Lecture Notes in Computer Science 1174
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Advisory Board: W. Brauer D. Gries J. Stoer

Ross Anderson (Ed.)

Information Hiding

First International Workshop
Cambridge, U.K., May 30 - June 1, 1996
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany

Juris Hartmanis, Cornell University, NY, USA

Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Ross Anderson
Cambridge University, Computer Laboratory
Pembroke Street, Cambridge CB2 3QG, UK
E-mail: rja14@cl.cam.ac.uk

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information hiding : first international workshop, Cambridge, UK, May 30 - June 1, 1996 ; proceedings / Ross Anderson (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1996
(Lecture notes in computer science ; Vol. 1174)
ISBN 3-540-61996-8
NE: Anderson, Ross [Hrsg.]; GT

CR Subject Classification (1991): E.3, K.6.5, D.4.6, E.4, C.2, J.1, K.4.1, K.5.1, H.4.3

ISSN 0302-9743
ISBN 3-540-61996-8 Springer-Verlag Berlin Heidelberg New York

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-Verlag. Violations are liable for prosecution under the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1996
Printed in Germany

Typesetting: Camera-ready by author
SPIN 10549111 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Foreword

Sometime in early 1995, I realised that there were at least five different research communities doing work on hiding information, and that they were mostly unaware of each others' existence.

Firstly, recent moves towards the digital distribution of films, music and other intellectual property have raised the question of how the ownership of digital objects can be established. One candidate technology is watermarking — embedding hidden copyright notices in digital objects to prove ownership in the event of a dispute. Doing this in ways that do not perceptibly degrade pictures or music, and yet are still hard for a pirate to remove, is an interesting technological challenge.

Secondly, a number of teams have been working on anonymous communications, digital cash, online elections and making mobile communications hard for third parties to trace. The big question here is whether the existing privacy properties of everyday transactions can be preserved in the electronic age, or whether technological progress will inevitably lead to a surveillance society.

Thirdly, computer security researchers and system builders have worried for over twenty years about covert channels — channels which arise when users of a shared resource (such as a computer operating system) can signal to each other by modulating the system's performance (e.g., by selective resource exhaustion). The concern is that a virus might use such a channel to leak information from a highly protected to a less protected part of the system. The related problem of subliminal channels in digital signature schemes, which was brought to the attention of the crypto community by Gus Simmons, has also inspired some interesting research.

Fourthly, there is steganography, in which people try to conceal the existence of messages, often in other messages. An example is when a prisoner of war spells out a message in Morse Code in the dots and dashes on the letters i, j, t and f in a letter home. This field has attracted renewed interest recently, as a result of various governments' recent attempts to ban or control the use of cryptography; programs have appeared on the Internet that let a user embed an encrypted file in a digital picture.

Finally, a number of essentially physical means of unobtrusive communication have been developed over the past fifty years or so, mainly at the instigation of the military. These include spread-spectrum and meteor scatter radio, and the use of highly directional media such as lasers.

These areas of study are closely linked, and it struck me that a workshop on the whole topic of information hiding could be timely and effective.

A suitable opportunity was given by a research programme in Computer Security, Cryptology and Coding Theory, which I was organising for the following year at the Isaac Newton Institute in Cambridge. So a programme committee was put together, consisting of myself, Robert Desourdis, Steve Low, Ira

Moskowitz, Andreas Pfitzmann, Gus Simmons and Michael Waidner — who between us covered all the above research groups; and in August 1995 we issued a call for papers.

The response far exceeded our expectations. At the workshop, which was held at the Isaac Newton Institute from the 30th May to the 1st June 1996, we heard of the latest research in a very wide range of applications, and managed to spend a significant amount of time in discussion, both formal and informal. This culminated in a closing plenary session, where we tackled the problem that everyone was using different terminology. After a long discussion and a number of votes, we arrived at some agreed terms and definitions, which are presented in the last paper in this volume.

The rest of the book consists of twenty refereed papers followed by three rump session papers. These must speak for themselves. However, we believe that this workshop will come to be seen as one of those landmark events that mark the birth of a new scientific discipline.

We would like to thank the staff at the Isaac Newton Institute, and in particular the Institute's conference secretary Mike Sekulla, for taking good care of the administrative arrangements. We are also grateful to the British government for funding the Newton programme through its Engineering and Physical Sciences Research Council; to both Trinity College and St John's College, Cambridge, for additional financial support; and to NM Rothschild for funding a visiting chair for Gus Simmons.

We plan to hold the second workshop in this series in Portland, Oregon, in April 1998.

Ross Anderson
Cambridge, September 1996

CONTENTS

The History of Steganography
David Kahn 1

Computer Based Steganography
Elke Franz, Anja Jerichow, Steffen Möller, Andreas Pfitzmann, Ingo Stierand 7

Hiding Data in the OSI Network Model
Theodore Handel, Maxwell Sandford 23

Stretching the Limits of Steganography
Ross Anderson 39

Trials of Traced Traitors
Birgit Pfitzmann 49

Establishing Big Brother Using Covert Channels and Other Covert Techniques
Yvo Desmedt 65

Covert Channels — A Context-Based View
Catherine Meadows, Ira Moskowitz 73

Covert Channel Analysis for Stubs
Mark Anderson, Maris Ozols 95

Anonymous Addresses and Confidentiality of Location
Ian Jackson 115

MIXes in Mobile Communication Systems: Location Management with Privacy
Hannes Federrath, Anja Jerichow, Andreas Pfitzmann 121

Hiding Routing Information
David Goldschlag, Michael Reed, Paul Syverson 137

The Newton Channel
Ross Anderson, Serge Vaudenay, Bart Preneel, Kaisa Nyberg 151

A Progress Report on Subliminal-Free Channels
Mike Burmester, Yvo Desmedt, Toshiya Itoh, Kouichi Sakurai, Hiroki Shizuya, Moti Yung 157

Modeling Cryptographic Protocols and their collusion analysis
Steven Low, Nicholas Maxemchuk 169

A Secure, Robust Watermark for Multimedia
Ingemar Cox, Joe Kilian, Tom Leighton, Talal Shamoon 183

Modulation and Information Hiding in Images
Joshua Smith, Barrett Comiskey 207

Watermarking Document Images with Bounding Box Expansion
Jack Brassil, Larry O'Gorman 227

The History of Subliminal Channels
Gustavus Simmons 237

Blind Decoding, Blind Undeniable Signatures, and Their Applications to Privacy Protection
Kouichi Sakurai, Yoshinori Yamane 257

Practical Invisibility in Digital Communication
Tuomas Aura 265

Fractal Based Image Steganography
Paul Davern, Michael Scott 279

Echo Hiding
Daniel Gruhl, Anthony Lu, Walter Bender 295

Tamper Resistant Software
David Aucsmith 317

Oblivious Key Escrow
Matt Blaze 335

Her Majesty's Orthography Service
Tom Berson 345

Information Hiding Terminology
Birgit Pfitzmann 347

Author Index **351**