Cybercrimes: A Multidisciplinary Analysis

A Multidisciplinary Analysis

Bearbeitet von
Sumit Ghosh, Elliot Turrini

Weitere Fachgebiete > EDV, Informatik > Hardwaretechnische Grundlagen > Computerkriminalität, Schadsoftware

schnell und portofrei erhältlich bei

beck-shop.de
DIE FACHBUCHHANDLUNG

Preface

What's so important about cybercrime? Isn't it just another form of crime – like a violent or financial crime? The answer is both yes and no. Yes, in this way that any crime is a violation of a criminal law. But no in three important ways. First, a single cybercriminal with just one computer, right knowledge, and Internet access can cause immense social harm that was previously considered impossible. Second, the potential harm from cybercrime increases every second of every day, as computing technologies become more ubiquitous in our lives. Third, cybercriminals are often much more difficult to apprehend than traditional criminals, rendering the enforcement of cybercrime laws even less effective at crime prevention than the general enforcement of criminals laws.

Today, computers are everywhere, starting from cash registers in the grocery stores to running our cars, medical instruments that automatically read our temperature and blood pressure, routine banking, navigating airlines, and directing electricity to our homes and businesses. Consider the future of biotechnology, where tiny computers in the form of smart devices will be implanted inside our bodies – similar to, but more powerful than a pace maker. These devices will interact with our bodies in some profoundly important ways, and send and receive wireless communications from our doctors. Today, and even more so tomorrow, virtually all of these computers are interlinked through computer networks. Increasingly, computers and networks will entrench literally every aspect of our civilization without exception.

For the first time in our civilization, computers and networks, together, constitute an amplifier of the human mind, where the amplification factor is at a billion and growing fast with no upper bound in sight. With such formidable potential and power, computers and networks are destined to fundamentally alter our world – even beyond what we can reasonably imagine.

To an ordinary citizen, cybercrimes may logically appear to be defined as crimes that involve computers in any role or capacity. In fact, governments, civil and criminal justice systems, and law enforcement agencies, worldwide, choose to use this broad, working definition to help guide them in their crafting of the laws of the land, legal thinking, and the development of law enforcement tactics. This understanding of cybercrimes is very useful; however, it is of limited depth and may impede our ability to adequately address the large and growing cybercrime problem.

The potential for cybercrimes to evolve into innumerable radically new forms at incredible speed, orders of magnitude faster than the mutation rate of biological bacteria and viruses, is very real. Unchecked and unabated, they can easily overwhelm societies and nations.

What prompted us, contributing authors, to come together and organize this book? We fear the almost unlimited harm that cybercriminals can impose in the future. While filmed long after this book began, the movie, "Live Free or Die Hard," is not science fiction. Parts of it represent real and growing threats. But, more importantly, the authors believe that a multi-discipline, holistic approach to cybercrime prevention is essential.

Overall, this book is a collaborative effort of all of the contributing authors, characterized by great mutual admiration and deep respect for each other. Specifically, this book represents a coalescence of three motivating factors. First, each of the authors had independently arrived at the same exact realization that cybercrimes pose a formidable challenge to the fast approaching cyberage and that the important underlying issues must be addressed to ensure a bright future. Second, in the course of his prosecutorial work at the US DOJ, co-author Elliot Turrini had become deeply convinced that cybercrime is an intellectually rich, multidimensional problem, which requires a unique multidisciplinary approach. Third, in the course of his interdisciplinary research spanning computer hardware description languages to networking, network security, computer architecture, programming languages, algorithms, banking, biology, genetics, medicine, business, financial services, and modeling and simulation, co-author Sumit Ghosh experienced a profound revelation that, as an amplifier of the human mind, the underlying principle of computers represents the seed of virtually every known discipline of knowledge, law included.

The co-authors passionately hope that this book will serve to raise a general awareness among everyone of what lies ahead in our future. From a pessimistic perspective, unless we as a society are very careful, we risk being drowned literally, not metaphorically, in cybercrimes. Being not too proud to borrow twice from contemporary cinema, consider the Matrix movies as the ultimate cybercrimes – which, by the way, are far more science fiction than "Live Free or Die Hard." From an optimistic perspective, with diligent prevention/security and effective investigation and prosecution of cybercrimes, we will be able to enjoy the wonderful benefits of computers without suffering the horrific potential harms from cybercrimes.

A better understanding of how perpetrators may hatch sinister plans, today and in the future, will help us preempt most of the destructive cybercrimes and foster greater advancement and fulfillment for all humanity. Computers and networks encapsulate amazing and incredible power, not the thermo-nuclear weapon kind, but grounded in thought and imagination with which we can shape our future for centuries, millennia, and beyond. As explained in Chap. 1, our optimism should be tempered by a recently coined economic principle called, "convenience overshoot," which shows that under America's form of capitalism, the economics of bringing new technologies to the market and the difficulties of predicting safety and security issues often lead to the commercial distribution of unsafe or insecure products. This

is an important principle, which should guide our thinking about cybercrime and security.

