

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

Sara Foresti Moti Yung Fabio Martinelli (Eds.)

Computer Security – ESORICS 2012

17th European Symposium
on Research in Computer Security
Pisa, Italy, September 10-12, 2012
Proceedings



Springer

Volume Editors

Sara Foresti
Università degli Studi di Milano
Dipartimento di Informatica
Via Bramante 65, 26013 Crema, Italy
E-mail: sara.foresti@unimi.it

Moti Yung
Google Inc. and
Columbia University, Computer Science Department
1214 Amsterdam Avenue, New York, NY 10025, USA
E-mail: moti@cs.columbia.edu

Fabio Martinelli
National Research Council (CNR)
Institute of Informatics and Telematics (IIT)
Information Security Group
Pisa Research Area
Via G. Moruzzi 1, 56125 Pisa, Italy
E-mail: fabio.martinelli@iit.cnr.it

ISSN 0302-9743
ISBN 978-3-642-33166-4
DOI 10.1007/978-3-642-33167-1
Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349
e-ISBN 978-3-642-33167-1

Library of Congress Control Number: 2012945787

CR Subject Classification (1998): K.6.5, E.3, D.4.6, K.4.4, C.2.0, J.1, H.4, D.2.4, H.2.7

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2012

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This volume contains the papers selected for presentation at the 17th European Symposium on Research in Computer Security (ESORICS 2012), held during September 10–12, 2012, in Pisa, Italy.

In response to the symposium’s “call for papers,” 248 papers were submitted to the conference from 43 countries. These papers were evaluated on the basis of their significance, novelty, technical quality, as well as on their practical impact or their level of advancement of the field’s foundations.

The Program Committee’s work was carried out electronically, yielding intensive discussions over a period of a few weeks. Of the papers submitted, 50 were selected for presentation at the conference (resulting in an acceptance rate of 20.16%). We note that many top-quality submissions were not selected for presentation because of the high technical level of the overall submissions, and we are certain that many of these submissions will, nevertheless, be published at other competitive forums in the future. Besides the technical program composed of the papers collated in these proceedings, the conference included three invited talks.

An event like ESORICS 2012 depends on the volunteering efforts of a host of individuals and support of numerous institutes. There is a long list of people who volunteered their time and energy to put together and organize the conference, and who deserve special thanks. Thanks to all the members of the Program Committee and the external reviewers for all their hard work in evaluating the papers. We are also very grateful to all the people whose work ensured a smooth organization process: the ESORICS Steering Committee, and its Chair Pierangela Samarati in particular, for their support; Giovanni Livraga, for taking care of publicity; Daniele Sgandurra, for maintaining the website; and the Local Organizing Committee, for helping with organization and taking care of local arrangements. We would also like to thank everyone who organized the workshops co-located with ESORICS. Special thanks are due to the keynote speakers, Gilles Barthe, Christian Cachin, and Ahmad-Reza Sadeghi, who enhanced the conference’s program by delivering illuminating talks in their respective research areas. A number of institutes deserve thanks as well: the Institute of Informatics and Telematics of National Research Council (CNR) for its support and for hosting the event, and the Dipartimento di Informatica of the Università degli Studi di Milano for its support.

Last but certainly not least, our thanks go to all the authors who submitted papers and all the symposium’s attendees. We hope you find the proceedings of ESORICS 2012 stimulating and a source of inspiration for your future research and education programs.

