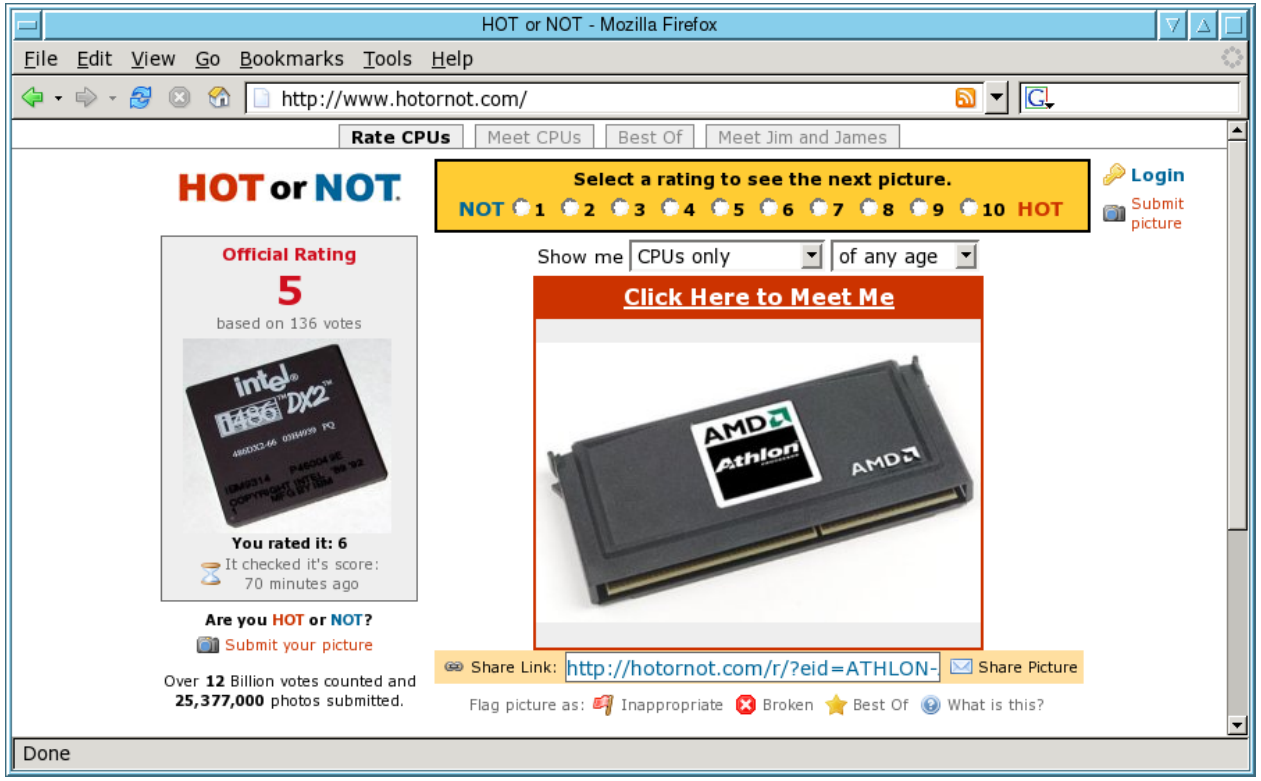
Hot or Not: Revealing Hidden Services by their Clock Skew



Steven J. Murdoch

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

University of Cambridge Computer Laboratory

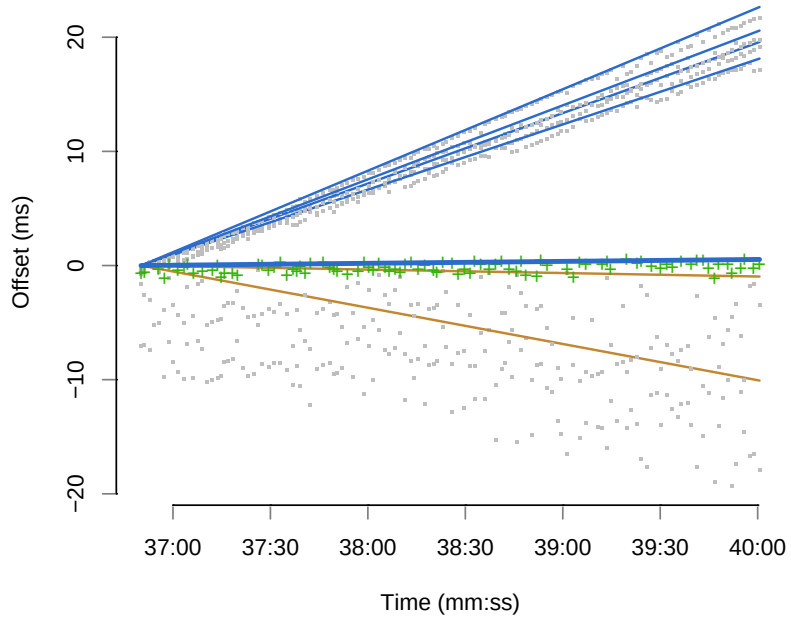
OpenNet Initiative

Summary

- Clock skew background and definitions
- Temperature effects on clock skew
- Developing attacks for Tor
- Other applications
- Defences and conclusions

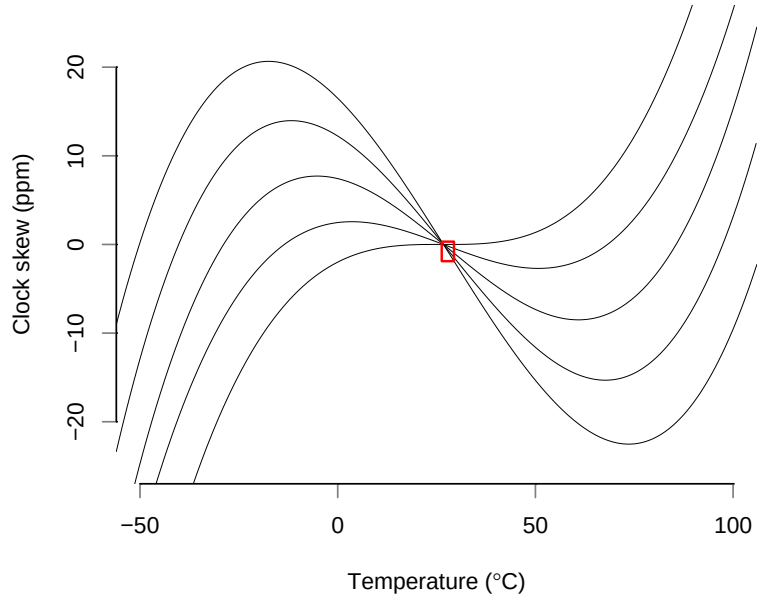
Clock skew (Kohno *et al.*)

