Global Initiatives to Secure Cyberspace

An Emerging Landscape

Advances in Information Security

Sushil Jajodia
Consulting Editor
Center for Secure Information Systems
George Mason University
Fairfax, VA 22030-4444
email: jajodia@gmu.edu

The goals of the Springer International Series on ADVANCES IN INFORMATION SECURITY are, one, to establish the state of the art of, and set the course for future research in information security and, two, to serve as a central reference source for advanced and timely topics in information security research and development. The scope of this series includes all aspects of computer and network security and related areas such as fault tolerance and software assurance.

ADVANCES IN INFORMATION SECURITY aims to publish thorough and cohesive overviews of specific topics in information security, as well as works that are larger in scope or that contain more detailed background information than can be accommodated in shorter survey articles. The series also serves as a forum for topics that may not have reached a level of maturity to warrant a comprehensive textbook treatment.

Researchers, as well as developers, are encouraged to contact Professor Sushil Jajodia with ideas for books under this series.

Additional titles in the series:

SECURE KEY ESTABLISHMENTS by Kim-Kwang Raymond Choo; ISBN: 978-0-387-87968-0

SECURITY FOR TELECOMMUNICATIONS NETWORKS by Patrick Traynor, Patrick McDaniel and Thomas La Porta; ISBN: 978-0-387-72441-6

INSIDER ATTACK AND CYBER SECURITY: Beyond the Hacker edited by Salvatore Stolfo, Steven M. Bellovin, Angelos D. Keromytis, Sara Sinclaire, Sean W. Smith; ISBN: 978-0-387-77321-6

INTRUSION DETECTION SYSTEMS edited by Robert Di Pietro and Luigi V. Mancini; ISBN: 978-0-387-77265-3

VULNERABILITY ANALYSIS AND DEFENSE FOR THE INTERNET edited by Abhishek Singh; ISBN: 978-0-387-74389-9

BOTNET DETECTION: Countering the Largest Security Threat edited by Wenke Lee, Cliff Wang and David Dagon; ISBN: 978-0-387-68766-7

PRIVACY-RESPECTING INTRUSION DETECTION by Ulrich Flegel; ISBN: 978-0-387-68254-9

SYNCHRONIZING INTERNET PROTOCOL SECURITY (SIPSec) by Charles A. Shoniregun; ISBN: 978-0-387-32724-2

SECURE DATA MANAGEMENT IN DECENTRALIZED SYSTEMS edited by Ting Yu and Sushil Jajodia; ISBN: 978-0-387-27694-6

NETWORK SECURITY POLICIES AND PROCEDURES by Douglas W. Frye; ISBN: 0-387-30937-3

Additional information about this series can be obtained from http://www.springer.com

Global Initiatives to Secure Cyberspace

An Emerging Landscape

Edited by

Michael Portnoy
Georgia Institute of Technology
Atlanta, GA, USA

Seymour Goodman
Georgia Institute of Technology
Atlanta, GA, USA

Contributors:

Michael Portnoy, Kathleen Minor, Andrew Howard, William Lee, Richard Givens, Irene Liscano, Delphine Nain, Seymour Goodman

Springer

Editors:
Michael Portnoy
Georgia Institute of Technology
Georgia Tech Information Security Center
Sam Nunn School of Int'l Affairs
Center for International Strategy,
Technology, & Policy
781 Marietta St.
Atlanta GA 30332
mportnoy@gatech.edu

Seymour Goodman
Georgia Institute of Technology
Georgia Tech Information Security Center
Sam Nunn School of Int'l Affairs
Center for International Strategy,
Technology, & Policy
781 Marietta St.
Atlanta GA 30332
goodman@cc.gatech.edu

ISBN-13: 978-0-387-09763-3 e-ISBN-13: 978-0-387-09764-0

Library of Congress Control Number: 2008936298

© 2009 Springer Science+Business Media, LLC.
All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.
The use in this publication of trade names, trademarks, service marks and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Printed on acid-free paper

springer.com

Preface

As cyberspace continues to rapidly expand, its infrastructure is now an integral part of the world's economy and social structure. Given this increasing interconnectivity and interdependence, what progress has been made in developing an ecosystem of safety and security? This study is the second phase of an initial attempt to survey and catalog the multitude of emerging organizations promoting global initiatives to secure cyberspace.

