THE ART OF INTRUSION

The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers

Kevin D. Mitnick
William L. Simon

Wiley Publishing, Inc.

THE ART OF INTRUSION

The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers

THE ART OF INTRUSION

The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers

Kevin D. Mitnick
William L. Simon

Wiley Publishing, Inc.

Vice President & Executive Group Publisher: Richard Swadley
Vice President and Executive Publisher: Bob Ipsen
Vice President and Publisher: Joseph B. Wikert
Executive Acquisitions Editor: Carol Long
Development Editors: Emilie Herman, Kevin Shafer
Editorial Manager: Kathryn Malm Bourgoine
Senior Production Editor: Angela Smith
Project Coordinator: April Farling
Copy Editor: Joanne Slike
Interior Design: Kathie S. Rickard
Text Design & Composition: Wiley Composition Services

Published by
Wiley Publishing, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Published by Wiley Publishing, Inc., Indianapolis, Indiana

Published simultaneously in Canada

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Website is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Website may provide or recommendations it may make. Further, readers should be aware that Internet Websites listed in this work may have changed or disappeared between then this work was written and when it is read.

For general information on our other products and services please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Library of Congress Cataloging-in-Publication Data:

Mitnick, Kevin D. (Kevin David), 1963-

The art of intrusion : the real stories behind the exploits of hackers, intruders, and deceivers / Kevin D. Mitnick, William L. Simon.

p. cm.

Includes index.

ISBN 0-7645-6959-7 (cloth)

1. Computer security. 2. Computer hackers. I. Simon, William L., 1930- II. Title.

QA76.9.A25M587 2005

005.8--dc22

2004025697

For Shelly Jaffe, Reba Vartanian, Chickie Leventhal,
Mitchell Mitnick

For Darci and Briannah

And for the late Alan Mitnick, Adam Mitnick,
Sydney Kramer, Jack Biello.

For Arynne, Victoria, Sheldon, and David, and for Vincent and Elena

Contents

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.

Acknowledgments

By Kevin Mitnick

This book is dedicated to my wonderful family, close friends, and, most of all, the people that made this book possible — the black-hat and white-hat hackers who contributed their stories for our education and entertainment.

The Art of Intrusion was even more challenging to write than our last book. Instead of using our combined creative talent to develop stories and anecdotes to illustrate the dangers of social engineering and what businesses can do to mitigate it, both Bill Simon and I relied heavily on interviewing former hackers, phone phreaks, and hackers turned security professionals. We wanted to write a book that would be both a crime thriller and an eye-opening guide to helping businesses protect their valuable information and computing resources. We strongly believe that by disclosing the common methodologies and techniques used by hackers to break into systems and networks, we can influence the community at large to adequately address these risks and threats posed by savvy adversaries.

I have had the extraordinary fortune of being teamed up with best-selling author Bill Simon, and we worked diligently together on this new book. Bill's notable skills as a writer include his magical ability to take information provided by our contributors and write it in such a style and manner that anyone's grandmother could understand it. More importantly, Bill has become more than just a business partner in writing, but a loyal friend who has been there for me during this whole development process. Although we had some moments of frustration and differences of opinion during the development phase, we always work it out to our mutual satisfaction. In a little over two years, I'll finally be able to write and publish the *The Untold Story of Kevin Mitnick,* after certain government restrictions expire. Hopefully, Bill and I will collaborate on this project as well.

Bill's wonderful wife, Arynne Simon, also has a warm place in my heart. I appreciate her love, kindness, and generosity that she has shown me in the last three years. My only disappointing experience is not being able to enjoy her great cooking. Now that the book is finally finished, maybe I can convince her to cook a celebration dinner!

Having been so focused on *The Art of Intrusion,* I haven't been able to spend much quality time with family and close friends. I became somewhat of a workaholic, similar to the days where I'd spend countless hours behind the keyboard exploring the dark corners of cyberspace.

I want to thank my loving girlfriend, Darci Wood, and her game-loving daughter Briannah for being supportive and patient during this time-consuming project. Thank you, baby, for all your love, dedication, and support that you and Briannah have provided me while working on this and other challenging projects.

