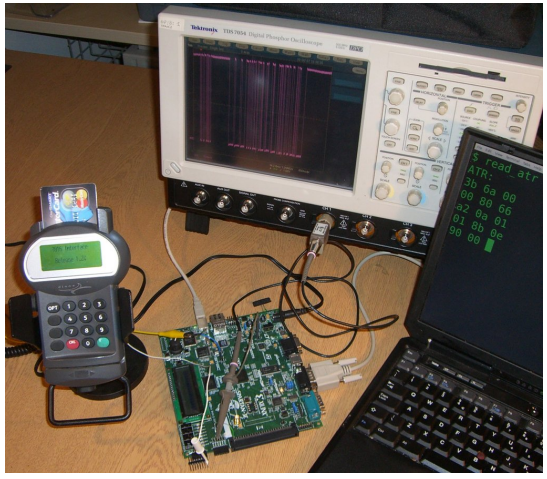
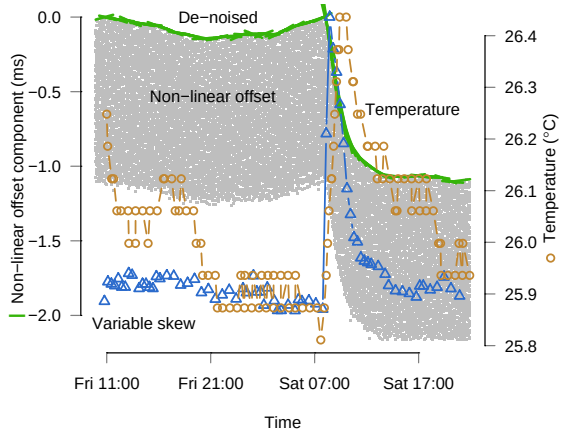
System-Level Failures in Security





Steven J. Murdoch

http://www.cl.cam.ac.uk/users/sjm217/

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

www.torproject.org

Chip & PIN is the most widely deployed smartcard payment system worldwide

- Chip & PIN, based on the EMV (EuroPay, Mastercard, Visa) standard, is deployed throughout most of Europe
- Visa is currently rolling out Chip & PIN in Canada
- Supports both credit and debit cards
- Customer inserts contact-smartcard at point of sale, and enters their PIN into a PIN Entry Device (PED)
- PIN is verified by card

More information: “Thinking Inside the Box: System-level Failures of Tamper Proofing”, IEEE Security & Privacy, 2008

Protocol overview (as used in the UK)

$$Card \rightarrow PED$$

- Card details (account number, cardholder name, expiry, etc.)
- Public key certificate and static digital signature of card details
- Copy of the magnetic strip details $*$

$$PED \rightarrow Card$$

- Transaction description (value, currency, type)
- PIN as entered by customer $*$

$$Card \rightarrow PED$$

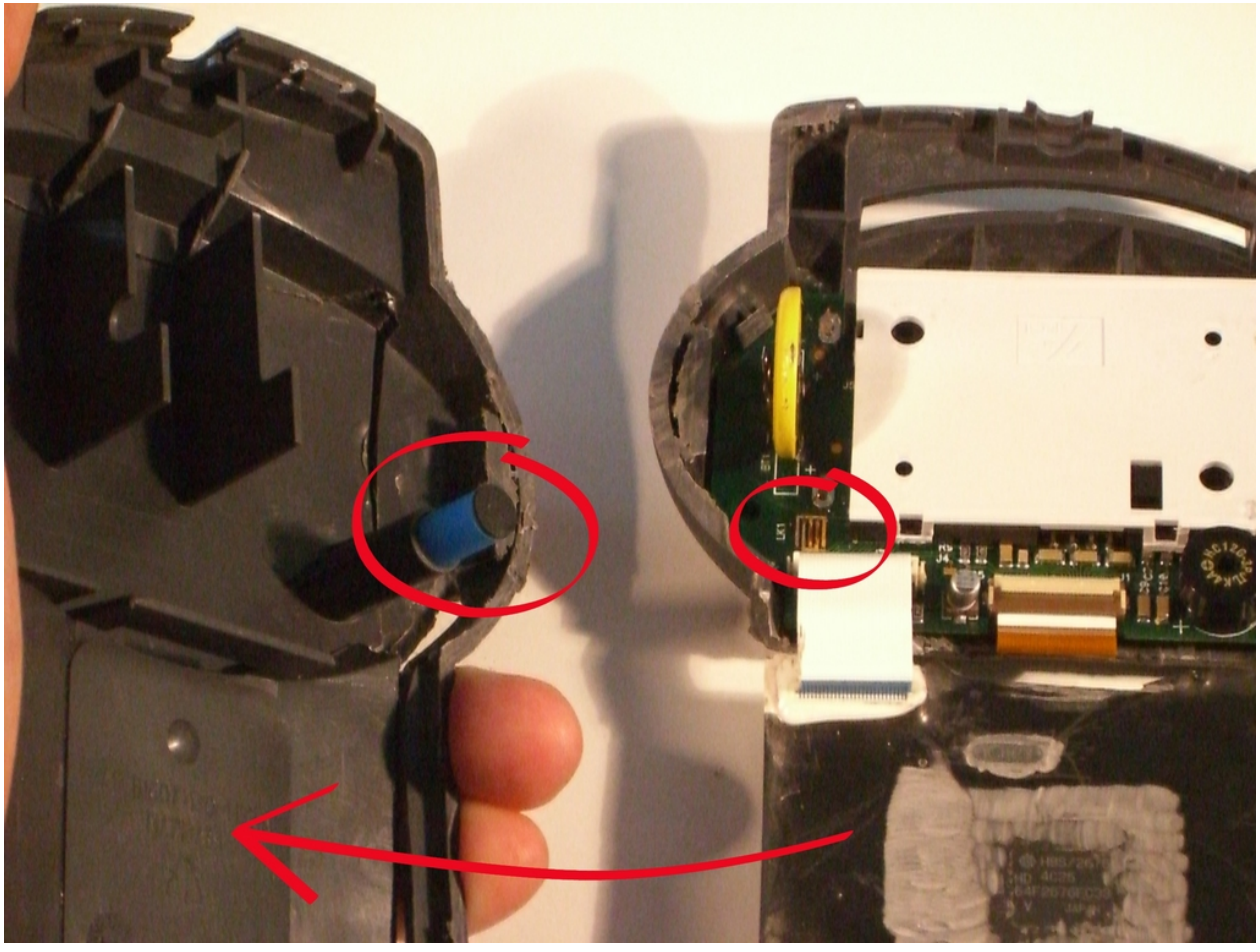
- Authorisation code (3DES CBC-MAC of transaction details, counter, and PIN verification result)

Tamper proofing is required to protect customers' PINs and banks' keys

- Various standard bodies require that PEDs be tamper proofed: Visa, EMV, PCI (Payment Card Industry), APACS (UK bank industry body)
- Evaluations are performed to well-established standards (Common Criteria)
- Visa requirement states that defeating tamper-detection would take more than 10 hours or cost over **USD $25,000 per PED**

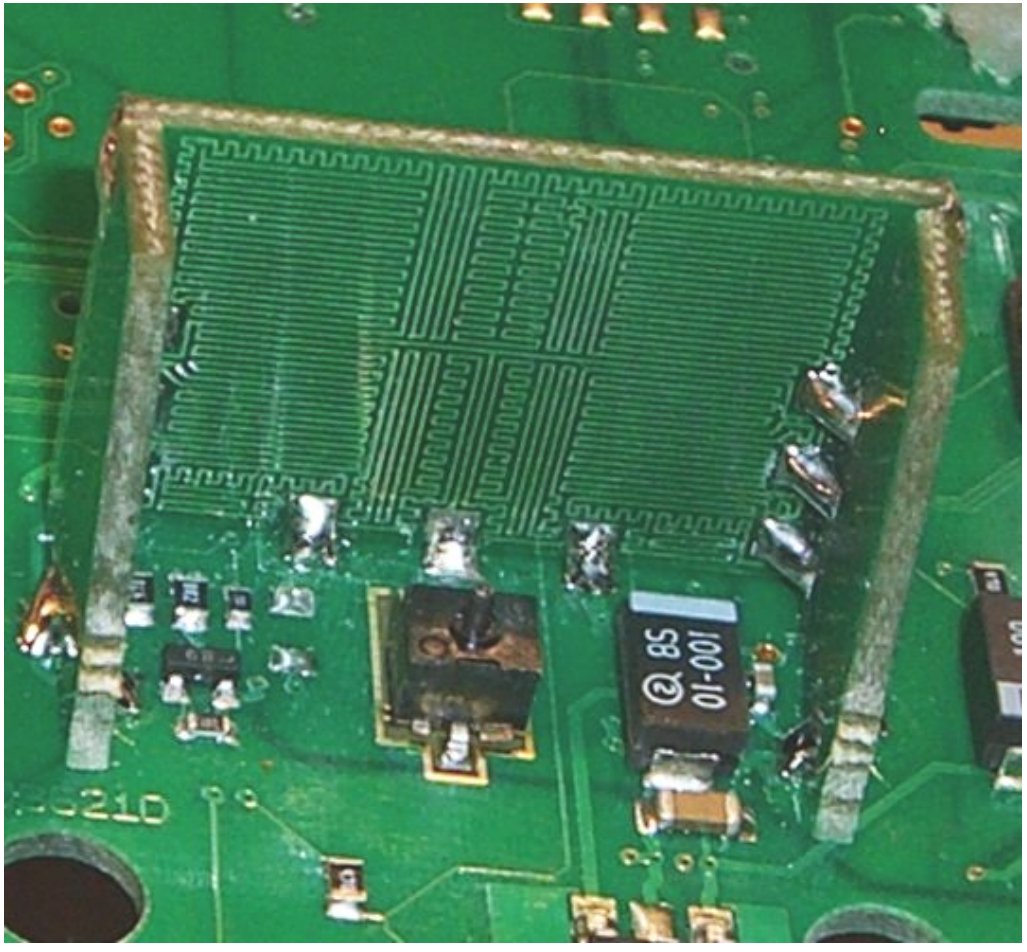
Do they work in practice?

