BYU
BRIGHAM YOUNG
UNIVERSITY

TrustBase

Principal Investigators: Kent Seamons and Daniel Zappala
Computer Science Department, BYU

An Architecture to Repair and Strengthen Certificate-based Authentication

Challenges

•Applications often do not properly validate the server’s certificate

•The CA system is vulnerable to being hijacked even when applications are implemented correctly

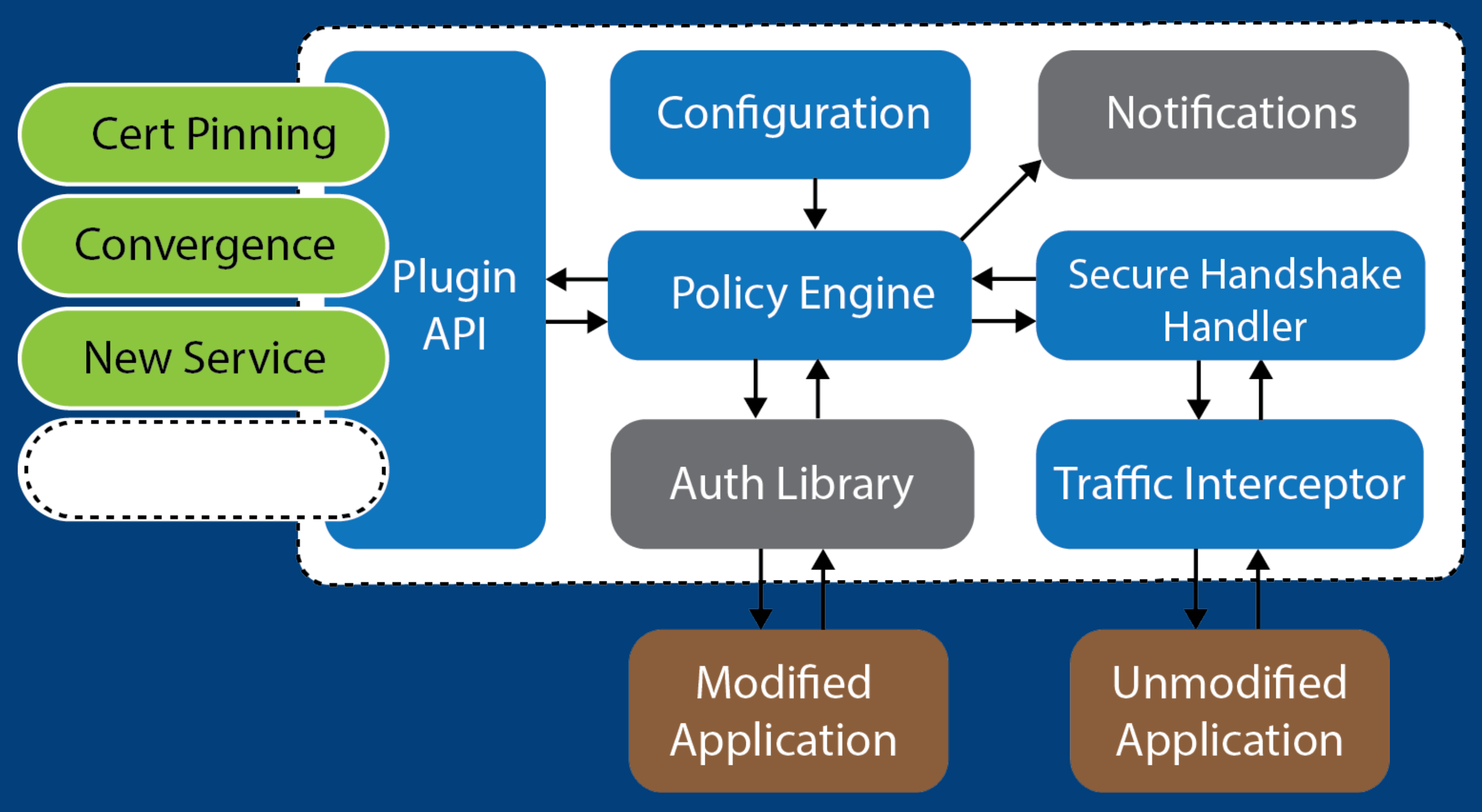
•Improvements to the CA system have difficulty being widely deployed and tested (Certificate Transparency, Notaries, Pinning, Revocation, etc.)

