



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](mailto: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](http://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*

<b>List of Figures and Tables</b>	<b>xiii</b>
<b>Acknowledgments</b>	<b>xv</b>
<b>Foreword</b>	<b>xvii</b>
<b>I Introduction</b>	<b>I</b>
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
<b>2 How Does IM Work?</b>	<b>31</b>
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
<b>4</b>	<b>IM Malware</b>	<b>81</b>
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
<b>5</b>	<b>IM Security for Enterprise and Home</b>	<b>113</b>
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

5.3.3	Install Patches to IM Software ASAP	126
5.3.4	Enforce Client-Side IM Settings	126
5.3.5	IM Proxy Gateways	126
5.3.6	VPNs	127
5.3.7	Antivirus	128
5.3.8	Set up Containment Wards	128
5.3.9	Secure Information with Encryption	129
5.3.10	IM System Rules, Policies, and Procedures	130
5.3.11	Monitor to Ensure IM Client Policy Compliance	131
5.4	Security Risks and Solutions for Specific Public IM Clients	132
5.4.1	MSN Messenger	132
5.4.2	Yahoo! Messenger	137
5.4.3	America Online Instant Messaging	145
5.4.4	ICQ	153
5.4.5	Beware of IM Third-Party Clients and Services	156
5.5	Home IM Security Best Practices	158
5.6	Summary	161
5.7	Endnotes	161
<b>6</b>	<b>IM Security Risk Management</b>	<b>165</b>
6.1	IM Is a Form of E-mail	165
6.2	IM Security and the Law	166
6.3	Cybersecurity and the Law	169
6.3.1	The 1996 National Information Infrastructure Protection Act	170
6.3.2	President's Executive Order on Critical Infrastructure Protection	170
6.3.3	The USA Patriot Act of 2001	171
6.3.4	The Homeland Security Act of 2002	175
6.4	IM Must Be Managed as a Business Record	188
6.5	IM Risk Management	189
6.6	Summary	191
6.7	Endnotes	191
<b>7</b>	<b>The Business Value of IM</b>	<b>195</b>
7.1	Ubiquitous Presence and Workflow	195
7.2	It's All about Culture	200
7.3	Overall ROI for IM	202
7.4	The Choice Is Yours	204
7.5	Endnotes	205

<b>8</b>	<b>The Future of IM</b>	<b>207</b>
8.1	The Pervasive Network	209
8.2	Peer-to-Peer Instant Messaging	211
8.3	Peer-to-Application (the Human-Computer Interface)	211
8.4	Machine-to-Machine (Application-to-Application)	212
8.5	Jabber	214
8.6	Security and Government Compliance	215
8.7	The Business Impact	217
8.8	Endnotes	218
<b>A</b>	<b>General Network Security</b>	<b>219</b>
A.1	Threats to Personal Privacy	220
A.2	Fraud and Theft	220
A.3	Internet Fraud	221
A.4	Employee Sabotage	223
A.5	Infrastructure Attacks	224
A.6	Malicious Hackers	224
A.7	Malicious Coders	225
A.8	Industrial Espionage	225
A.9	Social Engineering	228
A.9.1	Educate Staff and Security Personnel	229
A.9.2	Crafting Corporate Social Engineering Policy	231
A.9.3	Prevention	232
A.9.4	Audits	232
A.9.5	Privacy Standards and Regulations	232
A.9.6	NAIC Model Act	233
A.9.7	Gramm-Leach-Bliley Act	234
A.9.8	HIPAA	235
A.10	Summary	237
A.11	Endnotes	238
<b>B</b>	<b>Managing Access</b>	<b>241</b>
B.1	Access Control	241
B.1.1	Purpose of Access Control	241
B.1.2	Access Control Entities	242
B.1.3	Fundamental Concepts of Access Control	242
B.1.4	Access Control Criteria	244
B.1.5	Access Control Models	244
B.1.6	Uses of Access Control	249



B.1.7	Access Control Administration Models	249
B.1.8	Access Control Mechanisms	251
B.1.9	Internal Access Controls	251
B.1.10	Techniques Used to Bypass Access Controls	256
B.2	Password Management	257
B.2.1	SmartCards	258
B.2.2	Biometric Systems	258
B.2.3	Characteristics of Good Passwords	258
B.2.4	Password Cracking	259
B.2.5	Windows NT L0phtCrack (LC4)	260
B.2.6	Password Cracking for Self-Defense	260
B.2.7	UNIX Crack	261
B.2.8	John the Ripper	262
B.2.9	Password Attack Countermeasures	263
B.3	Physical Access	263
B.4	Summary	263
B.5	Endnotes	264

