Strengthening the security of key exchange protocols

Diss. ETH No. 21970

Strengthening the Security of Key Exchange Protocols

A thesis submitted to attain the degree of
Doctor of Sciences of ETH Zurich
(Dr. sc. ETH Zurich)

presented by
Michèle Feltz
MSc in Mathematics, University of Fribourg
born on August 4, 1986
citizen of Luxembourg

accepted on the recommendation of
Prof. Dr. David Basin, examiner
Prof. Dr. Cas Cremers, co-examiner
Prof. Dr. Marc Fischlin, co-examiner

2014

Abstract

Authenticated key exchange (AKE) protocols are central building blocks of security protocols such as TLS, IPsec, and SSH, that are used in modern distributed applications. The security of these protocols can however be affected by threats such as attacks on users' long-term secret keys, attacks based on malicious key registration, and attacks on the random number generator used by the protocol. The goal of this thesis is to model advanced security threats against authenticated key exchange protocols and to develop methods that strengthen the security of these protocols and make them secure against the considered threats.

In the first part of this thesis we extend existing security models to capture relevant attacks that lie outside the scope of these models. We advance the state-of-the-art by integrating perfect forward secrecy into a model that captures key compromise impersonation attacks and the leakage of session-specific randomness. We provide a generic security-strengthening transformation to achieve perfect forward secrecy, and show that two-message AKE protocols can achieve security in our model by applying our transformation to protocols that are secure in weaker models. Most security models for authenticated key exchange do not explicitly model the associated certification system, which includes the certification authority and its behaviour. We launch the first systematic analysis of AKE incorporating certification systems. To this end, we develop a framework that allows for explicit modelling of the public key certification process; this framework enables us to capture attacks based on dynamic adversarial registration of arbitrary public keys. We are the first to provide a generic approach to achieve strong security guarantees against adversaries who can register arbitrary public keys with a certification authority that does not perform any verification on combinations of identities and public keys.

In the second part of this thesis we explore the limits of AKE security with regard to different protocol classes. We derive a hierarchy of strong security models from impossibility results on the security of each protocol class. Our impossibility results show the impossibility of achieving certain security guarantees in specific protocol classes. In particular, we analyze the security of protocols in the presence of adversaries who can perform attacks based on choosing the randomness used in protocol sessions. We construct novel variants of the NAXOS protocol, which achieve security against such attacks.

Résumé

Les protocoles d'échange de clé sont des éléments centraux de protocoles de sécurité tels que TLS, IPsec, et SSH, qui sont utilisés dans de nombreuses applications distribuées de commerce électronique. La sécurité de ces protocoles peut cependant être affectée par des menaces comme, par exemple, des attaques sur les clés secrètes à long terme, des attaques basées sur l'exploitation de certificats frauduleux émis par des autorités de certification, et des attaques sur le générateur de nombres aléatoires utilisé par le protocole. L'objectif de cette thèse consiste à modéliser des menaces avancées contre les protocoles d'échange de clé et de développer des méthodes qui renforcent la sécurité de ces protocoles et les immunisent contre les attaques considérées.

Dans la première partie de cette thèse, nous étendons des modèles de sécurité existants à des attaques qui ne peuvent actuellement pas être prises en compte par ces modèles. Nous intégrons la notion de "perfect forward secrecy" dans un modèle qui prend en compte des attaques sur la clé secrète à long terme de l'auteur de la session sous attaque et la fuite de valeurs aléatoires spécifiques à des sessions. Nous proposons une transformation générique qui permet d'assurer la propriété de "perfect forward secrecy", et montrons que les protocoles d'échange de clé à deux messages peuvent garantir la sécurité dans notre modèle en appliquant notre transformation à des protocoles qui sont sûrs dans des modèles plus faibles. La plupart des modèles de sécurité ne modélisent pas explicitement le système de certification associé, qui comprend l'autorité de certification et son comportement. Nous procédons à une analyse systématique de l'échange de clé tenant compte du système de certification. Pour cela, nous développons un système de référence qui prend en compte la modélisation explicite du processus de certification; ce système nous permet de saisir des attaques basées sur l'enregistrement dynamique de clés publiques arbitraires. À notre connaissance, nous sommes les premiers à proposer une approche générique afin d'atteindre des garanties de sécurité élevées face à des adversaires qui peuvent obtenir des certificats pour des clés publiques arbitraires de la part d'une autorité de certification qui n'effectue aucune vérification de combinaisons d'identités et de clés publiques.

