Larte Dellinganno I Consigli Dellhacker Pi Famoso Del Mondo

Clarice Bean, aspiring actress and author, unsuccessfully tries to avoid getting into trouble as she attempts to help a friend in need by following the rules of the fictional, "exceptionordinarily" spy, Ruby Redfort.

The worldwide video game console market surpassed $10 billion in 2003. Current sales of new consoles is consolidated around 3 major companies and their proprietary platforms: Nintendo, Sony and Microsoft. In addition, there is an enormous installed "retro gaming" base of Ataria and Sega console enthusiasts. This book, written by a team led by Joe Grand, author of "Hardware Hacking: Have Fun While Voiding Your Warranty", provides hard-core gamers with they keys to the kingdom: specific instructions on how to crack into their console and make it do things it was never designed to do. By definition, video console game players like to have fun. Most of them are addicted to the adrenaline rush associated with "winning", and even more so when the "winning" involves beating the system by discovering the multitude of "cheats" built into most video games. Now, they can have the ultimate adrenaline rush---actually messing around with the soul of the machine and configuring it to behave exactly as the command. This book builds on the motto of "Have Fun While Voiding Your Warranty" and will appeal to the community of hardware geeks who associate unscrewing the back of their video console with para-jumping into the perfect storm. Providing a reliable, field-tested guide to hacking all of the most popular video gaming consoles Written by some of the most knowledgeable and recognizable names in the hardware hacking community Game Console Hacking is the first book on the market to show game enthusiasts (self described hardware geeks) how to disassemble, reconfigure, customize and re-purpose their Atari, Sega, Nintendo, Playstation and Xbox systems

Expert guidance on the art and science of driving secure behaviors Transformational Security Awareness empowers security leaders with the information and resources they need to assemble and deliver effective world-class security awareness programs that drive secure behaviors and culture change. When all other processes, controls, and technologies fail, humans are your last line of defense. But, how can you prepare them? Frustrated with ineffective training paradigms, most security leaders know that there must be a better way. A way that engages users, shapes behaviors, and fosters an organizational culture that encourages and reinforces security-related values. The good news is that there is hope. That’s what Transformational Security Awareness is all about. Author Perry Carpenter weaves together insights and best practices from experts in communication, persuasion, psychology, behavioral economics, organizational culture management, employee engagement, and storytelling to create a multidisciplinary masterpiece that transcends traditional security education and sets you on the path to make a lasting impact in your organization. Find out what you need to know about marketing, communication, behavior science, and culture management Overcome the knowledge-intention-behavior gap Optimize your program to work with the realities of human nature Use simulations, games, surveys, and leverage new trends like escape rooms to teach security awareness Put effective training together into a well-crafted campaign with ambassadors Understand the keys to sustained success and ongoing culture change Measure your success and establish continuous improvements Do you care more about what your employees know or what they do? It's time to transform the way we think about security awareness. If your organization is stuck in a security awareness rut, using the same ineffective strategies, materials, and information that might check a compliance box but still leaves your organization wide open to phishing, social engineering, and security-related employee mistakes and oversights, then you NEED this book.

L'arte dell'inganno. I consigli dell'hacker più famoso del mondoFeltrinelli EditoreTinaFeltrinelli EditoreEmotional design. Perché amiamo (o odiamo) gli oggetti della vita quotidianaApogeo EditoreHackersEdizioni Nuova Cultura

Use this book to learn how you can, at little or no expense, make virtually any movie using Machinima. The authors guide you from making your first Machinima movie to a grounding in both conventional filmmaking and Machinima technology that will let you tackle very complex film projects. The book focuses on the following Machinima platforms: The Sims 2: Arguably the most popular Machinima platform of all time, The Sims 2 allows you to tell stories ranging from romance to noir action. World Of Warcraft: Tell your own tales of heroism in the world of Azeroth, following in the footsteps of award-winning Machinima creators and even the makers of South Park. Medieval 2: Total War - This astonishing new game allows you to create Lord of the Rings-scale medieval battle films using just a home computer! MovieStorm: For the first time, unleash the power of Machinima as a professional user using a fully-featured, fully-licensed commercial Machinima platform. You'll be introduced to all aspects of Machinima production, from live filming in a game through the creation of sets, props and characters, as well as the basics of cinematography, storytelling and sound design.