This book would not have been possible without the love and support of my family. My mother, Shelly Jaffe, and my grandmother, Reba Vartanian, have given me unconditional love and support throughout my life. I am so fortunate to have been raised by such a loving and dedicated mother, who I also consider my best friend. My grandmother has been like a second mom to me, providing me with the same nurturing and love that usually only a mother can give. She has been extremely helpful in handling some of my business affairs, which at times interfered with her schedule. In every instance, she made my business a top priority, even when it was inconvenient to do so. Thank you, Gram, for helping me get the job done whenever I needed you. As caring and compassionate people, they've taught me the principles of caring about others and lending a helping hand to the less fortunate. And so, by imitating the pattern of giving and caring, I, in a sense, follow the paths of their lives. I hope they'll forgive me for putting them on the back burner during the process of writing this book, passing up chances to see them with the excuse of work and deadlines to meet. This book would not have been possible without their continued love and support that I'll forever hold close to my heart.

How I wish my Dad, Alan Mitnick, and my brother, Adam Mitnick, would have lived long enough to break open a bottle of champagne with me on the day our second book first appears in a bookstore. As a salesman and business owner, my father taught me many of the finer things that I will never forget.

My mother's late boyfriend, Steven Knittle, has been a father figure to me for the past 12 years. I took great comfort knowing that you were always there to take care of my mom when I could not. Your passing has had a profound impact on our family and we miss your humor, laughter, and the love you brought to our family. RIP.

My aunt Chickie Leventhal will always have a special place in my heart. Over the last couple years, our family ties have been strengthened, and our communication has been wonderful. Whenever I need advice or a place to stay, she is always there offering her love and support. During my intense devotion to writing this book, I sacrificed many opportunities to join her, my cousin, Mitch Leventhal, and her boyfriend, Dr. Robert Berkowitz, for our family get-togethers.

My friend Jack Biello was a loving and caring person who spoke out against the extraordinary mistreatment I endured at the hands of journalists and government prosecutors. He was a key voice in the Free Kevin movement and a writer who had an extraordinary talent for writing compelling articles exposing the information that the government didn't want you to know. Jack was always there to fearlessly speak out on my behalf and to work together with me preparing speeches and articles, and, at one point, represented me as a media liaison. While finishing up the manuscript for *The Art of Deception* (Wiley Publishing, Inc., 2002), Jack's passing left me feeling a great sense of loss and sadness. Although it's been two years, Jack is always in my thoughts.

One of my closest friends, Caroline Bergeron, has been very supportive of my endeavor to succeed on this book project. She is a lovely and brilliant soon-to-be lawyer living in the Great White North. Having met her during one of my speaking engagements in Victoria, we hit it off right away. She lent her expertise to proofreading, editing, and correcting the two-day social engineering seminar that Alex Kasper and I developed. Thank you, Caroline, for being there for me.

My colleague Alex Kasper is not only my best friend but also my colleague; we are currently working on delivering one-day and two-day seminars on how businesses can recognize and defend against social engineering attacks. Together we hosted a popular Internet talk radio show known as "The Darkside of the Internet" on KFI radio in Los Angeles. You have been a great friend and confidant. Thank you for your invaluable assistance and advice. Your influence has always been positive and helpful with a kindness and generosity that often extended far beyond the norm.

Paul Dryman has been a family friend for many, many years. Paul was my late father's best friend. After my dad's passing, Paul has been a father figure, always willing to help and talk with me about anything on my mind. Thank you, Paul, for your loyal and devoted friendship to my father and I for so many years.

Amy Gray has managed my speaking career for the last three years. Not only do I admire and adore her personality, but I value how she treats other people with such respect and courtesy. Your support and dedication to professionalism has contributed to my success as a public speaker and trainer. Thank you so much for your continued friendship and your commitment to excellence.

Attorney Gregory Vinson was on my defense team during my years-long battle with the government. I'm sure he can relate to Bill's understanding and patience for my perfectionism; he has had the same experience working with me on legal briefs he has written on my behalf. Gregory is now my business attorney diligently working with me on new contracts and negotiating business deals. Thank you for your wonderful support and diligent work, especially when needed on short notice.