- *Offset* is difference between two clocks (ms)
- *Skew* is the rate of change of offset (ppm)
- Can be detected remotely through ICMP/TCP timestamps (and other sources)
- 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



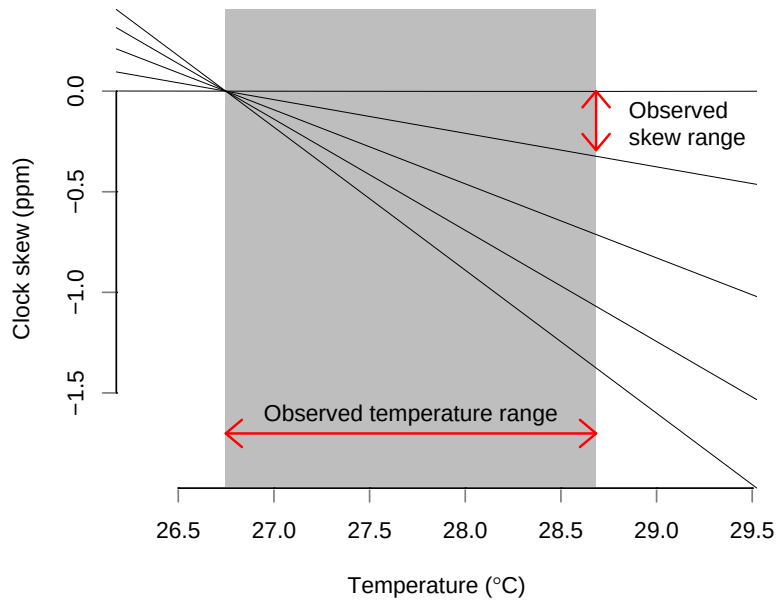
Effect of temperature on skew

- 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



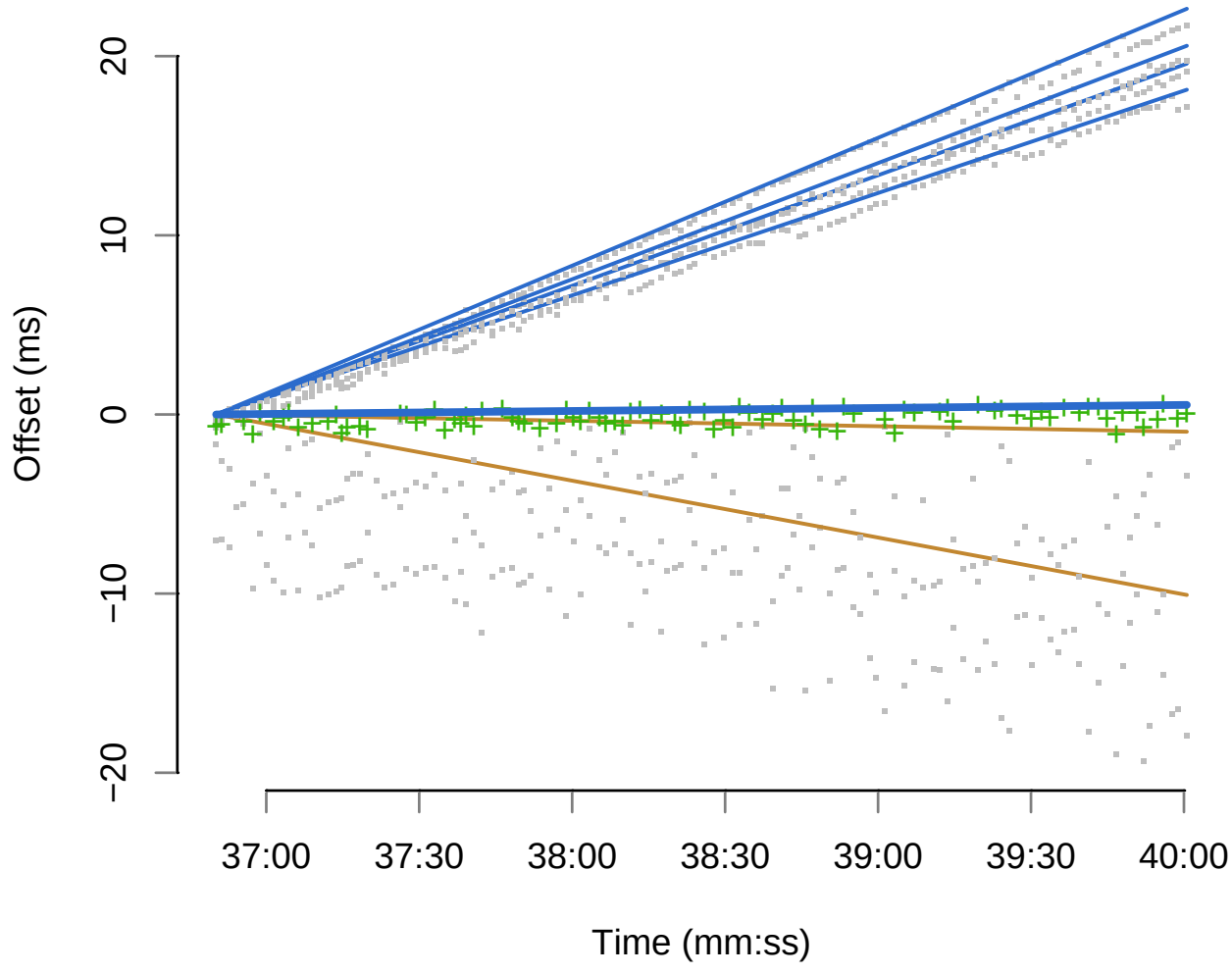
Effect of temperature on skew

