SAND2017-1113C

Locally Operated Cooperative Key Sharing

LOCKS

Michael Bierma, Aaron Brown, Troy DeLano,
Thomas M. Kroeger, Howard Poston

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2014-4080C

Background

Sandia National Laboratories

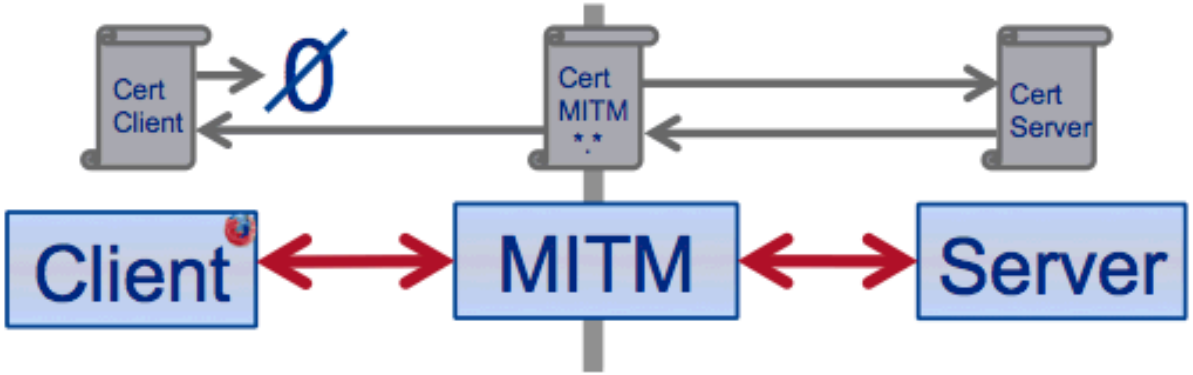
- Increase global TLS traffic 30-40x between 2012 and 2018
- Adversaries increasingly utilize encrypted protocols
- Challenge to network security monitoring
  - Web
  - Email

TLS

- 3 assurances
  - Integrity
  - Authenticity
  - Privacy
- Explain how the keys work

Existing Methods

- Man-in-the-middle



Existing Methods

- Endpoint monitoring
  - Pushing things to the edges

Existing Methods

Sandia National Laboratories

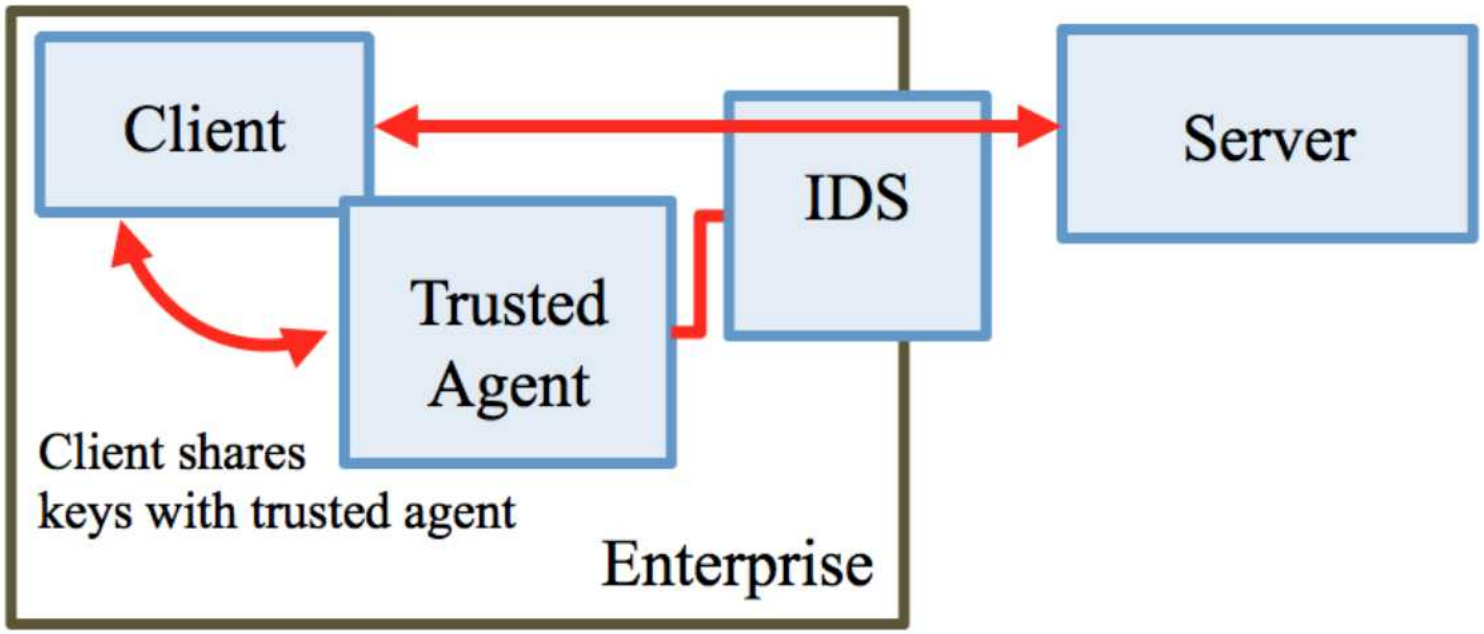
- Fixed keys
  - Moving away from this in TLS 1.3

