Security Models for Protocols with Protocol-Unaware Principals

Thomas Groß
IBM Zurich Research Lab, Rüschlikon, Switzerland
tgr@zurich.ibm.com

Klaus Kursawe
Katholieke Universiteit Leuven, Belgium
klaus.kursawe@esat.kuleuven.ac.be

Ahmad-Reza Sadeghi
Ruhr-University Bochum, Germany
sadeghi@crypto.rub.de

Justification

In security/cryptographic protocols the principals involved are assumed to precisely behave according to the protocol specifications, unless they are corrupted. This holds also for all the security models, analysis methods and proofs, proposed in the literature so far. We call such principals *protocol-aware*. However, the existing literature does not cover the case where one or more principals have no information about the protocol they are involved in. We call such principals *protocol-unaware*. Basically, these principals have own behavior that is independent of the protocol they take part in: this means they may react only to a set of predefined messages, may process and store security-critical information in potentially insecure places, and may need the assistance of other principals to access certain information (e.g., login information). Hence, they are a potential security risk for the surrounding protocol. We call this new paradigm *protocol unawareness*.

Prominent applications which our new paradigm of *protocol unawareness* covers are web-based applications. These applications have become very attractive to industry and into the focus of research. The main motivation of web-based applications is the low cost and the ease of use without expecting specific knowledge from users. Hence, users are provided with browsers that have only some basic capabilities. The browsers in these applications do not require the installation of any special client software. Hence, they are called *zero-footprint*. Further, also the corresponding security services must be zero-footprint, i.e., only a browser is used for user authentication, and additional security relevant attributes about the user are requested from a third party and transmitted through a secure channel. A concrete example of browser-based security protocols is identity federation, which aims at linking a user's (otherwise) distinct identities at several locations.

Our new paradigm arises from the reason that a protocol-unaware principal, such as standard browsers, sticks to its own, predefined behavior which can have crucial impact on the security of the protocol it is participating in: a standard browser reacts on a set of predefined messages (HTTP messages), adds information to responses *automatically*, and stores certain information such as histories in places which cannot always be assumed to be secure, e.g., in an Internet kiosk at airport. Standard browsers simply do not execute most of the established security protocols for key exchange, authentication, etc. The only exception is 2-party authentication through establishing SSL or TLS channels where the browser has a client-certificate on its own. However, this is not considered truly zero-footprint, as users have to obtain a client-certificate for their browser. Moreover, users may not easily use different browsers at different times (e.g., in a kiosk scenario). Indeed, these aspects of a standard browser, reflecting its protocol-unawareness, made concrete real world attacks on single sign-on protocols possible, e.g., on SAML (Security Assertion Markup Language).

Hence browser-based protocols are different from all protocols for which prior security proofs exist. Moreover, existing security proof techniques, both cryptographic techniques and formal-methods techniques, are not trivially applicable to protocols with protocol-unaware principals such as browser-based protocols.

Our main goal in this paper is to discuss the paradigm of security protocols with protocol-unaware principals, and to present methods, principles, and a systematic approach to practitioners to model and analyze security protocols with unawareness property in the practice. For this we focus on solutions for a widespread class of real world applications, here browser-based protocols, and discuss models for browsers as protocol-unaware principal. Due to lack of space, however, we restrict our consideration to an introduction.

NSPW offers a well-established platform and a good opportunity to discuss our ideas in more details with other researchers.

Attendance

One or two authors wish to attend the workshop.