Juan A. Garay
Arjen K. Lenstra
Masahiro Mambo
René Peralta (Eds.)

LNCS 4779

Information Security

10th International Conference, ISC 2007
Valparaíso, Chile, October 2007
Proceedings

Springer

Juan A. Garay   Arjen K. Lenstra
Masahiro Mambo   René Peralta (Eds.)

Information Security

10th International Conference, ISC 2007
Valparaíso, Chile, October 9-12, 2007
Proceedings

Springer

Volume Editors

Juan A. Garay
Bell Labs
600 Mountain Ave., Murray Hill, NJ 07974, USA
E-mail: garay@research.bell-labs.com

Arjen K. Lenstra
EPFL IC LACAL
INJ 330, Station 14, CH-1015 Lausanne, Switzerland
E-mail: arjen.lenstra@epfl.ch

Masahiro Mambo
University of Tsukuba
1-1-1 Tennoudai, Tsukuba, Ibaraki, 305-8573, Japan
E-mail: mambo@cs.tsukuba.ac.ip

René Peralta
NIST, Security Division, Information Technology Laboratory
Gaithersburg, MD. 20899, USA
E-mail: rene.peralta@nist.gov

Library of Congress Control Number: 2007936070

CR Subject Classification (1998): E.3, E.4, D.4.6, C.2, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-75495-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-75495-4 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12170333 06/3180 5 4 3 2 1 0

Lecture Notes in Computer Science 4779

Preface

The 10th Information Security Conference (ISC 2007) was held in Valparaíso, Chile, October 9–12, 2007. ISC is an annual international conference covering research in theory and applications of information security, aiming to attract high quality papers in all of its technical aspects. ISC was first initiated as a workshop (ISW) in Japan in 1997, ISW 1999 was held in Malaysia and ISW 2000 in Australia. The name was changed to the current one when the conference was held in Spain in 2001 (ISC 2001). The latest conferences were held in Brazil (ISC 2002), the UK (ISC 2003), the USA (ISC 2004), Singapore (ISC 2005), and Greece (ISC 2006). This year the event was sponsored by the Universidad Técnica Federico Santa María (Valparaíso, Chile), the Support Center for Advanced Telecommunications Technology Research, Foundation, SCAT(Tokyo, Japan), Microsoft Corporation, and Yahoo! Research.

Reflecting the conference's broad scope, this year's main Program Committee consisted of a relatively large number (49) of experts. Additionally, given the timely topic of cryptanalysis and design of hash functions and the NIST hash competition, the conference also featured a special Hash Subcommittee, chaired by Arjen Lenstra (EPFL and Bell Labs), as well as a panel on hashing, chaired by Bill Burr (NIST). The conference received 116 submissions, 29 of which were selected by the committee members for presentation at the conference, based on quality, originality and relevance. Each paper was anonymously reviewed by at least three committee members.

Extended abstracts of 28 of the selected papers (a decision was made that only papers whose authors could commit to presenting them at the conference would be published), many revised according to the reviewers' suggestions, appear in these proceedings. An important ISC interest is to encourage and promote student participation. In line with that interest, the ISC 2007 Program Committee had the pleasure of selecting three student-coauthored papers for the Best Student Paper award—one from each region ISC rotates among: Asia, Europe, and the Americas. The papers were, respectively, "Identity-Based Proxy Re-encryption Without Random Oracles," by Cheng-Kang Chu and Wen-Guey Tzeng (National Chiao Tung University, Taiwan), "Detecting System Emulators," by Thomas Raffetseder, Christopher Kruegel, and Engin Kirda (Technical University of Vienna, Austria), and "Impossible-Differential Attacks on Large-Block Rijndael," by Jorge Nakahara Jr. and Ivan Carlos Pavão (Catholic University of Santos, Brazil). The program also included invited lectures by Hugo Krawczyk (IBM's T.J. Watson Research Center, USA), and Brent Waters (SRI International, USA).

First and foremost, I am extremely grateful to the members of the Program Committee and Hash Subcommittee for their investment and effort in the process—many times difficult and delicate—of paper review and selection, as well as to the large number of external reviewers for their valuable help.

Electronic submissions were made possible by the Web Submission and Review Software developed by Shai Halevi, which was hosted at the Universidad Técnica Federico Santa María. Many thanks to Raul Monge for making that possible—and for his perennial availability when problems arose, to Shai for his support, and to Debbie Cook and Marcos Kiwi for their help in the handling of the submissions.

