Poster: Time and Time Again: Leveraging TCP Timestamps to Improve Remote Timing Attacks

Vik Vanderlinden, Tom Van Goethem, Mathy Vanhoef
DistriNet, KU Leuven

February 6, 2026

1 Paper abstract

One of the most well-known side-channel attacks is to infer secret information from the time it takes to perform a certain operation. Many systems have been shown to be vulnerable to such attacks, ranging from cryptographic algorithms, web applications, and even micro-architectural implementations. Exploiting these side-channel leaks over a networked connection is known to be challenging due to variations in the round-trip time, i.e., network jitter. Timing attacks have become especially challenging as processors become faster, resulting in smaller timing differences, systems become more complex, making it more difficult to collect consistent measurements, and networks become more congested, amplifying the network jitter.

In this work we introduce novel remote timing attack methods that are completely unaffected by the jitter on the network path, making them several times more efficient than timing attacks based on the round-trip time, and allow for smaller timing differences to be detected. More specifically, the execution time is inferred from the TCP timestamp values that are generated by the server upon acknowledging the request and sending the response. Furthermore, we show how sequential processing of incoming requests can be leveraged to inflate the time of the secret-dependent operation, resulting in a more accurate attack. Finally, through extensive measurements and a real-world case study we demonstrate that the techniques we introduce in this paper have various advantageous properties compared to other timing attack methods: few(er) prerequisites are required any TCP-based protocol is subject to these attacks, and the attacks can be executed in a distributed manner.

Vik Vanderlinden, Tom Van Goethem, and Mathy Vanhoef. Time and time again: Leveraging tcp timestamps to improve remote timing attacks. In *NDSS*, 2026

`https://dx.doi.org/10.14722/ndss.2026.230893`

References

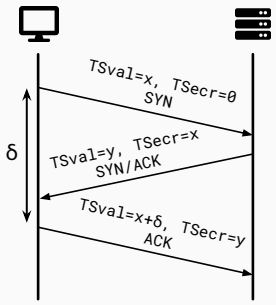
[VVGV26] Vik Vanderlinden, Tom Van Goethem, and Mathy Vanhoef. Time and time again: Leveraging tcp timestamps to improve remote timing attacks. In *NDSS*, 2026.

Time and Time Again: Leveraging TCP Timestamps to Improve Remote Timing Attacks

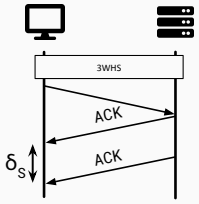
Vik Vanderlinden, Tom Van Goethem, and Mathy Vanhoef
DistriNet, KU Leuven, Belgium

TCP Timestamps

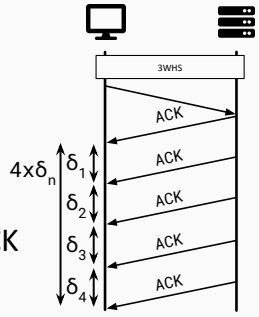
- TCP option
- Negotiated in 3WHS
- Performance improvements
- RTTM & PAWS
- Often follows real time



Attack Mechanisms



Immediate ACK + response

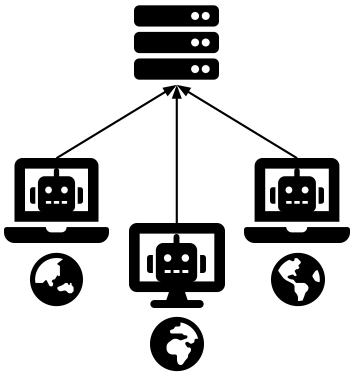


Runtime multiplication: coalesce requests, multiply timing differences

Results

Exploitable timing difference decreases by 5 times (ms timestamps) to 33 times (µs timestamps), going from a 25 µs resolution down to 5 µs and 750 ns respectively.

Number of requests required decreases by 5 to 50 times, e.g. for 25 µs from >10k requests to 200 requests



Because of complete independence, the attack works in a **distributed** manner: measurements from many servers can be combined regardless of location. Results are identical to those of the non-distributed attack.

Susceptibility

Custom crawls on over 550k Tranco domains

TCP Timestamps Option	88.90%
Immediate Acknowledgment	99.40%
Persistent Connections	95.55%
Runtime > 1 ms	69.34%

Real-world applicability

1. **TLS**
   - > First transatlantic exploit of Lucky 13
   - > Using µs-accurate timestamps
   - > CVE-2025-32998 - responsibly disclosed
2. Reproduced user enumeration against **SSH**
3. Reproduced user enumeration against **FTP**
   - With 900 req/s load to show robustness

Defenses

- Constant-time implementations (difficult)
- Decrease timestamp frequency (partially effective)
- Obfuscated timestamps:
  - > Effective, but require kernel support

Future work

- > Thorough testing of other TCP-based protocols
- > Testing non-TCP-based protocols with timestamps
- > Extensive evaluations of statistical tests for low-granularity data