The authors provide a breakdown and analysis of organizations by type, including international, regional, private-public, and non-governmental organizations. Concluding with a discussion of the progress made in recent years, the study explores current trends regarding the effectiveness and scope of coverage provided by these organizations and addresses several questions concerning the overall state of international cyber security.

The authors would like to thank Mr. Anthony Rutkowski for generously providing his time, guidance, and support. The authors would also like to thank the International Telecommunication Union (ITU) Telecommunication Development Sector (ITU-D) and the United States National Science Foundation (NSF Grant R3772) for partially supporting the research conducted in this study. In addition, the authors would like to thank the Georgia Institute of Technology's Center for International Strategy, Technology, and Policy (CISTP) for assistance in hosting the Cyber Security Organization Catalog, and the Georgia Tech Information Security Center (GTISC) for cooperation and promotion of this study.

Table of Contents

1 The International Landscape of Cyber Security 1

2 A Brief History of Global Responses to Cyber Threats 5
2.1 World Summit on the Information Society (WSIS) 6
2.2 Council of Europe Convention on Cybercrime 8

3 International Intergovernmental Organizations 11
3.1 United Nations (UN) 11
3.1.1 International Telecommunication Union (ITU) 11
3.1.1.1 ITU Telecommunication Standardization Sector (ITU-T) 13
3.1.1.2 ITU Telecommunication Development Sector (ITU-D) 15
3.1.1.3 ITU Radiocommunication Sector (ITU-R) 17
3.1.1.4 ITU Corporate Strategy Division (CSD) 17
3.1.1.5 WSIS Thematic Meeting on Countering Spam 18
3.1.1.6 World Trust Signatories Association (WTSA) 19
3.1.2 United Nations Office on Drugs and Crime (UNODC) 20
3.1.3 United Nations Office for Disarmament Affairs (UNODA) 21
3.2 Organisation for Economic Co-operation and Development (OECD) 22
3.3 North Atlantic Treaty Organization (NATO) 25
3.4 Group of Eight (G8) 26
3.5 World Customs Organization (WCO) 27
3.6 International Incident Response 28
3.6.1 G8 24/7 Network of Contacts for High-Tech Crime 28
3.7 International Law Enforcement Cooperation 29
3.7.1 International Criminal Police Organization (INTERPOL) 29
3.7.2 International Law Enforcement Telecommunications Seminar (ILETS) 32

4 Regional Intergovernmental Organizations 33
4.1 Europe 34
4.1.1 European Union (EU) 34
4.1.2 Council of Europe (COE) 38
4.1.3 Organization for Security and Co-operation in Europe (OSCE) 40
4.1.4 European Telecommunications Standards Institute (ETSI) 41
4.1.5 European Committee for Standardization (CEN) 42
4.1.6 ICT Standards Board (ICTSB) 43
4.1.7 European Network and Information Security Agency (ENISA) 44
4.1.8 European Incident Response 45
4.1.8.1 European Task Force on Computer Security Incident Response Teams (TF-CSIRT) 45
4.1.9 European Law Enforcement Cooperation 46