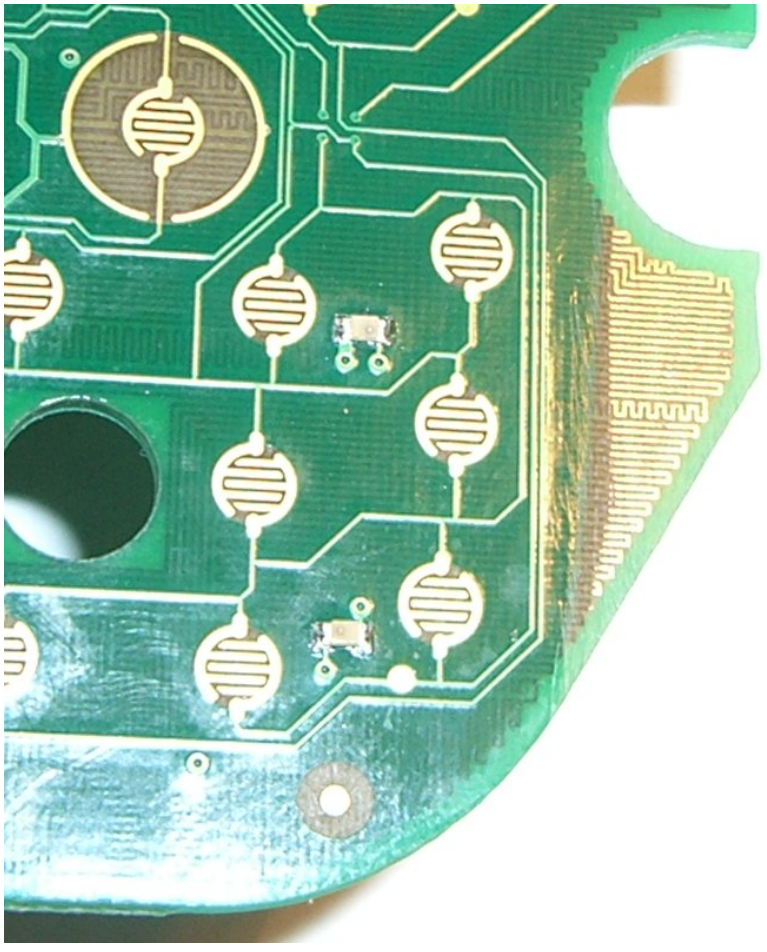
Protection measures: tamper switches



Dione Xtreme

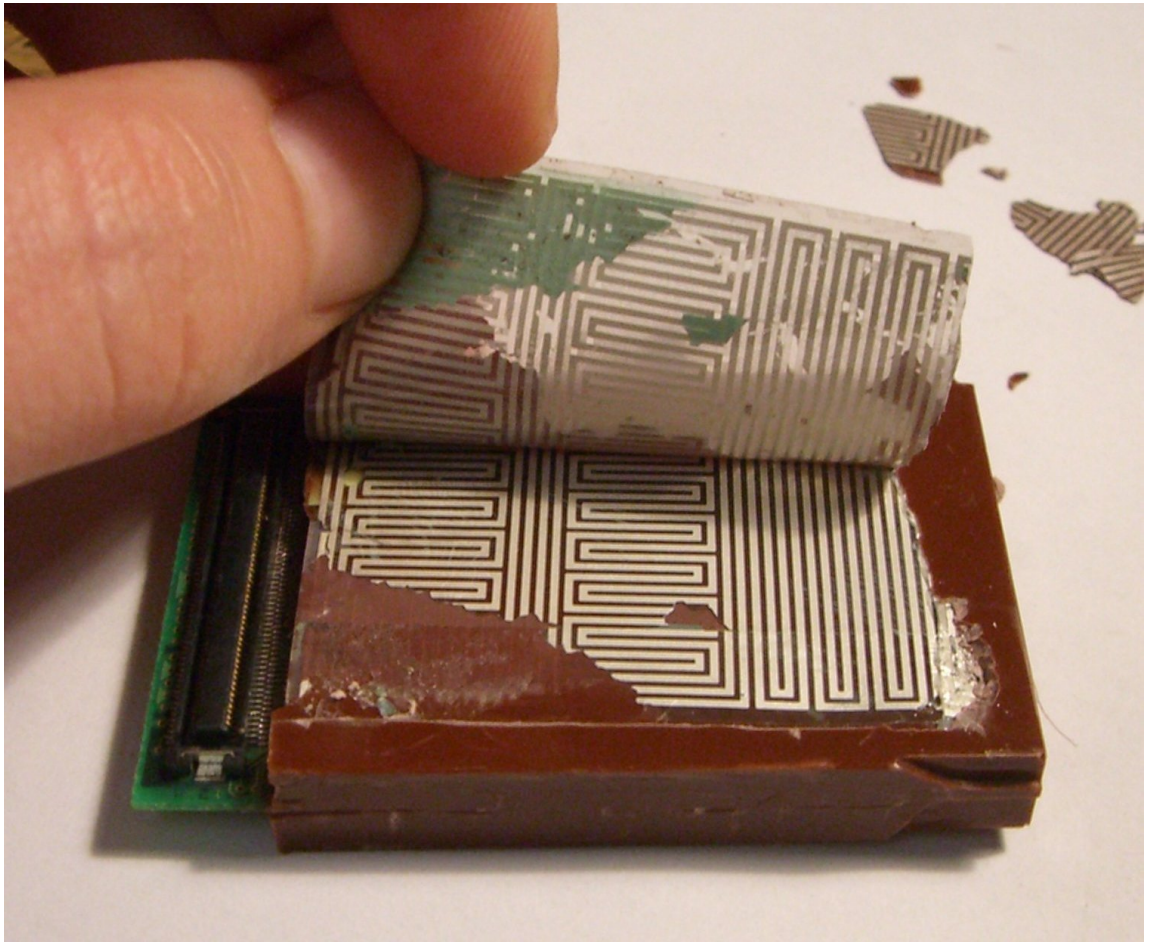
Protection measures: tamper meshes





Ingenico i3300

Protection measures: tamper meshes

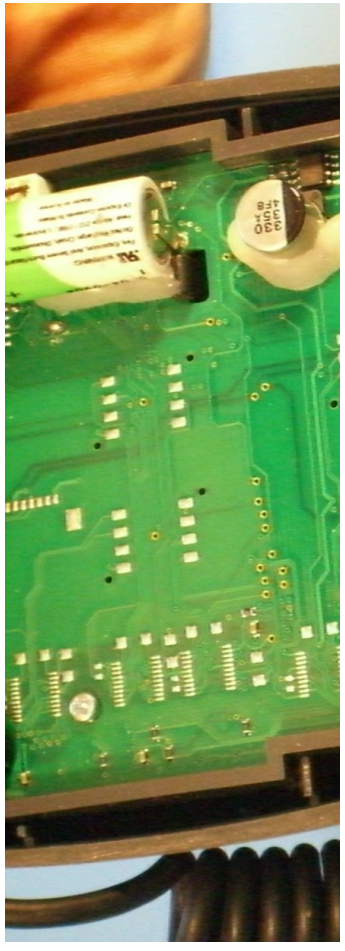


Ingenico i3300

Tamper resistance protects the banks' keys, not the customer's PIN

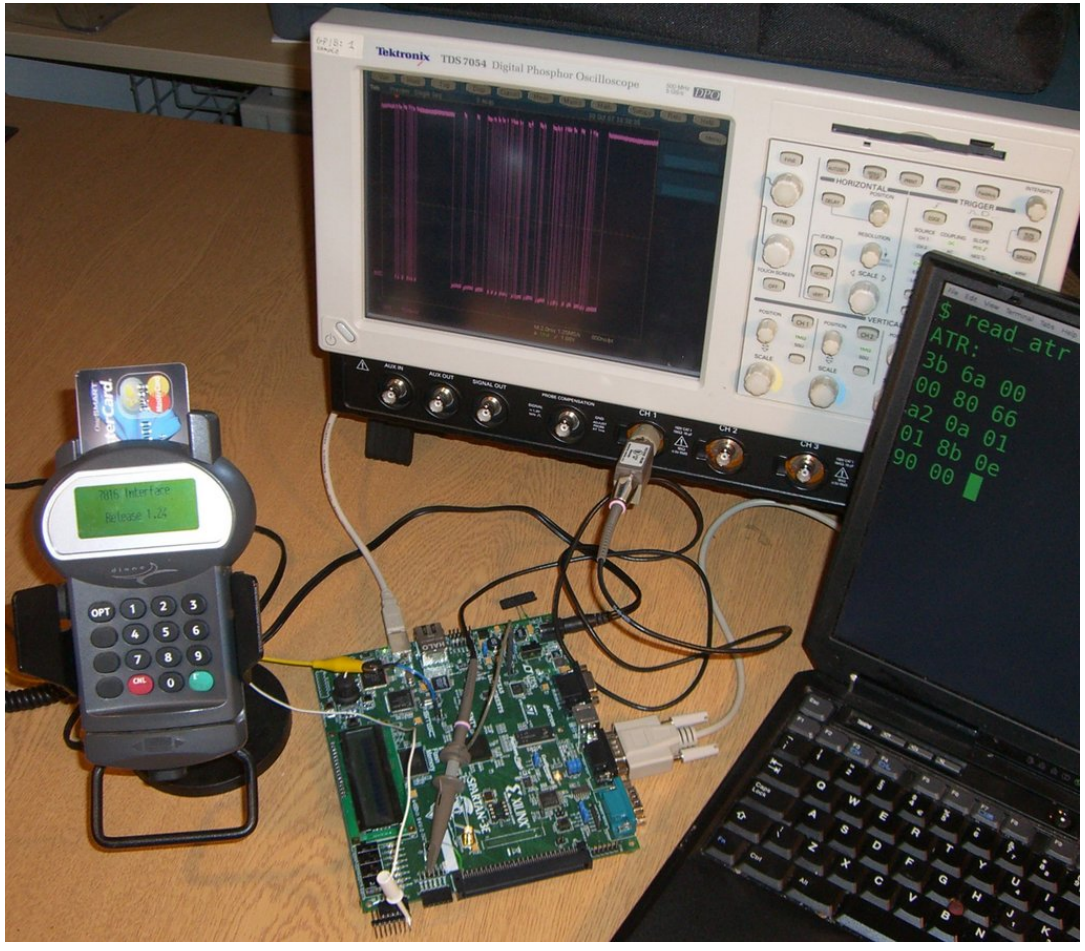
- Recall (*) that a copy of the magnetic strip details, and PIN, are sent unencrypted between card and PED
- If a fraudster can capture this information a fake card can be made, and used in some UK ATMs and many abroad
- We found that deployed tamper proofing measures failed to protect communications between card and PED
- To demonstrate the weakness, we tried our attacks on a real Ingenico PED

Holes in the tamper mesh allow the communication line to be tapped



An easily accessible compartment can hide a recording device

The Dione PED also routes card details outside the tamper resistant boundary



We constructed an FPGA design for capturing data

While the proximate failure is clear, the root causes are complex

The PEDs we examined failed to adequately protect the smartcard communication line. Because the UK system doesn't encrypt PINs, they are vulnerable. Why did this situation occur?

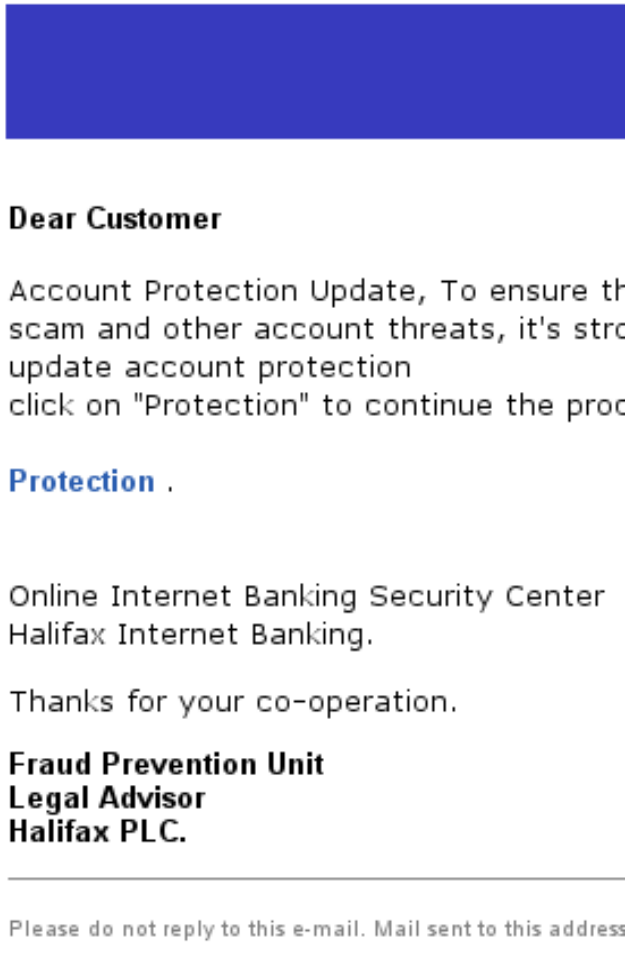
