Preface

Hackers play one-up among themselves. Clearly one of the prizes would be bragging rights from hacking into my security company's Web site or my personal system.

Another would be that they had made up a story of a hack and planted it on me and my co-author Bill Simon so convincingly that we were taken in, believed it as true, and included it in this book.

That has presented a fascinating challenge, a game of wits that the two of us have played time after time as we did the interviews for the book. For most reporters and authors, establishing authenticity is a fairly routine matter: Is this really the person he or she claims to be? Is this person or was this person really working for the organization he or she claims? Did this person have the position he or she says? Does this person have documentation to back up the story, and can I verify that the documents are valid? Are there reputable people who will support the story or parts of it?

With hackers, checking the bona fides is tricky. Most of the people whose stories appear in this book, other than a few who have already been to prison, would face felony charges if their true identities could be determined. So, asking for real names, or expecting to be offered as proof, is an iffy proposition.

These people have only come forward with their stories because they trust me. They know I've done time myself, and they are willing to rely on my not betraying them in a way that could put them in that position. Yet, despite the risks, many did offer tangible proof of their hacks.

Even so, it's possible — in fact, it's likely — that some people exaggerated their stories with details intended to make them more compelling, or spun a story that was a total fabrication, but constructed around enough workable exploits to give them the ring of truth.

Because of that risk, we have been diligent in holding to a high standard of reliability. Through all the interviews, I have challenged every technical detail, asking for in-depth explanations of anything that didn't

sound quite right, and sometimes following up later to see if the story was still the same or if he or she told it differently the second time around. Or, if this person "couldn't remember" when asked about some hard-to-accomplish step omitted from the story. Or, if this person just didn't seem to know enough to do what he or she claimed or couldn't explain how he or she got from point A to point B.

Except where specifically noted, every one of the main stories in this book has passed my "smell test." My co-author and I agreed on the believability of every person whose story we have included. Nevertheless, details have often been changed to protect the hacker and the victim. In several of the stories, the identities of companies are disguised. I modified the names, industries, and locations of targeted organizations. In some cases, there is misleading information to protect the identity of the victim or to prevent a duplication of the crime. However, the basic vulnerabilities and nature of the incidents are accurate.

At the same time, because software developers and hardware manufacturers are continually fixing security vulnerabilities through patches and new product versions, few of the exploits described in these pages still work as described here. This might lead the overconfident reader to decide that he or she need not be concerned, that, with vulnerabilities attended to and corrected, the reader and his or her company have nothing to be worried about. But the lesson of these stories, whether they happened six months ago or six years ago, is that hackers are finding new vulnerabilities every day. Read the book not to learn specific vulnerabilities in specific products, but to change your attitudes and gain a new resolve.

And read the book, too, to be entertained, awed, amazed at the continually surprising exploits of these wickedly clever hackers.

Some are shocking, some are eye-opening, some will make you laugh at the inspired nerve of the hacker. If you're an IT or security professional, every story has lessons for you on making your organization more secure. If you're a non-technical person who enjoys stories of crime, daring, risk-taking, and just plain guts, you'll find all that here.

Every one of these adventures involved the danger of a knock at the door, where a posse of cops, FBI agents, and Secret Service types would be waiting with handcuffs ready. And, in a number of the cases, that's exactly what happened.

For the rest, the possibility still remains. No wonder most of these hackers have never been willing to tell their stories before. Most of these adventures you will read here are being published for the very first time.