Security and Trust Architectures for Protecting Sensitive Data on Commodity Computing Platforms

Marcel Winandy

DISSERTATION

zur Erlangung des Grades eines Doktor-Ingenieurs
der Fakultät für Elektrotechnik und Informationstechnik
an der Ruhr-Universität Bochum

1. Berichter:	Prof. Dr.-Ing. Ahmad-Reza Sadeghi (Ruhr-Universität Bochum)
2. Berichter:	Prof. Dr. Chris Mitchell (Royal Holloway, University of London, UK)

Tag der mündlichen Prüfung: 18.01.2012

Bochum, 2012

RUHR
UNIVERSITÄT
BOCHUM
RUB

Berichte aus der Informatik

Marcel Winandy

Security and Trust Architectures for Protecting Sensitive Data on Commodity Computing Platforms

Shaker Verlag
Aachen 2012

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Zugl.: Bochum, Univ., Diss., 2012

Printed in Germany.

ISBN 978-3-8440-1315-3
ISSN 0945-0807

Shaker Verlag GmbH • P.O. BOX 101818 • D-52018 Aachen
Phone: 0049/2407/9596-0 • Telefax: 0049/2407/9596-9
Internet: www.shaker.de • e-mail: info@shaker.de

Kurzfassung (Summary in German)

Viele Computer-Anwendungen benötigen eine sichere Ausführungsumgebung, um die Vertraulichkeit und Integrität ihrer Daten zu schützen. Obwohl es bereits verschiedene Ansätze in der Kryptographie und in der Anwendungssicherheit gibt, schlagen diese in der Praxis letztendlich fehl aufgrund unsicherer Betriebssysteme und falscher Annahmen bezüglich der Vertrauenswürdigkeit der zugrunde liegenden Computerplattformen.

Die Entwicklung sicherer Betriebssysteme war und ist immer noch ein komplexes Problem. In der Vergangenheit entwickelte sich deshalb die Idee des *Sicherheitskerns*: Alle relevante Sicherheitsfunktionalität wurde innerhalb eines kleinen Kerns implementiert, der folgende Eigenschaften hatte: komplette Kontrolle über alle Objekte; Selbstschutz gegen Manipulation; und geringe Codegröße zur Erleichterung einer formalen Verifikation. Es stellte sich jedoch heraus, daß selbst die Konstruktion einer solchen kleinen vertrauenswürdigen Basis in der Praxis bereits aufwendig und schwierig war. Zudem wiesen frühe Implementierungen eine sehr schlechte Performanz auf. Daher ist die Idee des Sicherheitskerns nie in die Entwicklung von Standardbetriebssystemen eingeflossen.

In dieser Dissertation präsentieren wir Sicherheitsarchitekturen, die in der Lage sind, sensible Daten auch auf gewöhnlichen (PC-)Computerplattformen zu schützen. Die Integration von *Trusted Computing* Technologie in heutige Standardplattformen erlaubt die Einbettung zusätzlicher Sicherheitsfunktionen direkt in die Hardware. Außerdem besitzen moderne Prozessoren hardware-seitig unterstützte Virtualisierungstechnologie. Basierend auf diesen Funktionalitäten, sowie neuer Ergebnisse zur Konstruktion von Mikrokernen, verwenden wir die Idee der Sicherheitskerne wieder und entwerfen Sicherheitsarchitekturen, die Endbenutzer verwenden können, um ihre Systeme und ihre Daten gegen eine Vielzahl von Bedrohungen zu schützen.

Ein erster Beitrag dieser Arbeit ist die Verbesserung von Sicherheitsarchitekturen, die Virtualisierung verwenden. Ein wichtiger Aspekt in diesem Kontext ist die Virtualisierung von Hardware-Sicherheitsmodulen wie die des Trusted Platform Module (TPM). Wir präsentieren daher das *property-based vTPM*, ein flexibles und datenschutz-erhaltendes virtuelles TPM. Es integriert verschiedene Ansätze zur Ermittlung des Integritätszustandes einer Plattform und zur Erstellung von kryptographischen Schlüsseln. Dies ermöglicht einen flexibleren Umgang mit Softwareupdates und Migration von virtuellen Maschinen bei gleichzeitiger Beachtung der erforderlichen Sicherheitseigenschaften.

