

About the Series

This is the third in a series of booklets that SAGE is presenting to the system administration community. They are intended to fill a void in the current information structure, presenting topics in a thorough, refereed fashion, but staying small enough and flexible enough to grow with the community. Therefore, these booklets will be “living documents” that are updated as needed.

#1: Job Descriptions for System Administrators, Second Edition

Edited by Tina Darmohray

#2: A Guide to Developing Computing Policy Documents

Edited by Barbara L. Dijker

#3: System Security: A Management Perspective

By David Oppenheimer, David Wagner, and Michele D. Crabb

Edited by Dan Geer

About SAGE and USENIX

SAGE, The System Administrators Guild is a Special Technical Group within the USENIX Association dedicated to advancing the profession of systems administration.

USENIX is The Advanced Computing Systems Association.

3

Short Topics in

System Administration

System Security: A Management Perspective

David L. Oppenheimer, David A. Wagner, and Michele D. Crabb

Edited by Dan Geer

© Copyright 1997 by the USENIX Association
All Rights Reserved
ISBN 1-880446-85-5

Copies of these publications are available to members of SAGE for \$5.00 and to non-members for \$7.50. Outside the USA and Canada, please add \$3.50 per copy for postage (via printed matter).

For copies and for membership information, please contact:

The USENIX Association
2560 Ninth Street, Suite 215
Berkeley, CA 94107 USA
Telephone: 510.528.8649
Email: *office @ usenix.org*
Web: *http://www.usenix.org*

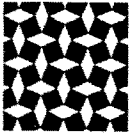
First Printing, March 1997
Second Printing, September 1997
Third Printing, July 1998

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this publication, and USENIX was aware of a trademark claim, the designations have been printed in caps or initial caps.

Printed in the United States of America, on 50% recycled paper, 10-15% post-consumer waste.

Acknowledgments

The authors offer their sincere appreciation to Barb Dijker and Dan Geer for their many helpful suggestions.



Contents

| | |
|---------------------------------------------------------------|------------|
| Foreword | vii |
| 1.0 Introduction | 1 |
| 2.0 Threats and Responses | 5 |
| 2.1 <i>Hardware Threats and Responses</i> | 5 |
| 2.2 <i>Authenticating People</i> | 12 |
| 2.3 <i>Protecting Software and Data</i> | 18 |
| 2.4 <i>Protecting Networks</i> | 31 |
| 2.5 <i>User Education and the Risks of Social Engineering</i> | 40 |
| 3.0 Financial Considerations and Risk Management | 43 |
| 3.1 <i>Identifying Your Assets</i> | 45 |
| 3.2 <i>Identifying the Threats</i> | 46 |
| 3.3 <i>Threat Frequency and Impact</i> | 49 |
| 3.4 <i>Evaluating and Testing Your Safeguards</i> | 50 |
| 3.5 <i>Formulating a Plan for Added Security</i> | 51 |
| 4.0 Trust Models | 53 |
| 5.0 Security Policies and Procedures: The Roadmap | 58 |
| 5.1 <i>Security Policies</i> | 58 |
| 5.2 <i>Policy Implementors</i> | 59 |
| 5.3 <i>Reviewing the Policy Implementation</i> | 60 |
| 5.4 <i>Assurance</i> | 61 |
| 5.5 <i>Incident Preparedness and Response</i> | 63 |
| 5.6 <i>Disaster Planning and Recovery</i> | 67 |
| 5.7 <i>Hiring Practices</i> | 70 |
| 5.8 <i>Computer Security and the Law</i> | 70 |

| | |
|---------------------------------------------------------------------------------------------|-----------|
| 6.0 The Orange Book | 72 |
| 6.1 <i>Terminology</i> | 72 |
| 6.2 <i>Orange Book Requirements</i> | 73 |
| 6.3 <i>The Trusted Product Evaluation Program</i> | 74 |
| 6.4 <i>Obtaining More Information</i> | 75 |
| 6.5 <i>Using the Orange Book to Your Advantage</i> | 75 |
| 7.0 Putting It All Altogether | 77 |
| 7.1 <i>Where Should You Begin?</i> | 77 |
| 7.2 <i>Maintaining Your Security Framework</i> | 78 |
| Appendix A: The Top Ten Computer Security Problems That Plague Organizations | 81 |
| Appendix B: Useful Computer Security Resources | 85 |
| B.1 <i>Organizations</i> | 85 |
| B.2 <i>Mailing Lists</i> | 87 |
| B.3 <i>Web Pages</i> | 89 |
| B.4 <i>USENET Newsgroups</i> | 90 |
| B.5 <i>Books</i> | 90 |

| | |
|---------------------------------------------------------------------------------------------|-----------|
| 6.0 The Orange Book | 72 |
| 6.1 <i>Terminology</i> | 72 |
| 6.2 <i>Orange Book Requirements</i> | 73 |
| 6.3 <i>The Trusted Product Evaluation Program</i> | 74 |
| 6.4 <i>Obtaining More Information</i> | 75 |
| 6.5 <i>Using the Orange Book to Your Advantage</i> | 75 |
| 7.0 Putting It All Altogether | 77 |
| 7.1 <i>Where Should You Begin?</i> | 77 |
| 7.2 <i>Maintaining Your Security Framework</i> | 78 |
| Appendix A: The Top Ten Computer Security Problems That Plague Organizations | 81 |
| Appendix B: Useful Computer Security Resources | 85 |
| B.1 <i>Organizations</i> | 85 |
| B.2 <i>Mailing Lists</i> | 87 |
| B.3 <i>Web Pages</i> | 89 |
| B.4 <i>USENET Newsgroups</i> | 90 |
| B.5 <i>Books</i> | 90 |