September 2012

Sara Foresti
Moti Yung
Fabio Martinelli

Organization

General Chair

Fabio Martinelli

National Research Council - CNR, Italy

Program Chairs

Sara Foresti

Università degli Studi di Milano, Italy

Moti Yung

Google Inc. and Columbia University, USA

Program Committee

Claudio A. Ardagna

Università degli Studi di Milano, Italy

Alessandro Armando

Università di Genova, Italy

Mikhail J. Atallah

Purdue University, USA

Michael Backes

Saarland University, Germany

David A. Basin

ETH Zurich, Switzerland

Kevin Bauer

Massachusetts Institute of Technology, USA

Joachim Biskup

University of Dortmund, Germany

Marina Blanton

University of Notre Dame, USA

Carlo Blundo

Università degli Studi di Salerno, Italy

Kevin R.B. Bulter

University of Oregon, USA

Srdjan Čapkun

ETH Zurich, Switzerland

Liqun Chen

HP Labs, UK

Seung-Geol Choi

University of Maryland, USA

Véronique Cortier

LORIA, France

Marco Cova

University of Birmingham, UK

Jason Crampton

University of London, UK

Frédéric Cuppens

Télécom Bretagne, France

Anupam Datta

Carnegie Mellon University, USA

Sabrina De Capitani di

Vimercati

Università degli Studi di Milano, Italy

Claudia Diaz

K.U. Leuven, Belgium

Sven Dietrich

Stevens Institute of Technology, USA

Roberto Di Pietro

Università di Roma Tre, Italy

Josep Domingo-Ferrer

Universitat Rovira i Virgili, Spain

Wenliang (Kevin) Du

Syracuse University, USA

Riccardo Focardi

Università Ca' Foscari di Venezia, Italy

Simon Foley

University College Cork, Ireland

Keith B. Frikken

Miami University, USA

Dieter Gollmann

TU Hamburg-Harburg, Germany

Dimitris Gritzalis
 Ryan Henry
 Amir Herzberg
 Sushil Jajodia
 Aaron Johnson
 Stefan Katzenbeisser
 KwangJo Kim
 Markulf Kohlweiss
 Michiharu Kudo
 Mirosław Kutylowski
 Adam J. Lee
 Wenke Lee
 Dongdai Lin
 Javier Lopez
 Wenjing Lou
 John C. Mitchell
 Atsuko Miyaji
 David Naccache
 Peng Ning
 Stefano Paraboschi
 Günther Pernul
 Benny Pinkas
 Michalis Polychronakis
 Jean-Jacques Quisquater
 Indrakshi Ray
 Kui Ren
 Peter Ryan
 Ahmad-Reza Sadeghi
 Rei Safavi-Naini
 Kouichi Sakurai
 Pierangela Samarati
 R. Sekar
 Elaine Shi
 Einar Snekkenes
 Abhinav Srivastava
 Carmela Troncoso
 Yevgeniy Vahlis
 Jaideep Vaidya
 Michael Waidner
 Shouhai Xu
 Ting Yu
 Jianying Zhou

AUEB, Greece
 University of Waterloo, Canada
 Bar-Ilan University, Israel
 George Mason University, USA
 U.S. Naval Research Lab, USA
 TU Darmstadt, Germany
 KAIST, Korea
 Microsoft Research, UK
 IBM Tokyo Research Laboratory, Japan
 Wroclaw University of Technology, Poland
 University of Pittsburgh, USA
 Georgia Institute of Technology, USA
 Chinese Academy of Sciences, China
 University of Malaga, Spain
 VirginiaTech, USA
 Stanford University, USA
 JAIST, Japan
 ENS, France
 North Carolina State University, USA
 Università degli Studi di Bergamo, Italy
 University of Regensburg, Germany
 Bar-Ilan University, Israel
 Columbia University, USA
 UCL Crypto Group, Belgium
 Colorado State University, USA
 Illinois Institute of Technology, USA
 University of Luxembourg, Luxembourg
 TU Darmstadt, Germany
 University of Calgary, Canada
 Kyushu University, Japan
 Università degli Studi di Milano, Italy
 Stony Brook University, USA
 PARC/UC Berkley, USA
 Gjøvik University College, Norway
 AT&T Labs - Research, USA
 K.U. Leuven, Belgium
 AT&T, USA
 Rutgers University, USA
 TU Darmstadt, Germany
 University of Texas at San Antonio, USA
 North Carolina State University, USA
 Institute for Infocomm Research, Singapore

