Stony Brook University

COLLEGE OF ENGINEERING AND APPLIED SCIENCES
Department of Computer Science
Stony Brook, NY 11794-2424

P 631.632.8426
E amir@cs.stonybrook.edu
https://amir.rahmati.com

Best Scientific Cybersecurity Paper Competition Committee,

Delegated authorization protocols like OAuth are the cornerstone to enable communications between critical cloud services and operate on sensitive user data. However, such interaction relies on rudimentary bearer credentials that cannot precisely govern data sharing. This limitation is increasingly dangerous in today's computing landscape, where autonomous AI agents are increasingly deployed to act on behalf of users, performing daily tasks such as reading emails, scheduling meetings, or retrieving financial data.

This paper introduces StatefulAuth, a groundbreaking authorization framework that fundamentally reimagines how cloud services enforce the principle of least privilege. The scientific contribution of this paper lies in identifying and addressing two foundational limitations of bearer-token-based systems:
(1) Server-side permission, which restricts the client applications to pre-specify their required privilege level, and
(2) Statelessness, which prevents authorization decisions from accounting for the history of data access. These limitations result in significant overprivilege and open avenues for abuse if tokens are leaked or misused.

To address these gaps, StatefulAuth pioneers the idea of stateful, client-defined authorization. It introduces two core abstractions: (1) Client-side permissions, which allow client application developers to provide an attenuation policy that further restricts a token's privilege beyond scopes pre-defined by the server; (2) Statefulness, which enables authorization decisions to depend on historical context, allowing policies to reflect how and when resources have been accessed over time. For example, in a GPT-powered trip planner that reads confirmation emails, StatefulAuth can enforce a read-at-most-once policy to ensure that emails already processed cannot be re-read, even if a token is compromised. This achieves a form of ``forward secrecy'', which is rarely seen in existing authorization systems.

The authors build their system atop real-world platforms and demonstrate that StatefulAuth can enforce powerful new security policies without disrupting application functionality. They go beyond theoretical contributions, offering a concrete, deployable framework that enhances both security and developer expressiveness.

As we enter the era of agentic computing, where AI agents autonomously operate complex workflows involving human data, the need for precise and guaranteed privilege boundaries becomes urgent. Existing techniques, including Macaroons and OAuth-RAR, acknowledge the need for constraints but still depend on the server to anticipate and support them. StatefulAuth breaks this mold by empowering clients to express their exact intent and enabling cloud services to enforce it during runtime.

This work is deeply impactful and timely. It not only advances the state of the art in cloud authorization, but also lays a principled foundation for securing the next generation of AI-driven systems. The ideas introduced in StatefulAuth are likely to influence both academic research and practical deployments in the years ahead.

For these reasons, I nominate this paper for the Best Scientific Cybersecurity Paper Competition and believe it exemplifies the type of innovative, high-impact cybersecurity research that this award seeks to recognize.

Best Regards,

Rahmati

Amir Rahmati

FAR BEYOND