The underlying theme of the book rests on three pillars. The first is that cybercrime is a severe societal threat. The endemic vulnerability of computing as seen through the constant battle to control the CPU; future changes in computing technology; continued expansion of computing throughout our lives; and our proven track record of the "convenience overshoot" all coalesce into a severe societal risk. Second, criminal prosecution is important but, by itself, it is not nearly a sufficient response to the threat. Third, we need a multi-disciplinary, holistic approach to cybercrime prevention and mitigation with a three-prong focus: raise attack cost; increase attack risk, and reduce attack motivation.

What sets this book apart is its unique and simultaneous blend of pragmatic practice and fundamental scientific analysis. This tone permeates the entire book and reflects the origin and genesis of the collaboration between Sumit Ghosh and Elliot Turrini. In 2001, the USA DOJ was anxious to find a way to trace an Internet Protocol (IP) packet back to its origin, so they could tag and track suspect IP data packets involved in money laundering and terrorism and subsequently apprehend the perpetrators. A number of very well known networking companies were eager to explore this urgent USA DOJ need and were willing to modify or alter the IP router technology. From fundamental analysis of networking, however, it followed that IP packets could never be traced back to the launch point with any degree of certainty. Today, it has become mainstream knowledge that the design of the store-and-forward IP protocol is fundamentally incompatible with security. Through the many, many discussions, the co-authors became thoroughly motivated not only to synergize their ideas but to extend the collaboration to include researchers and practitioners from related disciplines. Inspired by this project, co-author Sumit Ghosh had co-organized a USA National Science Foundation-sponsored workshop titled, "Secure Ultra Large Networks: Capturing User Requirements with Advanced Modeling and Simulation Tools," in 2003. The interdisciplinary approach of the workshop was very well received and some of the far-reaching presentation material have been incorporated in this book.

This book is organized into nine major parts, each addressing a specific area that bear direct and undeniable relationship to cybercrimes. Part I serves as introduction and presents a working definition of cybercrimes; Part II focuses on the computing and networking technology as it relates to cybercrimes and the technical and people challenges encountered by the cyberdefenders; Part III explains how to compute the economic impact of a cybercrime and develop security risk management strategies; Part IV addresses the vulnerabilities of our critical infrastructures and notes that the possibilities of Pearl Harbor-type and Katrina-type cyberattacks are very real, which may be accompanied by catastrophic consequences; Part V describes the psycho-social aspect of cybercrimes; Part VI focuses on efforts and challenges to regulate cybercrimes directly, through criminal penalties, as well as indirectly; Part VII explains how cybercrimes easily transcend national and other boundaries and lists specific disciplines that face formidable challenges from cybercrimes, worldwide; Part VIII elaborates on techniques to mitigate cybercrimes and stresses on a

multi-prong approach; and Part IX concludes the book with a scientific, engineering, and technological analysis of the future of cybercrimes. Each of these nine parts are elaborated through a number of self-contained chapters, totaling twenty chapters contributed by a total of 14 authors. Co-author/co-editor Sumit Ghosh has edited all of the chapters in an effort to ensure uniformity, continuity, and a smooth flow throughout the entire book.

Although the book has been primarily organized to serve as a reference for legal scholars, computer scientists, military personnel involved in cyberwarfare, national-level policy makers entrusted to protect the country's critical infrastructure, national and international intelligence communities, economic analysts, psychologists, and social scientists whose interests in cybercrimes are both specific and holistic, it is written to appeal to a much wider audience. The book may be read by anyone in the legal community or peripherally related disciplines who plans to specialize in cybercrimes, cyberattacks, and cyberlaws and their enforcement; front-line police officers; computer forensics specialists; law students; law makers at the State and Federal (Central) levels; judges; practicing lawyers; technical personnel involved in patent litigation; patent lawyers; product liability lawyers, economic analysts; central bankers, finance ministers, monetary policy makers, Interpol, and insurance company personnel involved in risk and actuarial analysis and in underwriting policies for data security. The book will also serve network and computer security specialists as well as those who wish to redesign products to withstand product liability lawsuits, grounded on a fundamental understanding of the nature of computers, networking, and cybercrimes. Even ordinary citizens who may be called from time to time to serve in the jury in litigations involving cybercrimes, especially in the USA, may find themselves well educated by reading this book so they can blend their wisdom along with technology to protect society and our collective future.

The co-authors/co-editors feel deeply honored and grateful to all of the contributing chapter authors, namely, Alan Boulanger, Paul Schneck, Richard Stanley, Michael Erbschloe, Michael Caloyannides, Emily Freeman, Dan Geer, Marc Rogers, Stewart Baker, Melanie Schneck-Teplinsky, Marc Goodman, and Jessica Herrera-Flanigan. A very special gratitude is due to Carey Nachenberg, Fellow at Symantec Corporation; and Leonard Bailey, senior counselor to the Assistant Attorney General for National Security at the US Department of Justice for selflessly giving their time and sharing their concerns, knowledge, and wisdom. Co-author Sumit Ghosh is indebted, beyond description, to Elliot Turrini for introducing him to the world of cyberlaw and to Leonard Bailey for mentoring, guiding, and advising him through the complex issues of critical infrastructure protection and criminal regulations. We also thank many others for their time. We are especially grateful to Anke Seyfried of Springer-Verlag (Law division) for her incredible enthusiasm and patience relative to this book project and the entire editorial and production staff at Springer-Verlag.

March 2010   *Sumit Ghosh*
                                                                                                        Elliot Turrini