How to Attack and Defend Your Website is a concise introduction to web security that includes hands-on web hacking tutorials. The book has three primary objectives: to help readers develop a deep understanding of what is happening behind the scenes in a web application, with a focus on the HTTP protocol and other underlying web technologies; to teach readers how to use the industry standard in free web application vulnerability discovery and exploitation tools – most notably Burp Suite, a fully featured web application testing tool; and finally, to gain knowledge of finding and exploiting the most common web security vulnerabilities. This book is for information security professionals and those looking to learn general penetration testing methodology and how to use the various phases of penetration testing to identify and exploit common web protocols. How to Attack and Defend Your Website is be the first book to combine the methodology behind using penetration testing tools such as Burp Suite and Damn Vulnerable Web Application (DVWA), with practical exercises that show readers how to (and therefore, how to prevent) pwning with SQLMap and using stored XSS to deface web pages. Learn the basics of penetration testing so that you can test your own website's integrity and security Discover useful tools such as Burp Suite, DVWA, and SQLMap Gain a deeper understanding of how your website works and how best to protect it

This guide concentrates on resources that are useful, in an easy-to-use format to enable architects, designers and engineers to access a wealth of knowledge. Information allows users to find, evaluate and contact the resources that can save time and money in day-to-day practice.

Not Born Digital addresses from multiple perspectives – ethical, historical, psychological, conceptual, aesthetic – the vexing problems and sublime potential of disseminating lyrics, the ancient form of transmission and preservation of the human voice, in an environment in which e-poetry and digitalized poetics pose a crisis (understood as opportunity and threat) to traditional page poetry. The premise of Not Born Digital is that the innovative contemporary poets studied in this book engage obscure and discarded, but nonetheless historically resonant materials to unsettle what Charles Bernstein, a leading innovative contemporary U.S. poet and critic of “official verse culture,” refers to as “frame lock” and “tone jam.” While other scholars have begun to analyze poetry that appears in new media contexts, Not Born Digital concerns the ambivalent ways page poets (rather than electronica based poets) have grappled with “screen memory” (that is, electronic and new media sources) through the re-purposing of “found” materials.

Hacker extraordinaire Kevin Mitnick delivers the explosive encore to his bestselling The Art of Deception Kevin Mitnick, the world's most celebrated hacker, now devotes his life to

helping businesses and governments combat data thieves, cybervandals, and other malicious computer intruders. In his bestselling The Art of Deception, Mitnick presented fictionalized case studies that illustrated how savvy computer crackers use "social engineering" to compromise even the most technically secure computer systems. Now, in his new book, Mitnick goes one step further, offering hair-raising stories of real-life computer break-ins-and showing how the victims could have prevented them. Mitnick's reputation within the hacker community gave him unique credibility with the perpetrators of these crimes, who freely shared their stories with him-and whose exploits Mitnick now reveals in detail for the first time, including: A group of friends who won nearly a million dollars in Las Vegas by reverse-engineering slot machines Two teenagers who were persuaded by terrorists to hack into the Lockheed Martin computer systems Two convicts who joined forces to become hackers inside a Texas prison A "Robin Hood" hacker who penetrated the computer systems of many prominent companies-andthen told them how he gained access With riveting "you are there" descriptions of real computer break-ins, indispensable tips on countermeasures security professionals need to implement now, and Mitnick's own acerbic commentary on the crimes he describes, this book is sure to reach a wide audience-and attract the attention of both law enforcement agencies and the media.

Franco Arminio (1960) was born and lives in Bisaccia (Irpinia d'Oriente), Italy. He has published some twenty books, and is also a photographer and maker of documentary films. As a paesologist he has written for years in journals and on the web in defense of small places. He conceived and developed the House of Paesology in Trevico and the festival of The Moon and the Badlands at Aliano (www.lalunaeicalanchi.it).

The world's most infamous hacker offers an insider's view of the low-tech threats to high-tech security Kevin Mitnick's exploits as a cyber-desperado and fugitive form one of the most exhaustive FBI manhunts in history and have spawned dozens of articles, books, films, and documentaries. Since his release from federal prison, in 1998, Mitnick has turned his life around and established himself as one of the most sought-after computer security experts worldwide. Now, in The Art of Deception, the world's most notorious hacker gives new meaning to the old adage, "It takes a thief to catch a thief." Focusing on the human factors involved with information security, Mitnick explains why all the firewalls and encryption protocols in the world will never be enough to stop a savvy grifter intent on rifling a corporate database or an irate employee determined to crash a system. With the help of many fascinating true stories of successful attacks on business and government, he illustrates just how susceptible even the most locked-down information systems are to a slick con artist impersonating an IRS agent. Narrating from the points of view of both the attacker and the victims, he explains why each attack was so successful and how it could have been prevented in an engaging and highly readable style reminiscent of a true-crime novel. And, perhaps most importantly, Mitnick offers advice for preventing these types of social engineering hacks through security protocols, training programs, and manuals that address the human element of security.

