accAAD: An Efficient Append-Only Authenticated Dictionary for Transparent Public Logs

Bhupatiraju, Vivek (School: Lexington High School)

Clients using public logs should be able to securely verify that data in the log has not been maliciously changed or removed by the log’s server. Unfortunately, this verification in existing logs is generally computation efficient for the server but bandwidth inefficient for the clients. As client-side bandwidth is far more expensive than server-side computation, this project centered around designing a bandwidth efficient public log. We first introduce a novel cryptographic primitive called an append-only authenticated dictionary (AAD), which formalizes this notion of a transparent public log. An AAD is managed by an untrusted server, and is audited by clients to make sure it maintains the append-only property: each key's value is set once and is never changed or removed. To prove this, the server computes cryptographic proofs that the client can verify. We then introduce accAAD, an efficient AAD based on bilinear accumulators. Using novel amortization and hash prefix tricks, all of accAAD’s cryptographic proofs are polylogarithmic in both computation and bandwidth, a significant improvement over previous work. This exceptional performance indicates accAAD is ready for implementation in important public logs, including secure public-key directories, certificate authorities, and software transparency schemes. This would improve efficiency of the logs and greatly reduce costs for clients.

Awards Won:

Association for Computing Machinery: Third Award of $1,500

National Security Agency Research Directorate : First Place Award "Science of Security" of $3,000