- 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



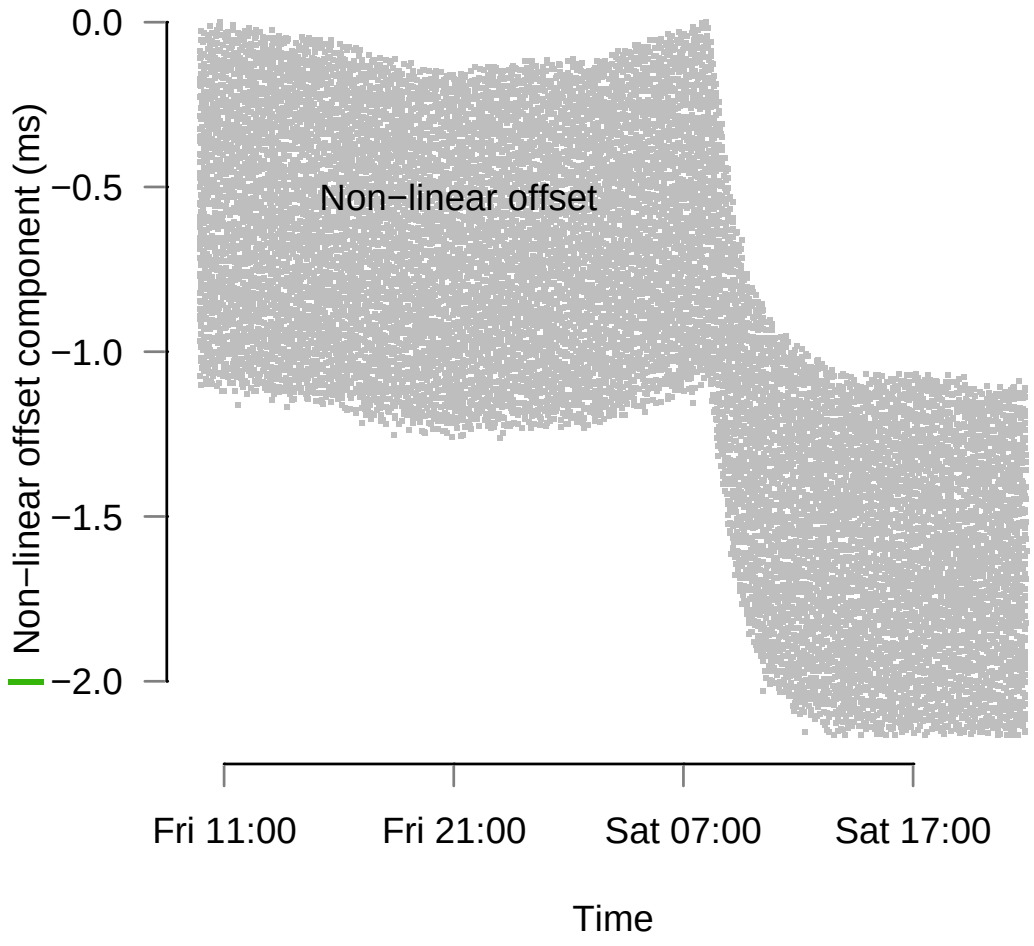
Measuring temperature

- Measure offset of candidate machine(s)
- Remove constant skew from offset
- Remove noise
- Differentiate
- Compare to temperature



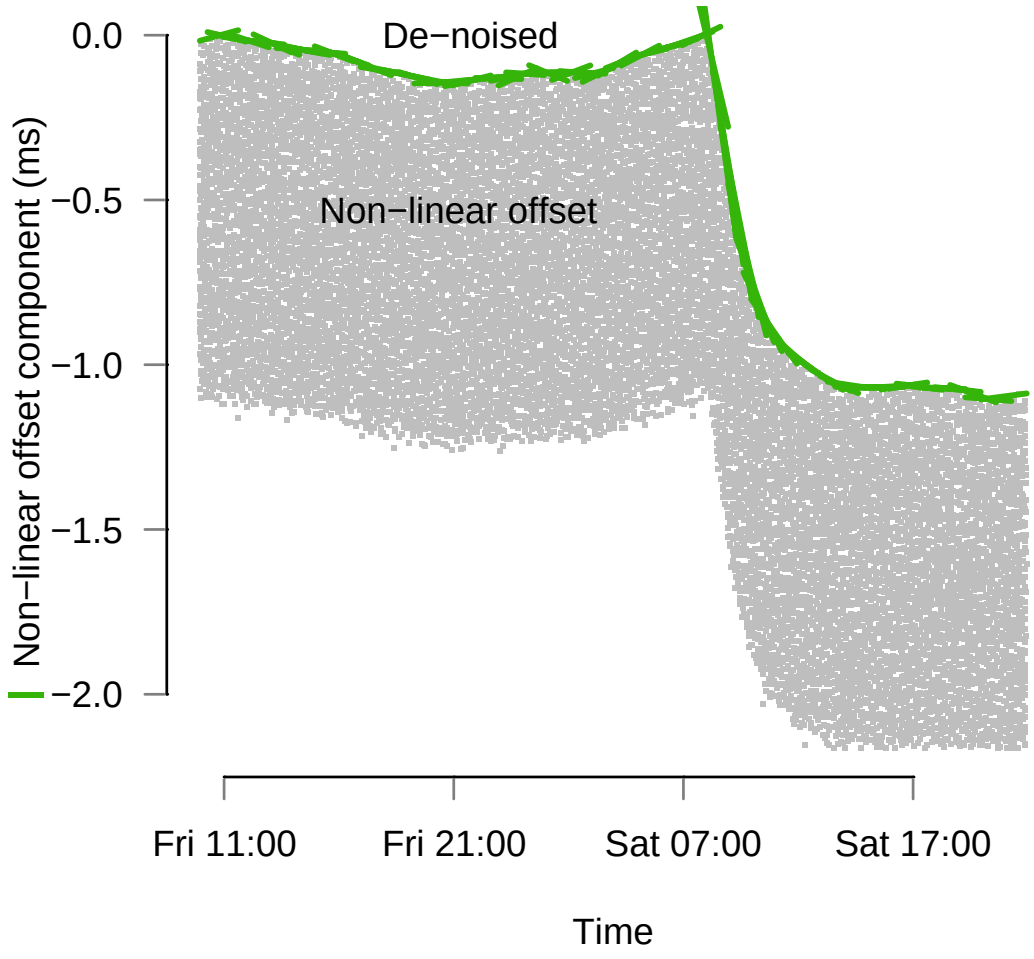
Measuring temperature

- Measure offset of candidate machine(s)
- Remove constant skew from offset
- Remove noise
- Differentiate
- Compare to temperature



