Vladimir Gorodetsky
Igor Kotenko
Victor A. Skormin (Eds.)

Communications in Computer and Information Science 1

Computer Network Security

Fourth International Conference
on Mathematical Methods, Models, and Architectures
for Computer Network Security, MMM-ACNS 2007
St. Petersburg, Russia, September 2007, Proceedings

Springer

Vladimir Gorodetsky Igor Kotenko
Victor A. Skormin (Eds.)

Computer Network Security

Fourth International Conference
on Mathematical Methods, Models, and Architectures
for Computer Network Security, MMM-ACNS 2007
St. Petersburg, Russia, September 13-15, 2007
Proceedings

Springer

Volume Editors

Vladimir Gorodetsky
Igor Kotenko
St. Petersburg Institute for Informatics and Automation
39, 14th Liniya, St. Petersburg, 199178, Russia
E-mail: {gor, ivkote}@mail.iias.spb.su

Victor A. Skormin
US Air Force, Binghamton University (SUNY)
Binghamton, NY 13902, USA
E-mail: vskormin@binghamton.edu

Library of Congress Control Number: 2007933896

CR Subject Classification (1998): C.2, D.4.6, K.4.4, H.2.8

ISSN 1865-0929
ISBN-10 3-540-73985-8 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-73985-2 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: 12101467 06/3180 5 4 3 2 1 0

Communications
in Computer and Information Science 1

Preface

This volume contains papers presented at the Fourth International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security (MMM-ACNS 2007) held in St. Petersburg, Russia, during September 13–15, 2007. The workshop was organized by the St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS) in cooperation with Binghamton University (SUNY, USA).

The organizers are proud that the MMM-ACNS workshops hosted by the St. Petersburg Institute for Informatics and Automation in 2001, 2003 and 2005 evolved into a bi-annual series recognized in the professional community. These events not only demonstrated the keen interest of the participating researchers in the subject matter and the opportunity to present and disseminate individual achievements, but also promoted the spirit of cooperation, camaraderie, free exchange of ideas, and intellectually stimulating interaction between colleagues.

Again, MMM-ACNS 2007 provided an international forum for sharing original research results among specialists in fundamental and applied problems of computer network security. An important distinction of the conference was its focus on mathematical aspects of information and computer network security addressing the ever-increasing demands for secure computing and highly dependable computer networks.

A total of 56 papers from 18 countries related to significant aspects of both theory and applications of computer network and information security were submitted to MMM-ACNS 2007. In total, 18 papers were selected for regular presentations and 12 for short presentations (32 % of acceptance for full papers and 53 % for all papers).

The MMM-ACNS 2007 program was enriched by invited papers presented by six distinguished invited speakers: Christian Collberg (University of Arizona, USA), Angelos D. Keromytis (Columbia University, USA), Paulo Verissimo (University of Lisbon, Portugal), Jean-Daniel Aussel (Gemalto, France), Mauricio Sanchez (ProCurve Networking, HP, USA) and Victor Serdiouk (DialogueScience, Inc., Russia) addressing important theoretical aspects and advanced applications.

The success of the workshop was assured by the team efforts of sponsors, organizers, reviewers and participants. We would like to acknowledge the contributions of the individual Program Committee members and thank the paper reviewers.

Our sincere gratitude goes to the participants of the workshop and all authors of the submitted papers. We are grateful to our sponsors: European Office of Aerospace Research and Development (EOARD) of the U.S. Air Force and the U.S. Office of Naval Research Global (ONRGlobal) for their generous support.

We also wish to express our gratitude to the Springer LNCS team managed by Alfred Hofmann for their help and cooperation.

September 2007

Vladimir Gorodetsky
Igor Kotenko
Victor Skormin

Organization

Workshop Chairmen

General Chairs

Rafael M. Yusupov	St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), Russia
Robert L. Herklotz	US Air Force Office of Scientific Research, USA

Program Committee Co-chairs

Vladimir Gorodetsky	St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), Russia
Igor Kotenko	St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), Russia
Victor Skormin	Binghamton University, State University of New York; National Research Council's Senior Research Associate with the Air Force, USA

Program Committee

Julien Bourgeois	University of Franche-Comte, France
David Chadwick	University of Kent, UK
Shiu-Kai Chin	Syracuse University, USA
Howard Chivers	Cranfield University, UK
Christian Collberg	University of Arizona, USA
Dipankar Dasgupta	University of Memphis, USA
Naranker Dulay	Imperial College London, UK
Dieter Gollmann	Hamburg University of Technology, Germany
Dimitris Gritzalis	Athens University of Economics and Business, Greece
Stefanos Gritzalis	University of the Aegean, Greece
Alexander Grusho	Moscow State University, Russia
Ming-Yuh Huang	The Boeing Company, USA
Sushil Jajodia	George Mason University, USA
Angelos Keromytis	Columbia University, USA
Victor Korneev	Federal Enterprise "R&D Institute "Kvant", Russia
Klaus-Peter Kossakowski	Presecure Consulting GmbH, Germany