It's two years after the Zero Day attacks, and cyber-security analyst Jeff Aiken is reaping the rewards for crippling Al-Qaida's assault on the computer infrastructure of the Western world. His company is flourishing, and his relationship with former government agent Daryl Haugen has intensified since she became a part of his team. But the West is under its greatest threat yet. A revolutionary, invisible trojan that alters data without leaving a trace---more sophisticated than any virus seen before---has been identified, roiling international politics. Jeff and Daryl are summoned to root it out and discover its source. As the trojan penetrates Western intelligence, and the terrifying truth about its creator is revealed, Jeff and Daryl find themselves in a desperate race to reverse it as the fate of both East and West hangs in the balance. A thrilling suspense story and a sober warning from one of the world's leading experts on cyber-security, Trojan Horse exposes the already widespread use of international cyber-espionage as a powerful and dangerous weapon, and the lengths to which one man will go to stop it.

The essential biography of the influential and beloved filmmaker George Lucas. On May 25, 1977, a problem-plagued, budget-straining independent science-fiction film opened in a mere thirty-two American movie theaters. Conceived, written, and directed by a little-known filmmaker named George Lucas, the movie originally called The Star Wars quickly drew blocks-long lines, bursting box-office records and ushering in a new way for movies to be made, marketed, and merchandised. It is now one of the most adored-and successful-movie franchises of all time. Now, the author of the bestselling biography Jim Henson delivers a long-awaited, revelatory look into the life and times of the man who created Luke Skywalker, Han Solo, and Indiana Jones. If Star Wars wasn't game-changing enough, Lucas went on to create another blockbuster series with Indiana Jones, and he completely transformed the world of special effects and the way movies sound. His innovation and ambition forged Pixar and Lucasfilm, Industrial Light & Magic, and THX sound. Lucas's colleagues and competitors offer tantalizing glimpses into his life. His entire career has been stimulated by innovators including Steven Spielberg and Francis Ford Coppola, actors such as Harrison Ford, and the very technologies that enabled the creation of his films-and allowed him to keep tinkering with them long after their original releases. Like his unforgettable characters and stories, his influence is unmatched.

An exotic dance that beguiles and entices... The enchanted and enchanting account of a contemporary Scheherazade, a wide-eyed American teller-of-tales who triumphs over harsh reality through the creative power of her own imagination...From the Paperback edition.

Nastasya has lived for hundreds of years, but for some reason, life never seems to get any better. She left her spoiled, rich girl life to find peace at River's Edge, a safe haven for wayward immortals. There, she learned to embrace River's Edge, despite som drama involving the sexy Reyn, who she wants but won't allow herself to have. But just as she's getting comfortable, her family's ties to dark magick force her to leave. She falls back into her old, hard partying ways, but will her decision lead her into the hands of a dark immortal? Or will it be her first step to embracing the darkness within her?

Predicated on the notion that mathematics has been a growing source of aesthetic inspiration in culture, this volume celebrates where the two intermesh. It is a meditation on the performances and cultural events, all mathematics-related, performed in Bologna in 2004, is dedicated to all those who are curious about mathematics, but also more generally about theatre, cinema, literature, arts and science. Thanks to the DVD, one can readers can relive various events through the voices and the images of the participants.

«Vuole sapere come l'ho ucciso ...? No, certo, non il freddo resoconto dei fatti di quella sera ... ma come ho fatto a prendere la decisione di ucciderlo ... come al solito ... sono le occasioni a fare gli assassini.» Comincia così la confessione di Luca Barberis, in una serie di e-mail indirizzate a Giulia Ambrosini, il giudice incaricato della sua cattura. Nelle lettere Luca si racconta e ricostruisce l'invisibile rete di potere fondata sull'inafferrabilità dei sistemi bancari informatici e la spregiudicatezza della finanza on-line. Figlio della Torino operaia, Luca si è lasciato stritolare da un mondo di potere che non gli appartiene. Una volta accortosi di essere una semplice pedina, l'istinto di vendetta lo ha inevitabilmente condotto sulla strada senza ritorno del crimine. Oltre ad essere un giallo avvincente, questo libro è anche un feroce attacco al lato oscuro della new economy, un monito duro e disincantato contro il miraggio della ricchezza facile ad ogni costo.