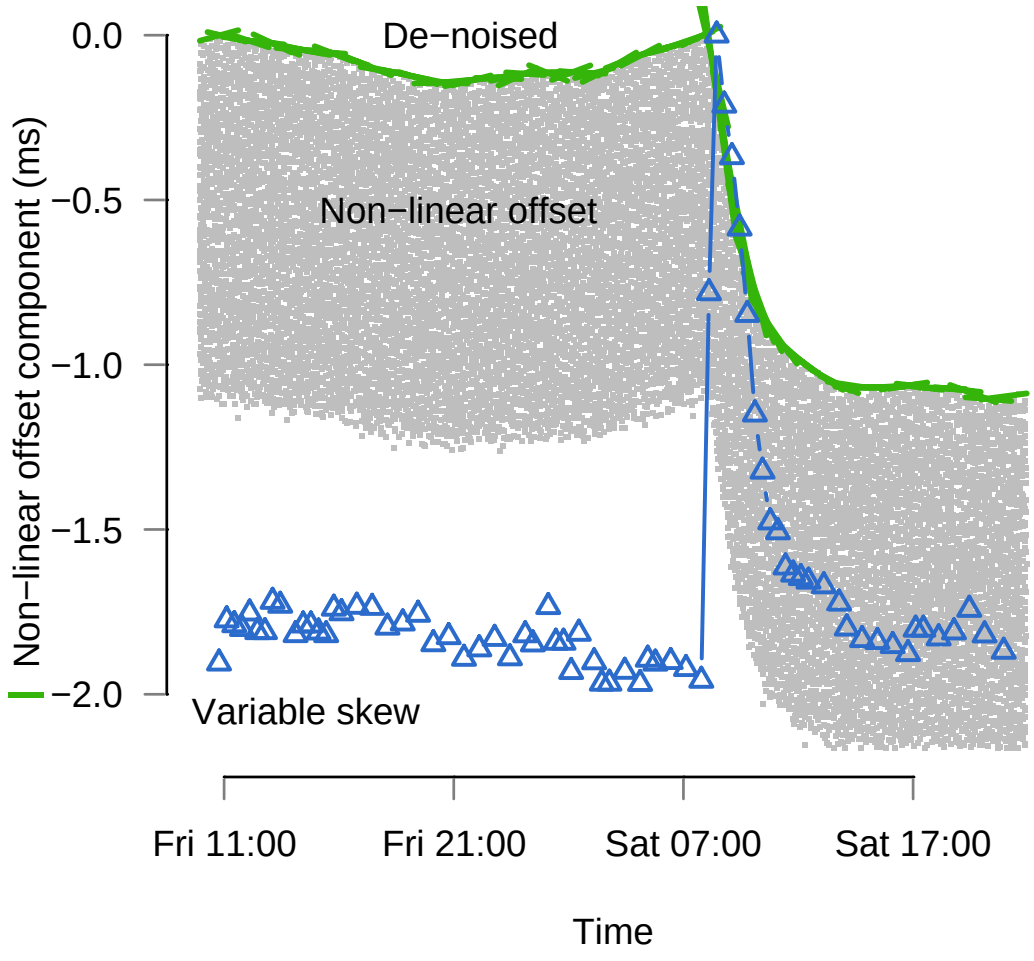
Measuring temperature

- Measure offset of candidate machine(s)
- Remove constant skew from offset
- Remove noise
- Differentiate
- Compare to temperature



