Diss. ETH No. 13156

Dynamic Security in Communication Systems

A dissertation submitted to the

SWISS FEDERAL INSTITUTE OF TECHNOLOGY ZÜRICH

for the degree of
Doctor of Technical Sciences

presented by

GERMANO CARONNI

Dipl. Informatik-Ing. ETH
born September 7, 1967
citizen of Mendrisio (TI)

accepted on the recommendation of
Prof. Dr. Bernhard Plattner, examiner
Prof. Dr. Ueli Maurer, co-examiner

1999

Abstract

The importance of communication security is increasing, because more and more valuable information is being transferred over computer networks. As of now, the provision of security (namely confidentiality, integrity, and authenticity) is an all-or-nothing issue: security is either provided to the maximum extent possible, or not at all. Offering security can be very expensive in terms of ease of use, management requirements, and computing overhead. As a consequence, security is often regarded as bad, not worth the benefits it provides. Currently, there are no mechanisms to fine-tune the strength of offered security and have applications use just the right amount of security to deter attackers.

In this thesis, dynamic aspects of security are explored. This covers Quality of Service (QoS) models and requirements for security, secure multimedia protocols, and peer and component authentication. Each of these issues is examined, and its dynamic properties are shown. The experimental platforms Da CaPo and WaveVideo are used to prototype some of the results. In essence, it is shown that it is possible to provide fine-grained, scalable security to applications and allow them to select at runtime the required amount of processing overhead necessary to achieve sufficient security.

The work first demonstrates the need for dynamic security and defines and discusses the fundamental properties of different aspects of security. These include the available cryptographic mechanisms and their properties, and where to place security functionality in a communication system. In conclusion, a coarse-grained system model is proposed. The then following examination of the state of the art clearly shows that the concept of merging security and QoS is novel. The same is true for protocols that provide a dynamically configurable amount of security, and for dynamically composable peer-authentication protocols with different properties.

In the next part, the focus is placed on QoS and security: the goal is to model dedicated security QoS parameters and to integrate them with

the traditional view of QoS. To this end, the new parameters are quantified by establishing a relationship to the monetary value of the data that are to be protected. Confidentiality and authenticity are then modelled from the user's perspective, and the mapping and translation down to the communication infrastructure is presented. The QoS parameters are used to select protocol and algorithm properties. Additionally, attack costs are evaluated, and the zero-cost attack is presented.

The ability to specify security requirements via QoS parameters allows the extension of multi-media protocols to provide dynamically configurable security functionality. In contrast to traditional solutions, in which security is provided on a multimedia data stream as a whole, dedicated security mechanisms that are embedded in the rest of the multimedia protocol allow very efficient processing. They receive QoS parameters to control their operations, and then provide, besides their more traditional tasks, confidentiality and authenticity for the transferred data. By varying the employed algorithms and the actual data coverage of the algorithm, computing power consumption can be reduced, while still maintaining an adequate degree of security. This property is critical when real-time behaviour is needed in software-only solutions. It is studied in the context of general purpose, audio, and video data. Results derived from a prototype are presented.

To conclude the thesis, the implementation of a framework capable of integrating the new functionalities is presented. For this, the existing QoS-capable middleware Da CaPo is extended. Securing Da CaPo communications is achieved by defining protocols that include encrypting and authenticating modules. Depending on the security requirements that the application specifies, the configuration process can employ these modules. A static key and certificate database allow for the storage and recovery of public keys and related information. The resulting functionality and performance are then evaluated, showing that fine-grained control over security is feasible, and the resulting performance is sufficient for real-world applications.

Zusammenfassung

Da mehr und mehr wertvolle Information über Computernetze übertragen wird, nimmt die Wichtigkeit von sicherer Kommunikation zu. Zur Zeit ist Sicherheit (hier vor allem Vertraulichkeit, Integrität und Authentizität) eine Alles-oder-Nichts Sache: Entweder wird Sicherheit in maximaler Stärke geboten, oder sie fehlt gänzlich. Benutzerfreundlichkeit, Administrierbarkeit und verfügbare Rechenleistung nehmen ab, wenn Sicherheit zur Verfügung gestellt wird. Als eine Folge dieser Nebenwirkungen wird Sicherheit häufig abgelehnt, da sie als unverhältnismässig aufwendig erscheint. Es gibt keine Mechanismen um eine Feinabstimmung der gebotenen Sicherheit zu erreichen. Eine Anwendung kann die Kommunikationsinfrastruktur nicht so einstellen, dass der gerade noch benötigte Overhead getrieben wird der nötig ist um Angreifer abzuschrecken.