Christopher Kruegel	Technical University of Vienna, Austria
Antonio Lioy	Politecnico di Torino, Italy
Javier Lopez	University of Malaga, Spain
Fabio Martinelli	CNR/IIT, Italy
Catherine Meadows	Naval Research Laboratory, USA
Nasir Memon	Polytechnic University Brooklyn, USA
Ann Miller	University of Missouri - Rolla, USA
Nikolay Moldovyan	Specialized Center of Program Systems "SPECTR", Russia
Wojciech Molisz	Gdansk University of Technology, Poland
David Nicol	University of Illinois at Urbana-Champaign, USA
Yoram Ofek	University of Trento, Italy
Monika Oit	Cybernetica, Estonia
Udo Prayer	IAIK, Austria
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Roland Rieke	Fraunhofer Institute for Secure Information Technology SIT, Germany
Andrei Sabelfeld	Chalmers University of Technology, Sweden)
Ravi Sandhu	George Mason University and NSD Security, USA
Antonio Gomez Skarmeta	University of Murcia, Spain
Anatol Slissenko	University Paris-12, France
Michael Smirnov	Fraunhofer-Gesellschaft Institute FOKUS, Germany
Igor Sokolov	The Institute of Informatics Problems of the Russian Academy of Sciences, Russia
Douglas Summerville	Binghamton University, USA
Shambhu Upadhyaya	University at Buffalo, USA
Alfonso Valdes	SRI International, USA
Vijay Varadharajaran	Macquarie University, Australia
Valery Vasenin	Moscow State University, Russia
Paulo Verissimo	University of Lisbon, Portugal
Diego Zamboni	IBM, Switzerland
Peter Zegzhda	St. Petersburg Polytechnical University, Russia

Reviewers

Elli Androulaki	Columbia University, USA
Daniele Beauquier	University Paris-12, France
Julien Bourgeois	University of Franche-Comte, France
David Chadwick	University of Kent, UK
Nikolaos Chatzis	Fraunhofer-Gesellschaft Institute FOKUS, Germany
Shiu-Kai Chin	Syracuse University, USA
Howard Chivers	Cranfield University, UK
Christian Collberg	University of Arizona, USA

Dipankar Dasgupta	University of Memphis, USA
Catalin Dima	University Paris-12, France
Naranker Dulay	Imperial College London, UK
Dieter Gollmann	Hamburg University of Technology, Germany
Vladimir Gorodetsky	St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, Russia
Dimitris Gritzalis	Athens University of Economics and Business, Greece
Stefanos Gritzalis	University of the Aegean, Greece
Alexander Grusho	Moscow State University, Russia
Thomas Hirsch	Fraunhofer-Gesellschaft Institute FOKUS, Germany
Ming-Yuh Huang	The Boeing Company, USA
Sushil Jajodia	George Mason University, USA
Angelos Keromytis	Columbia University, USA
Victor Korneev	Federal Enterprise "R&D Institute "Kvant", Russia
Klaus-Peter Kossakowski	Presecure Consulting GmbH, Germany
Igor Kotenko	St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, Russia
Christopher Kruegel	Technical University of Vienna, Austria
Regine Laleau	University Paris-12, France
Wei-Jen Li	Columbia University, USA
Antonio Lioy	Politecnico di Torino, Italy
Javier Lopez	University of Malaga, Spain
Fabio Martinelli	CNR/IIT, Italy
Catherine Meadows	Naval Research Laboratory, USA
Nasir Memon	Polytechnic University Brooklyn, USA
Ann Miller	University of Missouri - Rolla, USA
Nikolay Moldovyan	Specialized Center of Program Systems "SPECTR", Russia
Wojciech Molisz	Gdansk University of Technology, Poland
David Nicol	University of Illinois at Urbana-Champaign, USA
Peter Ochsenschleger	Fraunhofer Institute for Secure Information Technology SIT, Germany
Yoram Ofek	University of Trento, Italy
Monika Oit	Cybernetica, Estonia
Carla Piazza	University of Udine, Italy
Udo Prayer	IAIK, Austria
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Roland Rieke	Fraunhofer Institute for Secure Information Technology SIT, Germany

Carsten Rudolph	Fraunhofer-Gesellschaft Institute FOKUS, Germany
Alejandro Russo	Chalmers University of Technology, Sweden
Andrei Sabelfeld	Chalmers University of Technology, Sweden
Antonio Gomez Skarmeta	University of Murcia, Spain
Anatol Slissenko	University Paris-12, France
Dieter Gollmann	Hamburg University of Technology, Germany
Michael Smirnov	Fraunhofer-Gesellschaft Institute FOKUS, Germany
Yingbo Song	Columbia University, USA
Douglas Summerville	Binghamton University, USA
Shambhu Upadhyaya	University at Buffalo, USA
Alfonso Valdes	SRI International, USA
Vijay Varadharajaran	Macquarie University, Australia
Frederik Vercauteren	Katholieke Universiteit Leuven, Belgium
Paulo Verissimo	University of Lisbon, Portugal
Diego Zamboni	IBM, Switzerland
Peter Zegzhda	St. Petersburg Polytechnical University, Russia
Hang Zhao	Columbia University, USA