Eric Corley (aka Emmanuel Goldstein) has been an active supporter and close friend for over a decade. He has always looked out for my best interest and has publicly defended me when I was demonized by Miramax Films and certain other journalists. Eric has been extremely instrumental in getting the *word* out during the government's prosecution of me. Your kindness, generosity, and friendship mean more to me than words can express. Thank you for being a loyal and trusted friend.

Steve Wozniak and Sharon Akers have given much of their time to assist me and are always there to help me out. The frequent rearranging of your schedules to be there to support me is much appreciated and it warms me to call both of you my friends. Hopefully, now that this book is completed, we will have more time to get together for some gadget quality time. Steve — I'll never forget the time that you, Jeff Samuels, and I drove through the night in your Hummer to get to DEFCON in Las Vegas, switching drivers constantly so that we could all check our e-mail and chat with friends over our GPRS wireless connections.

And as I write these acknowledgments, I realize I have so many people to thank and to express appreciation to for offering their love, friendship, and support. I cannot begin to remember the names of all the kind and generous people that I've met in recent years, but suffice to say, I would need a large USB flash drive to store them all. There have been so many people from all over the world who have written me words of encouragement, praise, and support. These words have meant a great deal to me, especially during the times I needed it most.

I'm especially thankful to all my supporters who stood by me and spent their valuable time and energy getting the word out to anyone that would listen, voicing their concern and objection over my unfair treatment and the hyperbole created by those who sought to profit from the "The Myth of Kevin Mitnick."

I'm eager to thank those people who represent my professional career and are dedicated in extraordinary ways. David Fugate, of Waterside Productions, is my book agent who went to bat for me on many occasions before and after the book contract was signed.

I very much appreciate the opportunity that John Wiley & Sons has given me to author another book, and for their confidence in our ability to develop a best seller. I wish to thank the following Wiley people who made this dream possible: Ellen Gerstein; Bob Ipsen; Carol Long, who always promptly responds to my questions and concerns (my number one contact at Wiley and executive editor); and Emilie Herman and Kevin Shafer (developmental editors), who have both worked with us as a team to get the job done.

I have had too many experiences with lawyers, but I am eager to have a place to express my thanks for the lawyers who, during the years of my negative interactions with the criminal justice system, stepped up and offered to help me when I was in desperate need. From kind words to deep involvement with my case, I met many who don't at all fit the stereotype of the self-centered attorney. I have come to respect, admire, and appreciate the kindness and generosity of spirit given to me so freely by so many. They each deserve to be acknowledged with a paragraph of favorable words; I will at least mention them all by name, for every one of them lives in my heart surrounded by appreciation: Greg Aclin, Fran Campbell, Lauren Colby, John Dusenbury, Sherman Ellison, Omar Figueroa, Jim French, Carolyn Hagin, Rob Hale, David Mahler, Ralph Peretz, Alvin Michaelson, Donald C. Randolph, Alan Rubin, Tony Serra, Skip Slates, Richard Steingard, Honorable Robert Talcott, Barry Tarlow, John Yzurdiaga, and Gregory Vinson.