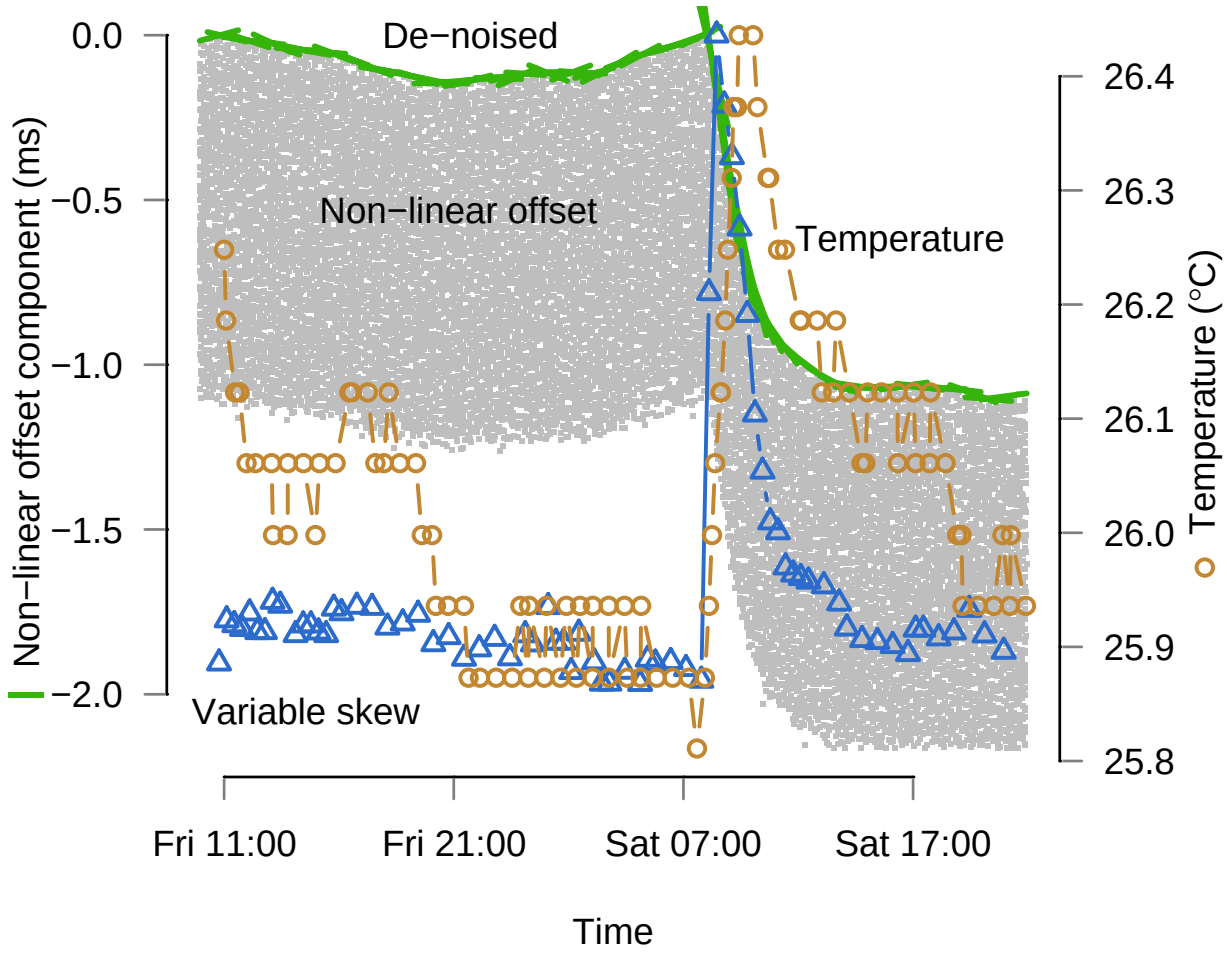
Measuring temperature

- Measure offset of candidate machine(s)
- Remove constant skew from offset
- Remove noise
- Differentiate
- Compare to temperature



Measuring temperature

- Measure offset of candidate machine(s)
- Remove constant skew from offset
- Remove noise
- Differentiate
- Compare to temperature

