

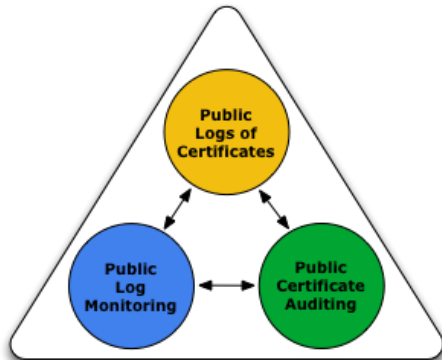


Verifiable Light-Weight Monitoring for Certificate Transparency Logs

Rasmus Dahlberg and Tobias Pulls

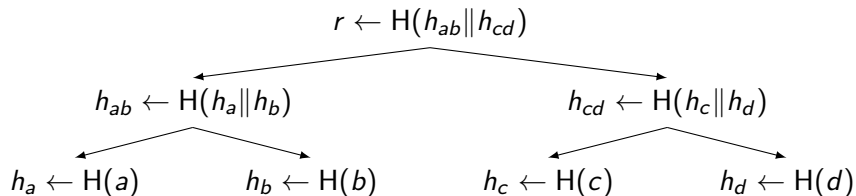
Certificate Transparency (CT)

- Add transparency to CA ecosystem
- Publicly log all certificates
- No need¹ to trust the log
 - ▶ Membership proofs
 - ▶ Append-only proofs



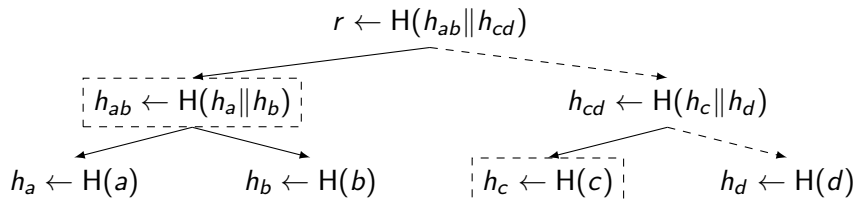
<http://www.certificate-transparency.org/what-is-ct>

¹As deployed right now we do trust the logs tho ☹



■ Append new certificates in batches

■ Sign tree head every hour ➡ STH

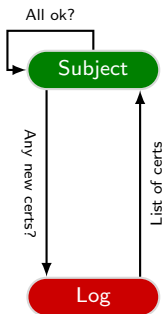


■ Traverse tree from root to leaf

■ Grab all sibling hashes on the way

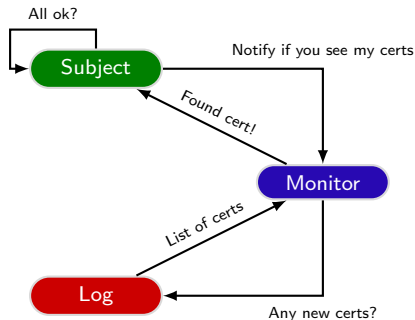
Two approaches towards monitoring a CT log

Self-monitoring



- ☹ Continuous uptime
- ☹ Download everything

Monitoring-as-a-service

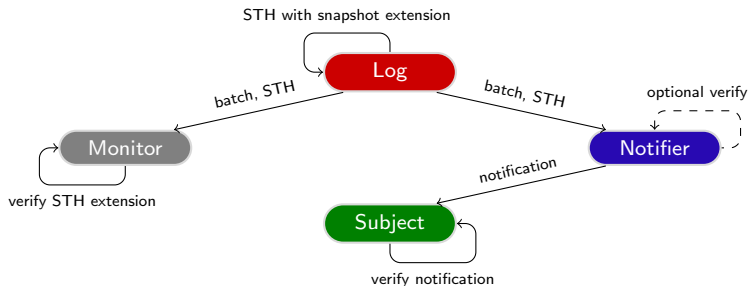


- 😊 Ezpz
- ☹ Trusted 3rd party

- CT/bis backwards compatibility
- Piggy-back on gossip-audit model
- Self-monitor wildcards w/o full download
- Reduced 3rd party monitoring trust



An overview of light-weight monitoring

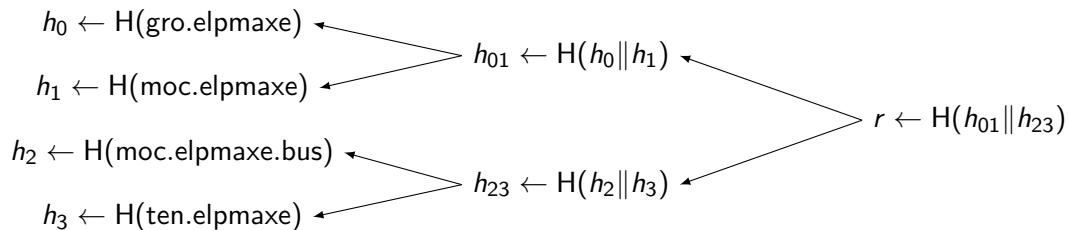


- A new Merkle tree for each batch

- Add snapshot to STH as extension

One wildcard (non-)membership notification per STH
How do you know if you got all notifications ➡ index extension

Wildcard notifications



■ Merkleize reverse-sorted list

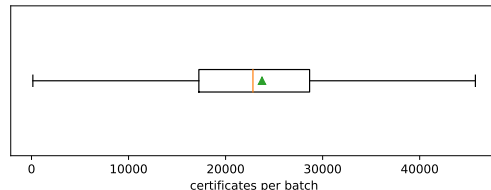
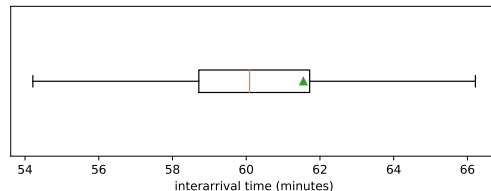
■ Wildcard proof \Rightarrow at most two audit paths

Security of this data structure? It is still just a Merkle tree...

