Stan (Tristan) Gurtler

tmgurtler@protonmail.com | tmgurtler.com | LinkedIn: tmgurtler | GitHub: tmgurtler

education

M.Math. (2021)
Computer Science
(Cryptography, Security, and Privacy)
University of Waterloo

B.S. (2018)
Computer Science
University of Illinois at Urbana-Champaign
Bronze Tablet

technologies

Ansible • Docker
SAML • OAuth • SQL

other skills

Communication
Collaboration
Accountability

areas of expertise

Java, C/C++, Applied Cryptography, Python, Information Security and Privacy, JavaScript, Linux System Administration, S/MIME, Software and Image Signing

experience

Software Engineer, Cisco Systems
May 2022 – ongoing. Collaboratively developed and maintained custom Java applications supporting various public key infrastructure projects within the company. Planned and executed implementation of new features, administered Linux servers, analyzed and brought service into compliance with evolving company security requirements, communicated and resolved technical issues with external vendor, and led customer support for service providing S/MIME certificates for company employees. Enabled SAML and OAuth authentication across team's applications. Modernized logging and secrets management to enable containerization of applications.

Research and Teaching Assistant, University of Waterloo
September 2018 – December 2021. Designed, implemented, and benchmarked system for managing reputation privately in tight-knit community settings (published in WPES 2022; c.f. PRSONA project, below). Reviewed and systematized previous work on privacy in reputation (published in PETS 2021). Designed and engineered experiments for research on use of private information retrieval with distributed hash tables (published in WPES 2021). Assisted with teaching of Computer Security and Privacy course.

projects

CryptoID *not available for external review*
Subject matter expert on team for the service, responsible for all development and operations. Optimized, maintained, and added features to existing codebase for the management and issuance of strong cryptographic tokens and certificates. The service allows users to obtain publicly-trusted S/MIME certificates (used for encrypted and signed email) as well as other RSA certificates signed by a company-internal chain (used for strong authentication). Worked with publicly-trusted S/MIME vendor to enable RSA4K S/MIME certificates. Added ability for service to interact with Hardware Security Modules (HSMs) to obtain random values with strong entropy. Responsible for compliance with company security requirements.

SoftWare and IMage Signing Service (SWIMS) *not available for external review*
Worked with multiple engineers to enhance features of service. The service manages cryptographic keys for every engineering team in company to perform required software and image signing. Implemented OAuth authentication. Integrated with company-wide user lifecycle management systems. Enabled NIST-compliant post-quantum signatures.

Private Reputation Supporting Ongoing Network Avatars (PRSONA) git-crysp.uwaterloo.ca/tmgurtler/PRSONA
Designed a novel system for managing reputation privately in tight-knit community settings. The system uses well-established cryptographic primitives (the ElGamal and BGN cryptosystems) and trust distributed across provider servers (using verifiable shuffle) to empower users to privately give feedback on the conduct of other members of a community. Implemented and benchmarked the system to confirm the system's real-world viability. Further information can be found in publication below.

selected publications

PRSONA: Private Reputation Supporting Ongoing Network Avatars doi.org/10.1145/3559613.3563197
Stan Gurtler and Ian Goldberg. PRSONA: Private reputation supporting ongoing network avatars. *Proceedings of the 21st Workshop on Privacy in the Electronic Society*, 55–68, 2022.

SoK: Privacy-Preserving Reputation Systems doi.org/10.2478/popets-2021-0007
Stan Gurtler and Ian Goldberg. SoK: Privacy-preserving reputation systems. *Proceedings on Privacy Enhancing Technologies*, 2021(1):107–127, 2021.