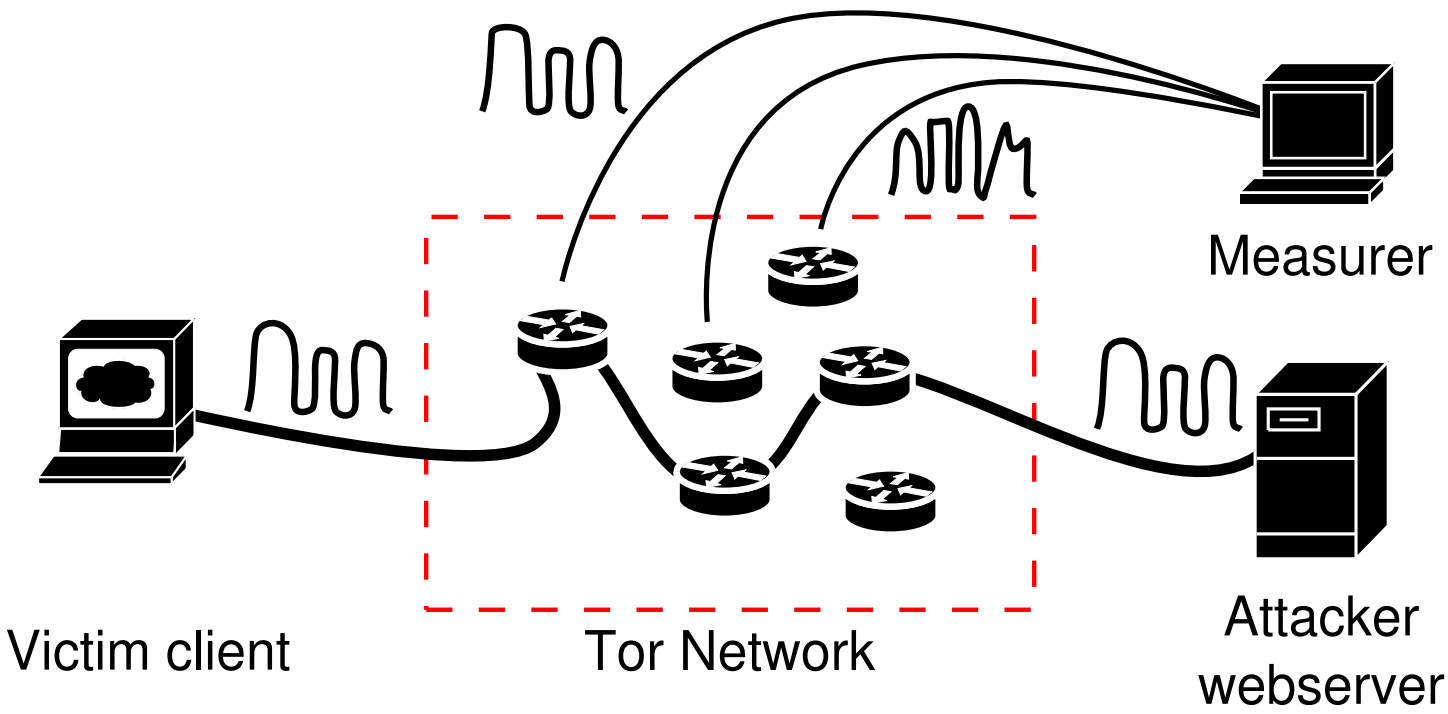


Tor

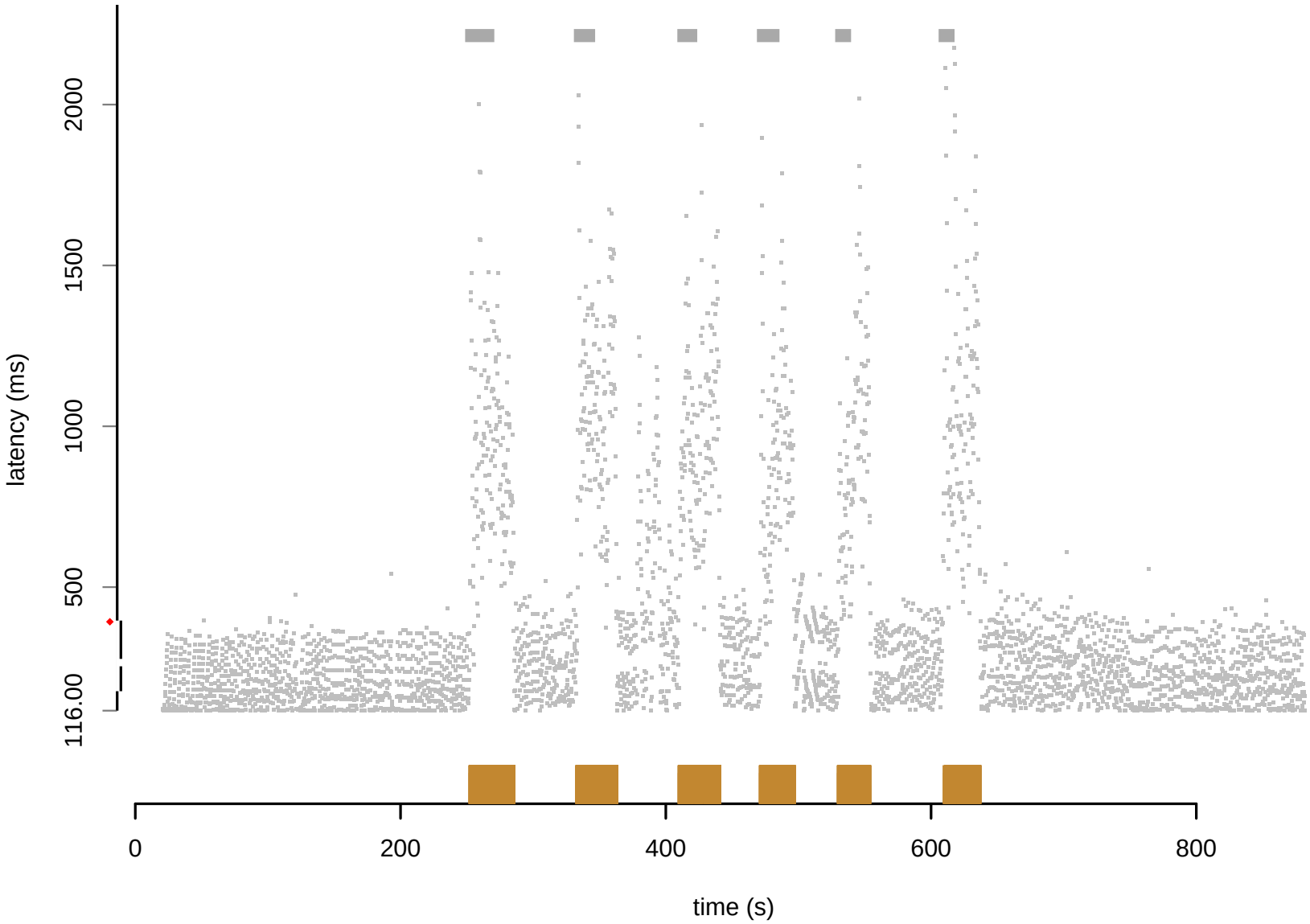
- Real-time TCP anonymisation system
- Supports anonymous operation of servers (hidden services)
- These protect the user operating the server and the service itself
- Constructs paths through randomly chosen volunteer nodes (around 800 currently)
- Multiple layers of encryption hide correlations between input and output data
- No intentional delay introduced (unlike mixes) so vulnerable to traffic analysis

Indirect traffic analysis (Murdoch, Danezis)

- Attacker inserts traffic pattern into anonymous stream
- Probes all Tor nodes for their latency
- Nodes along path that the anonymous stream takes will exhibit the same pattern

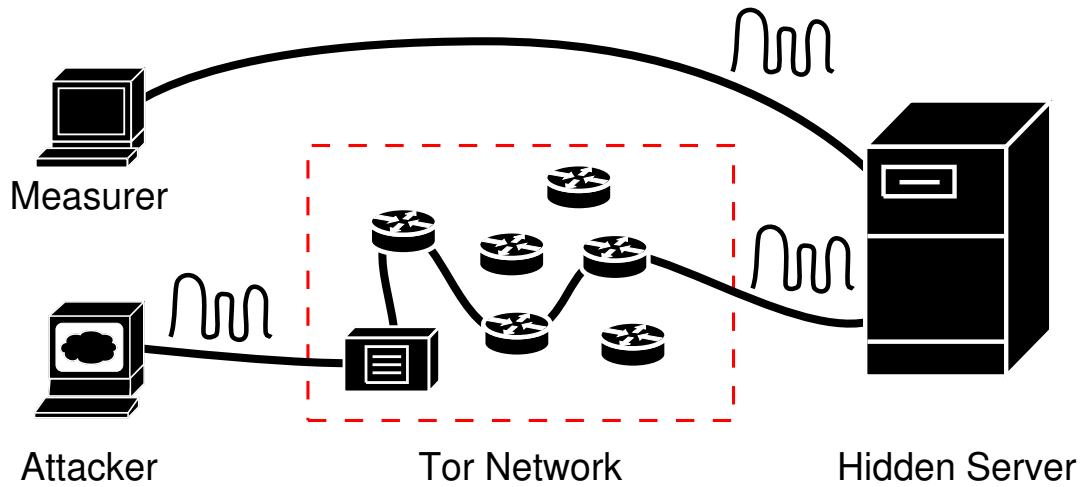


Latency analysis results



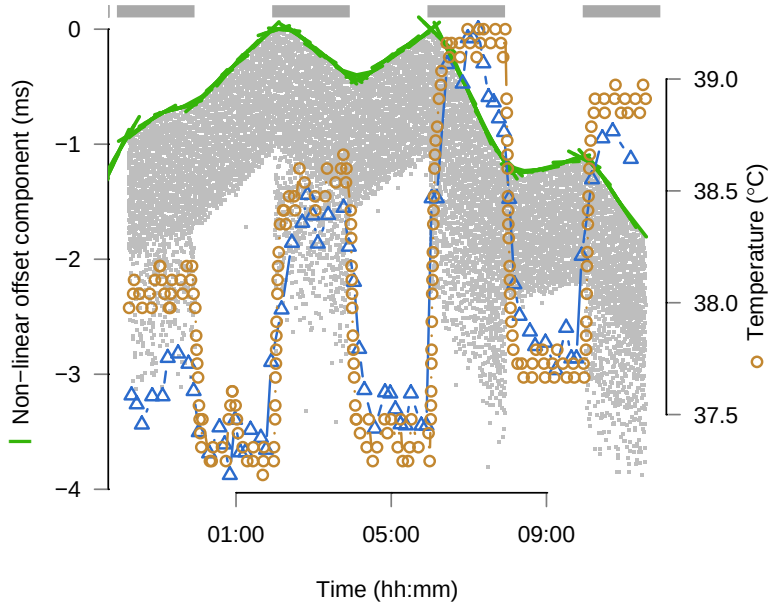
QoS defence introduces new attack

- Prevent one stream going through another node from interfering with 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
- This will cause the CPU to cool down and the clock skew will change accordingly, allowing connections to be tracked
- Validated with Tor hidden services on a private Tor network



