Monitoring and Metering

- Chapter 12 -

Hilal hamam

Agenda

- Introduction
- Prepayment meters
- Postage meters
- Tachographs and truck speed limiters
- Summary

Definitions

- **Metering**
- **To monitor** or **monitoring** generally means to be aware of the state of a system, to observe a situation for any changes which may occur over time, using a monitor or measuring device of some sort.[1]

- [1] from Wikipedia

Why is it interesting to us?

- Two sides -> conflict of interest
- Special case:

The monitoring device is with the customer!

Pre-payment (tickets):

- What is this?
- Why does it exist?
- Prepayment meter is profitable!

  - Reduces the administrative costs

- Token is a string of bits

  “meter 12345 dispense 50 KW + more details

Reminder

- Why is it interesting ?

  -> conflict of interest

  -> security issues

- Our goals ?
- As a supplier:

  Protection against systematic duplications and forgery -> loss of large amounts of money

- As a customer:

  To get what I paid for (maybe a little bit more ☺)

Prepayment electricity meter

- Security requirements : (customer)
- To supply the correct amount of electricity
- Fair price
- Good customer service
- We will focus on supplier side !

Prepayment electricity meter

- Security requirements (as a supplier):

  1. Token should not be easy to forge
  2. Genuine token should not work in the wrong meter
  3. Genuine token should not work in the right meter more the one time

How the system works

- Buy credit from **local** machine –

  Encrypted and **specific** for a meter –

  Something like “give meter 12345 50 KW”

- How can it be improved ?

  Customer requirements:

  1. Esay to buy credit
  2. Easy to load credit

What goes wrong ?

- The only evidence of how much electricity has been sold resides in the vending equipment itself

- No return channel from the meter to the vending station

Possible attacks

- Third parties
- To damage (or even destroy) the meter (in purpose or by accident)
- Manipulate the price
- Bugs in the system (220v to 180v)

Pre-payment summary (supplier)

Pre-payment is good in case

1. You control the market
2. No third parties
3. Local sales
4. Recycle technology (universal!)
5. Use multiple experts (universal!)

Postage meters

- What is this?
- 1979 improvement – “reset by phone” 500$
- 1981 another improvement – any sum of money
- 1990 moving to digital marks protected with digital signature

- Looks familiar?
- Two sides -> conflict of interest

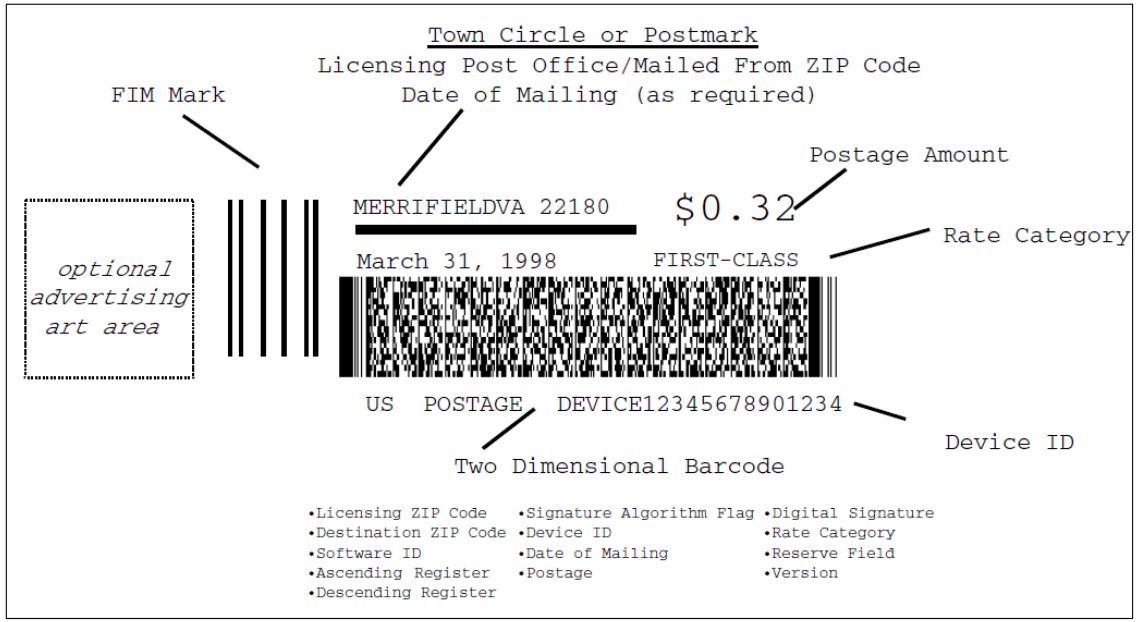
Postage meters

- Possible attacks?
  - Traditional ones (forging, coping, tampering with meter, etc.)
  - "Trust attack!"