Publicity Chair

Giovanni Livraga

Università degli Studi di Milano, Italy

Local Organizing Committee

Patrizia Andronico	National Research Council - CNR, Italy
Raffaella Casarosa	National Research Council - CNR, Italy
Adriana Lazzaroni (Chair)	National Research Council - CNR, Italy
Ilaria Matteucci	National Research Council - CNR, Italy
Paolo Mori	National Research Council - CNR, Italy
Marinella Petrocchi	National Research Council - CNR, Italy
Daniele Sgandurra	National Research Council - CNR, Italy

ESORICS Steering Committee

Michael Backes	Saarland University, Germany
Joachim Biskup	University of Dortmund, Germany
Frédéric Cuppens	Télécom Bretagne, France
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Yves Deswarte	LAAS, France
Dieter Gollmann	TU Hamburg-Harburg, Germany
Sokratis Katsikas	University of Piraeus, Greece
Mirosław Kutylowski	Wrocław University of Technology, Poland
Javier Lopez	University of Malaga, Spain
Jean-Jacques Quisquater	UCL Crypto Group, Belgium
Peter Ryan	University of Luxembourg, Luxembourg
Pierangela Samarati (Chair)	Università degli Studi di Milano, Italy
Einar Snekkenes	Gjøvik University College, Norway
Michael Waidner	TU Darmstadt, Germany

External Reviewers

Isaac Agudo	Jeffrey Bickford
Everaldo Aguiar	Norbert Bißmeyer
Hadi Ahmadi	Daniel Bleichenbacher
Mihhail Aizatulin	Jeremiah Blocki
Sadia Akhter	Eric Bodden
Joseph A. Akinyele	Andrey Bogdanov
Massimiliano Albanese	Christian Broser
Mehrdad Aliasgari	Sven Bugiel
José Bacelar Almeida	Shakeel Butt
Mashael Alsabah	Stefano Calzavara
Elena Andreeva	Roberto Carbone
Ero Balsa	Boaz Catane
Adam Bates	Aldar C-F. Chan
David Bernhard	Kai Yuen Cheong
Clara Bertolissi	Tom Chothia

Sherman Chow	Xinyi Huang
Cheng-Kang Chu	Marian Kamal Iskander
Michael Clarkson	Takamasa Isohara
Gabriele Costa	Mohammad Jafari
Cas Cremers	Limin Jia
Nora Cuppens	Jun Jiang
Paolo D'Arco	Xing Jin
Duc Dang Nguyen	Zachery Jorgensen
Luca Davi	Miltos Kandias
Alessandra De Benedictis	Yoshiaki Kasahara
Emiliano De Cristofaro	Dilsun Kaynar
Stéphanie Delaune	Aggelos Kiayias
Hua Deng	Felix Klaedtke
Rinku Dewri	Marek Klonowski
Alexandra Dmitrienko	Steve Kremer
Stelios Dritsas	Lukasz Krzywiecki
Francois Dupressoir	Dennis Kügler
Tariq Elahi	Jean Lancrenon
Nicholas Farnan	Hoi Le
Oriol Farràs	Fagen Li
Gerardo Fernandez	Giovanni Livraga
William Fitzgerald	Shoufu Luo
Andrea Forte	Tongbo Luo
Cedric Fournet	Weiliang Luo
Christoph Fritsch	Matteo Maffei
Andreas Fuchs	Krzysztof Majcher
Ludwig Fuchs	Pasquale Malacaria
Kazuhide Fukushima	Keith Martin
William Garrison	Takahiro Matsuda
Geri Georg	Toshihiko Matsuo
Wesley George	Damon McCoy
Marco Ghiglieri	Stefan Meier
Yossi Gilad	Florian Mendel
Oliver Gmelch	Alessio Merlo
Stefano Guarino	Hooman Mohajeri Moghaddam
Stuart Haber	Prashanth Mohan
Marit Hansen	Benjamin Mood
Sabri Hassan	Charles Morisset
Mitsuhiro Hattori	Francisco Moyano
Jens Hermans	Dieudonne Mulamba
Michael Herrmann	Alexios Mylonas
Shoichi Hirose	Jasvir Nagra
Yoshiaki Hori	Toru Nakanishi
Siv Hilde Houmb	Michael Netter
Jingyu Hua	Takashi Nishide