Other family members, personal friends, business associates who have given me advice and support, and have reached out in many ways, are important to recognize and acknowledge. They are JJ Abrams, Sharon Akers, Matt "NullLink" Beckman, Alex "CriticalMass" Berta, Jack Biello, Serge and Susanne Birbrair, Paul Block, Jeff Bowler, Matt "404" Burke, Mark Burnett, Thomas Cannon, GraceAnn and Perry Chavez, Raoul Chiesa, Dale Coddington, Marcus Colombano, Avi Corfas, Ed Cummings, Jason "Cypher" Satterfield, Robert Davies, Dave Delancey, Reverend Digital, Oyvind Dossland, Sam Downing, John Draper, Ralph Echemendia, Ori Eisen, Roy Eskapa, Alex Fielding, Erin Finn, Gary Fish and Fishnet Security, Lisa Flores, Brock Frank, Gregor Freund, Sean Gailey and the whole Jinx crew, Michael and Katie Gardner, Steve Gibson, Rop Gonggrijp, Jerry Greenblatt, Thomas Greene, Greg Grunberg, Dave Harrison, G. Mark Hardy, Larry Hawley, Leslie Herman, Michael Hess and everyone at Roadwired bags, Jim Hill, Ken Holder, Rochell Hornbuckle, Andrew "Bunnie" Huang, Linda Hull, Steve Hunt, all the great people at IDC, Marco Ivaldi, Virgil Kasper, Stacey Kirkland, Erik Jan Koedijk, the Lamo Family, Leo and Jennifer Laporte, Pat Lawson, Candi Layman, Arnaud Le-hung, Karen Leventhal, Bob Levy, David and Mark Litchfield, CJ Little, Jonathan Littman, Mark Loveless, Lucky 225, Mark Maifrett, Lee Malis, Andy Marton, Lapo Masiero, Forrest McDonald, Kerry McElwee, Jim "GonZo" McAnally, Paul and Vicki Miller, Elliott Moore, Michael Morris, Vincent, Paul and Eileen Navarino, Patrick and Sarah Norton, John Nunes, Shawn Nunley, Janis Orsino, Tom Parker, Marco Plas, Kevin and Lauren Poulsen, Scott Press, Linda and Art Pryor, Pyr0, John Rafuse, Mike Roadancer and the entire security crew from HOPE 2004, RGB, Israel and Rachel Rosencrantz, Mark Ross, Bill Royle, William Royer, Joel "ch0l0man" Ruiz, Martyn Ruks, Ryan Russell, Brad Sagarin, Martin Sargent, Loriann Siminas, Te Smith, Dan Sokol, Trudy Spector, Matt Spergel, Gregory Spievack, Jim and Olivia Sumner, Douglas Thomas, Cathy Von, Ron Wetzel, Andrew Williams, Willem, Don David Wilson, Joey Wilson, Dave and Dianna Wykofka, and all my friends and supporters from the boards on Labmistress.com and *2600* magazine.

By Bill Simon

In doing our first book, *The Art of Deception*, Kevin Mitnick and I forged a friendship. While writing this one, we continually found new ways of working together while deepening our friendship. So, my first words of appreciation go to Kevin for being an outstanding "travel companion" as we shared this second journey.

David Fugate, my agent at Waterside Productions and the man responsible for bringing Kevin and me together in the first place, tapped into his usual store of patience and wisdom to find ways of solving those few miserable situations that cropped up. When the going gets tough, every writer should be blessed with an agent who is as wise and as good a friend. Ditto for my longtime friend Bill Gladstone, the founder of Waterside Productions and my principal agent. Bill remains a key factor in the success of my writing career and has my everlasting gratitude.

My wife Arynne continues to inspire me anew each day with her love and her dedication to excellence; I appreciate her more than I can say in words. She has increased my proficiency as a writer because of her intelligence and willingness to be forthright by telling me straight out when

my writing has missed the mark. Somehow she gets through the steam of wrath that is my usual initial response to her suggestions, but in the end I accept the wisdom of her suggestions and do the rewrite.

Mark Wilson lent a helping hand that made a difference. Emilie Herman was a champion of an editor. And I can't overlook the work of Kevin Shafer, who took over after Emilie left.

Even a sixteenth book accumulates a debt to people who along the way have been more than a little helpful; of the many, I especially want to mention Kimberly Valentini and Maureen Maloney of Waterside, and Josephine Rodriguez. Marianne Stuber did her usual fast turnaround transcribing (not easy with all those strange technical terms and hacker slang) and Jessica Dudgeon kept the office on an even keel. Darci Wood was a champ about the time her Kevin dedicated to getting this book done.

Special thanks to daughter Victoria and son Sheldon for their understanding, and to my twin grandchildren Vincent and Elena, all of whom I trust I will be able to see more once this manuscript is delivered.

To the many who offered us stories, and especially to those whose compelling stories we chose to use, Kevin and I are deeply indebted. They came forward despite significant risks. Had their names been revealed, in many cases they would have faced being dragged away by the men in blue. Even those whose stories weren't used showed courage in their willingness to share, and deserve to be admired for it. We do, indeed, admire them.

