A Practical Approach for Establishing Trust Relationships between Remote Platforms Using Trusted Computing

Kurt Dietrich, Martin Pirker, Tobias Vejda, Ronald Toegl, Thomas Winkler, and Peter Lipp

Institute for Applied Information Processing and Communications (IAIK), Graz University of Technology, Inffeldgasse 16a, A–8010 Graz, Austria
{kdietrich,mpirker,tvejda,rtoegl,plipp}@iaik.tugraz.at, thomas.winkler@uni-klu.ac.at

Abstract. Over the past years, many different approaches and concepts in order to increase computer security have been presented. One of the most promising of these concepts is Trusted Computing which offers various services and functionalities like reporting and verifying the integrity and the configuration of a platform (attestation). The idea of reporting a platform’s state and configuration to a challenger opens new and innovative ways of establishing trust relationships between entities. However, common applications are not aware of Trusted Computing facilities and are therefore not able to utilise Trusted Computing services at the moment. Hence, this article proposes an architecture that enables arbitrary applications to perform remote platform attestation, allowing them to establish trust based on their current configuration. The architecture’s components discussed in this article are also essential parts of the OpenTC proof-of-concept prototype. It demonstrates applications and techniques of the Trusted Computing Group’s proposed attestation mechanism in the area of personal electronic transactions.

1 Introduction

Trusted Computing (TC) is constantly gaining ground in industry and the public perception of Trusted Computing is starting to improve [6]. A central role is played by the Trusted Computing Group (TCG) [18] which is specifying the core components, namely the Trusted Platform Modules (TPM) and surrounding software architectures like the TCG Software Stack (TSS) [15]. Based on these components, security and trust related services like remote attestation, sealing or binding are defined.

Hence, in the first contribution the question how trust relationships between remote platforms can be established by using TC is addressed. The approach presented in this paper allows to establish trusted communication channels by means of the TCG’s specified remote attestation. The approach introduces a so-called attestation proxy that is placed in front of the actual application and performs a mutual platform attestation of the two communication parties.
actual communication channel is only established if the attestation succeeded. This approach allows legacy applications to benefit from attested communication channels without the need to modify the application code.

As the proof-of-concept implementation is done in Java, the second contribution deals with the problem how TC concepts can be integrated into virtual machine based runtime environments such as Java™. Questions to be answered are how to measure loaded class and jar files, how to deal with external resources or how to handle calls to native code.

The basis for all TC related services is the TPM. The TPM is a hardware chip providing essential functionality for a TC enabled system like a RSA engine, a true random number generator or mechanisms to securely store and report the state of a system. While TPMS are produced and shipped by a variety of manufacturers, important software components like the trusted software stack are not widely available yet. The presented IAIK TSS for the Java Platform (jTSS [14]) provides TC services to applications and manages the communication with the TPM. The jTSS provides the foundations for the two main contributions of this work.

1.1 Related Work

The idea of remote attestation has been pursued by various research groups. Hence, many different approaches discussing this research area have been published. The most important are introduced in the following paragraphs.

The concept of Property-Based Attestation (PBA) [11] provides an alternative to the attestation mechanisms specified by the TCG henceforth called binary attestation. A Trusted Third Party (TTP) translates the actual system configuration into a set of properties and issues certificates for those properties. During the attestation process a (remote) verifier can decide whether or not the platform security properties meet the requirements of the respective use case. In literature, using TTPs for certification of properties is called delegation. This scenario avoids several (undesired) drawbacks of binary attestation. For instance, presenting the concrete system configuration to a verifier is not desirable from a privacy perspective and management of all possible configurations is a difficult task.

Alternatively, Semantic Remote Attestation (SRA) [12] uses language-based techniques to attest high level properties of an application. The proposal is based on the Java Virtual Machine (JVM) environment which is attested by binary attestation itself. The JVM can enforce a security policy on the running code based on data flow control and taint propagation mechanisms. Hence, this approach is a hybrid approach between binary attestation and attesting properties.

Moreover, the Trusted Computing Group - as the leading group for TC specifications - has published a concept for trusted network access also known as Trusted Network Connect (TNC) [22]. TNC enforces a policy based access and integrity control by measuring the state and configuration of a platform according to specified policies. Furthermore, TNC introduces the concept of isolation. Platforms that cannot be attested correctly are isolated. This means that they