Yuan Niu
 David Nuñez
 Kazumasa Omote
 Jose A. Onieva
 Kenneth Paterson
 Constantinos Patsakis
 Thea Peacock
 Riccardo Pelizzi
 Olivier Pereira
 Cristina Pérez Solá
 Betram Poettering
 Serena Elisa Ponta
 Hannah Pruse
 Bo Qin
 Silvio Ranise
 Paul Ratazzi
 Alfredo Rial
 Moritz Riesner
 Ruben Rios
 Rodrigo Roman
 Moustafa Saleh
 Benedikt Schmidt
 Thomas Schneider
 Dominique Schroeder
 Divya Sharma
 Entong Shen
 Haya Shulman
 Hervais Simo
 Arunesh Sinha
 Yannis Soudanis
 Deian Stefan
 Martin Stopczynski
 Mikhail Strizhov
 Pierre-Yves Strub
 Chunhua Su
 Nik Sultana
 Kun Sun
 Wenhai Sun
 Nikhil Swamy

Qiang Tang
 Isamu Teranishi
 Marianthi Theoharidou
 Manachai Toahchoodee
 Mohammad Torabi Dashti
 Bill Tsoumas
 Jalaj Uphadyay
 Anthony Van Herrewege
 Serge Vaudenay
 Antonio Villani
 Nick Virvilis
 Jose L. Vivas
 Bing Wang
 Huaqun Wang
 Lusha Wang
 Wenhao Wang
 Yifei Wang
 Bogdan Warinschi
 Michael Weber
 Wei Wei
 Joel Weinberger
 Szymon Wilczek
 Qianhong Wu
 Shuang Wu
 Haixia Xu
 Jia Xu
 Peng Xu
 Rui Xue
 Filip Zagórski
 Santiago Zanella Béguelin
 Lei Zhang
 Ning Zhang
 Rui Zhang
 Tongjie Zhang
 Xiao Zhang
 Xin Zhang
 Xianfeng Zhao
 Yao Zheng

Table of Contents

Security and Data Protection in Real Systems

Modeling and Enhancing Android's Permission System	1
<i>Elli Fragkaki, Lujo Bauer, Limin Jia, and David Swasey</i>	
Hardening Access Control and Data Protection in GFS-like File Systems	19
<i>James Kelley, Roberto Tamassia, and Nikos Triandopoulos</i>	
Attack of the Clones: Detecting Cloned Applications on Android Markets	37
<i>Jonathan Crussell, Clint Gibler, and Hao Chen</i>	
Boosting the Permissiveness of Dynamic Information-Flow Tracking by Testing	55
<i>Arnar Birgisson, Daniel Hedin, and Andrei Sabelfeld</i>	

Formal Models for Cryptography and Access Control

Effective Symbolic Protocol Analysis via Equational Irreducibility Conditions	73
<i>Serdar Erbatur, Santiago Escobar, Deepak Kapur, Zhiqiang Liu, Christopher Lynch, Catherine Meadows, José Meseguer, Paliath Narendran, Sonia Santiago, and Ralf Sasse</i>	
Deciding Epistemic and Strategic Properties of Cryptographic Protocols	91
<i>Henning Schnoor</i>	
Satisfiability and Feasibility in a Relationship-Based Workflow Authorization Model	109
<i>Arif Akram Khan and Philip W.L. Fong</i>	
Deciding Security for a Fragment of ASLan	127
<i>Sebastian Mödersheim</i>	