Author Index

Table of Contents

Invited Papers

Academia Track

Industry Track

Authentication, Authorization and Access Control

Full Papers

Short Papers

Language-Based Security, Trust Management and Covert Channels

Full Papers

Security Verification and Evaluation

Full Papers

Short Papers

Intrusion Detection and Prevention

Full Papers

Short Papers

Network Survivability and Privacy

Full Papers

Short Papers

Watermarking

Short Papers

Surreptitious Software: Models from Biology and History

Christian Collberg[1,⋆], Jasvir Nagra[2,⋆⋆], and Fei-Yue Wang[3]

[1] Department of Computer Science, University of Arizona, Tucson, AZ 85721, USA
christian@collberg.com

[2] Dipartimento di Informatica e Telecomunicazioni, University of Trento, Via Sommarive 14, 38050 Povo (Trento), Italy
jas@nagras.com

[3] Key Lab for Complex Systems and Intelligence Science, Institute of Automation, Chinese Academy of Sciences, ZhongGuanCun East Road 95, Beijing, Haidian, People's Republic of China
feiyue@gmail.com

Abstract. Over the last decade a bewildering array of techniques have been proposed to protect software from *piracy*, *malicious reverse engineering*, and *tampering*. While we can broadly classify these techniques as *obfuscation*, *watermarking/fingerprinting*, *birthmarking*, and *tamperproofing* there is a need for a more constructive taxonomy. In this paper we present a model of *Surreptitious Software* techniques inspired by defense mechanisms found in other areas: we will look at the way humans have historically protected themselves from each other and from the elements, how plants and animals have evolved to protect themselves from predators, and how secure software systems have been architected to protect against malicious attacks. In this model we identify a set of primitives which underlie many protection schemes. We propose that these primitives can be used to characterize existing techniques and can be combined to construct novel schemes which address a specific set of protective requirements.

Keywords: Software protection, defense mechanisms, taxonomy.

1 Introduction

Your computer program can contain many different kinds of secrets that you may feel need to be protected. For example, you may want to prevent a competitor from learning about a particularly elegant algorithm. You therefore *obfuscate* our program, i.e. make it so convoluted and complex that reverse engineering it becomes a daunting task. Or, you may want to bind the copy sold to each person who buys it to prevent them from illegally reselling it. You therefore *fingerprint* the program, i.e. embed a unique identifier into each copy you sell,

⋆ Supported in part by the Institute of Automation, Chinese Academy of Sciences.
⋆⋆ Supported by the European Commission, contract N° 021186-2, RE-TRUST project.

V. Gorodetsky, I. Kotenko, and V.A. Skormin (Eds.): MMM-ACNS 2007, CCIS 1, pp. 1–21, 2007.

allowing you to trace a pirated copy back to the original purchaser. Or, you may want to prevent a user from running a program after he has manipulated it, for example by removing a license check. You therefore *tamperproof* the program, i.e. make it unexecutable/self-destructing/self-repairing if it detects that its code has changed. Or, you may want to detect if part of your program has been incorporated into your competitor's program. You therefore check for *birthmarks*, unique characteristics of your code, within your competitor's code.

These techniques have collectively been referred to as *intellectual property protection of software*, or *software protection*, or *whitebox cryptography*. However, we will henceforth refer to the area as *Surreptitious Software*.

Over the last decade many algorithms have been proposed to protect secrets in programs. Seeing as the area has been (and is still) in a great deal of flux, a core set of ideas and techniques on which these algorithms are built has yet to be identified. It is the purpose of this paper to serve as a starting point for constructing such a classification scheme. Our goal is to identify a set of primitives which can be used to build algorithms protecting secrets in programs, and to use these primitives to model and classify software protection schemes that have been proposed in the literature. It is our hope that this model will provide a uniform language for researchers and practitioners, making it easier to discuss existing protection schemes and to invent new ones.

In software engineering, researchers have developed the concept of "design patterns" [1] to capture the rules-of-thumb that regularly occur during the development of large pieces of software. Garfinkel [2] also describes user-interface design patterns for security applications. The models of attacks and defenses we will describe in this paper are similar. Our motivation for identifying and classifying software protection schemes is to eliminate the need to develop new schemes from first principles. Instead we seek to model attacks and defenses that occur repeatedly so experiences and solutions can be reused. We hope that as a result, the insights gained from defending against any one instance of an attack can be generalized to the entire class of defenses.

We will seek inspiration for this model from defense mechanisms found in nature, from the way humans have protected themselves from each other and from the elements, and from protection schemes found in software systems. We will see how, since the dawn of time, plants, animals, and human societies have used surreption to protect themselves against attackers, and then see how (or if) these ideas can be applied to the intellectual property protection of software.

The model we present here is still in its infancy. In particular, to complement our model of the techniques used by the *defender* we're still working to model the techniques used by the *adversary*. Our ultimate goal is a model which will allow us to classify a proposed new software protection scheme as

1. a simple variant of another, previously published scheme, or,
2. a novel combination of two known schemes, which we can predict will have certain properties, or
3. a novel scheme not fitting the model, forcing us to reconsider the model itself.