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

Kubernetes • Docker
SAML • OAuth • SQL
Linux • Git • SCIM

other skills

Communication
Collaboration
Accountability

areas of expertise

Java, C/C++, Applied Cryptography, Python, Information Security and Privacy, JavaScript, Linux System Administration

experience

Software Engineer, Cisco Systems
May 2022 – ongoing. Developed and maintained custom Java applications supporting various public key infrastructure projects within the company. Enabled SAML and OAuth authentication across team's applications by developing for common internal library. Implemented SAML and OAuth using internal library in multiple applications. Modernized common logging code to enable containerization of applications. Designed and implemented System for Cross-domain Identity Management (SCIM) API for integration with partner team to manage group membership within applications. Refactored existing codebase to improve long-term maintainability as part of application modernization effort. Performed regular patching and other system administration tasks.

Research and Teaching Assistant, University of Waterloo
September 2018 – December 2021. Designed, implemented, and benchmarked novel system for managing reputation privately in tight-knit community settings (published in WPES 2023; 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 (or "Bring Your Own Token") *not available for external review*
Optimized, maintained, and added features to existing codebase for the management and issuance of strong cryptographic tokens and certificates. The system allows users to obtain S/MIME certificates (used for encrypted and signed email) and document signing certificates, which are typically used as a form of strong authentication and for mutual TLS. Added ability for service to interact with Hardware Security Modules (HSMs) to obtain random values with strong entropy. Optimized loading reports for administrators. Supported service directly for internal customers. Responsible for regular patching and other system administration tasks for the service.

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 straightforward cryptographic primitives (namely, the ElGamal cryptosystem and a prime-order instantiation of the BGN cryptosystem) and distributed trust across provider servers (using verifiable shuffle) to empower users to give feedback on the conduct of other members of a community while upholding four key privacy properties. Implemented and benchmarked this system, including all relevant non-interactive zero-knowledge proofs (NIZKs), to confirm the system's real-world viability. Further detail can be found here: uwspace.uwaterloo.ca/handle/10012/17747.

publications

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.

Do You Feel a Chill? Using PIR against Chilling Effects for Censorship-resistant Publishing doi.org/10.1145/3463676.3485612
Miti Mazmudar, Stan Gurtler, and Ian Goldberg. Do you feel a chill? Using PIR against chilling effects for censorship-resistant publishing. *Proceedings of the 20th Workshop on Privacy in the Electronic Society*, 53–57, 2021.