Beyond the hosting of the submission software, Raúl Monge and his team did a magnificent job managing and taking care of all aspects of the local organization. I am also most grateful to the general chairs, Masahiro Mambo and René Peralta, for all their hard work, assistance and advice on a myriad of issues related to this conference.

Finally, I wish to thank all the authors for submitting their work to ISC 2007, and the authors of the accepted papers for their contribution to the high technical quality of the program. As technology evolves and means of communication and interaction become increasingly more complex and sophisticated, so does the need not only for guaranteeing their soundness and safety when run in adversarial settings, but also for novel techniques that actually make them possible. Without a doubt, the new notions, methods and designs presented in these proceedings constitute an important step in those directions.

August 2007 Juan A. Garay

ISC 2007

The 10th International Security Conference
Valparaíso, Chile, October 9–12, 2007

ISC Steering Committee

Ed Dawson	Queensland University of Technology, Australia
Sokratis K. Katsikas	University of the Aegean, Greece
Javier López	University of Málaga, Spain
Masahiro Mambo	University of Tsukuba, Japan
Eiji Okamoto	University of Tsukuba, Japan
René Peralta	NIST, USA
Rebecca Wright	Rutgers University, USA
Yuliang Zheng	University of North Carolina–Charlotte, USA

General Chairs

Masahiro Mambo	University of Tsukuba, Japan
René Peralta	NIST, USA

Program Chair

Juan A. Garay	Bell Labs, USA

Hash Subcommittee Chair

Arjen Lenstra	EPFL, Switzerland and Bell Labs, USA

Organizing Chair

Raúl Monge	Universidad Técnica Federico Santa María, Chile

Program Committee

Michel Abdalla	ENS, France
Mikhail Atallah	Purdue University, USA
Michael Backes	Saarland University, Germany
Feng Bao	Institute for Infocomm Research, Singapore
Paulo Barreto	University of Sao Paulo, Brazil

John Black	University of Colorado, USA
Debbie Cook	Bell Labs, USA
Claudia Diaz	K.U. Leuven, Belgium
Glenn Durfee	PARC, USA
Nelly Fazio	IBM Research, USA
Matthias Fitzi	ETH Zürich, Switzerland
Stuart Haber	HP Labs, USA
Shai Halevi	IBM Research, USA
Amir Herzberg	Bar-Ilan University, Israel
Alejandro Hevia	University of Chile, Chile
Trent Jaeger	Penn State University, USA
Stasio Jarecki	University of California-Irvine, USA
Angelos Keromytis	Columbia University, USA
Aggelos Kiayias	University of Connecticut, USA
Kwangjo Kim	Information and Comms. University, Korea
Marcos Kiwi	University of Chile, Chile
Steve Kremer	ENS Cachan, France
Dong Hoon Lee	Korea University, Korea
Helger Lipmaa	University College London, UK
Breno de Medeiros	Florida State University, USA
Atsuko Mijayi	JAIST, Japan
Fabian Monrose	Johns Hopkins University, USA
Gregory Neven	K.U. Leuven, Belgium
Kaisa Nyberg	Helsinki Univ. of Tech. and Nokia, Finland
Carles Padró	Polytechnic University of Catalonia, Spain
Sarvar Patel	Alcatel-Lucent, USA
Sihan Qing	Chinese Academy of Sciences, China
Greg Rose	Qualcomm, USA
Rei Safavi-Naini	University of Calgary, Canada
Pierangela Samarati	University of Milan, Italy
Andre Scedrov	University of Pennsylvania, USA
Berry Schoenmakers	Technical University Eindhoven, Holland
Tom Shrimpton	Portland State University, USA
Michael Steiner	IBM Research, USA
Doug Tygar	University of California-Berkeley, USA
Wen-Guey Tzeng	National Chiao Tung University, Taiwan
Dominique Unruh	Saarland University, Germany
Ariel Waissbein	ITBA and Core Security, Argentina
Brent Waters	SRI International, USA
Susanne Wetzel	Stevens Institute of Technology, USA
Stephen Wolthusen	Royal Holloway University of London, UK
Moti Yung	Columbia University, USA
Xiaolan (Catherine) Zhang	IBM Research, USA