4.1.9.1 European Law Enforcement Organisation (Europol) 46
4.1.9.2 National Policing Improvement Agency (NPIA)..... 47
4.2 Asia-Pacific 48
4.2.1 Asia-Pacific Economic Cooperation (APEC)..... 48
4.2.2 Association of Southeast Asian Nations (ASEAN)..... 50
4.2.2.1 ASEAN Regional Forum (ARF)..... 50
4.2.2.2 ASEAN Telecommunications and IT Ministers (TELMIN)..... 51
4.2.3 Asia-Pacific Telecommunity (APT)..... 52
4.2.4 United Nations Economic and Social Commission for Asia and the Pacific (ESCAP)..... 53
4.2.5 China-Japan-Korea (CJK) 55
4.2.6 Asia-Pacific Incident Response..... 55
4.2.6.1 Asia Pacific Computer Emergency Response Team (APCERT) 55
4.2.7 Asia-Pacific Law Enforcement Cooperation..... 56
4.3 Americas..... 57
4.3.1 Organization of American States (OAS)..... 57
4.3.1.1 Inter-American Telecommunication Commission (CITEL) 58
4.3.2 Latin American Cooperation of Advanced Networks (CLARA) 59
4.3.2.1 CLARA Security Task Force (GT-Seg)..... 59
4.3.3 Americas Incident Response 60
4.3.3.1 Inter-American Committee Against Terrorism (CICTE)..... 60
4.3.3.2 CLARA Computer Security Incident Response Team (GT-CSIRT) 61
4.3.4 Americas Law Enforcement Cooperation 61
4.3.4.1 Group of Governmental Experts on Cyber-Crime 62

5 Private-Public and Non-Governmental Organizations (NGOs)..... 65
5.1 Advocacy Groups 65
5.1.1 Anti-Spam 65
5.1.1.1 Coalition Against Unsolicited Commercial Email (CAUCE)..... 65
5.1.1.2 London Action Plan (LAP)..... 66
5.1.1.3 Messaging Anti-Abuse Working Group (MAAWG)..... 66
5.1.1.4 Spamhaus Project..... 68
5.1.1.5 StopSpamAlliance (SSA) 68
5.1.1.6 The European Spambox Project (SPOTSPAM) 69
5.1.2 Anti-Phishing 70
5.1.2.1 Anti-Phishing Working Group (APWG) 70
5.1.3 Anti-Spyware 71
5.1.3.1 Anti-Spyware Coalition (ASC)..... 71
5.1.4 Anti-Botnets 72
5.1.4.1 International Botnet Task Force (BTF)..... 72
5.2 Incident Response 73
5.2.1 Computer Security Incident Response Teams (CSIRTs) 73
5.2.2 Forum of Incident Response and Security Teams (FIRST)..... 73

5.3 Policy, Education, & Public Awareness 74
5.3.1 Authentication and Online Trust Alliance (AOTA) 74
5.3.2 Global Information Infrastructure Commission (GIIC) 75
5.3.3 International Chamber of Commerce (ICC) 76
5.3.4 International Federation for Information Processing (IFIP) 77
5.3.5 Open Information Systems Security Group (OISSG) 78
5.3.6 Society for the Policing of Cyberspace (POLCYB) 79
5.3.7 SysAdmin, Audit, Network, Security (SANS) Institute 80
5.3.8 World Information Technology and Services Alliance (WITSA) 82
5.3.8.1 Global Internet Project (GIP) 84
5.4 Research, Development, & Standardization 85
5.4.1 3rd Generation Partnership Project (3GPP) 85
5.4.2 Central and Eastern European Networking Association (CEENet) 86
5.4.3 Cooperative Association for Internet Data Analysis (CAIDA) 86
5.4.4 GSM Association (GSMA) 87
5.4.5 Institute of Electrical and Electronics Engineers (IEEE) 88
5.4.6 International Organization for Standardization (ISO) 89
5.4.7 Internet Engineering Task Force (IETF) 91
5.4.8 Internet Research Task Force (IRTF) 91
5.4.9 Internet Society (ISOC) 92
5.4.10 Organization for the Advancement of Structured Information Standards (OASIS) 93
5.4.11 Trans-European Research and Education Networking Association (TERENA) 94
5.4.12 World Wide Web Consortium (W3C) 95

6 Making global cyberspace more secure…? 97
6.1 Further Analysis of Recent Advances in Cyber Security 97
6.2 Opportunities for Further Research 100

Appendix A – Abbreviations 103

Appendix B – Convention on Cybercrime CETS No.: 185 111

Index 115

References 123