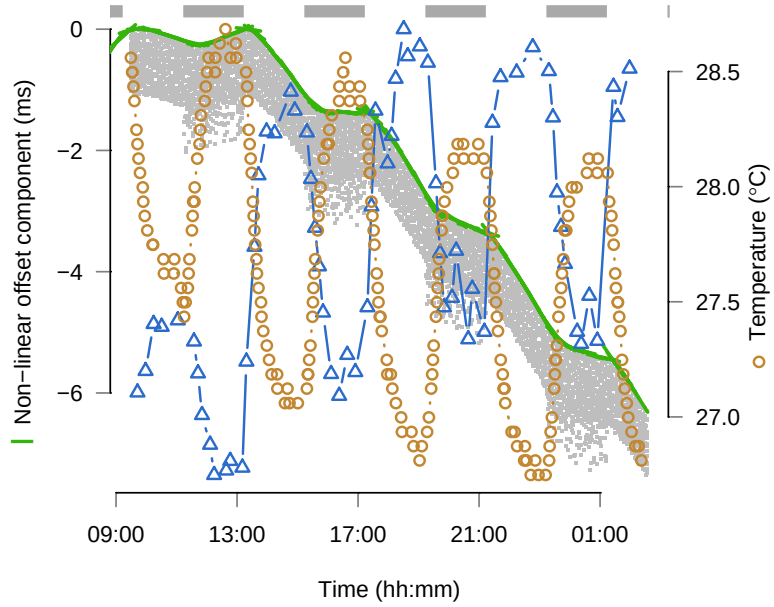
Temperature analysis results

- 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
- Sometimes opposite relationship between temperature and clock skew is observed
- Perhaps due to different crystal design, temperature compensation or other temperature dependent components



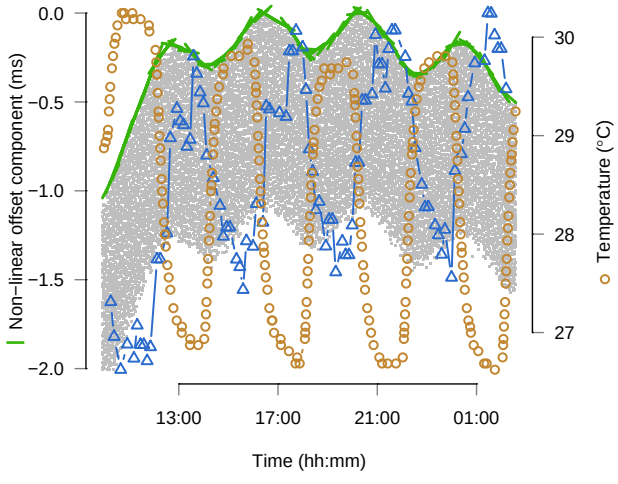
Temperature analysis results

- 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
- Sometimes opposite relationship between temperature and clock skew is observed
- Perhaps due to different crystal design, temperature compensation or other temperature dependent components