## **C Security Management Issues 265**

C.1	Organizational Security Management	266
C.1.1	Perceptions of Security	266
C.1.2	Placement of a Security Group in the Organization	266
C.1.3	Security Organizational Structure	267
C.1.4	Convincing Management of the Need	268
C.1.5	Legal Responsibilities for Data Protection	268
C.1.6	DHS Office of Private Sector Liaison	269
C.2	Security Management Areas of Responsibility	269
C.2.1	Awareness Programs	270
C.2.2	Risk Analysis	271
C.2.3	Incident Handling	272
C.2.4	Alerts and Advisories	273
C.2.5	Warning Banners	274
C.2.6	Employee Termination Procedures	274
C.2.7	Training	275
C.2.8	Personnel Security	275
C.2.9	Internet Use	276
C.2.10	E-mail	276
C.2.11	Sensitive Information	276
C.2.12	System Security	277
C.2.13	Physical Security	277
C.3	Security Policies	278



C.4	Basic Approach to Policy Development	278
C.4.1	Identify What Needs Protection and Why	279
C.4.2	Determine Likelihood of Threats	279
C.4.3	Implement Protective Measures	280
C.4.4	What Makes a Good Security Policy?	281
C.4.5	Review and Assess Regularly	283
C.5	Security Personnel	283
C.5.1	Coping with Insider Threats	283
C.5.2	How to Identify Competent Security Professionals	285
C.5.3	How to Train and Certify Security Professionals	286
C.5.4	Security-Related Job Descriptions	289
C.6	Management of Security Professionals	295
C.6.1	Organizational Infrastructure	295
C.6.2	Reporting Relationships	296
C.6.3	Working Relationships	297
C.6.4	Accountability	297
C.7	Summary	298
C.8	Endnotes	298
<b>D</b>	<b>IM Policy Essentials</b>	<b>299</b>
D.1	ABC Inc. Information Security Acceptable Use Policy	300
D.2	ABC Inc. E-mail/IM Use Policy	306
D.3	ABC Inc. E-mail/IM Retention Policy	308
<b>E</b>	<b>Glossary, References, and Policy Issues</b>	<b>311</b>
E.1	IM Specific Glossary	311
E.2	General Security Glossary	316
E.3	References	342
	<b>Index</b>	<b>349</b>

### I.3.1 IM and Its History

In our fast-paced world there are times when even the rapid response of e-mail is not fast enough. There is no way for you to know if the person you are sending e-mail to is online at that moment. This is one of the reasons why IM has gained popularity, acceptance, and become a desired tool in the workplace. IM provides us with the ability to maintain a list of people, often called a buddy list or contact list, whom we want or need to interact with. IM monitors our list of people and their status of being online or offline. If they are online, we can send messages back and forth. Businesses today are increasingly viewing IM as an excellent productivity and communication tool that complements voice mail and e-mail. In order for there to be complete acceptance, there needs to be specific security, accountability, and uniformity among IM solution providers. There needs to be policies that protect critical organizational interests and comply with federal mandates and regulations. Corporations want IM solutions that provide seamless security, full audit trails, identity controls, and administrative controls. Most corporations agree that message encryption is essential.

There are three basic types of IM, as follows:

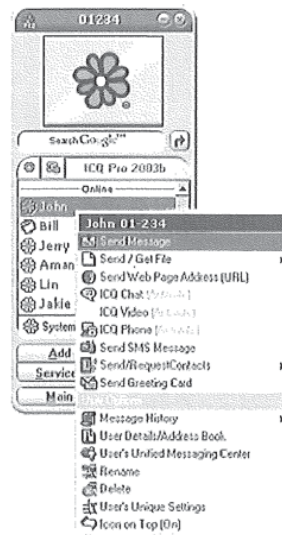
1. Public messaging
2. Enterprise messaging
3. Wireless messaging

In 1987, a computer scientist at MIT developed an instant-messaging program called Zephyr in order to provide a system that was faster than e-mail, which had begun to be bogged down, so that urgent messages regarding the school's network and server could be received instantly in case, for example, the school's network server was going down. Soon, students adopted Zephyr as a form of easy communication that could be used while they worked at their computers. This technology was quickly adopted by other universities, and the simple early warning system that Zephyr was originally designed to be was repurposed, becoming a popular tool of conversation and information exchange called IM. IM as we know it today was created in July 1996 by four young Israeli entrepreneurs. Yair Goldfinger, Arik Vardi, Sefi Vigiser, and Amnon Amir, started a company called Mirabilis in order to introduce a new way of communication over the Internet. They created a technology that would enable Internet users to locate each other online on the Internet and create peer-to-peer communi-

cation channels easily. They called their technology ICQ (I seek you) and released it in November 1996. Within six months, 850,000 users had been registered by Mirabilis. By June 1997, Mirabilis was able to handle 100,000 concurrent users and had become the world's largest Internet communications network. Mirabilis and ICQ were acquired by America Online, Inc., in June 1998 for \$287 million. AOL had also created its own Instant Messenger system. By that time, Microsoft had created its own IM client and service, MSN Messenger, and another Internet heavyweight, Yahoo!, created one as well. Because IM services evolved from proprietary systems created by companies to make a profit, their systems remain unable to interoperate because of the desire to control the IM market. AOL and ICQ, even though owned by the same company, are not interoperable. ICQ currently has two clients: ICQ4 Lite Edition with Xtraz (Figure 1.1) and ICQPro™ (Figure 1.2) [5,6].