Chapter 1

Hacking the Casinos for a Million Bucks

Every time [some software engineer] says, "Nobody will go to the trouble of doing that," there's some kid in Finland who will go to the trouble.

— Alex Mayfield

There comes a magical gambler's moment when simple thrills magnify to become 3-D fantasies — a moment when greed chews up ethics and the casino system is just another mountain waiting to be conquered. In that single moment the idea of a foolproof way to beat the tables or the machines not only kicks in but kicks one's breath away.

Alex Mayfield and three of his friends did more than daydream. Like many other hacks, this one started as an intellectual exercise just to see if it looked possible. In the end, the four actually beat the system, taking the casinos for "about a million dollars," Alex says.

In the early 1990s, the four were working as consultants in high-tech and playing life loose and casual. "You know — you'd work, make some money, and then not work until you were broke."

Las Vegas was far away, a setting for movies and television shows. So when a technology firm offered the guys an assignment to develop some software and then accompany it to a trade show at a high-tech convention there, they jumped at the opportunity. It would be the first in Vegas for each of them, a chance to see the flashing lights for themselves, all expenses paid; who would turn that down? The separate suites for each in a major hotel meant that Alex's wife and Mike's girlfriend could be included in the fun. The two couples, plus Larry and Marco, set off for hot times in Sin City.

Alex says they didn't know much about gambling and didn't know what to expect. "You get off the plane and you see all the old ladies playing the slots. It seems funny and ironic, and you soak that in."

After the four had finished doing the trade show, they and the two ladies were sitting around in the casino of their hotel playing slot machines and enjoying free beers when Alex's wife offered a challenge:

> *"Aren't these machines based on computers? You guys are into computers, can't you do something so we win more?"*

The guys adjourned to Mike's suite and sat around tossing out questions and offering up theories on how the machines might work.

Research

That was the trigger. The four "got kinda curious about all that, and we started looking into it when we got back home," Alex says, warming up to the vivid memories of that creative phase. It took only a little while for the research to support what they already suspected. "Yeah, they're computer programs basically. So then we were interested in, was there some way that you could crack these machines?"

There were people who had beaten the slot machines by "replacing the firmware" — getting to the computer chip inside a machine and substituting the programming for a version that would provide much more attractive payoffs than the casino intended. Other teams had done that, but it seemed to require conspiring with a casino employee, and not just any employee but one of the slot machine techies. To Alex and his buddies, "swapping ROMs would have been like hitting an old lady over the head and taking her purse." They figured if they were going to try this, it would be as a challenge to their programming skills and their intellects. And besides, they had no advanced talents in social engineering; they were computer guys, lacking any knowledge of how you sidle up to a casino employee and propose that he join you in a little scheme to take some money that doesn't belong to you.

But how would they begin to tackle the problem? Alex explained:

> *We were wondering if we could actually predict something about the sequence of the cards. Or maybe we could find a back door [software code allowing later unauthorized access to the program] that some programmer may have put in for his own benefit. All programs are written by programmers, and programmers are*

> *mischievous creatures. We thought that somehow we might stumble on a back door, such as pressing some sequence of buttons to change the odds, or a simple programming flaw that we could exploit.*

Alex read the book *The Eudaemonic Pie* by Thomas Bass (Penguin, 1992), the story of how a band of computer guys and physicists in the 1980s beat roulette in Las Vegas using their own invention of a "wearable" computer about the size of a pack of cigarettes to predict the outcome of a roulette play. One team member at the table would click buttons to input the speed of the roulette wheel and how the ball was spinning, and the computer would then feed tones by radio to a hearing aid in the ear of another team member, who would interpret the signals and place an appropriate bet. They should have walked away with a ton of money but didn't. In Alex's view, "Their scheme clearly had great potential, but it was plagued by cumbersome and unreliable technology. Also, there were many participants, so behavior and interpersonal relations were an issue. We were determined not to repeat their mistakes."

Alex figured it should be easier to beat a computer-based game "because the computer is completely deterministic" — the outcome based on by what has gone before, or, to paraphrase an old software engineer's expression, good data in, good data out. (The original expression looks at this from the negative perspective: "garbage in, garbage out.")

