Secure end-to-end communication in remote internet voting

DISS. ETH NO. 23433

SECURE END-TO-END COMMUNICATION IN REMOTE INTERNET VOTING

A thesis submitted to attain the degree of

DOCTOR OF SCIENCES of ETH ZURICH

(Dr. sc. ETH Zurich)

presented by

MICHAEL SCHLÄPFER

MSc ETH CS

born on 03.08.1978

citizen of Wald AR and Basel BS

accepted on the recommendation of

Prof. Dr. D. Basin
Prof. Dr. S. Čapkun
Prof. Dr. C. Schürmann
Dr. S. Radomirović

2016

Abstract

Electronic communication becomes more and more important in our everyday life. We use various kinds of computer systems and services to write e-mails, to search the Internet for information, and to manage all kinds of data. With this development and the growing rate of Internet users, more and more services are provided over the Internet. A security-critical application in this context is that of electronic voting over the Internet. The corresponding infrastructure is not entirely under the election authority's control. Rather the voters' personal computers and public networks are used to vote and to submit the vote. Many of the current solutions neglect the fact, that a voter's personal computer may be compromised and that the voter may make mistakes while voting. Although these problems are not specific to Internet voting but an inherent problem in any security-critical communication application, only few research results exist with this respect.

In this context, the Swiss Federal Chancellery's *Vote électronique* project aims to gain a deeper understanding of the possible security problems imposed by insecure client computers and erroneous user behavior. The corresponding questions serve as starting points for the research in this thesis. We split the client-side security problems regarding electronic communication applications into two problem areas: *insecure platforms* and *human error*. Regarding these problem areas, we provide formal methods for the automated analysis of communication protocols with respect to the corresponding problem area. We use these formal methods to characterize secure electronic communication using insecure client computers and examine the influence of erroneous user behavior.

Zusammenfassung

Elektronische Kommunikation spielt eine zunehmend bedeutende Rolle und ist aus unserem täglichen Leben kaum mehr wegzudenken. Wir verwenden unterschiedliche Dienste und Systeme um Informationen im Internet zu suchen, um Nachrichten auszutauschen und um Daten zu verwalten. Mit der wachsenden Bedeutung des Internets werden auch immer mehr Programme und Dienste angeboten, welche Daten über öffentliche Netzwerke austauschen. Eine sicherheitskritische Anwendung in diesem Zusammenhang ist elektronisches Wählen über das Internet. Hierbei wird die verwendete Infrastruktur nicht komplett durch die Wahlbehörden kontrolliert. Vielmehr werden die Computer der Wähler und öffentliche Netzwerke verwendet, um die Stimmen abzugeben und zu übermitteln. Viele aktuelle Lösungsansätze ignorieren hierbei den Umstand, dass der Wähler einen kompromittierten Computer verwenden oder auch einfach einen Fehler in der Bedienung machen könnte. Obwohl diese Probleme nicht nur Wahlsystemen, sondern allen elektronischen Kommunikationsanwendungen zu Grunde liegt, wurden sie bislang wenig erforscht.

Vor diesem Hintergrund zielt das *Vote électronique* Projekt der Schweizerischen Bundeskanzlei darauf ab, ein vertieftes Verständnis für den Einfluss unsicherer Computer und fehlerhaften Verhaltens der Benutzer auf die Sicherheitseigenschaften von elektronischen Wahlsystemen zu entwickeln. Die diesbezüglichen Fragestellungen dienen als Grundlage für die vorliegende Forschungsarbeit. Wir teilen die benutzerseitigen Probleme elektronischer Kommunikationsanwendungen in zwei Problembereiche auf: *Unsichere Benutzersysteme* und *menschliche Fehler*. Für beide Problembereiche präsentieren wir formale Modelle um die automatisierte Analyse von Kommunikationsprotokollen im jeweiligen Problemkontext zu ermöglichen. Wir verwenden die formalen Modelle um sichere Kommunikation über unsichere Benutzersysteme zu charakterisieren und den Einfluss fehleranfälliger Benutzer zu untersuchen.