Lecture Notes in Computer Science 1768

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

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

Andreas Pfitzmann (Ed.)

Information Hiding

Third International Workshop, IH'99
Dresden, Germany, September 29 - October 1, 1999
Proceedings

Volume Editor

Andreas Pfitzmann
Technische Universität Dresden, Fakultät Informatik
Institut für Systemarchitektur, 01062 Dresden, Germany
E-mail: pfitza@inf.tu-dresden.de

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information hiding : third international workshop ; proceedings /
IH '99, Dresden, Germany, September 29 - October 1, 1999. Andreas
Pfitzmann (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong
Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 2000
(Lecture notes in computer science ; Vol. 1768)
ISBN 3-540-67182-X

CR Subject Classification (1998): E.3, K.6.5, K.4.1, K.5.1, D.4.6, E.4, C.2, H.4.3,
H.5.5, H.3

ISSN 0302-9743
ISBN 3-540-67182-X Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by DA-TeX Gerd Blumenstein
Printed on acid-free paper SPIN: 10719724 06/3142 5 4 3 2 1 0

Preface

Now that I have compiled these proceedings, it is a great pleasure to thank all involved.

The first thanks go to the scientific community interested in hiding information or in stopping other people doing this. At the initiative of Ross Anderson in 1995, we came together for the first international meeting at IH'96 in Cambridge, and subsequently met at IH'98 in Portland. Our community now consists of about 200 people collaborating around the world – and making remarkable progress. It is our common conviction that in the long run, much more security is achieved by open discussion and public selection of mechanisms and implementations than by ”security by obscurity”. This is especially true for large commercial systems, and it is most probably also true within the field of information hiding. Trying to hide the design and implementation of hiding mechanisms may be particularly tempting – since hiding is an issue anyway. But as shown by the breaks of quite a few digital copy- protection systems within the last few years, ”security by obscurity” may prove not to be commercially viable, at least not in civil societies.

The scientific community submitted 68 papers to this conference IH'99. This was many more papers than we had expected, and they were of much higher quality than we had dared to hope for. Many thanks to all authors.

To cope with this situation, the program committee, consisting of Ross Anderson (Cambridge University), David Aucsmith (Intel, Portland, OR), Jean-Paul Linnartz (Philips Research, Eindhoven), Steve Low (University of Melbourne), Ira Moskowitz (US Naval Research Laboratory), Jean-Jacques Quisquater (Université catholique de Louvain), Michael Waidner (IBM Research, Zurich), and me, decided to ask additional experts to help in the review of papers.

We got reviews by Christian Cachin (IBM Research, Zurich), LiWu Chang (US Naval Research Laboratory), Elke Franz (Dresden Univ. of Technology), Ton Kalker (Philips Research, Eindhoven), Herbert Klimant (Dresden Univ. of Technology), Markus Kuhn (Cambridge University), Peter Lenoir (Philips Research, Eindhoven), Thomas Mittelholzer (IBM Research, Zurich), Luke O'Connor (IBM Research, Zurich), Fabien Petitcolas (Cambridge University), Ahmad-Reza Sadeghi (Univ. des Saarlandes), Andreas Westfeld (Dresden Univ. of Technology), and Jan Zöllner (Dresden Univ. of Technology). Thanks to all program committee members and reviewers who between them contributed over 200 reviews, which I batched and delivered in anonymized form to the whole program committee. (Special thanks go to Ross Anderson for handling all reviews of papers of which I was one of the authors.)

Due to the space limitations of a three day, single stream workshop, the program committee could only accept 33 papers to allow speaker slots of 30 minutes. This meant we had – regrettably – to reject some papers which deserved acceptance. As a result, we did not provide space for an invited talk this year. To open the floor to additional ideas, we did arrange a rump session.

Within the program committee, we had quite a few discussions on the merits of borderline papers, but in the end, we achieved a consensus on the program. Many thanks to all members of the committee; it was a pleasure to work with you. It was an achievement that, in spite of a very tight schedule and many more papers than expected, we managed to finish the job and to provide feedback to all the authors three days before schedule.

IH'99 would have never become a reality without the organizational help of my secretary Martina Gersonde, who handled everything to do with accommodation, registration, printing the pre-proceedings, and organizing the various social events. During her holidays, Anja Jerichow stepped in. They and Kerstin Achtruth provided all sorts of services during the workshop. Petra Humann and Andreas Westfeld provided IT support both around and during the workshop. Hannes Federrath, being the art director of our institute in his spare time, handled all issues concerning our website and added the flavor and style to our basic functionality. As all preparation for the workshop was done completely online to avoid the costs of printing and mailing, this was especially valuable.

At this year's information hiding workshop, watermarking was the big dominating theme – at least for industry. At IH'96 and IH'98, we had a much more balanced mixture of the different fields of information hiding. I hope this will be the case again for IH'01, wherever it will take place. IH'99 could be called the "Workshop on Watermarking Resistant to Common Lossy Compression". We now know fairly well how to achieve this, but have more or less no idea how to achieve real security against well targeted attacks on watermarks. Industry's hope of copy protection by watermarking either needs a real scientific breakthrough – which I do not expect since there are so many kinds of slight changes an un-marking tool might make after the watermark has been embedded – or a more realistic perspective: systems that use copyright registration as the primary control mechanism and watermarking only as a secondary means to help keep honest people honest. If this is not commercially viable, then other means are needed to reward content providers than giving them the illusion of copy control. Perhaps as a researcher outside of industry, it falls to me to say this so frankly.

November 1999 Andreas Pfitzmann

Table of Contents

Fundamentals of Steganography

Steganography: Paradigms and Examples

Beyond Symmetric Steganography

Watermarking: Proving Ownership

Watermarking: Detection and Decoding

Watermarking: Embedding Techniques

Watermarking: New Designs and Applications

Watermarking: Improving Robustness

Watermarking and Software Protection

The Difficulty of Separating Private and Public Information

Stego-Engineering