This looked right up his alley. As a youngster, Alex had been a musician, joining a cult band and dreaming of being a rock star, and when that didn't work out had drifted into the study of mathematics. He had a talent for math, and though he had never cared much for schooling (and had dropped out of college), he had pursued the subject enough to have a fairly solid level of competence.

Deciding that some research was called for, he traveled to Washington, DC, to spend some time in the reading room of the Patent Office. "I figured somebody might have been stupid enough to put all the code in the patent" for a video poker machine. And sure enough, he was right. "At that time, dumping a ream of object code into a patent was a way for a patent filer to protect his invention, since the code certainly contains a very complete description of his invention, but in a form that isn't terribly user-friendly. I got some microfilm with the object code in it and then scanned the pages of hex digits for interesting sections, which had to be disassembled into [a usable form]."

Analyzing the code uncovered a few secrets that the team found intriguing, but they concluded that the only way to make any real progress would be to get their hands on the specific type of machine they wanted to hack so they could look at the code for themselves.

As a team, the guys were well matched. Mike was a better-than-competent programmer, stronger than the other three on hardware design. Marco, another sharp programmer, was an Eastern European immigrant who looked like a teenager. But he was something of a daredevil, approaching everything with a can-do, smart-ass attitude. Alex excelled at programming and was the one who contributed the knowledge of cryptography they would need. Larry wasn't much of a programmer and because of a motorcycle accident couldn't travel much, but was a great organizer who kept the project on track and everybody focused on what needed to be done at each stage.

After their initial research, Alex "sort of forgot about" the project. Marco, though, was hot for the idea. He kept insisting, "It's not that big a deal, there's thirteen states where you can legally buy machines." Finally he talked the others into giving it a try. "We figured, what the hell." Each chipped in enough money to bankroll the travel and the cost of a machine. They headed once again for Vegas — this time at their own expense and with another goal in mind.

Alex says, "To buy a slot machine, basically you just had to go in and show ID from a state where these machines are legal to own. With a driver's license from a legal state, they pretty much didn't ask a lot of questions." One of the guys had a convenient connection to a Nevada resident. "He was like somebody's girlfriend's uncle or something, and he lived in Vegas."

They chose Mike as the one to talk to this man because "he has a sales-y kind of manner, a very presentable sort of guy. The assumption is that you're going to use it for illegal gambling. It's like guns," Alex explained. A lot of the machines get *gray-marketed* — sold outside accepted channels — to places like social clubs. Still, he found it surprising that "we could buy the exact same production units that they use on the casino floor."

Mike paid the man 1,500 bucks for a machine, a Japanese brand. "Then two of us put this damn thing in a car. We drove it home as if we had a baby in the back seat."

Developing the Hack

Mike, Alex, and Marco lugged the machine upstairs to the second floor of a house where they had been offered the use of a spare bedroom. The thrill of the experience would long be remembered by Alex as one of the most exciting in his life.

> *We open it up, we take out the ROM, we figure out what processor it is. I had made a decision to get this Japanese machine that looked like a knockoff of one of the big brands. I just figured the*

> *engineers might have been working under more pressure, they might have been a little lazy or a little sloppy.*
>
> *It turned out I was right. They had used a 6809 [chip], similar to a 6502 that you saw in an Apple II or an Atari. It was an 8-bit chip with a 64K memory space. I was an assembly language programmer, so this was familiar.*

The machine Alex had chosen was one that had been around for some 10 years. Whenever a casino wants to buy a machine of a new design, the Las Vegas Gaming Commission has to study the programming and make sure it's designed so the payouts will be fair to the players. Getting a new design approved can be a lengthy process, so casinos tend to hold on to the older machines longer than you would expect. For the team, an older machine seemed likely to have outdated technology, which they hoped might be less sophisticated and easier to attack.

The computer code they downloaded from the chip was in binary form, the string of 1's and 0's that is the most basic level of computer instructions. To translate that into a form they could work with, they would first have to do some *reverse engineering* — a process an engineer or programmer uses to figure out how an existing product is designed; in this case it meant converting from machine language to a form that the guys could understand and work with.