Postage meters - Solution

- In 2000 , a design indicium based on digital signatures, generated by tamper-resistant processors

  in the postage meters



Postage meter Summary

- Similar to prepayment electricity but …

- The customers are companies!

  -> Makes the different

Tachographs

- What is it ?

Tachographs

- Why does it exist ?

- Two sides -> conflict of interest (money , time …)
- Special case: The monitoring device is with the customer

  (drivers in this case)

Tachographs

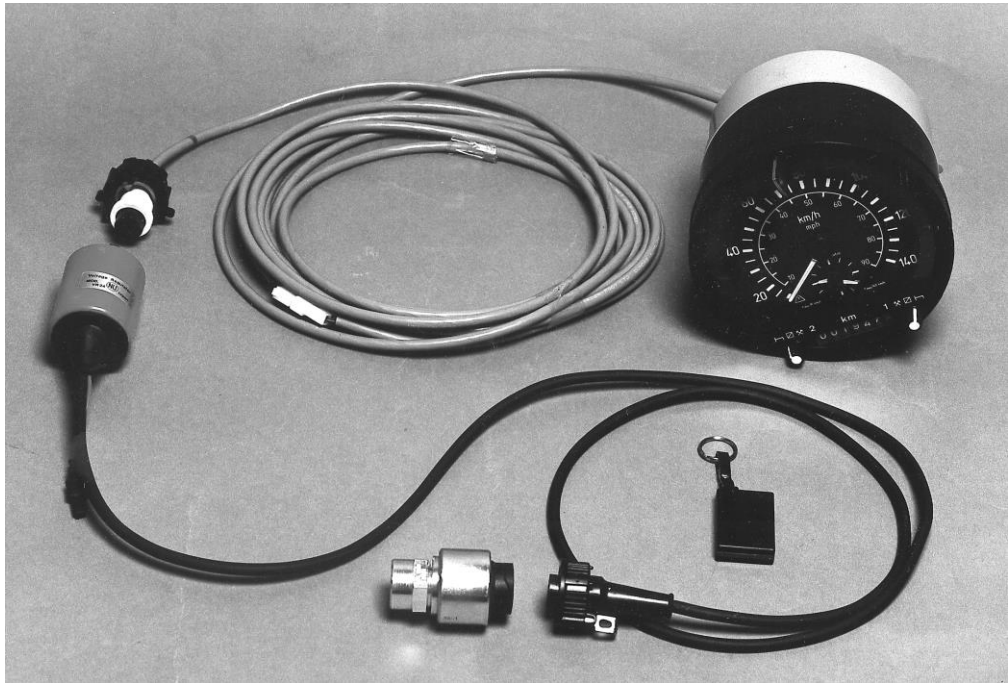
- Possible attacks

- Exploiting weaknesses (majority of the attacks)
    1. Dundee-Southampton example “ ghosting “
    2. Different enforcement policy (in Europe)
    3. Setting the clock wrongly

Tachograph manipulation

- Tampering with instrument

1. Miscalibration
2. High-tech attack



The digital tachograph project

- The countermeasures taken against tachograph manipulation vary by country
- Moving to the electronic tachograph. “driver card” instead of paper chart
- Using smartcard – with 32 K memory –
- Moving from analogue to digital isn’t always an improvement

Problems

- Still not able to combat the procedural frauds
- Drivers have more than one digital card
- Easy to damage the smart card - short circuit –
- Loss of details, binary signal – yes or no –
- Erasing evidences from smart card by “powerful” cards

Summary

- Many security systems are concerned one way or another with monitoring or metering some aspect of the environment
- The world moves from analogue to digital technology
- Global design vs local design
- Money (benefits vs cost)
- Trust


Thank you!