In dieser Doktorarbeit werden dynamische Aspekte der Sicherheit erkundet. Dies deckt Dienstgütemodelle und Sicherheitsanforderungen, sichere Multimedia-Protokolle, sowie die Authentisierung von Kommunikationspartnern und Systemkomponenten ab. Jedes dieser Themen wird untersucht und die dynamischen Eigenschaften werden beleuchtet. Die experimentellen Plattformen Da CaPo++ und WaveVideo werden verwendet, um einige der Resultate prototypisch zu implementieren. Im Wesentlichen wird gezeigt, dass es möglich ist, Anwendungen fein abgestufte Sicherheit zugänglich zu machen. Dies erlaubt es ihnen, zur Laufzeit zu bestimmen, welches Mass an Rechenleistung nötig ist, um Daten ausreichend zu schützen.

Zu Beginn der Arbeit wird der Bedarf für dynamische Sicherheit klargestellt, und die grundlegenden Eigenschaften verschiedener Sicherheitsaspekte werden definiert und diskutiert. Dies schliesst die verfügbaren kryptographischen Mechanismen und ihre Eigenschaften ein, und die Frage wo Sicherheitsfunktionen in einem Kommunikationssystem integriert werden sollen. Als Schlussfolgerung wird ein grobkörniges Systemmodell vorgestellt. Die darauffolgende Untersuchung des

Standes der bisherigen Forschung auf diesem Gebiet zeigt klar auf, dass das Konzept der Verschmelzung von Sicherheit und Dienstgütemodellen neu ist. Das Gleiche gilt für Protokolle mit dynamisch konfigurierbarer Sicherheitsstärke, und für die Möglichkeit, zur Laufzeit dynamisch Authentisierungsprotokolle aus verschiedenen Modulen mit unterschiedlichen Eigenschaften zusammenzusetzen.

Anschliessend konzentriert sich die Arbeit auf die Aspekte der Dienstgüte und Sicherheit. Das Ziel ist hier eine Modellierung dedizierter Sicherheits-Dienstgüteparameter, und ihre Verschmelzung mit der bisherigen Sichtweise von Dienstgüte in Kommunikationssystemen. Um dies zu erreichen werden die Parameter quantisiert, indem ein Bezug zum Geldwert der zu schützenden Informationen geschaffen wird. Dann werden Vertraulichkeit und Authentizität aus Sicht des Benutzers modelliert und ihre Uebersetzung und Abbildung bis hinunter zur Kommunikationsinfrastruktur wird verfolgt. Die Dienstgüteparameter werden verwendet um die Eigenschaften von Protokollen und Algorithmen zu wählen. Zusätzlich werden die Kosten von Angriffen evaluiert, und die Nullkostenattacke wird präsentiert.

Die Möglichkeit, Sicherheitsanforderungen über QoS Parameter zu spezifizieren erlaubt die Erweiterung von Multimedia-Protokollen um dynamisch konfigurierbare Sicherheit. Im Gegensatz zu traditionellen Lösungen, in denen Sicherheit auf einen Datenstrom als Ganzes angewandt wird, ist es dank der Integration dedizierter Sicherheitsmechanismen in das Protokoll möglich, eine sehr effiziente Datenverarbeitung zu gewährleisten. Die Sicherheitsmechanismen erhalten konkretisierte Dienstgüteparameter zur Steuerung ihres Verhaltens, und müssen neben ihren sonstigen Aufgaben Vertraulichkeit und Authentizität übertragener Daten gewährleisten. Durch Veränderung der verwendeten Algorithmen, und durch Variation der tatsächlichen Ab-deckung von Daten durch den Algorithmus kann die benötigte Rechenleistung reduziert werden. Dabei wird nach wie vor ein angemessenes Mass an Sicherheit aufrechterhalten. Diese Eigenschaft ist unumgänglich wenn Echtzeitverhalten in reinen Softwarelösungen erreicht werden soll, und sie wird im Zusammenhang mit kontinuierlichen Daten-strömen wie Audio und Video näher untersucht. Daraus abgeleitete Resultate werden präsentiert.

Zum Abschluss der Arbeit wird die Implementation einer Systemlösung präsentiert, die diese neuen Funktionen unterstützen kann. Um

dies zu erreichen wird die vorhandene Systemlösung Da CaPo, die von sich aus Dienstgüte unterstützt, erweitert. Die Sicherung von Kommunikationsbeziehungen in Da CaPo wird erzielt indem Protokolle definiert werden die Authentisierungs- und Verschlüsselungsmodule beinhalten. Abhängig von den Sicherheitsanforderungen wie sie durch die Anwendung spezifizierbar sind kann der Konfigurationsprozess diese Module verwenden. Eine statische Schlüssel- und Zertifikatsdatenbank gestatten das anwendungsunabhängige Speichern und Laden öffentlicher Schlüssel und ähnlicher Informationen. Die entstandene Funktionalität und Leistungsfähigkeit wird evaluiert. Die Evaluation zeigt, dass eine feinkörnige Kontrolle von Sicherheitseigenschaften machbar ist, und dass die resultierende Leistungsfähigkeit ausreichend ist, um reale Anwendungen möglich zu machen.