- PoC: 351 lines of Go²
- Interesting metrics
 - ▶ Snapshot creation time
 - ▶ Proof generation time
 - ▶ Proof verification time
 - ▶ Bandwidth overhead
- Two log characteristics that matter
 - ▶ STH frequency
 - ▶ Batch size

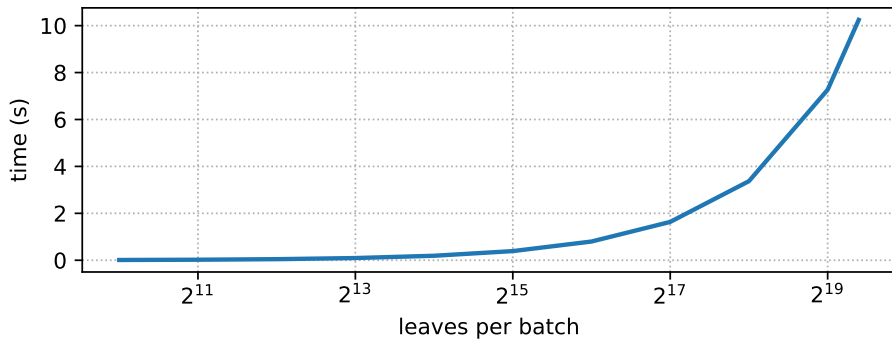
We observed all Chrome-included logs for eight months to determine these characteristics

Google's Icarus Log



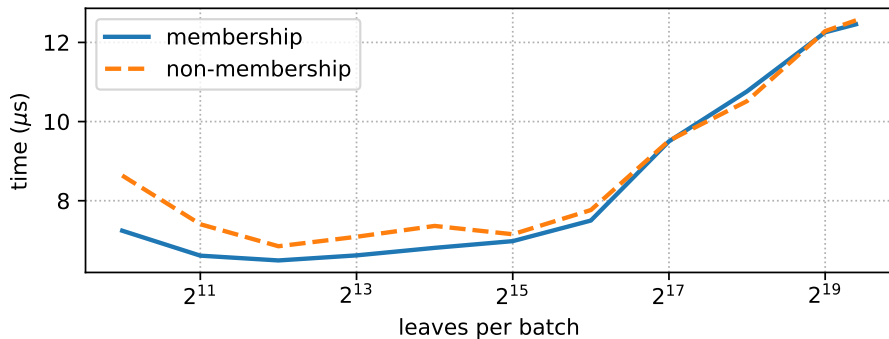
² <https://github.com/rgdd/lwm>

Snapshot creation time



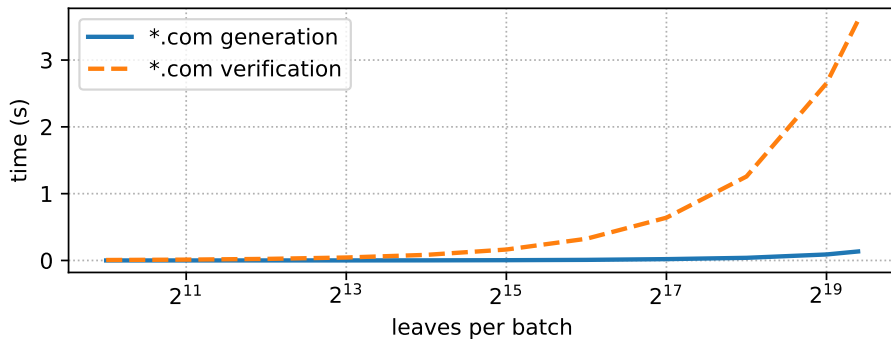
Negligible in comparison to STH issuance rate (1h)

Proof generation time



At least 288M non-membership proofs per hour on a single core

Proof generation and verification for *.com



352k matches in max batch ➡ 29k proofs per hour on a single core

Audit paths max batch size \Rightarrow 1 KB

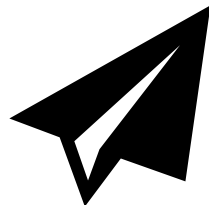
Self-monitor compare to median batch size of 32.6 MB

Notifier 288M audit paths per hour \Rightarrow 640 Mbps



<http://blog.coviam.com/wp-content/uploads/2016/07/Performance-Evaluation-Process-z.jpg>

- Unfortunate if CT monitoring relies on trusted parties
- Light-weight monitoring
 - ▶ One verifiable wildcard notification per batch
 - ▶ Untrusted notification component with push/pull model
 - ▶ Untrusted log \Rightarrow rely on one honest monitor
 - ▶ Trusted log \Rightarrow no need to also trust monitor



Any questions?

