Diss. ETH No. 20702

User-Centered Security Mechanisms for Protecting Information Sharing in the Cloud

A dissertation submitted to
ETH Zurich

for the degree of
Doctor of Sciences

presented by
Iulia Ion
M.Sc. in Computer Science, International University in Germany
born October 25, 1983
citizen of Romania

accepted on the recommendation of
Prof. Dr. Friedemann Mattern, examiner, ETH Zurich
Prof. Dr. Marc Langheinrich, co-examiner, University of Lugano
Prof. Dr. Srdjan Čapkun, co-examiner, ETH Zurich
Prof. Dr. Lujo Bauer, co-examiner, Carnegie Mellon University

2012

Abstract

End-users have become accustomed to the ease with which cloud-based systems allow them to exchange messages, pictures, and other files with colleagues, friends, and family. This convenience, however, typically comes at the expense of disclosing this (often highly personal) information to the service provider in the process. Furthermore, users have little control over which third-parties—e.g., storage providers, unauthorized friends, hackers, advertisement companies, and governmental agencies—access their data.

Several studies have identified security and privacy as the biggest concerns for companies when adopting cloud-based solutions, but not much is known about end-users' attitudes and practices. Given the high amount of personal information that users often disclose on such platforms, detractors claim that users care little or not at all about their privacy. To disprove such beliefs, we conducted an extensive cross-cultural study. Our results show that consumers have strong privacy concerns, trust local storage more than the cloud when storing sensitive data, and are only partially aware of the risks they face in the cloud.

Based on this initial study, we identify the need for novel, user-centered security mechanisms to help non-technical users protect the information they share in the cloud. A number of systems have been proposed to limit the service providers' access to this information, yet these systems typically require trusted servers, are platform specific (e.g., work for Facebook only), or fail to hide that confidential communication is taking place. In this thesis, we present a novel system that enables users to share data over any web-based cloud storage platform, while both protecting the confidentiality of the communicated data and hiding the fact that the exchanged data is confidential. We provide a proof-of-concept implementation of our system in the form of a publicly available Firefox plugin, and demonstrate the viability of our approach through a performance evaluation.

To bootstrap secure communications in systems like the one we propose, current solutions leave it as an exercise for the user to manually verify key material (e.g., public key fingerprints) through offline channels with potentially hundreds of online contacts. Instead, in our system, we take advantage of users' encounters and we verify keys automatically through a secure, direct connection between users' mobile devices. The usability of the device pairing protocol used to establish the secure connection is crucial, as overly complex mechanisms might prompt users to choose a lower security level, or lead them to abandon security altogether. To this end, we conducted a comparative usability study of existing device pairing methods. Unlike previous work, our study places pairing tasks in specific real-life situations. Our results disprove the commonly held belief that users always choose the easiest method. Instead, users prefer different methods in different situations, depending on their time constraints, relationship to the interacting partner, social conventions appropriate for the place, and perceived security needs and guarantees.

Kurzfassung

Benutzer haben sich an die Leichtigkeit gewöhnt, mit der Cloud-basierte Systeme es ermöglichen, Nachrichten, Bilder und andere Dateien mit Kollegen, Freunden oder der Familie auszutauschen. Allerdings geschieht diese Bequemlichkeit typischerweise auf Kosten der Bekanntgabe dieser (oft sehr persönlichen) Informationen gegenüber dem Dienstanbieter. Ausserdem haben Benutzer wenig Kontrolle darüber, welche Drittparteien—z. B. Speicheranbieter, unautorisierte Freunde, Hacker, Werbefirmen oder Regierungsbehörden—auf ihre Daten zugreifen.

Verschiedene Studien haben Sicherheit und Datenschutz bei der Einführung Cloud-basierter Lösungen als die größten Vorbehalte von Unternehmen eingeschätzt, jedoch ist wenig über das Verhalten und die Praktiken der Endbenutzer bekannt. Angesichts der grossen Menge an persönlichen Informationen, die Benutzer unbedarft auf solchen Plattformen ablegen, behaupten Kritiker, dass Benutzer sich nur wenig oder überhaupt nicht um ihre Privatsphäre kümmern. Um solche Annahmen zu prüfen, haben wir eine umfassende interkulturelle Studie durchgeführt. Unsere Ergebnisse zeigen, dass die Benutzer erhebliche Sorgen hinsichtlich ihrer Privatsphäre haben, sie der lokalen Speicherung mehr als der Cloud vertrauen um sensible Daten zu speichern, und sie nur teilweise die Risiken kennen, denen sie in der Cloud ausgesetzt sind.

Basierend auf dieser Studie identifizieren wir den Bedarf an neuen, benutzerfokussierten Sicherheitsmechanismen, um nichttechnische Anwender beim Schutz der Informationen, die sie in der Cloud teilen, zu unterstützen. Eine Reihe von Systemen ist in der Literatur vorgeschlagen worden, um den Zugang der Dienstanbieter zu diesen Informationen zu begrenzen, jedoch benötigen diese Systeme typischerweise vertrauenswürdige Server, sind plattform-spezifisch (z. B. funktionieren nur für Facebook) oder verbergen die vertrauliche Art der Kommunikation nicht. In dieser Arbeit stellen wir ein neues System vor, das es den Benutzern ermöglicht, Dateien über beliebige Web-basierte

Cloud-Speicherplattformen zu teilen und gleichzeitig die Vertraulichkeit der übermittelten Daten zu schützen und die vertrauliche Art der Kommunikation zu verschleiern. Wir liefern eine Proof-of-Concept-Implementierung unseres Systems in Form eines öffentlich zugänglichen Firefox-Plugins und demonstrieren die Machbarkeit unserer Lösung durch eine Leistungsevaluation.

Um sichere Kommunikation einzuleiten, verlangen aktuelle Lösungen von den Benutzern, Schlüsselmaterial (z. B. Public-Key-Fingerprints) über Offline-Kanäle für möglicherweise Hunderte von Online-Kontakten manuell zu verifizieren. Im Unterschied dazu nutzen wir in unserem System das physische Zusammentreffen von Nutzern, um Schlüssel automatisch über eine sichere, direkte Verbindung zwischen den Mobilgeräten der Nutzer zu überprüfen. Die Gebrauchstauglichkeit der verwendeten Methode zur Gewährleistung einer sicheren Verbindung ist von entscheidender Wichtigkeit, da komplexe Mechanismen Benutzer veranlassen können, eine niedrigere Sicherheitsstufe zu wählen oder die Sicherheit vollkommen aufzugeben. Zu diesem Zweck haben wir eine vergleichende Benutzbarkeitsstudie existierender Gerätepaarungs-Protokolle durchgeführt. Im Gegensatz zu früheren Studien platziert unsere Studie die Aufgaben in spezifische realitätsbezogene Situationen. Unsere Ergebnisse widerlegen die allgemein verbreitete Meinung, dass die Benutzer immer die einfachste Methode wählen. Stattdessen bevorzugen Anwender in verschiedenen Situationen unterschiedliche Methoden, abhängig von ihren zeitlichen Einschränkungen, der Beziehung zum interagierenden Partner, angemessenen gesellschaftlichen Konventionen bezogen auf den jeweiligen Ort sowie empfundenen Sicherheitsanforderungen und erwarteten Sicherheitsgarantien.