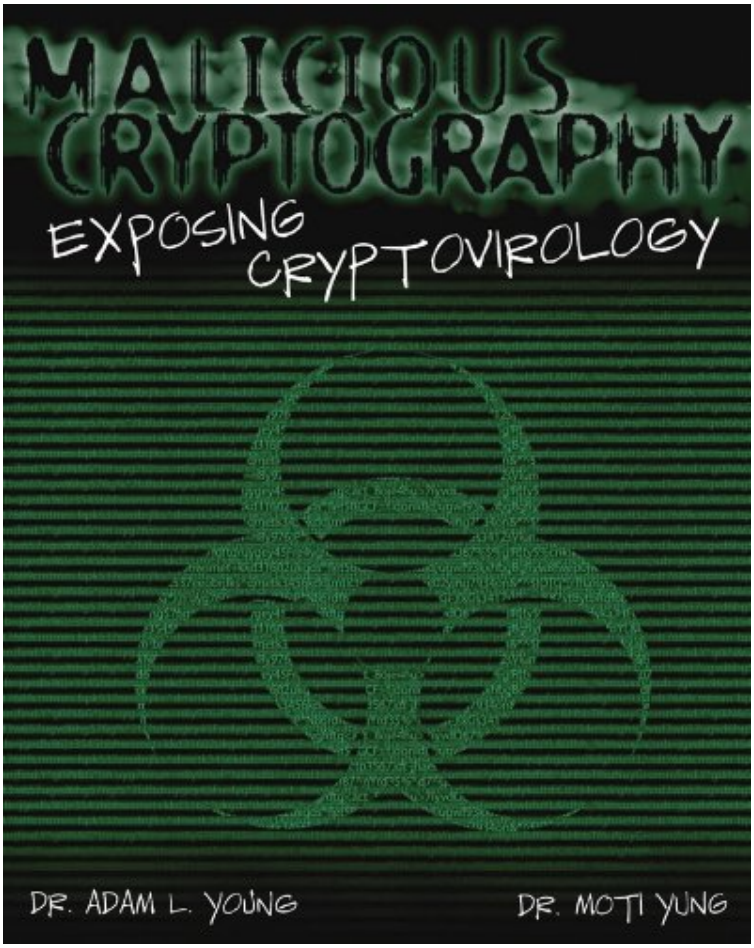
Malicious Cryptography: Exposing Cryptovirology

Adam Young, Moti Yung
*audiobook | *ebooks | Download PDF | ePub | DOC*



#1652623 in eBooks 2008-05-05 2008-05-05File Name: B000WDVM84 | File size: 25.Mb

Adam Young, Moti Yung : Malicious Cryptography: Exposing Cryptovirology before purchasing it in order to gage whether or not it would be worth my time, and all praised Malicious Cryptography: Exposing Cryptovirology:

24 of 26 people found the following review helpful. ExcellentBy Dr. Lee D. CarlsonBypassing computer security systems has sometimes been called an art rather than a science by those who typically do not interact with computing machines at a level that would allow them to appreciate the science behind security attacks. This book does not address the strategies of how to bypass security systems, but instead concentrates on how to use cryptographic methods to corrupt the machines once access has been acquired. Clearly the authors are very excited about the developments in cryptovirology, a relatively young field, that have taken place in the last five years. Their goal though is not to train hackers to break into systems, but rather to coach the reader on how to find vulnerabilities in these systems and then repair them. The subject of cryptovirology is fascinating, especially in the mathematics that is uses, and a thorough knowledge of its power will be required for meeting the challenges of twenty-first century network computing. After a "motivational chapter" that it meant to shed insight on what it is like to be a hacker, this being done through a collection of short stories, the authors move on to giving a general overview of the field of cryptovirology in