Alex needed a *disassembler* to translate the code. The foursome didn't want to tip their hand by trying to purchase the software — an act they felt would be equivalent to going into your local library and trying to check out books on how to build a bomb. The guys wrote their own disassembler, an effort that Alex describes as "not a piece of cake, but it was fun and relatively easy."

Once the code from the video poker machine had been run through the new disassembler, the three programmers sat down to pour over it. Ordinarily it's easy for an accomplished software engineer to quickly locate the sections of a program he or she wants to focus on. That's because a person writing code originally puts road signs all through it — notes, comments, and remarks explaining the function of each section, something like the way a book may have part titles, chapter titles, and subheadings for sections within a chapter.

When a program is compiled into the form that the machine can read, these road signs are ignored — the computer or microprocessor has no need for them. So code that has been reverse-engineered lacks any of these useful explanations; to keep with the "road signs" metaphor, this recovered code is like a roadmap with no place names, no markings of highways or streets.

They sifted through the pages of code on-screen looking for clues to the basic questions: "What's the logic? How are the cards shuffled? How are replacement cards picked?" But the main focus for the guys at this juncture was to locate the code for the random number generator (RNG). Alex's guess that the Japanese programmers who wrote the code for the machine might have taken shortcuts that left errors in the design of the random number generator turned out to be correct; they had.

Rewriting the Code

Alex sounds proud in describing this effort. "We were programmers; we were good at what we did. We figured out how numbers in the code turn into cards on the machine and then wrote a piece of C code that would do the same thing," he said, referring to the programming language called "C."

> *We were motivated and we did a lot of work around the clock. I'd say it probably took about two or three weeks to get to the point where we really had a good grasp of exactly what was going on in the code.*
>
> *You look at it, you make some guesses, you write some new code, burn it onto the ROM [the computer chip], put it back in the machine, and see what happens. We would do things like write routines that would pop hex [hexadecimal] numbers on the screen on top of the cards. So basically get a sort of a design overview of how the code deals the cards.*
>
> *It was a combination of trial and error and top-down analysis; the code pretty quickly started to make sense. So we understood everything about exactly how the numbers inside the computer turn into cards on the screen.*
>
> *Our hope was that the random number generator would be relatively simple. And in this case in the early 90's, it was. I did a little research and found out it was based on something that Donald Knuth had written about in the 60's. These guys didn't invent any of this stuff; they just took existing research on Monte Carlo methods and things, and put it into their code.*
>
> *We figured out exactly what algorithm they were using to generate the cards; it's called a linear feedback shift register, and it was a fairly good random number generator.*

But they soon discovered the random number generator had a fatal flaw that made their task much easier. Mike explained that "it was a relatively simple 32-bit RNG, so the computational complexity of cracking it was within reach, and with a few good optimizations became almost trivial."

So the numbers produced were not truly random. But Alex thinks there's a good reason why this has to be so:

> *If it's truly random, they can't set the odds. They can't verify what the odds really are. Some machines gave sequential royal flushes. They shouldn't happen at all. So the designers want to be able to verify that they have the right statistics or they feel like they don't have control over the game.*
>
> *Another thing the designers didn't realize when they designed this machine is that basically it's not just that they need a random number generator. Statistically there's ten cards in each deal — the five that show initially, and one alternate card for each of those five that will appear if the player chooses to discard. It turns out in these early versions of the machine, they basically took those ten cards from ten sequential random numbers in the random number generator.*

So Alex and his partners understood that the programming instructions on this earlier-generation machine were poorly thought out. And because of these mistakes, they saw that they could write a relatively simple but elegantly clever algorithm to defeat the machine.

The trick, Alex saw, would be to start a play, see what cards showed up on the machine, and feed data into their own computer back at home identifying those cards. Their algorithm would calculate where the random generator was, and how many numbers it had to go through before it would be ready to display the sought-after hand, the royal flush.

> *So we're at our test machine and we run our little program and it correctly tells us the upcoming sequence of cards. We were pretty excited.*

Alex attributes that excitement to "knowing you're smarter than somebody and you can beat them. And that, in our case, it was gonna make us some money."

They went shopping and found a Casio wristwatch with a countdown feature that could be set to tenths of a second; they bought three, one for each of the guys who would be going to the casinos; Larry would be staying behind to man the computer.