Dans la seconde partie de cette thèse, nous explorons les limites de la sécurité de l'échange de clé par rapport à différentes catégories de protocoles. Nous dérivons une hiérarchie de modèles de sécurité de résultats d'impossibilité sur la sécurité de chaque catégorie. Nos résultats d'impossibilité montrent l'impossibilité d'atteindre certaines garanties de sécurité dans des catégories de protocoles spécifiques. En particulier, nous analysons la sécurité de protocoles en présence d'adversaires qui effectuent des attaques basées sur le choix de valeurs aléatoires utilisées dans des sessions. Nous construisons de nouvelles variantes du protocole NAXOS qui assurent la sécurité contre de telles attaques.

Zusammenfassung

Schlüsselaustauschprotokolle sind zentrale Komponenten von Sicherheitsprotokollen wie TLS, IPsec, und SSH, die in modernen verteilten Applikationen benutzt werden. Die Sicherheit dieser Protokolle kann jedoch durch diverse Gefahren beeinträchtigt werden, wie Angriffe auf die langfristigen geheimen Schlüssel von Teilnehmern, Angriffe, die auf der Ausstellung von Zertifikaten für beliebige Schlüssel des Angreifers basieren, und Angriffe auf den Zufallsgenerator der vom Protokoll benutzt wird. Ziel dieser Dissertation ist es, Gefahren für Schlüsselaustauschprotokolle zu modellieren und Methoden zu entwickeln, welche die Sicherheit dieser Protokolle verstärkt.

In dem ersten Teil dieser Dissertation erweitern wir existierende Sicherheitsmodelle um Angriffe zu modellieren, welche ausser Reichweite dieser Modelle liegen. Wir integrieren "perfect forward secrecy" in ein Modell, welches Angriffe auf die langfristigen geheimen Schlüssel von gewissen Teilnehmern vor dem Ende einer Sitzung sowie den Verlust von sitzungsspezifischen Zufallswerten modelliert. Wir schlagen eine generische sicherheitstärkende Transformation vor, die uns erlaubt, "perfect forward secrecy" zu garantieren. Wir zeigen, dass Schlüsselaustauschprotokolle mit nur zwei Nachrichten schon Sicherheit in unserem Modell erreichen können, indem wir unsere Transformation auf schwächere Protokolle anwenden. Die meisten Sicherheitsmodelle modellieren nicht das dazugehörige Zertifizierungssystem, welches die Zertifizierungsinstanz und deren Verhalten einschliesst. Wir starten die erste systematische Untersuchung von Schlüsselaustauschprotokollen unter Berücksichtigung von Zertifizierungssystemen. Zu diesem Zweck entwickeln wir ein System das explizites Modellieren des Zertifizierungsprozesses von öffentlichen Schlüsseln berücksichtigt. Dieses System erlaubt es uns Angriffe zu modellieren, die auf der dynamischen Registrierung von beliebigen öffentlichen Schlüsseln basieren. Unter der Annahme, dass die Zertifizierungsinstanz die Informationen, die in den Anfragen enthalten sind, wie Identität oder öffentlichen Schlüssel, nicht überprüft, führen wir eine generische Methode ein um starke Garantien zu erzielen gegen Angreifer, die Zertifikate über beliebige öffentliche Schlüssel verwenden, welche von dieser Zertifizierungsinstanz ausgestellt wurden.

In dem zweiten Teil dieser Dissertation erforschen wir die Grenzen des sicheren Schlüsselaustausches bezüglich verschiedener Protokollklassen. Aus unseren Unmöglichkeitsresultaten leiten wir eine Hierarchie von starken Sicherheitsmodellen ab. Im Speziellen untersuchen wir die Sicherheit von Protokollen gegen Angreifer die sitzungsspezifische Zufallswerte manipulieren können. Wir präsentieren neue Varianten des NAXOS Protokolls und beweisen deren Sicherheit gegen solche Angriffe.