Hash Subcommittee

John Black	University of Colorado, USA
Shai Halevi	IBM Research, USA
Paul Hoffman	VPN Consortium, USA
John Kelsey	NIST, USA
Vlastimil Klima	Czech Republic
Stefan Lucks	Bauhaus-University Weimar, Germany
Tom Shrimpton	Portland State University, USA
Martijn Stam	EPFL, Switzerland
Ron Steinfeld	Macquarie University, Australia
Marc Stevens	Technical University Eindhoven, Holland

External Reviewers

Andre Adelsbach
Claudio Ardagna
Georges Baatz
Joonsang Baek
Billy Brumley
Matt Burnside
Reza Curtmola
George Danezis
Marie Duflot
Ratna Dutta
Sara Foresti
Ezequiel Gutesman
Martin Hirt
Susan Hohenberger
Bill Horne
Sotiris Ioannidis
Florent Jacquemard
Charanjit Jutla
Marcelo Kaihara
Darko Kirovski
Tetsutaro Kobayashi
Vladimir Kolesnikov
Yuichi Komano
Gaicheng Li
Hafiz Malik
Michael de Mare
Toshihiko Matsuo
Vishal Misra
Rossana Motta
Ginger Myles
Cedric Ng
Antonio Nicolosi
Prasad Rao
Mohammed-Reza Reyhanitabar
Mark Ryan
Siamak Shahandashti
Nicholas Sheppard
Seonghan Shin
Johan Sjoedin
Mitsuru Tada
Katsuyuki Takashima
Qiang Tang
Carmela Troncoso
Duc Liem Vo
Shabsi Walfish
Guilin Wang
Wendy Hui Wang
Qianhong Wu
Yongdong Wu
Angelika Zavou
Hong-Sheng Zhou

Sponsoring Institutions

Universidad Técnica Federico Santa María, Valparaíso, Chile
Support Center for Advanced Telecommunications Technology Research, Foundation, Japan
Microsoft Corporation
Yahoo! Research

Lecture Notes in Computer Science

Sublibrary 4: Security and Cryptology

Vol. 4779: J.A. Garay, A.K. Lenstra, M. Mambo, R. Peralta (Eds.), Information Security. XIII, 437 pages. 2007.

Vol. 4734: J. Biskup, J. López (Eds.), Computer Security – ESORICS 2007. XIV, 628 pages. 2007.

Vol. 4727: P. Paillier, I. Verbauwhede (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2007. XIV, 468 pages. 2007.

Vol. 4691: T. Dimitrakos, F. Martinelli, P.Y.A. Ryan, S. Schneider (Eds.), Formal Aspects in Security and Trust. VIII, 285 pages. 2007.

Vol. 4677: A. Aldini, R. Gorrieri (Eds.), Foundations of Security Analysis and Design IV. VII, 325 pages. 2007.

Vol. 4657: C. Lambrinoudakis, G. Pernul, A M. Tjoa (Eds.), Trust and Privacy in Digital Business. XIII, 291 pages. 2007.

Vol. 4637: C. Kruegel, R. Lippmann, A. Clark (Eds.), Recent Advances in Intrusion Detection. XII, 337 pages. 2007.

Vol. 4622: A. Menezes (Ed.), Advances in Cryptology - CRYPTO 2007. XIV, 631 pages. 2007.

Vol. 4593: A. Biryukov (Ed.), Fast Software Encryption. XI, 467 pages. 2007.

Vol. 4586: J. Pieprzyk, H. Ghodosi, E. Dawson (Eds.), Information Security and Privacy. XIV, 476 pages. 2007.

Vol. 4582: J. López, P. Samarati, J.L. Ferrer (Eds.), Public Key Infrastructure. XI, 375 pages. 2007.

Vol. 4579: B. M. Hämmerli, R. Sommer (Eds.), Detection of Intrusions and Malware, and Vulnerability Assessment. X, 251 pages. 2007.

Vol. 4575: T. Takagi, T. Okamoto, E. Okamoto, T. Okamoto (Eds.), Pairing-Based Cryptography – Pairing 2007. XI, 408 pages. 2007.

Vol. 4521: J. Katz, M. Yung (Eds.), Applied Cryptography and Network Security. XIII, 498 pages. 2007.

Vol. 4515: M. Naor (Ed.), Advances in Cryptology - EUROCRYPT 2007. XIII, 591 pages. 2007.

Vol. 4499: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security II. IX, 117 pages. 2007.

Vol. 4464: E. Dawson, D.S. Wong (Eds.), Information Security Practice and Experience. XIII, 361 pages. 2007.

