PS4CT: Provable Security for Certificate Transparency

zorawar '20 | Advisor: Dr. Chris Armen
Department of Computer Science, Trinity College

Overview

- PS4CT is an automated, distributed system that builds on the CT Infrastructure to manage the lifecycle of HTTPS Certificates
- PS4CT *monitors* HTTPS certificates and *reports* bad certificates
- PS4CT offers the security protections of CT + proactive and provable security

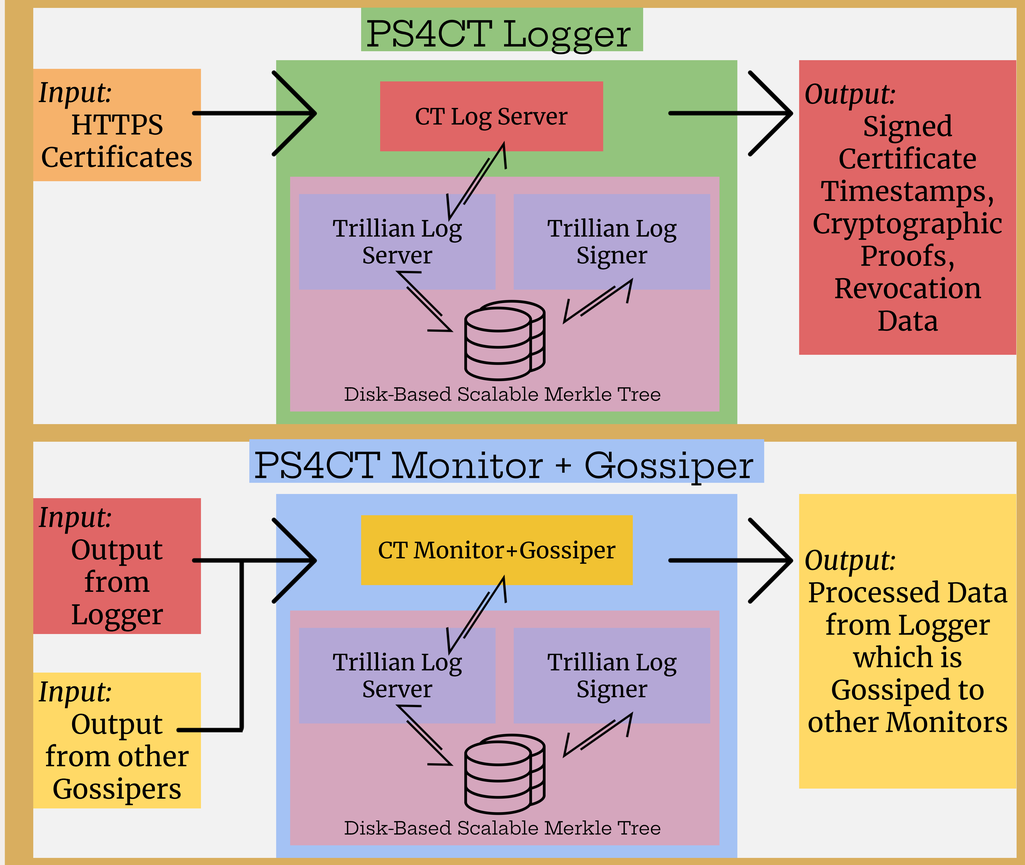
Motivation

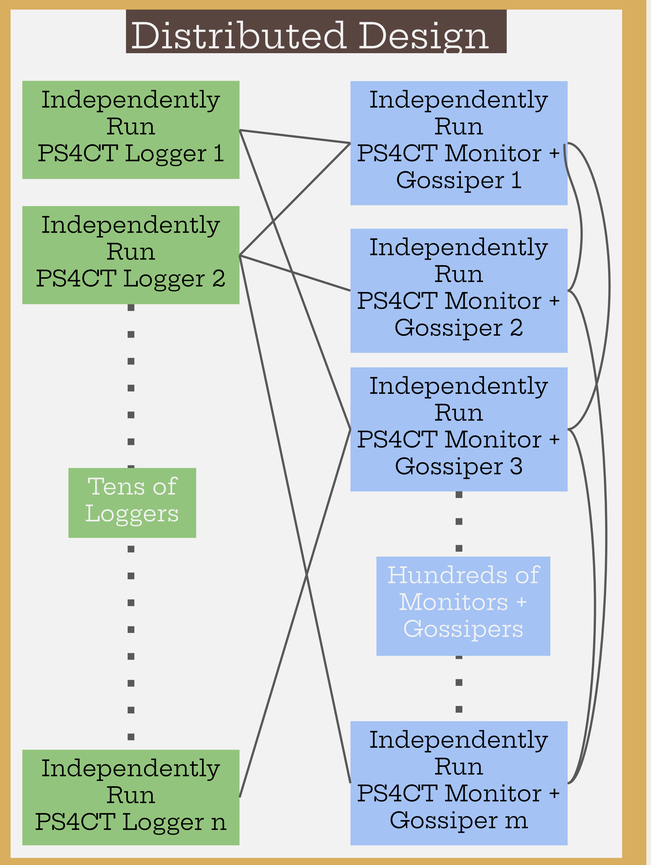
- Public-Key Infrastructure (PKI) is critical for secure internet communications but is broken.
- Google developed CT to solve part of the PKI problem with a Trusted-Third Party (TTP) requirement
- PS4CT seeks to eliminate the TTP requirement with provable security

Technologies Used

- Written in Go
- Containerized with docker
- Integration Testing on The DETER Project
- Deployed to WWW with Azure
- Additionally:
  Google CT+Trillian, Google Protobuf, Travis CI, GitHub/git, MySQL, bash

Features





Further Work

- Disseminating Certificate Revocation data
- Verifying Cryptography Implementation
- Thorough testing of Log Misbehavior
- Opening a PR with Google's CT repository

Acknowledgements

This extension to CT was implemented based on research produced by Dr. Ewa Syta (TrinColl), Dr. Amir Herzberg (UConn), and Hemi Leibowitz (Bar-Ilan Uni.) and included some development work by Jeremy Bennet (UConn).

Winner of the 2020 Travelers Foundation Senior Research Prize