Engineering challenges: There are 3 662 pages in the public Visa Chip & PIN specification. Due to the complex inter-module security dependencies it is unreasonable to expect every engineer to have a full understanding

Economic incentives: Banks set the standards for PED security – their keys appear to be reasonably well protected. Customers have little say – their PINs are left vulnerable

Failure of certification: Both of these devices passed their necessary certification requirements, despite the flaws we found

Online banking fraud is a significant and growing problem in the UK

- 174% increase in users between 2001 and 2007
- 185% increase in fraud in 2007–2008 (£ 21.4m in first 6 months of 2008)
- Simple fraud techniques dominate in the UK:
  - Phishing emails
  - Keyboard loggers
- Still work, and still used by fraudsters, due to the comparatively poor security



Dear Customer

Account Protection Update, To ensure th
scam and other account threats, it's strc
update account protection
click on "Protection" to continue the proc

Protection .

Online Internet Banking Security Center
Halifax Internet Banking.

Thanks for your co-operation.

Fraud Prevention Unit
Legal Advisor
Halifax PLC.

Please do not reply to this e-mail. Mail sent to this address

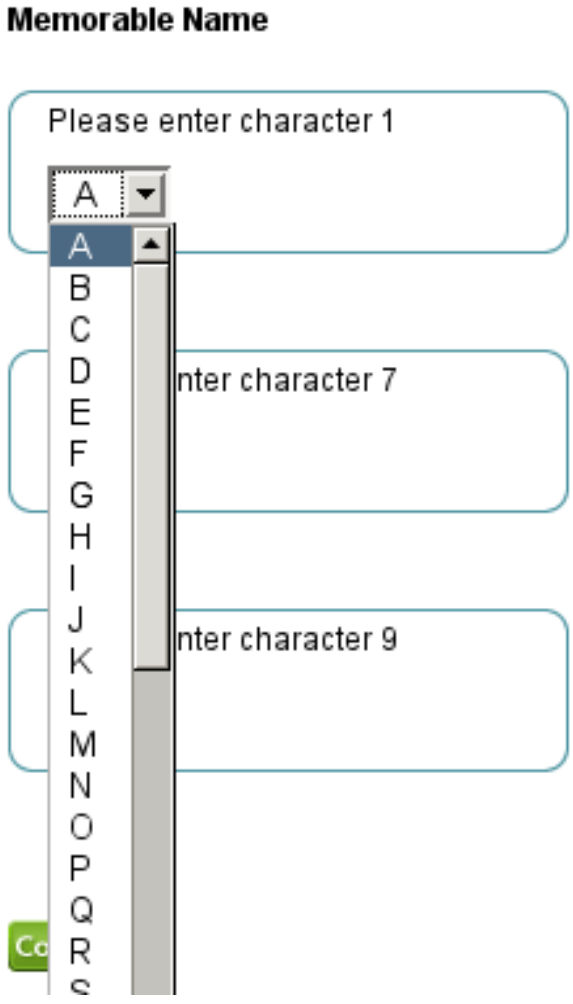
More information: “Optimised to fail: Card readers for online banking”, Financial Cryptography and Data Security 2009