Vol. 4462: D. Sauveron, K. Markantonakis, A. Bilas, J.-J. Quisquater (Eds.), Information Security Theory and Practices. XII, 255 pages. 2007.

Vol. 4450: T. Okamoto, X. Wang (Eds.), Public Key Cryptography – PKC 2007. XIII, 491 pages. 2007.

Vol. 4437: J.L. Camenisch, C.S. Collberg, N.F. Johnson, P. Sallee (Eds.), Information Hiding. VIII, 389 pages. 2007.

Vol. 4392: S.P. Vadhan (Ed.), Theory of Cryptography. XI, 595 pages. 2007.

Vol. 4377: M. Abe (Ed.), Topics in Cryptology – CT-RSA 2007. XI, 403 pages. 2006.

Vol. 4356: E. Biham, A.M. Youssef (Eds.), Selected Areas in Cryptography. XI, 395 pages. 2007.

Vol. 4341: P.Q. Nguyên (Ed.), Progress in Cryptology - VIETCRYPT 2006. XI, 385 pages. 2006.

Vol. 4332: A. Bagchi, V. Atluri (Eds.), Information Systems Security. XV, 382 pages. 2006.

Vol. 4329: R. Barua, T. Lange (Eds.), Progress in Cryptology - INDOCRYPT 2006. X, 454 pages. 2006.

Vol. 4318: H. Lipmaa, M. Yung, D. Lin (Eds.), Information Security and Cryptology. XI, 305 pages. 2006.

Vol. 4307: P. Ning, S. Qing, N. Li (Eds.), Information and Communications Security. XIV, 558 pages. 2006.

Vol. 4301: D. Pointcheval, Y. Mu, K. Chen (Eds.), Cryptology and Network Security. XIII, 381 pages. 2006.

Vol. 4300: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security I. IX, 139 pages. 2006.

Vol. 4298: J.K. Lee, O. Yi, M. Yung (Eds.), Information Security Applications. XIV, 406 pages. 2007.

Vol. 4296: M.S. Rhee, B. Lee (Eds.), Information Security and Cryptology – ICISC 2006. XIII, 358 pages. 2006.

Vol. 4284: X. Lai, K. Chen (Eds.), Advances in Cryptology – ASIACRYPT 2006. XIV, 468 pages. 2006.

Vol. 4283: Y.Q. Shi, B. Jeon (Eds.), Digital Watermarking. XII, 474 pages. 2006.

Vol. 4266: H. Yoshiura, K. Sakurai, K. Rannenberg, Y. Murayama, S.-i. Kawamura (Eds.), Advances in Information and Computer Security. XIII, 438 pages. 2006.

Vol. 4258: G. Danezis, P. Golle (Eds.), Privacy Enhancing Technologies. VIII, 431 pages. 2006.

Vol. 4249: L. Goubin, M. Matsui (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2006. XII, 462 pages. 2006.

Vol. 4237: H. Leitold, E.P. Markatos (Eds.), Communications and Multimedia Security. XII, 253 pages. 2006.

Vol. 4236: L. Breveglieri, I. Koren, D. Naccache, J.-P. Seifert (Eds.), Fault Diagnosis and Tolerance in Cryptography. XIII, 253 pages. 2006.

Vol. 4219: D. Zamboni, C. Krügel (Eds.), Recent Advances in Intrusion Detection. XII, 331 pages. 2006.

Vol. 4189: D. Gollmann, J. Meier, A. Sabelfeld (Eds.), Computer Security – ESORICS 2006. XI, 548 pages. 2006.

Vol. 4176: S.K. Katsikas, J. López, M. Backes, S. Gritzalis, B. Preneel (Eds.), Information Security. XIV, 548 pages. 2006.

Vol. 4117: C. Dwork (Ed.), Advances in Cryptology - CRYPTO 2006. XIII, 621 pages. 2006.

Vol. 4116: R. De Prisco, M. Yung (Eds.), Security and Cryptography for Networks. XI, 366 pages. 2006.

Vol. 4107: G. Di Crescenzo, A. Rubin (Eds.), Financial Cryptography and Data Security. XI, 327 pages. 2006.

Vol. 4083: S. Fischer-Hübner, S. Furnell, C. Lambrinoudakis (Eds.), Trust and Privacy in Digital Business. XIII, 243 pages. 2006.

Vol. 4064: R. Büschkes, P. Laskov (Eds.), Detection of Intrusions and Malware & Vulnerability Assessment. X, 195 pages. 2006.