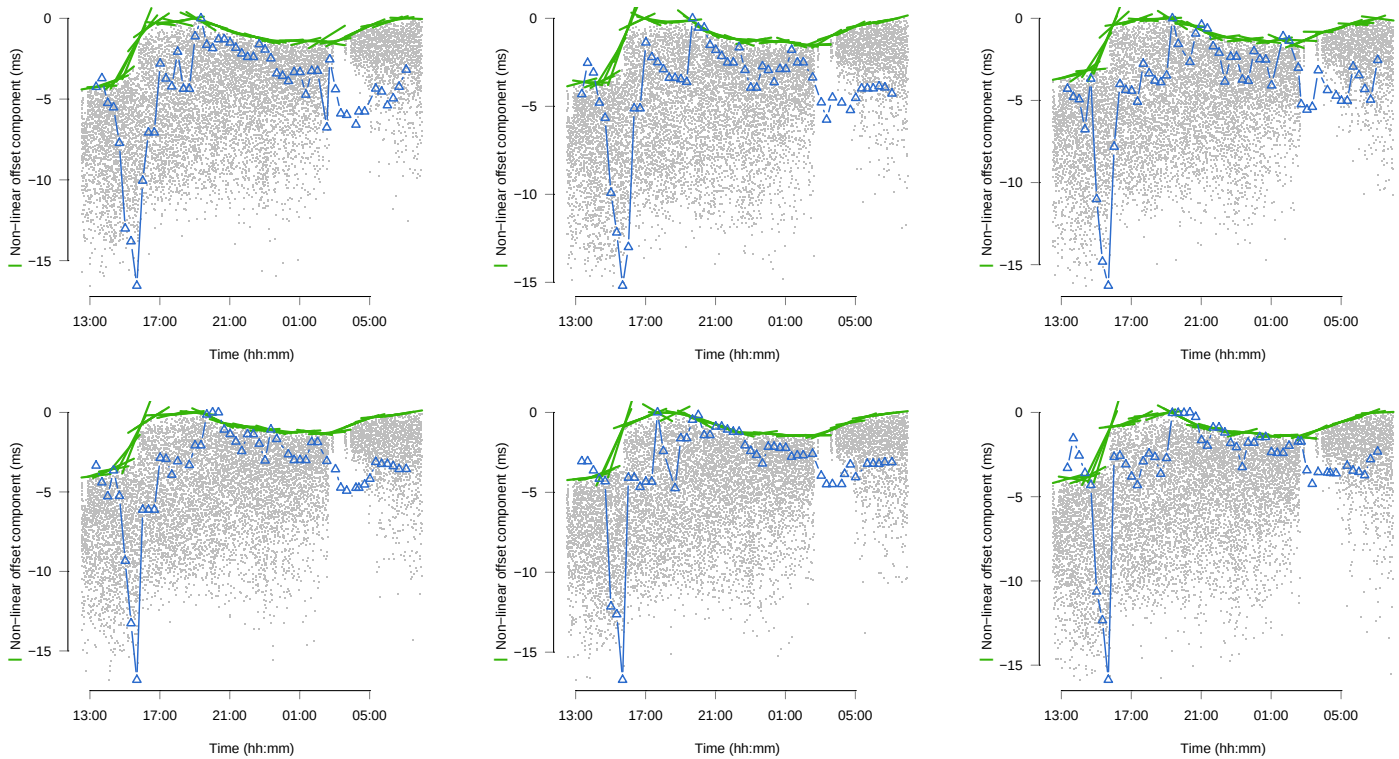
Other covert channels

- Inter-process communication through modulating temperature load
  - Fixed scheduling will not defend against this
  - Relies on second time source, affected differently by temperature; could be remote (NTP) or local (sound card)
- Temperature effects can cross “air-gap” security barriers
  - Confirmed in rack-mount computers; plausible for “blade” arrangements too



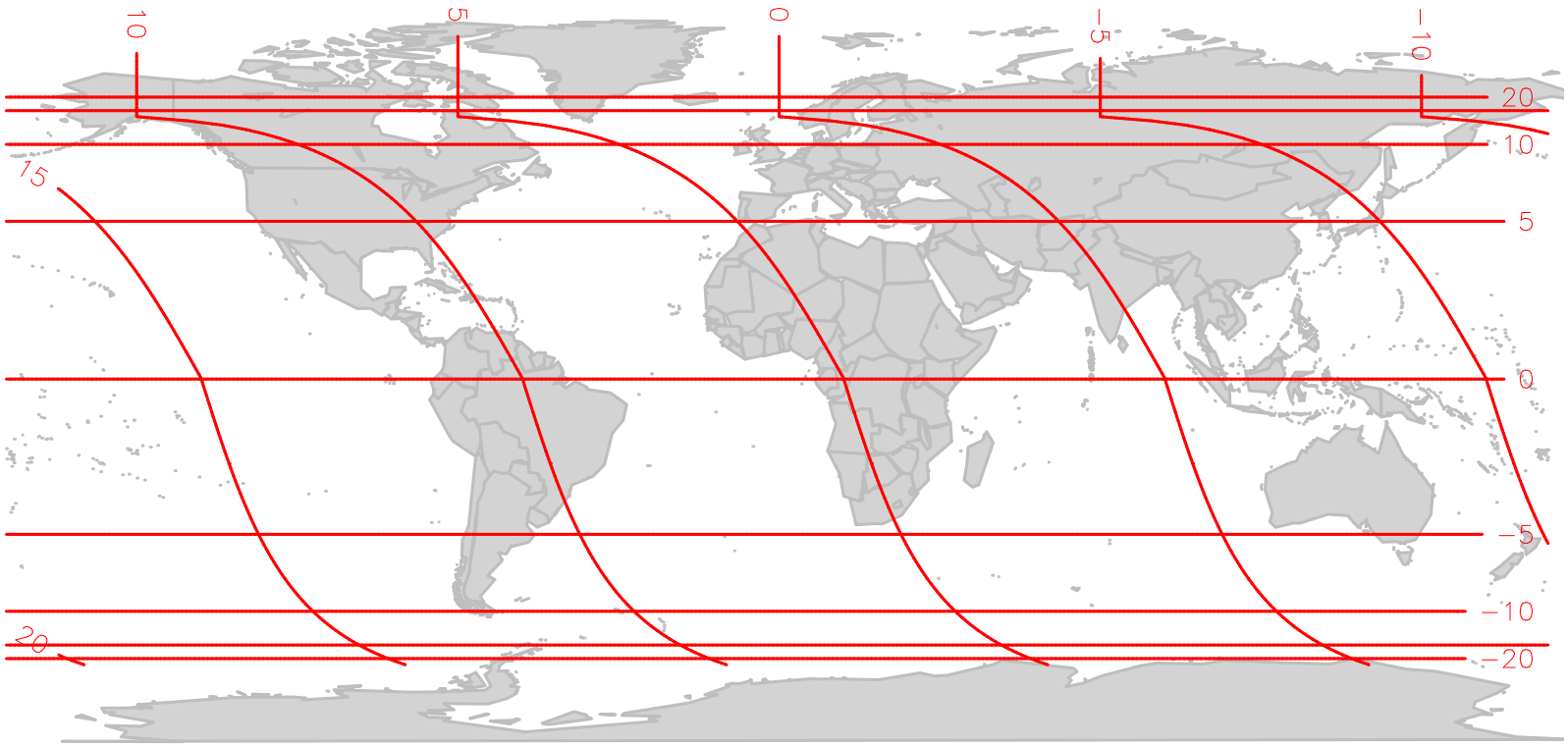
Machine and environment identification

- Kohno *et al.* already showed how to identify computers through clock skew
- Temperature information can indicate environment
- Applied to investigate suspected “Sybil” attack on Tor, to discover than the 30 suspicious Tor nodes were actually 2 physical machines



Geolocation

- If length of day and middle/start/end of day can be found, locations of measurement can be found
- Imprecise, time-consuming and affected by local conditions (air conditioning) but perhaps could provide coarse-grained coordinates



Defences and conclusions

- Temperature covert channels are an effective attack in several situations
  - However, they are only likely to be the best attack against systems which are already well hardened against conventional techniques
- Timing information is difficult to hide
  - TCP timestamps improve performance on high-speed networks
  - Even if all explicit timestamps are removed, implicit ones, such as packet emission on a timer interrupt, will remain
- Temperature compensated crystals have a typical skew of ± 1 ppm, so may not be adequate to prevent this attack
- Oven controlled crystals are several orders of magnitude better and so might be more successful
- Covert channel analysis research is a useful source of ideas for other security systems