The AOL and ICQ clients cannot communicate with one another, and AOL maintains both systems and market dominance in the IM field. All this may change soon. Conditions of the AOL-Time Warner merger required AOL to open up its IM systems [7]. In its analysis of IM, the FCC concluded that the merger would combine an essential input of AOL's dominant IM service and future IM-based services—chiefly, the Names and Presence Directory (NPD)—with assets of Time Warner, including its cable

**Figure 1.2**  
*ICQ™Pro.*



facilities and Road Runner ISP. An IM provider's NPD consists of a database of its users' unique IM names, their Internet addresses, and a "presence detection" function, which indicates to the provider that a certain user is online and allows the provider to alert others to this information. The FCC noted that these features created a market with strong network effects. AOL, with by far the largest NPD, resisted making its IM services interoperable with other providers' services. The merger brought Time Warner's cable Internet platform and content library under AOL's control and gave AOL Time Warner a significant and anticompetitive first-mover advantage in the market for advanced, IM-based high-speed services (AIHS). Potential AIHS applications include those using streaming video (lengthy, high-quality, one- or two-way video). The merger would frustrate the objectives of the Communications Act by preventing the emergence of a competitive and innovative market for advanced, IM-based services. This would violate key Communications Act principles, including the further development of healthy competition in the Internet and interactive services arena. The FCC did not establish an interoperability protocol. Rather, the FCC's remedy requires AOL Time Warner to follow a protocol developed by the industry or to create a protocol with other IM providers pursuant to contracts. Thus, the FCC did not create and will not review an Internet protocol.

The FCC imposed an "IM condition" on the merger to avert market harm now so that it would not be required to regulate IM in the future. Given AOL Time Warner's likely domination of the potentially competitive business of new, IM-based services, especially advanced, IM-based high-speed services applications, the FCC ruled that AOL Time Warner may not offer any AIHS steaming video applications that use a Names and Presence Directory (NPD) over the Internet via AOL Time Warner broadband facilities until the company demonstrates that it has satisfied one of three pro-competitive options filed by the FCC. AOL Time Warner must file a progress report with the FCC, 180 days from the release date of the order and every 180 days thereafter, describing in technical depth the actions it has taken to achieve interoperability of its IM offerings and other offerings. These reports will be placed on public notice for comment. The IM condition was set to sunset five years after the release of the order.

AOL Time Warner was directed to show that it had implemented an industry-wide standard for server-to-server interoperability. AOL Time Warner had to show that it had entered into a contract for server-to-server interoperability with at least one significant, unaffiliated provider of NPD-based services within 180 days of executing the first contract. AOL Time Warner also had to show that it entered into two additional contracts with



significant, unaffiliated, actual or potential competing providers. AOL Time Warner was given the opportunity to seek relief by showing by clear and convincing evidence that this condition no longer serves the public interest, convenience, or necessity because there has been a material change in circumstances.

Since the FCC ruling, several competing companies have joined together to advocate an IM protocol similar to those that allow the interoperability of e-mail systems. Other companies have taken a different approach rather than wait for an agreed-upon standard. Jabber is one company that has created a client program capable of communicating with various IM systems. In less than two decades, the concept of IM has become an international tool of communication.

### **1.3.2 IM as an Integrated Communications Platform**

The IM platform can be the basis for true integrated communications by incorporating additional technology (such as extending it into the wireless realm with mobile phones and personal digital assistants [PDAs]) or by adding other means of communication (such as voice chat or video chat). With the addition of IP telephony (VoIP) capability, the messaging service can even extend to telephony, making it possible to communicate with anyone at any time. It can be used as a personal communications portal to create a single point of contact for all methods of communication, allowing a user to initiate any kind of communication from one place, using a single contact list. Using IM as an integrated communications platform allows for one-click communication. Instead of having to run through a list of home, office, mobile, pager numbers, and e-mail addresses, someone trying to reach another person can simply click on that person's name. It also enables users to control how others communicate with them. If they prefer that calls go to their mobile phones when they are away from the office, they can set their profile so that the system directs calls that way. The system would route communications according to that person's preferences. When additional features such as integrated communications, reachability, and communications profiles are part of IM, the market for IM will increase from personal to professional use, creating better business markets for messaging services and making these services more of a revenue-generating opportunity for service providers [8].