A variety of solutions have been proposed to resist phishing

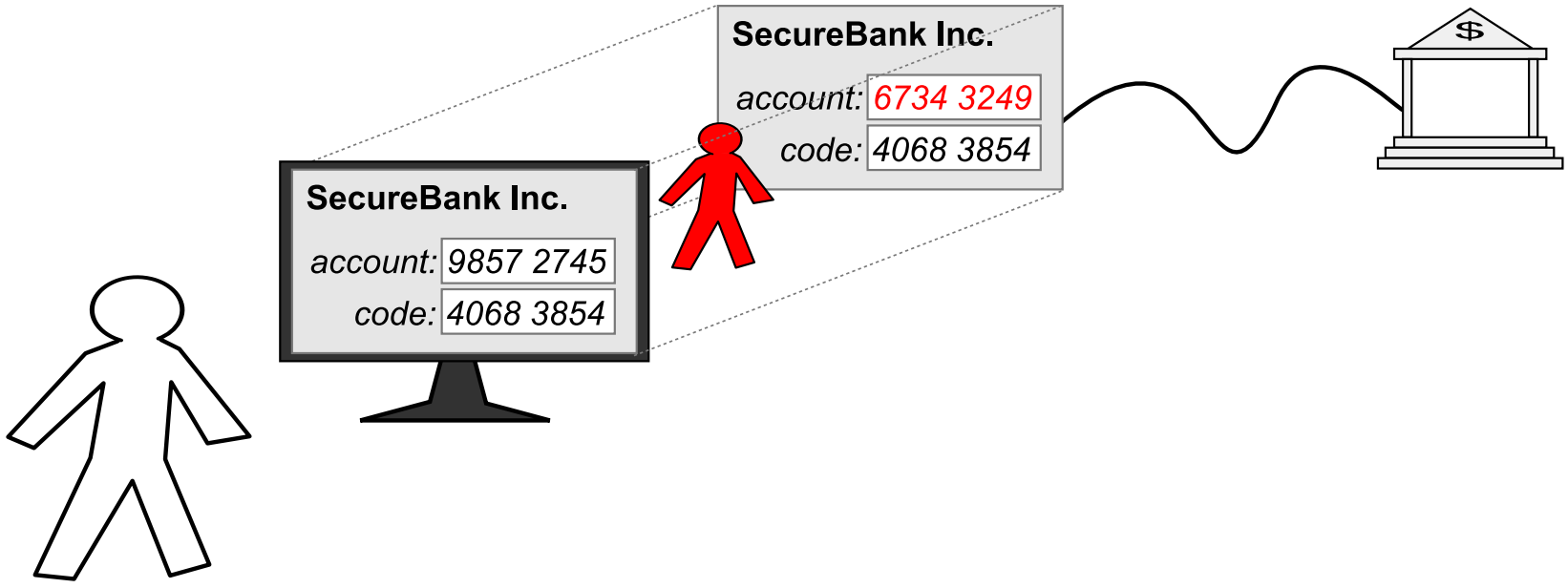
- On-screen keyboards
- Picture passwords
- One-time-passwords/iTAN
- Device fingerprinting

All of these defences have been broken by fraudsters

- Malware
- Man in the Middle (MITM)
- Combination: Man in the Browser



Man in the browser



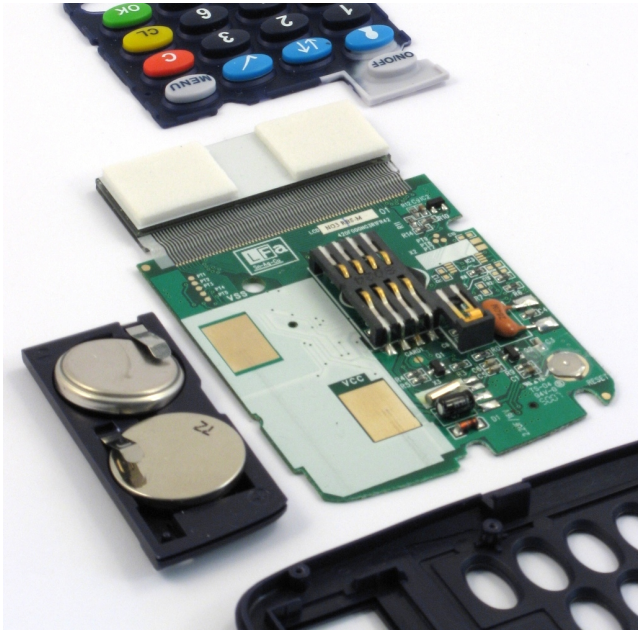
Malware embeds itself into the browser

Changes destination/amount of transaction in real-time

Any one-time password is valid, and mutual authentication succeeds

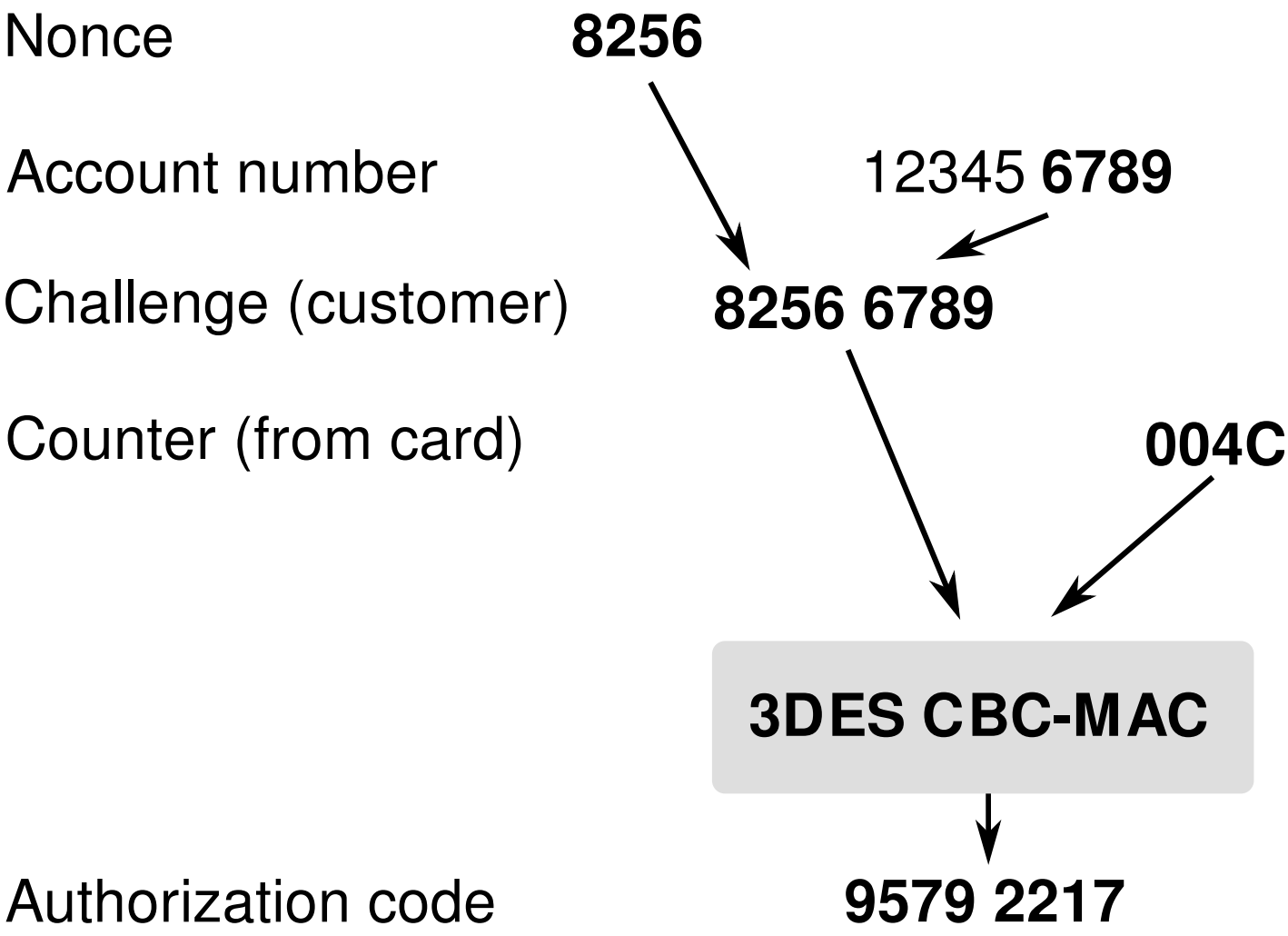
Patches up online statement so customer doesn't know

Some UK banks have rolled out disconnected smart card readers



CAP (chip authentication programme) protocol specification secret, but based on EMV (Europay, Mastercard, Visa) open standard for credit/debit cards

Protocol as perceived by bank (RBS/Natwest online)



Protocol as perceived by customer

- Reader prompts for 8-digit number
- Untrusted website provides number
- If customer enters a number where the last 4 digits are not the last 4 digits of the destination account number, the protocol is insecure
- There are signs that this may already have been exploited