Solution

•Certificate validation as an operating system service

•Pluggable platform to research, develop, deploy certificate validation alternatives

TrustBase Overview



Cert Pinning
Convergence
New Service
Plugin API
Configuration
Notifications
Policy Engine
Secure Handshake Handler
Auth Library
Traffic Interceptor
Modified Application
Unmodified Application

TrustBase intercepts TLS handshakes for all existing applications without modification. Modified apps have the option to call TrustBase directly for certificate validation.

Approach: Certificate authentication as an operating system service

Overview

- Secure existing applications
- Strengthen the CA system
- Provide platform for research, development, and deployment of alternative authentication systems
- Validation is complicated, and too much evidence shows that developers make mistakes

Concentrating security in the OS

- Administrator is in control, can enforce validation on all apps, can choose policy among a variety of authentication services
- Risk: vulnerabilities affect all applications, can lead to MitM attacks
- Benefit: community effort focused on one correct implementation, errors likely to be patched more quickly than one broken app

Deployment and Performance Goals

- Full application coverage (all apps)
- Universal deployment (all operating systems)
- Negligible performance overhead
- Research platform for experimentation
- Proper and full certificate validation using OpenSSL

Preprint Available: https://arxiv.org/abs/1610.08570

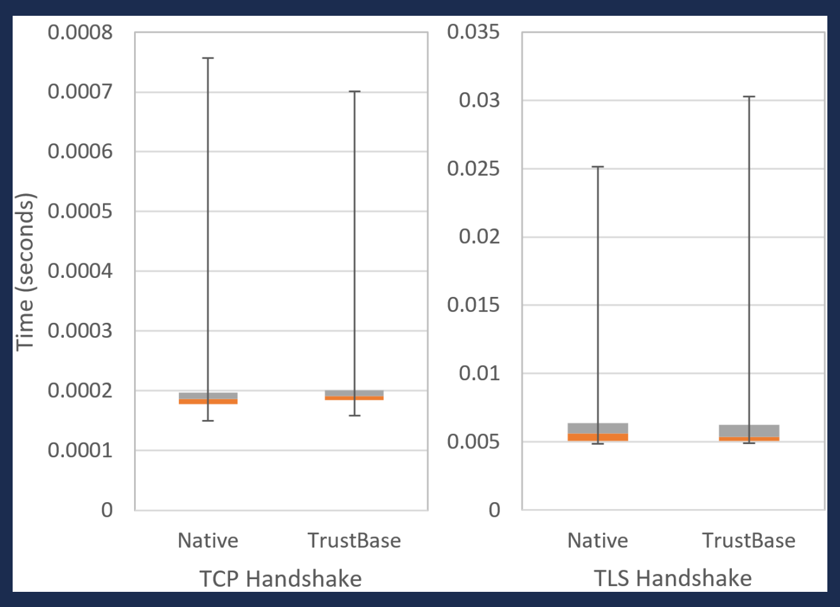
Alternatives to CA System

We have built the following plug-ins for TrustBase

- Whitelisting
- Certificate Pinning
- Certificate Revocation / OSCP
- DANE
- Notaries (Convergence-based)

Performance

- Only 212 bytes of memory overhead per connection (plus observed handshake data)
- No memory or time overhead after validation
- Negligible timing overhead for both TCP and TLS handshakes (see chart on right)
- Non-TLS connections unaffected



Handshake Timings

Coverage

- 100% coverage of SSL/TLS using local applications
- Thwart remote TLS MitM attackers
- Thwart local TLS MitM attackers
  - Local malware is the most prominent TLS MitM offender [O’Neill et al. IMC 2016]
- Provides STARTTLS pinning for implicit TLS
- Additional context for plugins allow exotic new authentication strategies
- Compatible with TLS inspection firewalls

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
Jan. 9 -11th 2017 Arlington, VA