Ein weiterer Beitrag ist der Entwurf und die Implementierung einer Sicherheitsarchitektur gegen Phishing-Angriffe, d.h. Angriffe, die versuchen Passwörter eines Be-

nutzers zu stehlen. Die Hauptidee hierbei ist ein *trusted password wallet (TruWallet)*, das sich anstelle des Benutzers um den Login-Vorgang auf Webseiten kümmert. Dazu speichert TruWallet sicher alle Passwörter des Benutzers und führt die Login-Vorgänge aus. Im Gegensatz zu anderen Ansätzen liefert TruWallet Schutz gegen die stärkste Art des Phishing-Angriffs, nämlich gegen Phishing-Malware, die auf dem Rechner des Anwenders läuft.

Wir zeigen ferner eine Sicherheitsarchitektur, um über mehrere Plattformen hinweg gemeinsam genutzte Informationen zu schützen. Diese Architektur basiert auf dem Konzept von *Trusted Virtual Domains (TVDs)* und realisiert im wesentlichen eine verteilte Informationsflußkontrolle. Wir erweitern dieses Konzept über die übliche Verwendung in Rechenzentren hinaus und beziehen auch Plattformen von Endanwendern ein. Um deren spezielle Anforderungen zu berücksichtigen, entwerfen wir eine transparente Verschlüsselung von mobilen Datenträgen (z.B. USB-Sticks), die konform zu einer gegebenen Informationssicherheitspolitik arbeitet. Außerdem evaluieren wir eine vollständige Implementierung des TVD-Konzepts auf einem existierenden Desktop-Betriebssystem.

Schließlich schauen wir uns einige besondere Anwendungsszenarien an, die zwar ebenfalls eine vertrauenswürdige Plattform benötigen, aber nicht notwendigerweise einen permanent laufenden Software-Sicherheitskern. Dazu nutzen wir die erweiterten Funktionen moderner Hauptprozessoren, um eine sichere Ausführungsumgebung bereitzustellen, auf der wir einen *Unidirectional Trusted Path (UTP)* realisieren, d.h. einen vertrauenswürdigen Kommunikationspfad in nur eine Richtung: vom lokalen Anwender zu einer entfernten Partei. Wir evaluieren eine vollständige Implementierung dieses Ansatzes und zeigen, daß UTP eine Alternative für CAPTCHAs sein kann und daß man damit eine sichere Transaktionsbestätigung für Online-Einkäufe realisieren kann.

Die vorgestellten Sicherheitsarchitekturen dieser Dissertation ermöglichen den Schutz sensibler Daten (sowohl persönlicher als auch gemeinsam genutzter) auf heute üblichen Computerplattformen. Die präsentierten Ergebnisse zeigen, daß eine sichere Ausführung von Anwendungen ermöglicht werden kann, wenn man eine kleine Sicherheitsschicht unter der normalen Betriebssystemumgebung ausführt. Dies kann so realisiert werden, ohne die Funktionsvielfalt und Kompatibilität vorhandener Standardbetriebssysteme zu verlieren.

Abstract

Many applications rely on a secure execution environment in order to provide confidentiality and integrity of their data. Although various approaches both in cryptography and application security exist, they finally fail because of insecure operating systems and false assumptions in practice about the trustworthiness of the underlying computing platform.

The design and implementation of secure operating systems was and is still a complex problem. The idea of the *security kernel* evolved in the past to overcome this problem: All relevant security functionality was implemented in a small kernel which provided a complete control over shared objects, a sufficient protection of itself against tampering, and was small enough to allow a formal verification of its correctness. However, it turned out that even the construction of this small trusted computing base was already a hard problem in practice and early implementations suffered from poor performance. Hence, the idea was not adopted in mainstream operating systems.

In this thesis, we present security architectures that are able to protect sensitive data on commodity computing platforms. The incorporation of *trusted computing* concepts in commodity platforms allows for additional security functionality embedded directly into the hardware. In addition, modern main processors include support for hardware virtualization. Based on these functionalities as well as recent results in the construction of microkernels, we reuse the idea of security kernels and design security architectures that end-users can use to protect their systems and their data against a number of threats.

The first major contribution of this thesis is the improvement of security architectures that use virtualization. A crucial aspect in this context is the virtualization of hardware security modules like the Trusted Platform Module (TPM). We therefore present the *property-based vTPM*, a flexible and privacy-preserving design of a virtual TPM. It integrates different approaches for measuring the platform's state and for key generation, which results in enhanced support of both software updates and migration of virtual machines, without losing the required security properties.

Another main contribution is the design and implementation of a security architecture against phishing attacks, i.e., attacks that try to steal passwords from users. The key idea is a *trusted password wallet (TruWallet)* that removes the burden of authentication from users when they login to web sites. TruWallet stores all passwords and automatically performs the login at the server on behalf of the user. In contrast to other approaches against phishing, the combination of the wallet, an underlying security kernel, and the incorporation of trusted computing functionality provides protection measures against the

strongest type of phishing attacks, i.e., phishing malware running on the user's computer.

