Poster: Beyond Classical Security: Solutions for Modern Secure Societies

Reyhane Falanji, Niklas Carlsson, Mikael Asplund

May 24, 2026

Abstract

Our societies have evolved drastically over the past century and have become increasingly intertwined with technology. Yet, the security primitives used to secure modern digital systems were largely designed around 40 years ago. Despite their sound foundations and the improvements made over the years, these primitives sometimes fall short of addressing the needs of modern societies, particularly those arising from increasingly complex systems that are continuously designed and deployed. Furthermore, these primitives were originally developed with military objectives in mind, prioritizing rigorous security guarantees while not necessarily adapting to broader societal and human-centered requirements. Finally, attempts to force existing primitives into modern security solutions have introduced substantial avoidable complexity and overhead without fully delivering the properties that contemporary systems truly require.

In our research, we explore ways of incorporating alternative cryptographic primitives into existing systems to provide solutions that better match the requirements of the systems under study. As one avenue of exploration, we investigate DNS systems, and in particular DNSSEC negative responses. Currently, generating authenticated negative responses in DNS is both computationally and communication-wise costly. Reliance on conventional signatures has resulted in responses that are both excessively large and vulnerable to additional security concerns, such as revealing the entire zone through what is known as a zone enumeration attack. We take a fundamentally different approach to this problem. By using primitives that enable direct proofs of non-membership, we are able to improve both the security and efficiency of DNS negative responses.

In another line of work, we introduce a mechanism for on-the-fly modification of authenticated signed messages by a designated modifier, without requiring interaction with the original signer. This reduces the need for repeated back-and-forth communication with the signer, an assumption that is often unrealistic in highly dynamic environments such as vehicular networks.

Such changes, however, naturally introduce new challenges. To better understand these challenges, we study and analyze the modifications required for existing systems in order to facilitate the adaptation process. Furthermore, we investigate the accountability implications of deploying such solutions in vehicular networks and similar systems, and formally prove the guarantees that can be achieved. In addition, we introduce the notion of evidence-based accountability as an alternative to continuous monitoring, thereby establishing a foundation for reducing monitoring requirements while still preserving accountability guarantees. This notion enables systems to support richer and more flexible functionality while maintaining accountability properties, ultimately providing all participating entities — including human citizens — with a safer and more trustworthy platform from which to benefit.