More improvements require higher unidirectional bandwidth

For usability, customer should not have to type in full challenge

Device explains what authorization code implies

Tor is a low-latency, distributed anonymity system

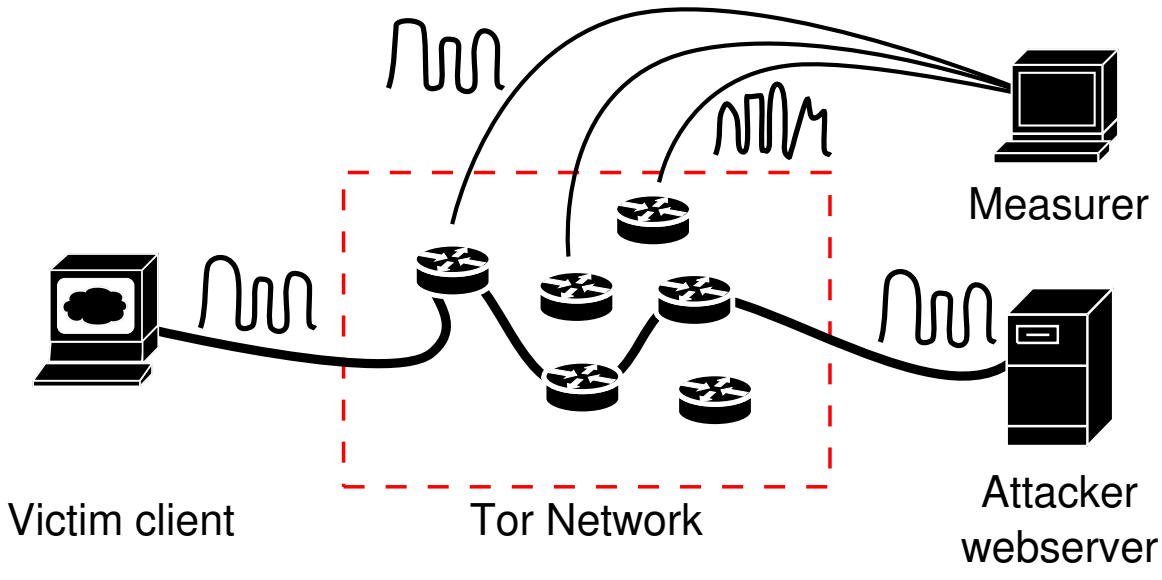
- Real-time TCP anonymisation system (e.g. web browsing)
- Supports anonymous operation of servers (hidden services)
- These protect the user operating the server and the service itself
- Constructs paths through randomly chosen nodes (around 1 000 now)
- Multiple layers of encryption hide correlations between input and output data
- No intentional delay introduced

More information: “An Improved Clock-skew Measurement Technique for Revealing Hidden Services”, USENIX Security, 2008

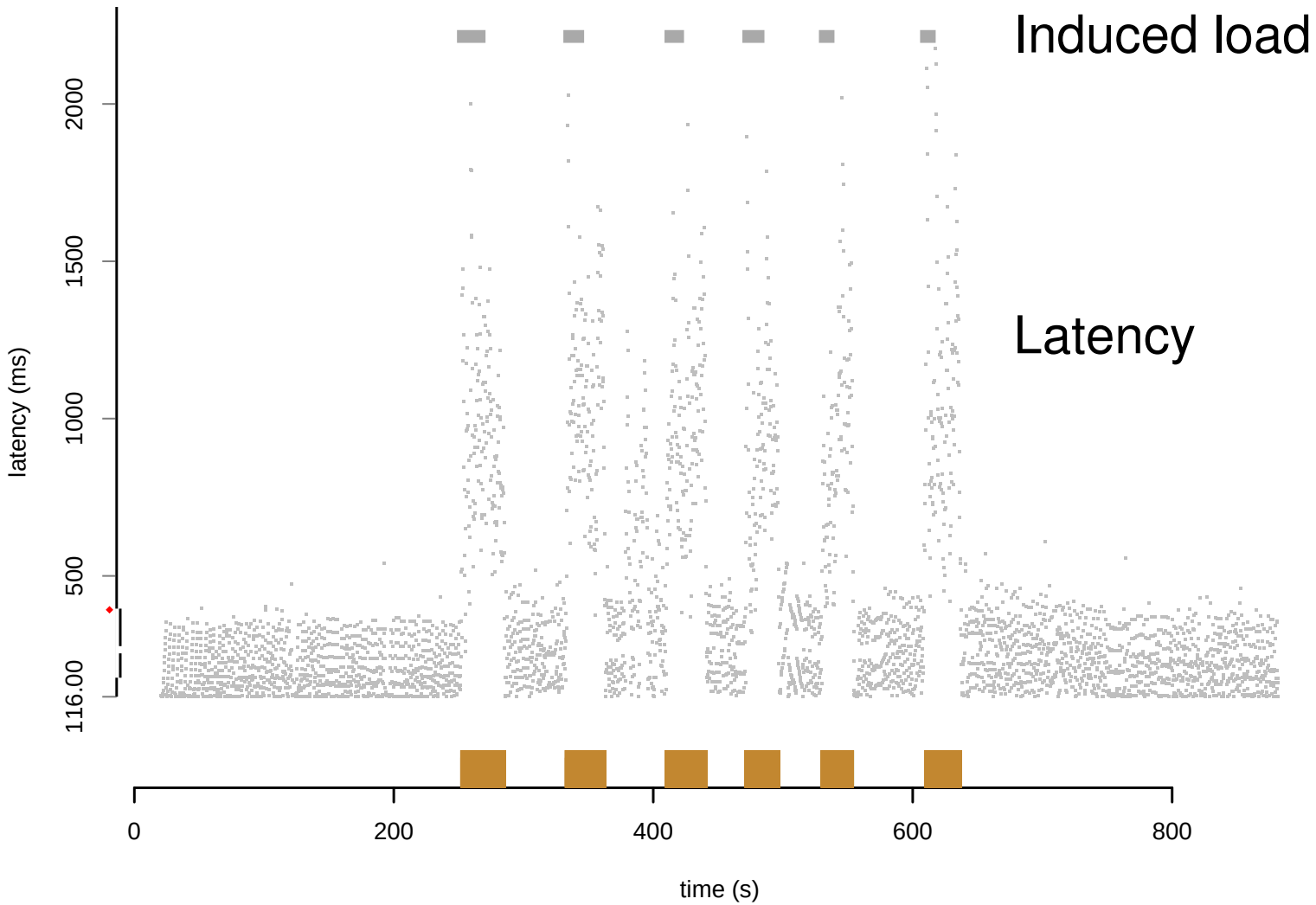
Even if an attacker cannot observe the network, traffic analysis is still possible

Attacker inserts traffic pattern into anonymous stream
Measurer probes all Tor nodes for their latency

Nodes along path that the anonymous stream takes will exhibit the same pattern

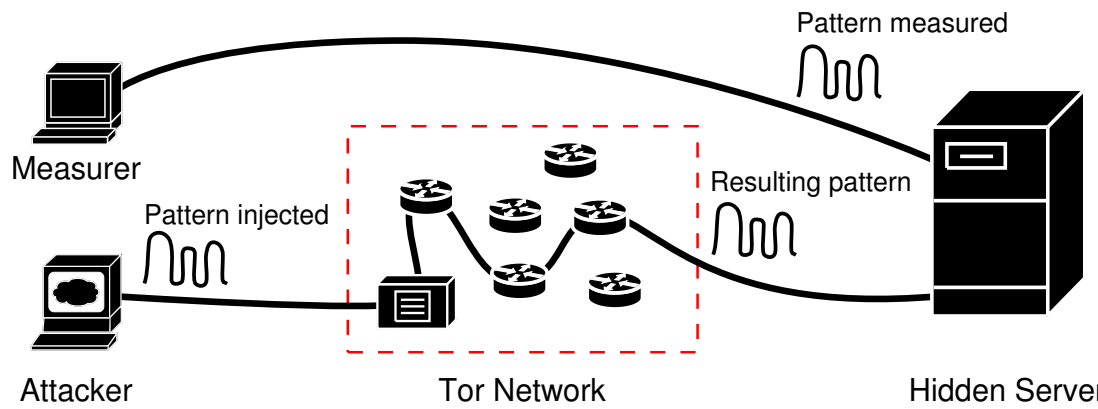


The latency of one connection going through a Tor node is strongly affected by its network load



The attack can be resisted with QoS features but there remains a temperature covert channel

- Prevent streams going through a node from interfering any others
- Hard QoS guarantee on every stream, and no more connections accepted than there is capacity
- When one stream is not used, no other streams may use the resources released, so CPU will be idle
- Then the CPU will cool down
- If we can measure the temperature of a remote PC we can validate guesses



Measured clock skew acts as a fingerprint of a computer (Kohno *et al.*, 2005)

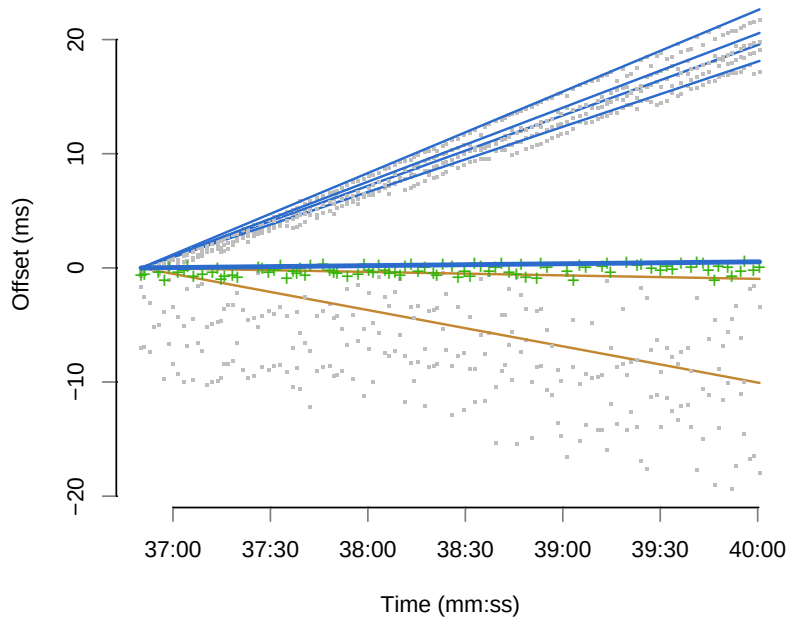
Offset:

- The difference between two clocks (ms)

↓

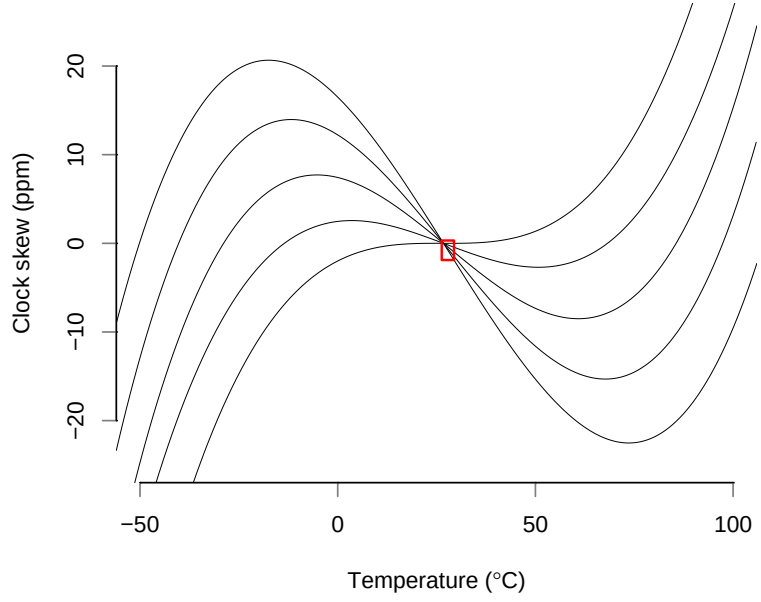
Skew:

- The rate of change of offset (ppm)
- Stable on one machine ($\pm$1–2 ppm), but varies over different machines (up to $\pm$50 ppm)
- Can give 4–6 bits of information on machine identity



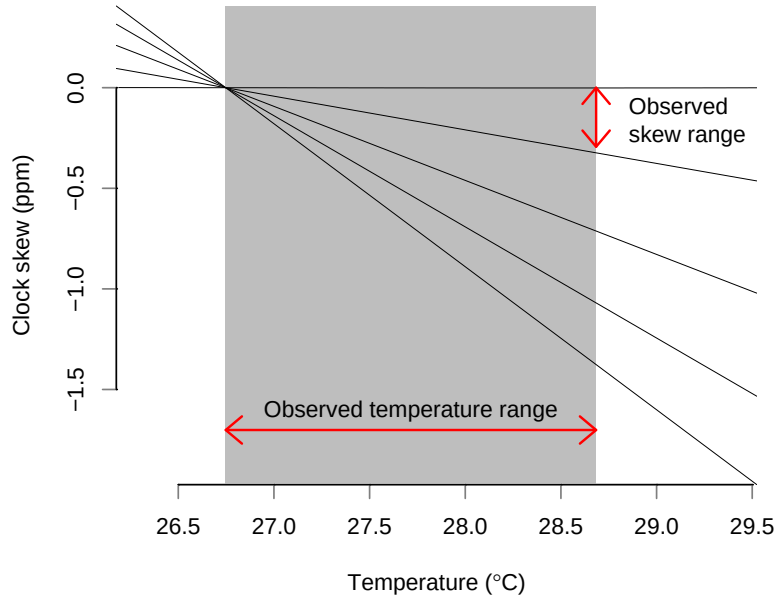
Temperature has a small, but remotely measurable, effect on clock skew

- Skew of typical clock crystal will change by ± 20 ppm over 150 °C operational range
- In typical PC temperatures, only around ± 1 ppm
- By requesting timestamps and measuring skews, an estimate of temperature changes can be derived
- Even in a well-insulated building, changes in temperature over the day become apparent



Temperature has a small, but remotely measurable, effect on clock skew

- Skew of typical clock crystal will change by ± 20 ppm over 150 °C operational range
- In typical PC temperatures, only around ± 1 ppm
- By requesting timestamps and measuring skews, an estimate of temperature changes can be derived
- Even in a well-insulated building, changes in temperature over the day become apparent



Clock skew variations are not visible in raw network traces, but can be extracted with numerical analysis

Measure offset of candidate machine(s)

↓

Remove constant skew from offset

↓

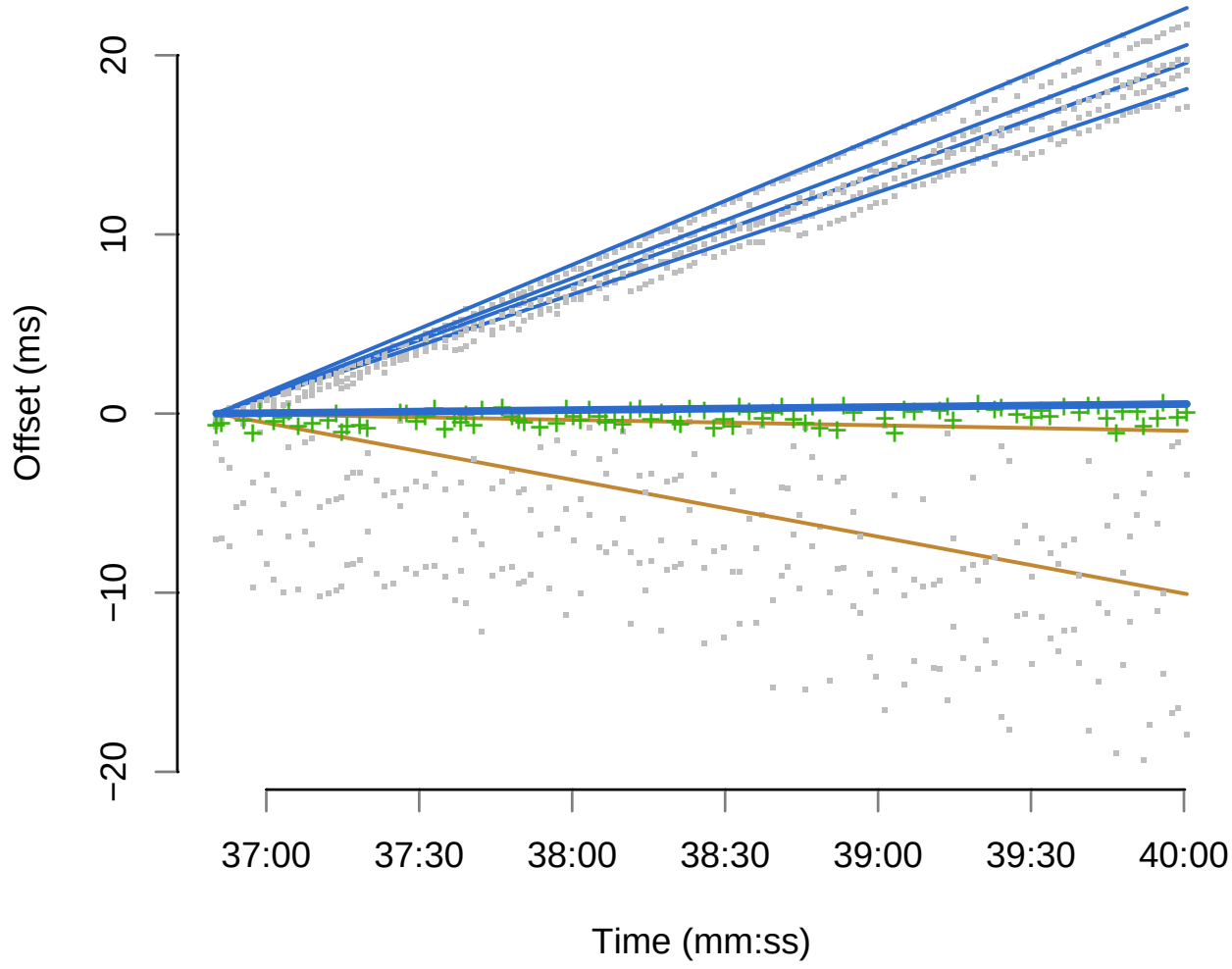
Remove noise

↓

Differentiate

↓

Compare to temperature



Clock skew variations are not visible in raw network traces, but can be extracted with numerical analysis

Measure offset of candidate machine(s)

