Lecture Notes in Computer Science 1525
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

David Aucsmith (Ed.)

Information Hiding

Second International Workshop, IH'98
Portland, Oregon, USA, April 14-17, 1998
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

David Aucsmith
Intel Corporation
JF3-373
Hillsboro, OR 97124-5961, USA
E-mail: awk@intel.com

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information hiding : second international workshop ; proceedings / IH '98, Portland, Oregon, USA, April 14 - 17, 1998. David Aucsmith (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1998
(Lecture notes in computer science ; Vol. 1525)
ISBN 3-540-65386-4

CR Subject Classification (1998): E.3, K.6.5, D.4.6, E.4, C.2, J.1, K.4.1, K.5.1, H.4.5, H.3.4

ISSN 0302-9743
ISBN 3-540-65386-4 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN 10692859 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Preface

The mid-1990s saw an exciting convergence of a number of different information protection technologies, whose theme was the hiding (as opposed to encryption) of information. Copyright marking schemes are about hiding either copyright notices or individual serial numbers imperceptibly in digital audio and video, as a component in intellectual property protection systems; anonymous communication is another area of rapid growth, with people designing systems for electronic cash, digital elections, and privacy in mobile communications; security researchers are also interested in 'stray' communication channels, such as those which arise via shared resources in operating systems or the physical leakage of information through radio frequency emissions; and finally, many workers in these fields drew inspiration from 'classical' hidden communication methods such as steganography and spread-spectrum radio.

The first international workshop on this new emergent discipline of information hiding was organised by Ross Anderson and held at the Isaac Newton Institute, Cambridge, from the 30th May to the 1st June 1996, and was judged by attendees to be a successful and significant event. In addition to a number of research papers, we had invited talks from David Kahn on the history of steganography and from Gus Simmons on the history of subliminal channels. We also had a number of discussion sessions, culminating in a series of votes on common terms and definitions. These papers and talks, together with minutes of the discussion, can be found in the proceedings, which are published in this series as Volume 1174.

Delegates were unanimous in their wish to have further conferences on this topic, and so the second workshop was held in Portland, Oregon, in April 1998 under my chairmanship. I was well supported by a program committee consisting of Ross Anderson (Cambridge), Steve Low (Melbourne), Ira Moskowitz (US Navy Labs), Andreas Pfitzmann (Dresden), Jean-Jacques Quisquater (Louvain), and Michael Waidner (IBM), who helped select 25 papers from 41 submissions. The standard was extremely high.

These papers cover a wider range of topics than was the case in 1996, and show how this young field is growing. Papers describe the application of copyright marks to protect banknotes, software, and circuit designs, as well as new ways of hiding data in images; how to provide anonymity in applications from file systems to biometrics; how to hide information in everything from audio and video conferencing traffic to the stray RF emanations from personal computers; some significant improvements in the art of image marking; the use for the first time of techniques such as game theory in analysing systems; and a number of practical papers showing how existing marking and hiding systems can be attacked.

The papers in this volume must stand for themselves. However, we can see three directions of growth, all of them encouraging. Firstly, the range of applications in which information hiding techniques are being used is increasing. Secondly, we are starting to understand some of the earliest applications (such as hiding copyright marks in digital images) more deeply. And thirdly, as people find interesting new ways to break some of the first-generation schemes, we are starting to see the rapid coevolution of attack and defence, which has pushed forward the state of the art in such fields as cryptography, computer security, and electronic warfare.

The future of information hiding looks extremely promising.

Finally, I would like to thank Fabien Petitcolas of Cambridge for his invaluable assistance in helping me edit these proceedings, Gary Graunke at Intel for handling the administrative arrangements for the conference, and Intel Corporation for its sponsorship of this event.

October 1998

David Aucsmith
Program Chair
Intel Architecture Labs
Portland, Oregon

Table of Contents

Steganography

Other Applications

Copyright Marking

Attacks

Theory