chapter 2. The reader gets his first dose of zero-knowledge interactive proofs (ZKIPs), which allow a prover to convince a verifier of a fact without revealing to it why the fact is true. The authors point out that viruses are vulnerable once found, since their rudimentary programming can be then studied and understood. This motivates the introduction of public key cryptography into the payload of the virus, and it is at this point that the field of cryptovirology is born. Chapter 3 is more of a review of modular arithmetic, entropy generators, and pseudorandom number generators and can be skipped for those readers familiar with these. The authors emphasize the need for effective random number generators and in using multiple sources for entropy generation. They also introduce the very interesting concept of a `mix network', which allows two mutually distrusting parties to communicate securely and anonymously over a network. `Onion routing' is discussed as a method for implementing asynchronous mix networks. Mix networks can be used to hide the propagation history of a worm or virus. In chapter 4, the authors discuss how to implement anonymous communication and how to launch a cryptotrojan attack that utilizes an anonymous communication channel. There are many applications of anonymous communication, one being E-money, and also, unfortunately, money laundering. The authors describe in fair detail how to conduct criminal operations with mix networks and anonymous money. This same technology though allows freedom of speech in geographical areas that are not sympathetic to it. Electronic voting, so controversial at the present time, is discussed as an activity that is very susceptible to the threat of stegotrojans or government violation of anonymity. Techniques for doing deniable password snatching using cryptovirology, and for countering it using zero-knowledge proofs, are also discussed. Chapter 5 introduces techniques for preventing the reading of counters when a virus is propagating from one machine to another. Known as `cryptocounters', the authors discuss various techniques for constructing them, such as the ElGamal and Paillier public key cryptosystems. Private information retrieval (PIR), which allows the secure and private theft of information, is discussed in chapter 6, wherein the authors present a few schemes for performing PIR. These schemes, unfortunately, allow the theft of information without revealing anything about the information sought and without revealing anything about what is taken. The authors also introduce a concept that they call `questionable encryptions', which are algorithms to produce valid encryptions or fake encryptions depending on the inputs. Related to question encryption, and also discussed in this chapter, are `deniable encryptions', which allow the sender to produce fake random choices that result in the true plaintext to be kept secret. Also discussed is the topic of `cryptographic computing', which allows computations with encrypted data without first having to decrypt it. The modular arithmetic used in this chapter is fascinating and well worth the read. Chapter 7 is by far the most interesting of the entire book, and also the most disconcerting if its strategies are ever realized. The goal of the chapter is to find out to what extent a virus can be constructed whose removal will damage the host machine. This, in the author's opinion, would be a genuine `digital disease', and they discuss various scenarios for bringing it about, which are at present not realized, but could be in the near future. The approach discussed involves game theory, and the authors show how the payload of a virus can survive even after discovery of the virus. They give a very detailed algorithm on how to attack a brokerage firm, including the assumptions that must be satisfied by such an attack. The attack is mounted by deploying a distributed cryptovirus that tries to find three suitable host machines, and the attack consists of three phases, the first involving replication leading to the infection of the three machines, the second involving preparation for the attack, and third involving playing the two-player game. The host machines, to be acceptable for launching the attack, must either be "brokerage" machines, which have sensitive information available to the virus, or "reclusive" machines, which are machines that are not subjected to much scrutiny. The goal of the virus, according to the authors, is to give the malware purchasing power, and not direct monetary gain. The virus may then evolve over time to become a portfolio manager, and may even act as a surrogate for purchasing shares on behalf of the firm or client. Other possibilities for the virus are discussed, and the authors overview the security of the attack and its utility. I did not read the rest of the chapters in the book, so I will omit their review.1 of 1 people found the following review helpful. Entertaining, but gets dense quickly.By Matt DoblerThe first chapter starts out like a bad cyberpunk novel, with random definitions sprinkled in for fun. The math assumes you already know a decent chunk of cryptography, statistics, and formal maths, but it tends to lose the formality at the drop of a hat.I wouldn't recommend this as your first cryptography book, unless you'e spent a good amount of time learning the basics on wikipedia.0 of 0 people found the following review helpful. I find it hard to put down!By Fred CI have learned and continue learning from this book! I can't wait to read this book over again. I'm sure I missed something and will try to find it! Thanks guys!

Hackers have uncovered the dark side of cryptographythat device developed to defeat Trojan horses, viruses, password theft, and other cyber-crime. Its called cryptovirology, the art of turning the very methods designed to protect your data into a means of subverting it. In this fascinating, disturbing volume, the experts who first identified cryptovirology show you exactly what youre up against and how to fight back. They will take you inside the brilliant and devious mind of a hackeras much an addict as the vacant-eyed denizen of the crackhouseso you can feel the rush and recognize your opponents power. Then, they will arm you for the counterattack. This book reads like a futuristic fantasy, but be assured, the threat is ominously real. Vigilance is essential, now. Understand the mechanics of computationally secure information stealing Learn how non-zero sum Game Theory is used to develop survivable

malware Discover how hackers use public key cryptography to mount extortion attacks Recognize and combat the danger of kleptographic attacks on smart-card devices Build a strong arsenal against a cryptovirology attack

The authors of this book explain these issues and how to fight against them. (Computer Law Security Report, 1st September 2004)From the Back Cover"Tomorrows hackers may ransack the cryptographers toolkit for their own nefarious needs. From this chilling perspective, the authors make a solid scientific contribution, and tell a good story too." Matthew Franklin, PhD Program Chair, Crypto 2004 WHAT IF HACKERS CONTROL THE WEAPONS USED TO FIGHT THEM? Hackers have unleashed the dark side of cryptographythat device developed to defeat Trojan horses, viruses, password theft, and other cybercrime. Its called cryptovirology, the art of turning the very methods designed to protect your data into a means of subverting it. In this fascinating, disturbing volume, the experts who first identified cryptovirology show you exactly what youre up against and how to fight back. They will take you inside the brilliant and devious mind of a hackeras much an addict as the vacant-eyed denizen of the crackhouseso you can feel the rush and recognize your opponents power. Then, they will arm you for the counterattack. Cryptovirology seems like a futuristic fantasy, but be assured, the threat is ominous ly real. If you want to protect your data, your identity, and yourself, vigilance is essentialnow. Understand the mechanics of computationally secure information stealing Learn how non-zero sum Game Theory is used to develop survivable malware Discover how hackers use public key cryptography to mount extortion attacks Recognize and combat the danger of kleptographic attacks on smart-card devices Build a strong arsenal against a cryptovirology attack About the AuthorDr. Adam Young (Herndon, VA) is a research scientist at Cigital, Inc. a software security company.He isinvolved in research for the Department of Defense and is a well-known cryptography consultant holding six US patents and two international patents of novel methods for security implementation. Dr. Moti Yung (New York, NY) is Senior Researcher at Columbia University and a well-known cryptography consultant. Previously the VP/Chief Scientist at CertCo, Inc. Moti is on the Steering Committee for the Cryptographers Track for RSA 2004. He is the holder of numerous technology US patents, won the IBM Outstanding Innovation Award, and co-discovered, with Adam, numerous cryptovirology attacks.