↓

Remove constant skew from offset

↓

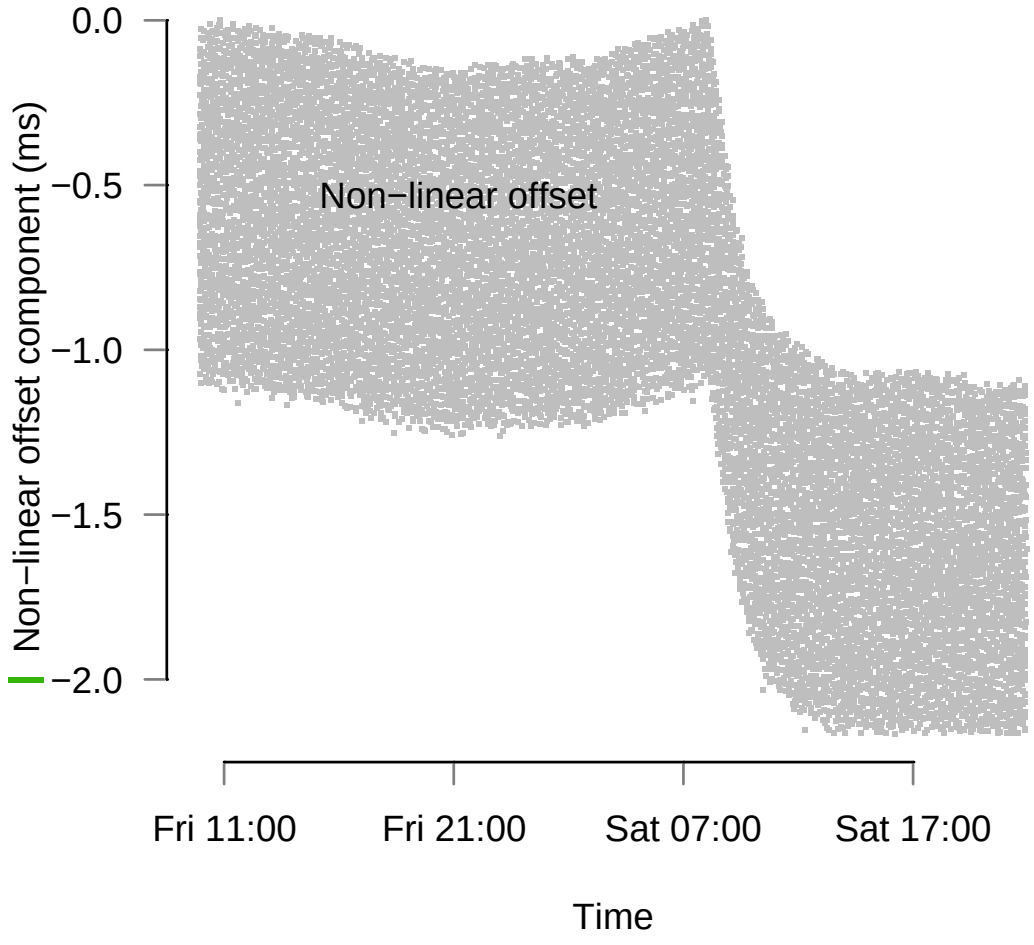
Remove noise

↓

Differentiate

↓

Compare to temperature



Clock skew variations are not visible in raw network traces, but can be extracted with numerical analysis

Measure offset of candidate machine(s)

↓

Remove constant skew from offset

↓

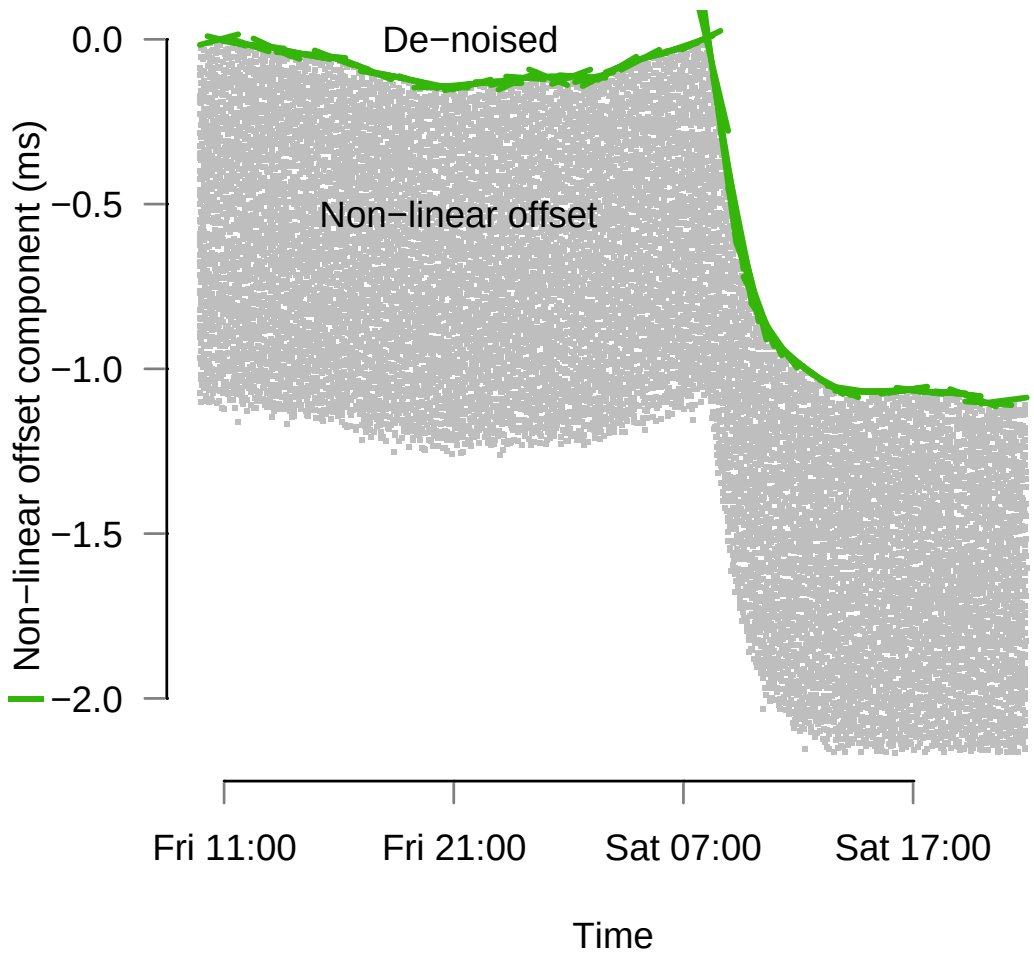
Remove noise

↓

Differentiate

↓

Compare to temperature



Clock skew variations are not visible in raw network traces, but can be extracted with numerical analysis

Measure offset of candidate machine(s)

↓

Remove constant skew from offset

↓

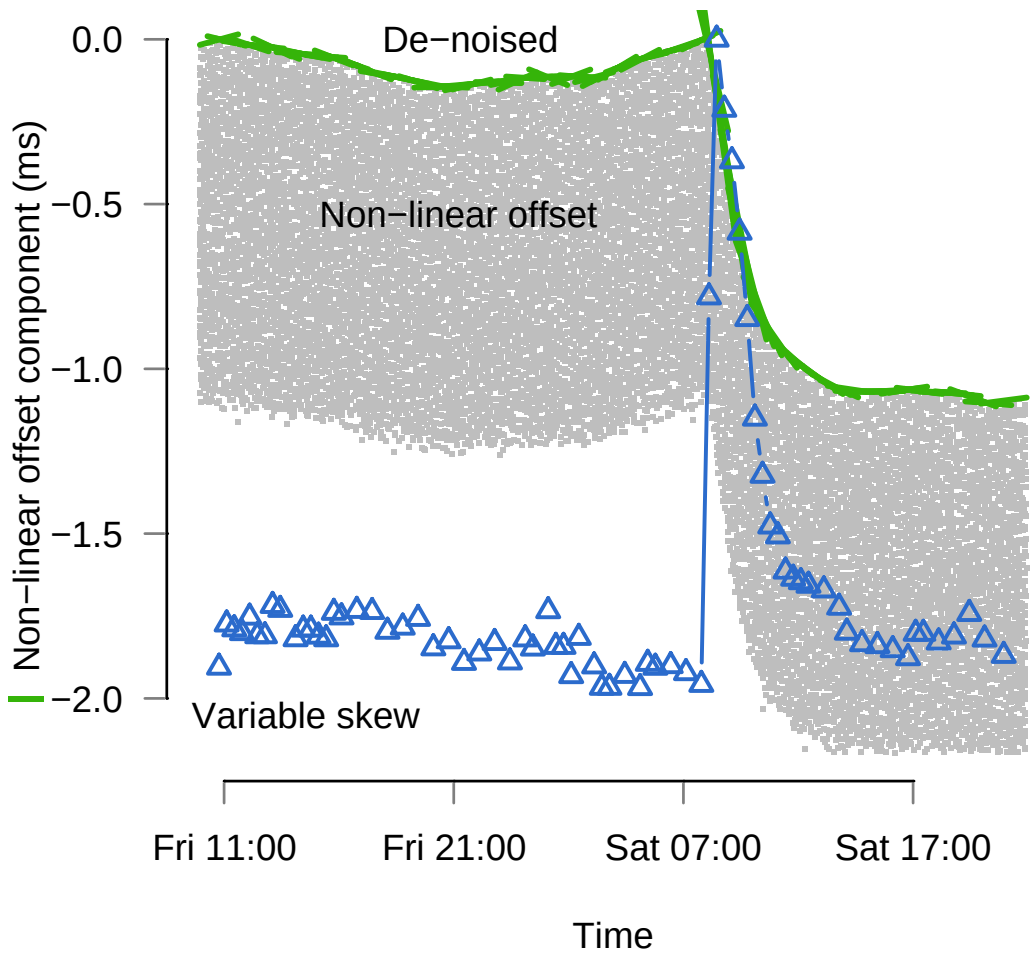
Remove noise

↓

Differentiate

↓

Compare to temperature



Clock skew variations are not visible in raw network traces, but can be extracted with numerical analysis

