Spyware and Adware

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.

For a complete list of titles published in this series, go to www.springer.com/series/5576

John Aycock

Spyware and Adware

Springer

John Aycock
Department of Computer Science
University of Calgary
2500 University Drive N.W.
Calgary, Alberta, Canada T2N 1N4
aycock@ucalgary.ca

ISSN 1568-2633
ISBN 978-0-387-77740-5 e-ISBN 978-0-387-77741-2
DOI 10.1007/978-0-387-77741-2
Springer New York Dordrecht Heidelberg London

Library of Congress Control Number: 2010935807

for melissa and amanda

Contents

List of Figures

Preface

It was a dark and stormy night.

Actually, I don't remember now. What I *do* remember is that in November 2004, I sent a lone email to my department head at the University of Calgary, with a carefully-worded question: what is the department's tolerance for potentially controversial courses?

There was some historical precedent for that precise wording. I had sent him a similar email message early in 2003 as a prelude to starting my course on computer viruses and malware [26]. That course was one of a handful in the world, and I believe the only one in Canada at the time, to take a "hands-on" approach to computer viruses, where students created their own viruses and anti-virus software in a secure laboratory environment [25].

Fast-forward to 2005. Spam and spyware, the course initiated by my innocent-looking 2004 email, makes its debut [24]. It also was hands-on, and was and is, to the best of my knowledge, the only course of its kind in the world. I wish I would be proven wrong on this claim, because I think that both are important topics that should be taught to computer science students – after all, these students are the next generation of Internet defenders.

One problem I had teaching this course was the lack of good textbooks, for spyware in particular. Even in 2010, four offerings of the course later, there is still no contender. The information *is* out there, though, and this book is the result of my efforts to gather all this information together and organize it in some meaningful way.

There are three things that have been deliberately excluded from this book. First, I spend time in my class teaching about spyware-related legal aspects, and I have included none of this. The laws regarding spyware are still in flux currently, and in any case are jurisdiction-specific. Second, there is also ethics content relating to spyware in my course, but there are lots and lots of good ethics books already. Third, I am excluding certainty. While it would be great to say that spyware always does *this* and spyware never does *that*, it would be very foolish to do so. Spyware is software that can be made to do an infinite number of things, in an infinite number of ways. Instead, except when specific examples are discussed, I will stick to the *can*s

and *may*s and *could*s and *might*s that suggest the full scary potential of spyware. There are few certainties in malicious software, sorry.

I have avoided using code (except pseudocode) as much as possible in this book. The ideas and concepts are the most important things here, and I assume that the reader has enough programming experience to determine implementation specifics. Also, code tends to give books the same shelf life as a loaf of bread. I'd prefer to avoid that. Some knowledge of operating systems and networking is also useful, although I try to explain more esoteric points as needed.

Some words of caution: implementation and/or use of some techniques described in this book may not be legal in the reader's part of the world. This information is not provided to help the "bad guys," who probably already know all this anyway, but facilitate the training of the "good guys." Also note that some techniques are covered by patents. While I have made attempts to cite relevant patents when possible, their language can be very broad in scope, and it is almost certain that I have inadvertently missed some. Citations to patent applications and assigned patents are for reference purposes only and are not meant to endorse the validity of their claims.

On the topic of references, each chapter has notes that contain citations, s(n)ide comments, and extra information. To avoid disrupting the flow of the text when reading, the margins contain small circles indicating the lines that have associated notes.

I would like to thank Ken Barker and the Department of Computer Science for supporting this course to begin with. Although the details are several levels above my pay grade, I probably also owe thanks to more senior administrative people at the University of Calgary for backing my security courses too. Many thanks to all the students that have taken the course; their questions helped keep me on my toes. This book was proofread and commented on in whole or part by Angelo Borsotti, Heather Crawford, Jörg Denzinger, Shannon Jaeger, Jim Uhl, and Mike Zastre. Heather Crawford and James Ong pointed me to some helpful references, Philip Fong answered my questions about information flow control, and Jason Franklin clarified a point about a paper of his. Their collective advice has hopefully kept my details correct and my modifiers from dangling.

John Aycock