Title: Formal Security Analysis: Authentication, Attestation and Beyond

Abstract:

Nowadays, trustworthy communications are needed in the cyber systems. In order to provide the security, various security protocols are developed. However, designing security protocol is challenging and error-prone, which is well illustrated by many attacks found in the security protocols. Hence, it is necessary to provide a verification framework where the security protocols can be formally checked.

In our first work, we analyze a complex vehicle charging protocol to show the strengths and weaknesses of existing verification methods. Many interesting properties are analyzed such as secrecy, authentication and privacy. The analysis shows that manual modeling abstractions are generally needed to ensure the termination of the verification, making the protocol specification less intuitive and more laborious. Additionally, false alarms can be introduced when verification considers specific domain knowledge.

Then, in our second work, we propose a security protocol verification framework, where the security protocols can be intuitively specified and efficiently verified. Comparing with the existing methods, our verification method requires no abstraction during the verification and works for an unbounded number of protocol sessions. Our research shows that this framework can be applied to specific domains, e.g., the timed domain, easily. The correctness of our verification algorithm has been formally proved. We implement our method into a tool and use it to verify many timed and untimed security protocols successfully.

Security protocols in real-world use not only cryptography primitives but also physical properties. Hence, we investigate a family of software-based attestation protocols that are in this category so as to provide an analysis approach for them. These attestation protocols, comparing with traditional hardware-based (e.g., TPM-based) attestation protocols, do not require any hardware support in the attestation. Instead, their security are provided by the computation limitation of the target devices. We analyze these protocols in three stages.
First, we propose a generic specification for them that captures most existing software-based attestation protocols. Then, we formalize various security criteria that should be satisfied by the generic scheme. Finally, we apply the security criteria back to the existing software-based attestation protocols. Using this approach, we find several security flaws successfully.