

Does Bob Go to Jail?

Ross Anderson

Cambridge

Signatures and Evidence

Over the last quarter century, thousands of crypto papers have had punchlines like:

‘So the judge raises S to the power e , finds it’s equal to $h(M)$, and sends Bob to jail’

No-one knew if this would actually work!

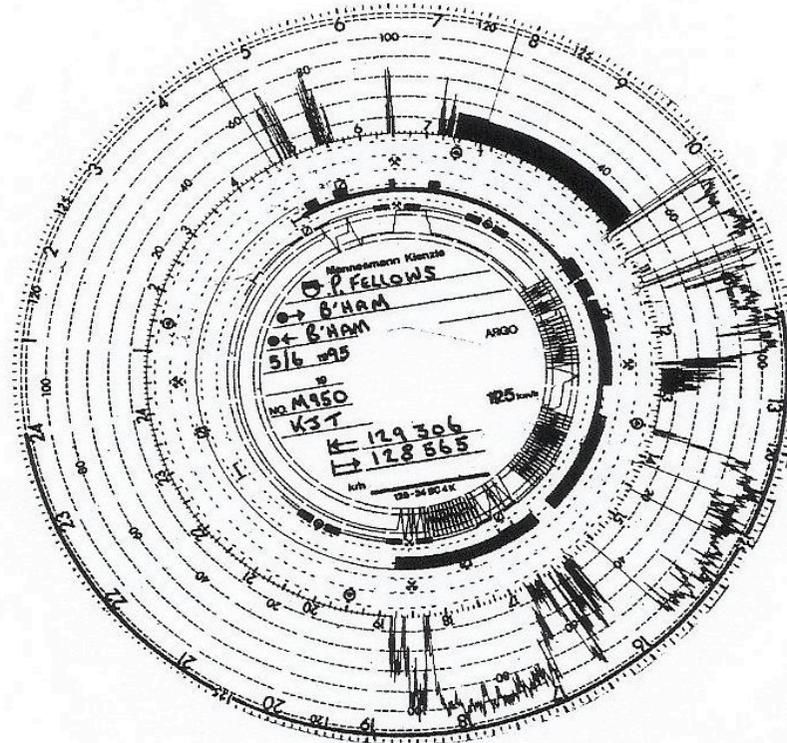
Empirical Evidence

- Since late 2006, criminal courts in Europe have been presented with more and more digitally signed evidence
- These are records from the new digital tachographs (see my book “Security Engineering”), introduced for new vehicles 2005–6

What's a Tachograph?

- It's a device that records vehicle speed and driver working hours, and is mandatory in most trucks and buses in Europe
- Used to be based on a waxed paper chart
- Migrating to an electronic vehicle unit that takes smartcards (driver, mechanic, police)
- Now: signed digital records instead of paper

Traditional Technology



Attacks on Tachographs

- Procedural exploits were 68% of all driver offences, 71% of all operator offences
- Typical method: ghosting
- 25% of driver offences and 21% of operator offences involved tampering with power, impulses, cables and seals
- Latest hack: bogus gearbox



New Technology



Digitally Signed Data

- Prosecution of most offences depends on careful interpretation of data
- Waxed paper was tamper-evident; the forensics people used microscopes
- Now the data from cards and vehicle units is digitally signed instead
- How did the courts cope?

Courts and Digital Signatures

- It turns out that the courts don't like digital signatures
- Reason: they're in hex!
- Judges don't like this
- So what could the police do?

Fixing the problem

- When all else fails, use standard procedures – treat tachograph records like you treat CDs or DVDs!
 - Print the record out
 - Print it out again
 - Put the second copy in a plastic bag and seal it for the appeal court
 - Fill in the log book
- The courts are now happy to fine the driver and put some points on his license

Fixing the problem (2)

- The vendors are happy, as 15% of European trucks use digital kit, versus the 10% forecast by now
- The drivers must be happy too, or they wouldn't be upgrading from analogue to digital before they have to