Security and Privacy in Mobile and Wireless Networks

A Probabilistic Framework for Localization of Attackers in MANETs . . .	145
<i>Massimiliano Albanese, Alessandra De Benedictis, Sushil Jajodia, and Paulo Shakarian</i>	

Robust Probabilistic Fake Packet Injection for Receiver-Location Privacy in WSN	163
<i>Ruben Rios, Jorge Cuellar, and Javier Lopez</i>	

Privacy-Aware Message Exchanges for Geographically Routed Human Movement Networks	181
<i>Adam J. Aviv, Micah Sherr, Matt Blaze, and Jonathan M. Smith</i>	

Counteracting Man-in-the-Middle Attacks

Trust No One Else: Detecting MITM Attacks against SSL/TLS without Third-Parties	199
<i>Italo Dacosta, Mustaque Ahamad, and Patrick Traynor</i>	

X.509 Forensics: Detecting and Localising the SSL/TLS Men-in-the-Middle	217
<i>Ralph Holz, Thomas Riedmaier, Nils Kammenhuber, and Georg Carle</i>	

A Practical Man-in-the-Middle Attack on Signal-Based Key Generation Protocols	235
<i>Simon Eberz, Martin Strohmeier, Matthias Wilhelm, and Ivan Martinovic</i>	

Network Security

The Silence of the LANs: Efficient Leakage Resilience for IPsec VPNs	253
<i>Ahmad-Reza Sadeghi, Steffen Schulz, and Vijay Varadharajan</i>	

Security of Patched DNS	271
<i>Amir Herzberg and Haya Shulman</i>	

Revealing Abuses of Channel Assignment Protocols in Multi-channel Wireless Networks: An Investigation Logic Approach	289
<i>Qijun Gu, Kyle Jones, Wanyu Zang, Meng Yu, and Peng Liu</i>	

Users Privacy and Anonymity

Exploring Linkability of User Reviews	307
<i>Mishari Almishari and Gene Tsudik</i>	

Formal Analysis of Privacy in an eHealth Protocol	325
<i>Naipeng Dong, Hugo Jonker, and Jun Pang</i>	

PRIVATUS: Wallet-Friendly Privacy Protection for Smart Meters	343
<i>Jinkyu Koo, Xiaojun Lin, and Saurabh Bagchi</i>	

Location Privacy

SHARP: Private Proximity Test and Secure Handshake with Cheat-Proof Location Tags	361
<i>Yao Zheng, Ming Li, Wenjing Lou, and Y. Thomas Hou</i>	
Secure Proximity Detection for NFC Devices Based on Ambient Sensor Data	379
<i>Tzipora Halevi, Di Ma, Nitesh Saxena, and Tuo Xiang</i>	
Enhancing Location Privacy for Electric Vehicles (at the <i>Right Time</i>)	397
<i>Joseph K. Liu, Man Ho Au, Willy Susilo, and Jianying Zhou</i>	
Design and Implementation of a Terrorist Fraud Resilient Distance Bounding System	415
<i>Aanjhan Ranganathan, Nils Ole Tippenhauer, Boris Škorić, Dave Singelée, and Srdjan Čapkun</i>	

Voting Protocols and Anonymous Communication

Applying Divertibility to Blind Ballot Copying in the Helios Internet Voting System	433
<i>Yvo Desmedt and Pyrros Chaidos</i>	
Defining Privacy for Weighted Votes, Single and Multi-voter Coercion	451
<i>Jannik Dreier, Pascal Lafourcade, and Yassine Lakhnech</i>	
TorScan: Tracing Long-Lived Connections and Differential Scanning Attacks	469
<i>Alex Biryukov, Ivan Pustogarov, and Ralf-Philipp Weinmann</i>	
Introducing the gMix Open Source Framework for Mix Implementations	487
<i>Karl-Peter Fuchs, Dominik Herrmann, and Hannes Federrath</i>	

