TrInc: Small trusted hardware for large distributed systems

D. Levin, J. Douceur, J. Lorch and T. Moscibroda
Presented by Clint Sbisa

March 8, 2010

Introduction

- TrInc: Trusted incrementer
- Monotonic counter and a key
- Trusted Platform Module (TPM)

Background

- Equivocation
- Trusted hardware

Design

- Preventing equivocation
- API depends on internal state
- Trinkets (communicate over USB or other channel)

Design

- Private/public key and identity
- Attestations
- Certificates
- Checking attestations
- Counters (and metacounter)
- Queue of attestations

Analysis

- Equivocation
- Timeliness
- Minimality

Case study: A2M

- Trusted logs (append)
- Attestations for actions (appending, deleting, lookups)
- Decreased complexity

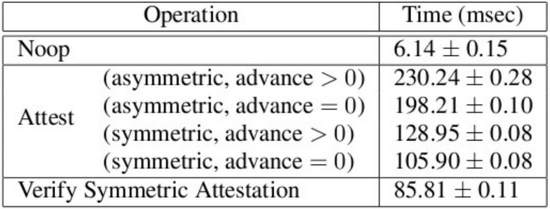
Case study: PeerReview

- Enabling accountability by using witnesses
- Interaction among witnesses
- Clear proof of misbehavior
- Challenge-response no longer needed, no witness-to-witness communication

Case study: BitTorrent

- Open incentives
- Under-reporting pieces to peers to obtain higher download
- Count number of pieces recieved

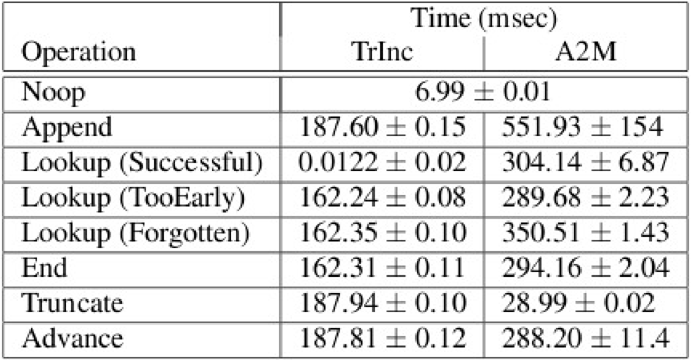
Implementation



Operation		Time (msec)
Noop		6.14 ± 0.15
Attest	(asymmetric, advance > 0)	230.24 ± 0.28
	(asymmetric, advance $= 0$)	198.21 ± 0.10
	(symmetric, advance > 0)	128.95 ± 0.08
	(symmetric, advance $= 0$)	105.90 ± 0.08
Verify Symmetric Attestation		85.81 ± 0.11

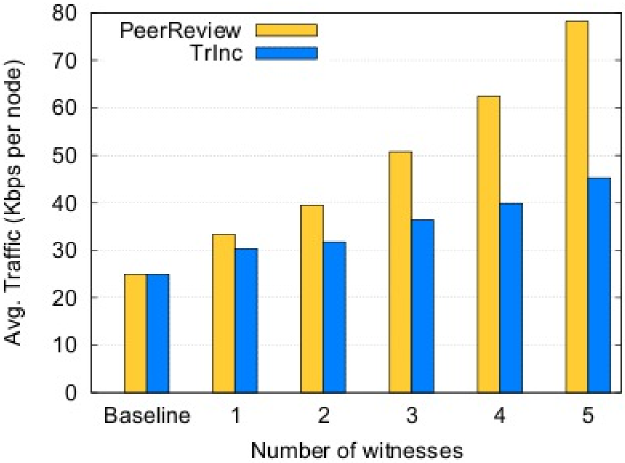
- Gemalto .NET SmartCards
- Slow!

Evaluation: A2M

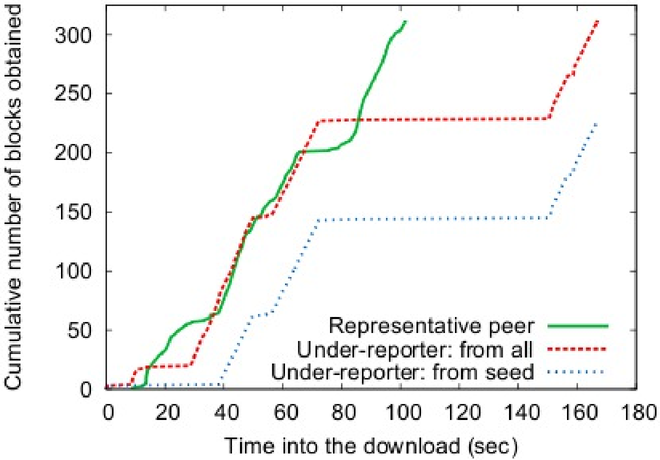


	Time (msec)	
Operation	TrInc	A2M
Noop	6.99 ± 0.01	
Append	187.60 ± 0.15	551.93 ± 154
Lookup (Successful)	0.0122 ± 0.02	304.14 ± 6.87
Lookup (TooEarly)	162.24 ± 0.08	289.68 ± 2.23
Lookup (Forgotten)	162.35 ± 0.10	350.51 ± 1.43
End	162.31 ± 0.11	294.16 ± 2.04
Truncate	187.94 ± 0.10	28.99 ± 0.02
Advance	187.81 ± 0.12	288.20 ± 11.4

Evaluation: PeerReview



Evaluation: BitTorrent



Conclusion

- Need for hardware
- Slow– not acceptable for some protocols
- Adoption