

Preface

On behalf of the Organizing Committee, I am pleased to present to you the proceedings of the first Workshop on Insider Attack and Cyber Security held in Washington DC in June 2007. This book serves to educate all interested parties in academia, government and industry and that helps set an agenda for an ongoing research initiative to solve one of the most vexing problems encountered in securing our critical IT infrastructure, the insider threat. In some sense, the insider problem is the ultimate security problem. Insider threats, awareness and dealing with nefarious human activities in a manner that respects individual liberties, and privacy policies of organizations, while providing the best protection of critical resources and services that may be subjected to insider attack, is a very hard problem requiring a substantial effort by a large research community. We hope this book helps establish a community of researchers focused on addressing the insider problem.

The book contains a number of invited papers authored by attendees of the workshop. We believe the material that has been selected is of wide interest to the security research community. Papers have been invited that help define the nature and scope of the insider attack problem. Several papers provide an overview of technical solutions that have been proposed and discuss how they fail to solve the problem in its entirety. An essential theme of the workshop was to educate researchers as to the true nature of the problem in real-world settings. Papers are provided that describe the nature and scope of the insider problem as viewed by the financial industry. The book concludes with technical and legal challenges facing researchers who study and propose solutions to mitigate insider attacks.

We wish to thank Cliff Wang of the Army Research Office, Daniel Schutzer of the Financial Services Technology Consortium and Eric Goetz of the Institute for Information Infrastructure Protection for supporting our effort and sponsoring the Workshop, and Shari Pfleeger of Rand Corporation for providing the venue for our meeting and assistance in organizing the Workshop. We also thank the reviewers who served anonymously to vet the technical papers included here. Finally, we are especially grateful to Shlomo Hershkop and Sara Sinclair for their remarkable effort to organize and format the individual papers to produce a final cohesive manuscript.

January 2008

Salvatore J. Stolfo

<http://www.springer.com/978-0-387-77321-6>

Insider Attack and Cyber Security

Beyond the Hacker

Stolfo, S.J.; Bellovin, S.M.; Hershkop, S.; Keromytis, A.D.;

Sinclair, S.; Smith, S. (Eds.)

2008, XII, 223 p. 20 illus., Hardcover

ISBN: 978-0-387-77321-6