codes.
  - the meter number,
  - the date,
  - the amount of postage ever sold by the meter.
  - the amount of credit remaining in it.
  - all protected with a digital signature.

Postage Meters

- the value counter consist 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.
- If the balance fails, the meter locks up and can only be accessed by inspectors.
- Moving to digital postal meters involves a nontrivial investment but enables much better control than was possible in the old days.

Summary

- The new digital prepayment electricity meters have been a success.
- Digital tachographs have been much less impressive; they just do what the old analogue systems did, but less well.
- Our third example, postage meters, appear to be a success.