Vol. 4058: L.M. Batten, R. Safavi-Naini (Eds.), Information Security and Privacy. XII, 446 pages. 2006.

Vol. 4047: M.J.B. Robshaw (Ed.), Fast Software Encryption. XI, 434 pages. 2006.

Vol. 4043: A.S. Atzeni, A. Lioy (Eds.), Public Key Infrastructure. XI, 261 pages. 2006.

Vol. 4004: S. Vaudenay (Ed.), Advances in Cryptology - EUROCRYPT 2006. XIV, 613 pages. 2006.

Vol. 3995: G. Müller (Ed.), Emerging Trends in Information and Communication Security. XX, 524 pages. 2006.

Vol. 3989: J. Zhou, M. Yung, F. Bao (Eds.), Applied Cryptography and Network Security. XIV, 488 pages. 2006.

Vol. 3969: Ø. Ytrehus (Ed.), Coding and Cryptography. XI, 443 pages. 2006.

Vol. 3958: M. Yung, Y. Dodis, A. Kiayias, T.G. Malkin (Eds.), Public Key Cryptography - PKC 2006. XIV, 543 pages. 2006.

Vol. 3957: B. Christianson, B. Crispo, J.A. Malcolm, M. Roe (Eds.), Security Protocols. IX, 325 pages. 2006.

Vol. 3956: G. Barthe, B. Grégoire, M. Huisman, J.-L. Lanet (Eds.), Construction and Analysis of Safe, Secure, and Interoperable Smart Devices. IX, 175 pages. 2006.

Vol. 3935: D.H. Won, S. Kim (Eds.), Information Security and Cryptology - ICISC 2005. XIV, 458 pages. 2006.

Vol. 3934: J.A. Clark, R.F. Paige, F.A.C. Polack, P.J. Brooke (Eds.), Security in Pervasive Computing. X, 243 pages. 2006.

Vol. 3928: J. Domingo-Ferrer, J. Posegga, D. Schreckling (Eds.), Smart Card Research and Advanced Applications. XI, 359 pages. 2006.

Vol. 3919: R. Safavi-Naini, M. Yung (Eds.), Digital Rights Management. XI, 357 pages. 2006.

Vol. 3903: K. Chen, R. Deng, X. Lai, J. Zhou (Eds.), Information Security Practice and Experience. XIV, 392 pages. 2006.

Vol. 3897: B. Preneel, S. Tavares (Eds.), Selected Areas in Cryptography. XI, 371 pages. 2006.

Vol. 3876: S. Halevi, T. Rabin (Eds.), Theory of Cryptography. XI, 617 pages. 2006.

Vol. 3866: T. Dimitrakos, F. Martinelli, P.Y.A. Ryan, S. Schneider (Eds.), Formal Aspects in Security and Trust. X, 259 pages. 2006.

Vol. 3860: D. Pointcheval (Ed.), Topics in Cryptology – CT-RSA 2006. XI, 365 pages. 2006.

Vol. 3858: A. Valdes, D. Zamboni (Eds.), Recent Advances in Intrusion Detection. X, 351 pages. 2006.

Vol. 3856: G. Danezis, D. Martin (Eds.), Privacy Enhancing Technologies. VIII, 273 pages. 2006.

Vol. 3786: J.-S. Song, T. Kwon, M. Yung (Eds.), Information Security Applications. XI, 378 pages. 2006.

Vol. 3108: H. Wang, J. Pieprzyk, V. Varadharajan (Eds.), Information Security and Privacy. XII, 494 pages. 2004.

Vol. 2951: M. Naor (Ed.), Theory of Cryptography. XI, 523 pages. 2004.

Vol. 2742: R.N. Wright (Ed.), Financial Cryptography. VIII, 321 pages. 2003.