Moving Forward

Sandia National Laboratories

- Goals
  - Enable enterprise-scale encrypted traffic DPI
  - No integrity compromise
  - No authentication compromise

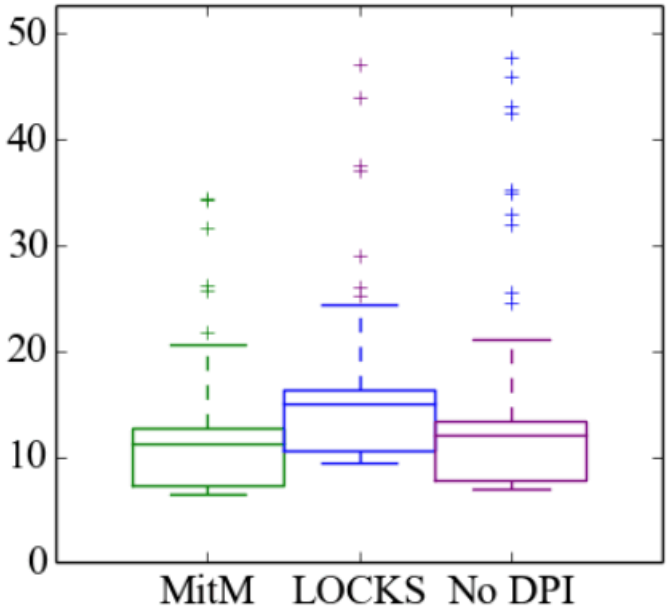
Architecture



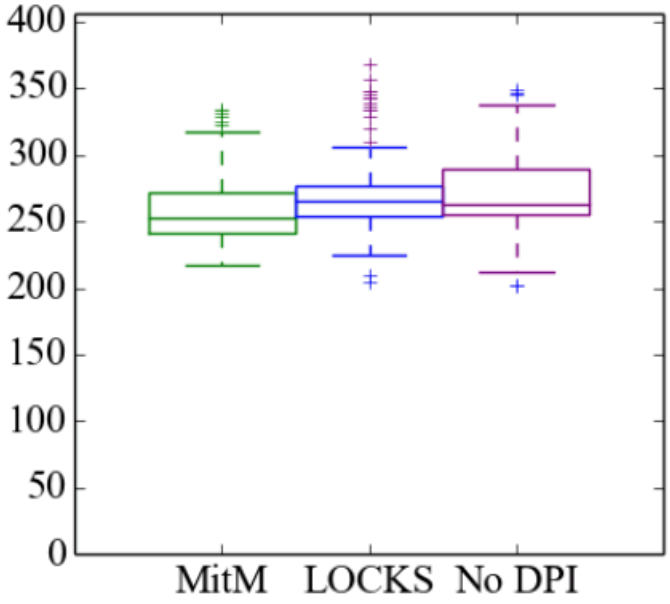
Benefits

- TLS operates as designed
- No need to manage root CA at boundary
- Users can control their keys
- Theoretic efficiency > MITM
- Allows for rich set of enterprise policies