We also present a security architecture to protect shared information across different computing platforms. This architecture is based on the existing concept of *Trusted Virtual Domains (TVDs)*, which essentially realizes a distributed enforcement of information flow control. We extend this concept beyond its usually proposed usage in data centers to include individual computing platforms of end-users. To address the specific needs of end-users, we design a transparent cryptographic data protection of mobile storage devices (e.g., USB memory sticks) according to the information security policy, and we evaluate a full implementation of the TVD concept on an existing desktop operating system.

Finally, we look into special application scenarios that require a trustworthy platform, but which can be realized without the need for a persistently running security kernel in software. We therefore leverage the enhanced functionality of modern processors to provide a secure execution environment, and build a *Unidirectional Trusted Path (UTP)*, i.e., a trusted path from the local user to a remote party. We evaluate a full implementation of this approach, and we show how it can be used as alternative for CAPTCHAs, or to create a secure transaction confirmation for online purchases.

The security architectures presented in this thesis enable the protection of sensitive personal data and the protection of information sharing on commodity computing platforms. The results demonstrate that a secure execution of applications can be provided by introducing a small security layer underneath the normal operating environment without losing the feature-richness and compatibility of commodity operating systems.

Acknowledgements

This thesis is the result of research work I did at the System Security Group at Horst Görtz Institute for IT-Security at Ruhr-University Bochum. Writing this thesis did not only include a number of years of research, but it also included the support, collaboration, and companionship of several people I would like to thank.

First of all, I like to thank my thesis advisor Ahmad-Reza Sadeghi. He provided me with an open, cooperative but also challenging research environment in which I could bring in my own research ideas. I am grateful for his professional advice and the time he spent to give me all the valuable feedback. I am glad for the opportunity he gave me to work in so many interesting projects and the various insights I gained throughout them.

Next, I like to thank my thesis committee, in particular Chris Mitchell for being one of the referees of my thesis and spending his valuable time on reading it.

Special thanks go to my co-authors and (former) colleagues Christian Stüble, Hans Löhr, Sebastian Gajek, and Luigi Catuogno. We worked on many papers together that built the basis for this thesis. I enjoyed the myriad of research discussions we had (including one or the other espresso). Many thanks also go to my colleagues Biljana Cubaleska, Lucas Davi, Alexandra Dmitrienko, Thomas Schneider, Steffen Schulz, and Christian Wachsmann, and my former colleagues Yacine Gasmi, Mark Manulis, Patrick Stewin, Martin Unger, and Marko Wolf for various discussions on ideas and designs as well as writing papers together. A special "thank you" goes to Frederik Armknecht for sharing the same humor and the creation of "Trusty", our virtual mascot for trusted computing.

Many thanks go to all the other colleagues at the Horst Görtz Institute for IT-Security with whom I had the chance to meet, chat, discuss, or simply enjoy lunch together.

Further special thanks go to Jonathan McCune for being a great host and friend during my short visit at Carnegie Mellon University. It was a real pleasure to work and doing research with him.

Moreover, I like to thank all the (former) students or colleagues who helped with implementing the various prototypes that I used throughout my research: Sören Bleikertz, Atanas Filyanov, Thomas Fischer, Sören Heisrath, Christoph Kowalski, Andreas Krügersen, Thomas Pöppelmann, Johannes Rave, Marcel Selhorst, and Oskar Senft. I also like to thank all the people at Sirrix AG whom I worked with throughout various projects during my research, in particular Ammar Alkassar and (again) Christian Stüble for their useful comments and discussions, and Rani Husseiki and (again) Oskar Senft for their pleasant company while sharing the office room with them.

While working at a university, it is always good to have friends in the secretariat who can help you with all the administrative stuff. Therefore, I very much like to thank Nadine Palacios and Justine Spalik for being great team assistants. I was able to save a lot of time due to their help. In addition, I want to thank Tobias Hommel and Zecir "Eko" Hadzic for their valuable work as IT admins and keeping the systems running (in particular the subversion repositories for all the papers I was working on).

I specially like to thank Adrian Spalka, who was my diploma thesis advisor at the University of Bonn. He inspired me for the field of computer security and to pursue a PhD in academic research. I am grateful for all the discussions we had and the way he taught me to ask the right questions.

Finally, I like to thank my wife Brigitte for her patience, love, and support to pursue this long-term project of acquiring my PhD. And I like to thank our families, in particular my parents, Ingrid and Günter, my sister Michaela, as well as Christa, Rainer, and Daniela, for their constant support and encouragment.

Contents

List of Figures

List of Tables