Private Computation in Cloud Systems

Secure and Efficient Outsourcing of Sequence Comparisons	505
<i>Marina Blanton, Mikhail J. Atallah, Keith B. Frikken, and Qutaibah Malluhi</i>	
Third-Party Private DFA Evaluation on Encrypted Files in the Cloud	523
<i>Lei Wei and Michael K. Reiter</i>	
New Algorithms for Secure Outsourcing of Modular Exponentiations . . .	541
<i>Xiaofeng Chen, Jin Li, Jianfeng Ma, Qiang Tang, and Wenjing Lou</i>	

Formal Security Models

Towards Symbolic Encryption Schemes	557
<i>Naveed Ahmed, Christian D. Jensen, and Erik Zenner</i>	
Decision Procedures for Simulatability	573
<i>Charanjit S. Jutla and Arnab Roy</i>	
Model-Checking Bisimulation-Based Information Flow Properties for Infinite State Systems	591
<i>Deepak D'Souza and K.R. Raghavendra</i>	

Identity Based Encryption and Group Signature

Identity-Based Traitor Tracing with Short Private Key and Short Ciphertext	609
<i>Fuchun Guo, Yi Mu, and Willy Susilo</i>	
Identity-Based Encryption with Master Key-Dependent Message Security and Leakage-Resilience	627
<i>David Galindo, Javier Herranz, and Jorge Villar</i>	
Unique Group Signatures	643
<i>Matthew Franklin and Haibin Zhang</i>	

Authentication

Relations among Notions of Privacy for RFID Authentication Protocols	661
<i>Daisuke Moriyama, Shin'ichiro Matsuo, and Miyako Ohkubo</i>	
PE(AR) ² : Privacy-Enhanced Anonymous Authentication with Reputation and Revocation	679
<i>Kin Ying Yu, Tsz Hon Yuen, Sherman S.M. Chow, Siu Ming Yiu, and Lucas C.K. Hui</i>	
Dismantling iClass and iClass Elite	697
<i>Flavio D. Garcia, Gerhard de Koning Gans, Roel Verdult, and Milosch Meriac</i>	

Encryption Key and Password Security

Evaluation of Standardized Password-Based Key Derivation against Parallel Processing Platforms	716
<i>Markus Dürmuth, Tim Güneysu, Markus Kasper, Christof Paar, Tolga Yalcin, and Ralf Zimmermann</i>	

Beyond eCK: Perfect Forward Secrecy under Actor Compromise and Ephemeral-Key Reveal	734
<i>Cas Cremers and Michèle Feltz</i>	

Bleichenbacher's Attack Strikes again: Breaking PKCS#1 v1.5 in XML Encryption	752
<i>Tibor Jager, Sebastian Schinzel, and Juraj Somorovsky</i>	

On the Security of Password Manager Database Formats	770
<i>Paolo Gasti and Kasper B. Rasmussen</i>	

Malware and Phishing

Scalable Telemetry Classification for Automated Malware Detection	788
<i>Jack W. Stokes, John C. Platt, Helen J. Wang, Joe Faulhaber, Jonathan Keller, Mady Marinescu, Anil Thomas, and Marius Gheorghescu</i>	

Abstraction-Based Malware Analysis Using Rewriting and Model Checking	806
<i>Philippe Beaucamps, Isabelle Gnaedig, and Jean-Yves Marion</i>	

Detecting Phishing Emails the Natural Language Way	824
<i>Rakesh Verma, Narasimha Shashidhar, and Nabil Hossain</i>	

Software Security

JVM-Portable Sandboxing of Java's Native Libraries	842
<i>Mengtao Sun and Gang Tan</i>	

Codejail: Application-Transparent Isolation of Libraries with Tight Program Interactions	859
<i>Yongzheng Wu, Sai Sathyanarayan, Roland H.C. Yap, and Zhenkai Liang</i>	

SOCIALIMPACT: Systematic Analysis of Underground Social Dynamics	877
<i>Ziming Zhao, Gail-Joon Ahn, Hongxin Hu, and Deepinder Mahi</i>	

Author Index	895
-------------------------------	-----