Evaluation: Browser Latency

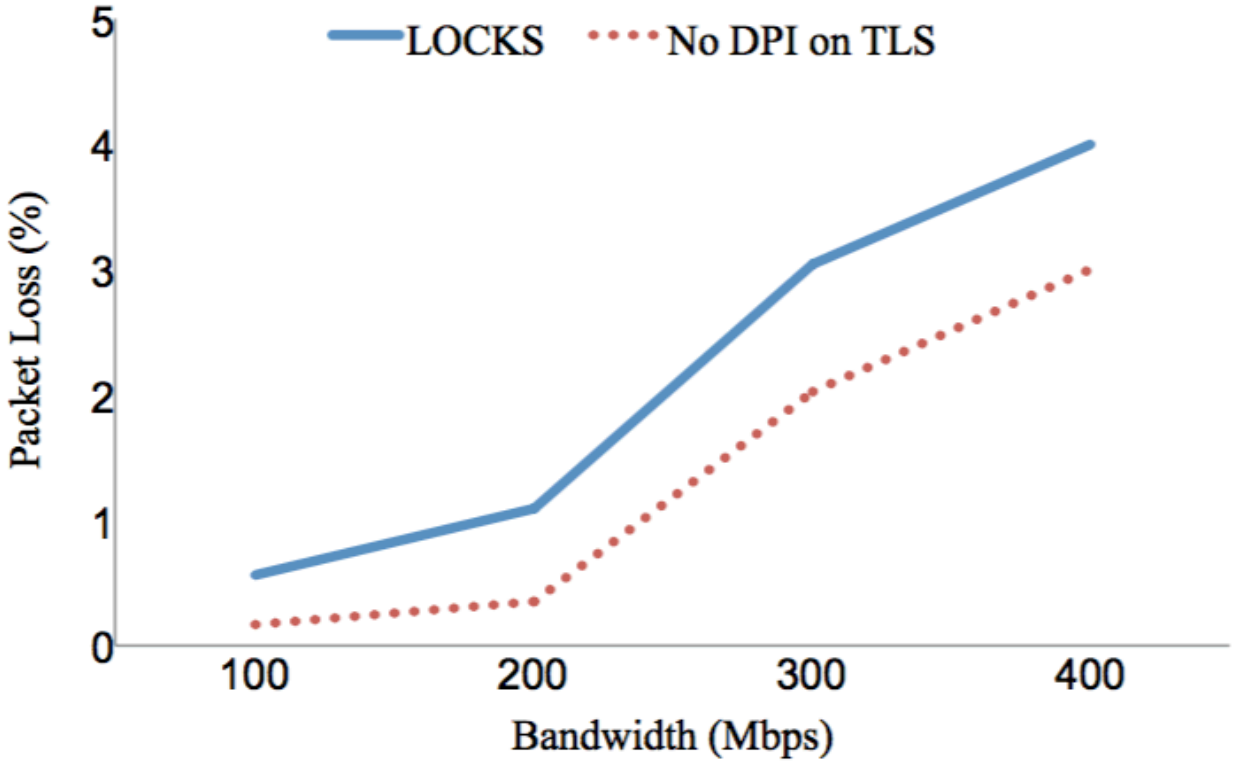


(a) 100KB files



(b) 10MB files

Evaluation: IDS Performance



Conclusion

Sandia National Laboratories

- Developed enterprise-scale DPI system for encrypted traffic
- Comparable performance to current solutions
- Provides rich set of enterprise policies
- **Doesn’t break TLS**

Questions

Sandia National Laboratories

References

Test Architecture