Table of Contents

Intrusion Detection

Digital Rights Management

Symmetric-Key Cryptography

Cryptographic Protocols and Schemes

Identify-Based Cryptography

Cryptanalysis

Network Security

Software Obfuscation

Public-Key Cryptosystems

Elliptic Curves and Applications

Database Security and Privacy

Detecting System Emulators

Thomas Raffetseder, Christopher Kruegel, and Engin Kirda*

Secure Systems Lab, Technical University of Vienna, Austria
{tr,chris,ek}@seclab.tuwien.ac.at

Abstract. Malware analysis is the process of determining the behavior and purpose of a given malware sample (such as a virus, worm, or Trojan horse). This process is a necessary step to be able to develop effective detection techniques and removal tools. Security companies typically analyze unknown malware samples using simulated system environments (such as virtual machines or emulators). The reason is that these environments ease the analysis process and provide more control over executing processes. Of course, the goal of malware authors is to make the analysis process as difficult as possible. To this end, they can equip their malware programs with checks that detect whether their code is executing in a virtual environment, and if so, adjust the program's behavior accordingly. In fact, many current malware programs already use routines to determine whether they are running in a virtualizer such as VMware.

The general belief is that system emulators (such as Qemu) are more difficult to detect than traditional virtual machines (such as VMware) because they handle all instructions in software. In this paper, we seek to answer the question whether this belief is justified. In particular, we analyze a number of possibilities to detect system emulators. Our results shows that emulation can be successfully detected, mainly because the task of perfectly emulating real hardware is complex. Furthermore, some of our tests also indicate that novel technologies that provide hardware support for virtualization (such as Intel Virtualization Technology) may not be as undetectable as previously thought.

1 Introduction

The Internet has become an integral part of our lives. Today, we interact with hundreds of services, do business online, and share information without leaving the comfort of our offices or homes. Unfortunately, the Internet has turned into a hostile environment. As the importance of online commerce and business has increased, miscreants have started shifting their focus to Internet-based scams and attacks. Such attacks are easy to perform and highly profitable. A popular technique is to develop malware (such as a Trojan horse or spyware) that is installed on victims' machines. Once deployed, the malicious software can then

* This project was supported by the Austrian Science Foundation (FWF) under grants P-18157 and P-18764, the FIT-IT project Pathfinder, and the Secure Business Austria competence center.

J. Garay et al. (Eds.): ISC 2007, LNCS 4779, pp. 1–18, 2007.

be used to capture the victims' sensitive information (such as passwords or credit card numbers) and perform illegal online financial transactions.

When an unknown malware sample is obtained by a security organization such as an anti-virus company, it has to be analyzed in depth. The goal is understand the actions the malware performs, both to devise defense and detection mechanisms as well as to estimate the damage it can inflict. To perform the analysis, running the executable in a virtual machine such as the one provided by VMware [1] is a popular choice. In this case, the malware can only affect the virtual PC and not the real one[1]. A virtual environment also has the benefit that it offers tight control over program execution, allowing the analyst to pause the system at any time and inspect the contents of the memory. In addition, the analyst can make use of snapshots that capture the state of the system at a certain point in time. This allows us to observe the effects of different actions (e.g., what happens if the malware process is killed?; what happens if a certain registry key does not exist?) without having to reinstall the system after each experiment. Instead, one can just revert back to a previously stored snapshot.

Obviously, an important question is whether a malware program can detect if it is executed in a virtual environment. If malicious code can easily detect that it is running in a simulator, it could try to thwart analysis by simply changing the way it behaves. Unfortunately, it is possible to detect the presence of virtual machines (VMs) such as VMware. In fact, a number of different mechanisms have been published [2,3] that explain how a program can detect if it is run inside a VM. These checks and similar techniques are already used by malware (e.g., [4] is using a simple detection technique). Thus, the analysis results obtained by executing malicious code inside a VM become questionable. Because of the availability of checks that can identify virtual machines, there is a general belief among security professionals that software emulation is better suited for analysis than virtualization. The reason is that an emulator does not execute machine instructions directly on the hardware, but handles them in software. Also, a number of malware analysis tools (e.g., Cobra [5] or TTAnalyze [6]) have been presented recently that claim to be stealthy (that is, undetectable by malicious code) because they are based on software emulation.

In this paper, we aim to answer the question whether software emulation is as stealthy as hoped for. Unfortunately, our results show that there are several possible methods that can be used to distinguish emulated environments from a real computer. Most of these techniques aim at identifying elements of the computer hardware that are difficult to faithfully emulate in software. In addition, we developed a number of specific checks to detect Qemu [7], a popular system emulator that forms the basis for malware analysis tool such as TTAnalyze [6]. These checks allow a program to identify observable differences in the behavior of the CPU cache, the implementation of the instruction set (such as bugs present on a particular CPU), MSRs (model-specific processor registers),

[1] Note that the software emulating the PC itself may have implementation flaws that could allow malicious code to break out of the virtual PC. However, such errors are not common.