

S E C U R I T Y



John W. Rittinghouse
James F. Ransome

IM Security

Foreword by
Howard A. Schmidt

Elsevier Digital Press
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA
Linacre House, Jordan Hill, Oxford OX2 8DP, UK

Copyright © 2005, John W. Rittinghouse and James F. Ransome. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher.

Permissions may be sought directly from Elsevier's Science & Technology Rights Department in Oxford, UK: phone: (+44) 1865 843830, fax: (+44) 1865 853333, e-mail: permissions@elsevier.com.uk. You may also complete your request on-line via the Elsevier homepage (<http://elsevier.com>), by selecting "Customer Support" and then "Obtaining Permissions."

⊗ Recognizing the importance of preserving what has been written, Elsevier prints its books on acid-free paper whenever possible.

Library of Congress Cataloging-in-Publication Data
Application Submitted.

ISBN: 1-55558-338-5

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

For information on all Elsevier Digital Press publications
visit our Web site at www.books.elsevier.com

05 06 07 08 09 10 9 8 7 6 5 4 3 2 1

Printed in the United States of America

Contents

List of Figures and Tables	xiii
Acknowledgments	xv
Foreword	xvii
I Introduction	I
1.1 Purpose and Audience	1
1.2 What to Expect from This Book	2
1.3 What Is IM?	2
1.3.1 IM and Its History	3
1.3.2 IM as an Integrated Communications Platform	6
1.3.3 Common IM Application Approaches	7
1.3.4 Who Uses IM?	7
1.3.5 What Are the Advantages of Using IM?	11
1.3.6 What Are the Risks of Using IM?	15
1.4 Summary	27
1.5 Endnotes	27
2 How Does IM Work?	31
2.1 High-Level View of IM	31
2.1.1 The Presence Service	32
2.1.2 The Instant Messaging Service	38
2.2 Basic IM Features	40
2.3 Enterprise Instant Messaging Considerations	42
2.3.1 Operating System	42
2.3.2 Database	43
2.3.3 Directory Services	43
2.3.4 Interoperability	43

2.3.5	Schema Change Requirements	43
2.3.6	Standards Based for Third-Party Support	44
2.3.7	Compliance Management	44
2.3.8	Remote Access	44
2.3.9	Cost Considerations	44
2.4	An Enterprise EIM Nightmare Scenario	45
2.5	An Overview of Mobile and Wireless Instant Messaging	46
2.5.1	What Is Mobile Instant Messaging?	46
2.5.2	What Is Wireless Instant Messaging?	47
2.5.3	Short Message Service	47
2.5.4	Wireless Application Protocol	47
2.5.5	General Packet Radio Service	48
2.5.6	The Future of WIM	48
2.5.7	The Future of MIM	49
2.6	Selecting and Securing a WIM Solution	49
2.7	Summary	51
2.8	Endnotes	52

3 IM Standards and Protocols 53

3.1	Extensible Messaging and Presence Protocol—RFC 2778	53
3.1.1	Jabber and the IM Community	57
3.2	Jabber Protocol and XMPP	58
3.2.1	Architectural Design	59
3.3	Instant Messaging/Presence Protocol—RFC 2779	65
3.4	Session Initiation Protocol	66
3.4.1	SIP Security	68
3.4.2	Existing Security Features in the SIP Protocol	69
3.4.3	Signaling Authentication Using HTTP Digest Authentication	69
3.4.4	S/MIME Usage within SIP	69
3.4.5	Confidentiality of Media Data in SIP	70
3.4.6	TLS Usage within SIP	70
3.4.7	IPsec Usage within SIP	71
3.4.8	Security Enhancements for SIP	71
3.4.9	SIP Authenticated Identity Body	71
3.4.10	SIP Authenticated Identity Management	71
3.4.11	SIP Security Agreement	72
3.4.12	SIP End-to-Middle, Middle-to-Middle, Middle-to-End Security	73
3.4.13	SIP Security Issues	73
3.5	SIP for IM and Presence Leveraging Extensions	75

3.6	The Future of IM Standards	76
3.7	Endnotes	78
4	IM Malware	81
4.1	Overview	81
4.1.1	Instant Messaging Opens New Security Holes	83
4.1.2	Legal Risk and Unregulated Instant Messaging	85
4.2	The Use of IM as Malware	86
4.3	What Is Malware?	87
4.3.1	Viruses	88
4.3.2	Worms	88
4.3.3	Wabbits	88
4.3.4	Trojan Horses	89
4.3.5	Spyware	90
4.3.6	Browser Hijackers	90
4.3.7	Blended Threats	91
4.3.8	Backdoors	91
4.3.9	Exploits	93
4.3.10	Rootkits	93
4.4	How Is IM Used as Malware?	95
4.4.1	As a Carrier	96
4.4.2	As a Staging Center	99
4.4.3	As a Vehicle for General Hacking	100
4.4.4	As a Spy	104
4.4.5	As a Zombie Machine	107
4.4.6	As an Anonymizer	109
4.5	Summary	111
4.6	Endnotes	111
5	IM Security for Enterprise and Home	113
5.1	How Can IM Be Used Safely in Corporate Settings?	116
5.1.1	Understanding IM and Corporate Firewalls	116
5.1.2	Understanding IM File Transfers and Corporate Firewalls	119
5.1.3	Blocking and Proxying Instant Messaging	120
5.1.4	IM Detection Tools	122
5.2	Legal Risk and Corporate Governance	122
5.2.1	Legal Issues with Monitoring IM Traffic	124
5.3	Corporate IM Security Best Practices	124
5.3.1	Start from the Firewall	125
5.3.2	Consider the Desktop	125

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.