Measure offset of candidate machine(s)

↓

Remove constant skew from offset

↓

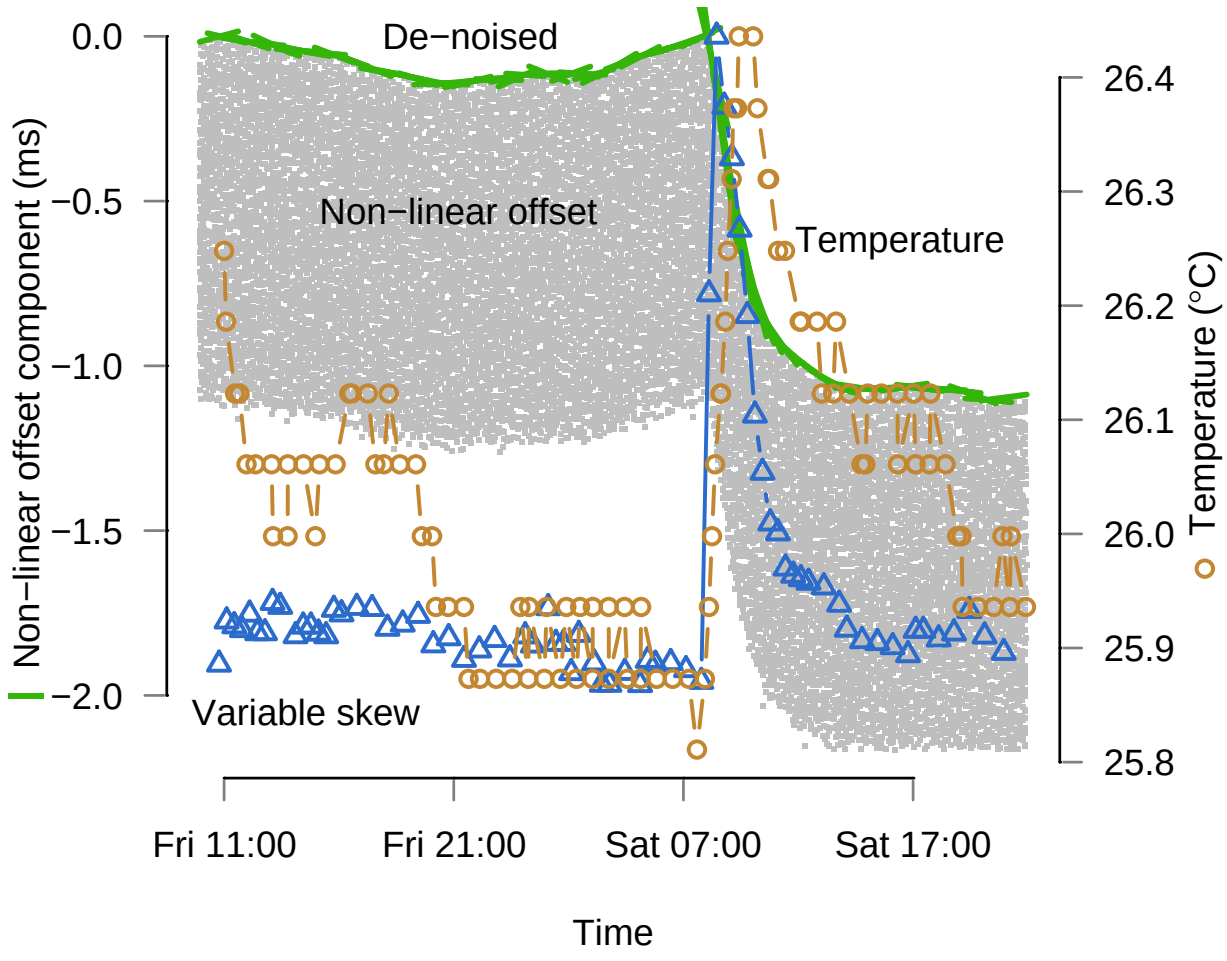
Remove noise

↓

Differentiate

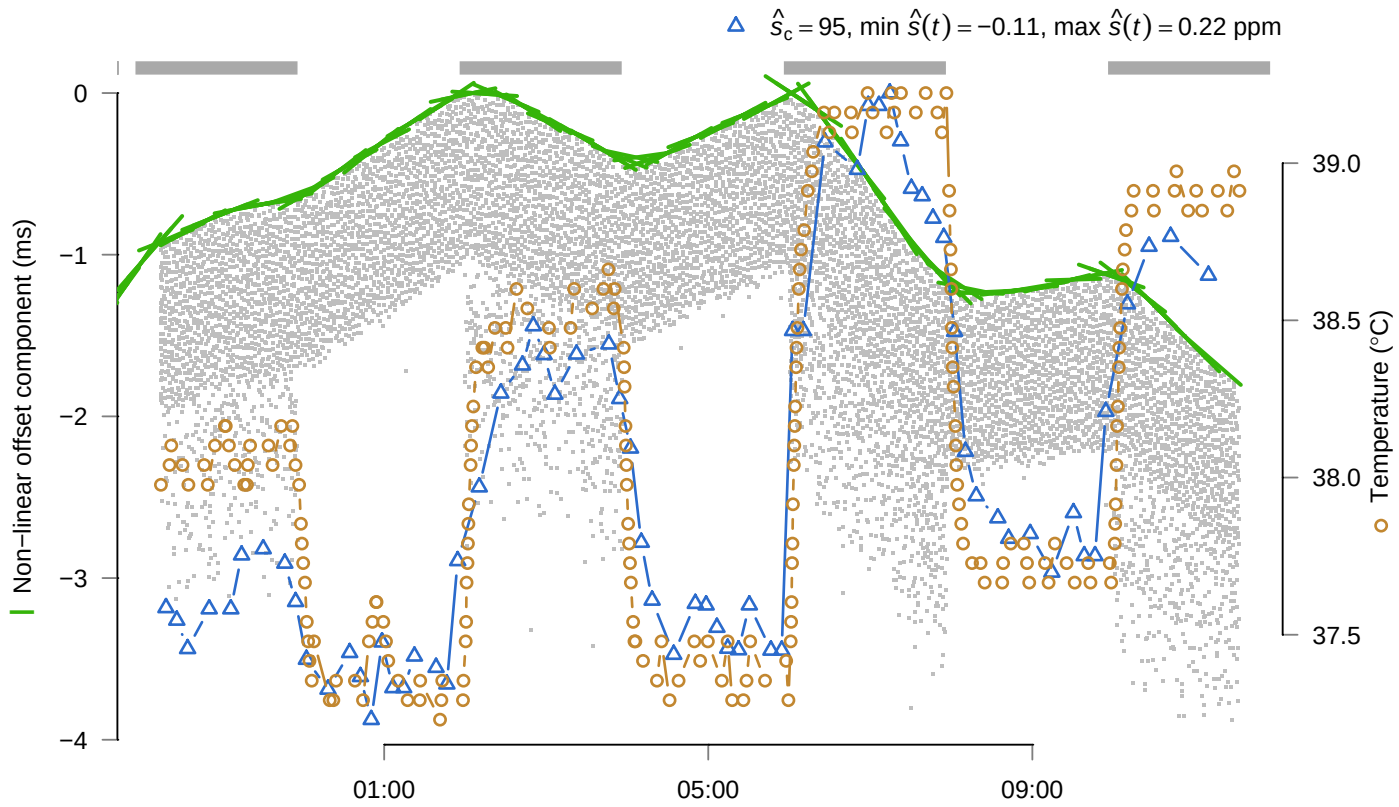
↓

Compare to temperature



The load of a hidden service can be estimated by measuring temperature induced clock skew

- Attacker induces load by making requests to the hidden server
- Here, a periodic 2 hour on, 2 hour off pattern was used
- Measurer records clock offset and derives temperature



In conclusion, system security is as important as security of components

- Chip & PIN PEDs were insecure because the designers of hardware tamper resistance failed to take into account options chosen by UK banks
- A concise security architecture document would have helped prevent this flaw, and constrained system development
- CAP was insecure because it failed to consider the human as part of the security protocol
- Alternative technologies perform better, due to better usability testing prior to deployment
- QoS failed to protect Tor because the abstraction chosen for modelling the system did not match reality
- As systems become more complex finding appropriate abstractions will be increasingly difficult