They were ready to start testing their method. One of the team would begin to play and would call out the hand he got — the denomination and suit of each of the five cards. Larry would enter the data into their own computer; though something of an off-brand, it was a type popular with nerds and computer buffs, and great for the purpose because it had a much faster chip than the one in the Japanese video poker machine. It took only moments to calculate the exact time to set into one of the Casio countdown timers.

When the timer went off, the guy at the slot machine would hit the Play button. But this had to be done accurately to within a fraction of a second. Not as much of a problem as it might seem, as Alex explained:

> *Two of us had spent some time as musicians. If you're a musician and you have a reasonable sense of rhythm, you can hit a button within plus or minus five milliseconds.*

If everything worked the way it was supposed to, the machine would display the sought-after royal flush. They tried it on their own machine, practicing until all of them could hit the royal flush on a decent percentage of their tries.

Over the previous months, they had, in Mike's words, "reverse engineering the operation of the machine, learned precisely how the random numbers were turned into cards on the screen, precisely when and how fast the RNG iterated, all of the relevant idiosyncrasies of the machine, and developed a program to take all of these variables into consideration so that once we know the state of a particular machine at an exact instant in time, we could predict with high accuracy the exact iteration of the RNG at any time within the next few hours or even days."

They had defeated the machine — turned it into their slave. They had taken on a hacker's intellectual challenge and had succeeded. The knowledge could make them rich.

It was fun to daydream about. Could they really bring it off in the jungle of a casino?

Back to the Casinos — This Time to Play

It's one thing to fiddle around on your own machine in a private, safe location. Trying to sit in the middle of a bustling casino and steal their money — that's another story altogether. That takes nerves of steel.

Their ladies thought the trip was a lark. The guys encouraged tight skirts and flamboyant behavior — gambling, chatting, giggling, ordering drinks — hoping the staff in the security booth manning the "Eye in the Sky" cameras would be distracted by pretty faces and a show of flesh. "So we pushed that as much as possible," Alex remembers.

The hope was that they could just fit in, blending with the crowd. "Mike was the best at it. He was sort of balding. He and his wife just looked like typical players."

Alex describes the scene as if it had all happened yesterday. Marco and Mike probably did it a little differently, but this is how it worked for Alex: With his wife Annie, he would first scout a casino and pick out one video poker machine. He needed to know with great precision the exact cycle time of the machine. One method they used involved stuffing a video camera into a shoulder bag; at the casino, the player would position the bag so the camera lens was pointing at the screen of the video poker machine, and then he would run the camera for a while. "It could be tricky," he remembers, "trying to hoist the bag into exactly the right position without looking like the position really mattered. You just don't want to do anything that looks suspicious and draws attention." Mike preferred another, less demanding method: "Cycle timing for unknown machines out in the field was calculated by reading cards off the screen at two times, many hours apart." He had to verify that the machine had not been played in between, because that would alter the rate of iteration, but that was easy: just check to see that the cards displayed were the same as when he had last been at the machine, which was usually the case since "high stakes machines tended to not be played often."

When taking the second reading of cards displayed, he would also synchronize his Casio timer, and then phone the machine timing data and card sequences back to Larry, who would enter it into their home-base computer and run the program. Based on those data, the computer would predict the time of the next royal flush. "You hoped it was hours; sometimes it was days," in which case they'd have to start all over with another machine, maybe at a different hotel. At this stage, the timing of the Casio might be off as much as a minute or so, but close enough.

Returning plenty early in case someone was already at the target machine, Alex and Annie would go back to the casino and spend time on other machines until the player left. Then Alex would sit down at the target machine, with Annie at the machine next to him. They'd started playing, making a point of looking like they were having fun. Then, as Alex recalls:

> *I'd start a play, carefully synchronized to my Casio timer. When the hand came up, I'd memorize it — the value and suit of each of the five cards, and then keep playing until I had eight cards in sequence in memory. I'd nod to my wife that I was on my way and head for an inconspicuous pay phone just off the casino floor. I had about eight minutes to get to the phone, do what I had to do, and get back to the machine. My wife kept on playing.*