Making TLS an Operating System Service

ACSAC 2017 — Work in Progress
Daniel Zappala
Apps use TLS to negotiate secure connections
Who do you trust?

Certificate Authority system

- CAs have been hacked
- Governments own or can coerce CAs

Application developers

- Often get authentication wrong
Who should you trust?

System administrator or OS vendor

- In a position to configure software, enforce policies, apply patches
- You pay them — they have the right incentive
TrustBase

Imagine Certificate Transparency or OCSP automatically enforced for all apps on the system

- Platform for developing and installing numerous enhancements to the CA system
- Provides policy to determine how these are composed and required
- Policy and enhancements applied and enforced for all applications

See USENIX Security 2017 paper
Secure Socket API

int sock = socket(PF_INET, SOCK_STREAM, IPPROTO_TLS)
Secure Socket API

Application

TrustBase

Crypto Daemon

Userspace

Operating System

TLS Socket

TCP Socket

Kernel

Internet
Secure Socket API

---

Working

- server-side and client-side socket API

In progress

- sane defaults, admin configuration, setsockopt() for some developer configuration
owntrust.org

- Paper and code for TrustBase
- Paper and code for secure socket API coming