

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
LINCOLN LABORATORY

244 WOOD STREET
LEXINGTON, MASSACHUSETTS 02420-9108

14 April 2026

Area Code 781
981-4113

Dear Selection Committee,

I am pleased to nominate the paper “Rethinking Trust in Forge-Based Git Security” published in the Proceeding of the 2025 Network and Distributed Systems Security (NDSS’25) Symposium for the NSA’s Best Scientific Cybersecurity Paper competition. This work represents a significant and rare contribution that clearly aligns with the principles of Security Science as defined by NSA, advancing not merely security practice but the foundational understanding of trust, verifiability, and system integrity in modern software supply chains.

At its core, the paper identifies a fundamental limitation in today’s software development ecosystem: the reliance on non-verifiable trusted third parties (Git forges) for enforcing repository security. It rigorously analyzes this model and demonstrates that current systems lack the ability to prove integrity, creating inherent and systemic vulnerabilities. This framing moves beyond incremental security improvements and instead articulates a generalizable scientific problem: how to design systems whose security properties are independently verifiable and not reliant on centralized trust assumptions.

The authors respond with gittuf, a principled system that introduces a new, formalizable model of decentralized security for version control systems. The contribution is not simply a new mechanism, but a coherent framework grounded in verifiable properties, including:

- Decentralized policy declaration with threshold-based consensus,
- Cryptographically verifiable, append-only global state (the Reference State Log),
- Independent, universal policy verification by all participants.

These elements collectively establish provable security guarantees about repository integrity even under compromise of critical components such as the forge or privileged users. Importantly, the system provides a basis for reasoning about system behavior under adversarial conditions, including explicit threat models (policy tampering, log manipulation, enforcement bypass) and demonstrable resilience to each. This directly satisfies the Security Science objective of enabling prediction and analysis of system behavior under attack.

The paper’s contributions extend beyond a single system or domain. It articulates generalizable principles for trustworthy system design, including:

- Eliminating single points of trust through distributed verification,
- Enforcing separation of duties via threshold cryptography,
- Embedding transparency and auditability into system state itself.

These principles are broadly applicable across distributed systems, supply chain security, and beyond, thus transcending specific implementations, a key requirement of Security Science.

Equally important, the work includes rigorous empirical validation. The authors demonstrate that the proposed framework:

- Protects against a range of real-world attacks drawn from historical incidents,
- Introduces minimal overhead (under 4% storage and sub-second verification latency),
- Scales to large, real-world repositories such as Git and Kubernetes.

This combination of formal reasoning, system design, and quantitative evaluation exemplifies the integration of theory and practice expected of scientific contributions.

Finally, the work contributes to a unifying scientific framework for software supply chain security, bridging cryptographic trust models, distributed systems, and human operational workflows. It advances the field toward measurable, composable, and verifiable security guarantees, rather than ad hoc defenses or isolated mechanisms.

In summary, this paper exemplifies Security Science by defining fundamental limits and assumptions in current systems, introducing verifiable, generalizable constructs and models, enabling prediction and principled system design, and demonstrating measurable and scalable impact.

For these reasons, I strongly recommend this paper for the NSA Best Scientific Cybersecurity Paper award.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Hamed Okhravi', with a stylized flourish at the end.

Hamed Okhravi, Ph.D.
NDSS'25 Program Co-Chair
Senior Staff
MIT Lincoln Laboratory