The Art of UNIX Programming poses the belief that understanding the unwritten UNIX engineering tradition and mastering its design patterns will help programmers of all stripes to become better programmers. This book attempts to capture the engineering wisdom and design philosophy of the UNIX, Linux, and Open Source software development community as it has evolved over the past three decades, and as it is applied today by the most experienced programmers. Eric Raymond offers the next generation of "hackers" the unique opportunity to learn the connection between UNIX philosophy and practice through careful case studies of the very best UNIX/Linux programs.

James Kakalios explores the scientific plausibility of the powers and feats of the most famous superheroes — and discovers that in many cases the comic writers got their science surprisingly right. Along the way he provides an engaging and witty commentary while introducing the lay reader to both classic and cutting-edge concepts in physics, including: What Superman’s strength can tell us about the Newtonian physics of force, mass, and acceleration How Iceman’s and Storm’s powers illustrate the principles of thermal dynamics The physics behind the death of Spider-Man’s girlfriend Gwen Stacy Why physics professors gone bad are the most dangerous evil geniuses!

"Il grande sonno", uscito nel 1939, è il primo romanzo di Chandler in cui compare la figura dell'investigatore Philip Marlowe.

Follows the sensational cat-and-mouse cyberspace manhunt between elusive California computer hacker Kevin Mitnick, a criminal who outwitted the FBI, and Tsutomu Shimomura, a computer crime expert who vowed to stop Mitnick. Original.

"If I had this book 10 years ago, the FBI would never have found me!" -- Kevin Mitnick This book has something for everyone---from the beginner hobbyist with no electronics or coding experience to the self-proclaimed "gadget geek." Take an ordinary piece of equipment and turn it into a personal work of art. Build upon an existing idea to create something better. Have fun while voiding your warranty! Some of the hardware hacks in this book include: * Don't toss your iPod away when the battery dies! Don't pay Apple the $99 to replace it! Install a new iPod battery yourself without Apple's "help" * An Apple a day! Modify a standard Apple USB Mouse into a glowing UFO Mouse or build a FireWire terabyte hard drive and custom case * Have you played Atari today? Create an arcade-style Atari 5200 paddle controller for your favorite retro videogames or transform the Atari 2600 joystick into one that can be used by left-handed players * Modern game systems, too! Hack your PlayStation 2 to boot code from the memory card or modify your PlayStation 2 for homebrew game development * Videophiles unite! Design, build, and configure your own Windows- or Linux-based Home Theater PC * Ride the airwaves! Modify a wireless PCMCIA NIC to include an external antenna connector or load Linux onto your Access Point * Stick it to The Man! Remove the proprietary barcode encoding from your CueCat and turn it into a regular barcode reader * Hack your Palm! Upgrade the available RAM on your Palm m505 from 8MB to 16MB · Includes hacks of today's most popular gaming systems like Xbox and PS/2. · Teaches readers to unlock the full entertainment potential of their desktop PC. · Frees iMac owners to enhance the features they love and get rid of the ones they hate.

This book explores the enduring appeal of child pornography and its ramifications for criminal justice systems around the world. It is based on an extensive review of academic literature and newspaper coverage, a trawl of websites frequented by those with a sexual interest in children, a survey of how police investigate these offences, examination of prosecutors' decisions, and interviews with judges. It provides a framework for understanding the contemporary nature of this problem, especially the harms it causes, its intimate relationship with new technologies and the challenges it poses to law enforcement authorities. The internet plays a pivotal role. Its sheer size, the anarchic way it grows, the lack of any boundaries to its expansion and its disregard for national borders make it a legal environment without parallel. An unwavering focus on the threat of sexual abuse has contributed to the emergence of a context where routine dealings with children are viewed through a 'paedophilic' lens. This can have the unfortunate consequence of distracting attention from more urgent concerns (such as poverty and neglect), which make children vulnerable to sexual exploitation. In this way an emphasis on the sexualisation of children could be said to aggravate the problem that it sets out to address. The book: provides a comprehensive analysis of child pornography issues in all of their complexity, including legal, psychological, criminal justice and social perspectives. presents significant volume of original empirical data gathered from police, prosecutors and judges. includes new qualitative and quantitative information set against a background of shifting international developments. The analysis is explicitly comparative. draws on a variety of sources including support groups for paedophiles, newspaper coverage of court cases involving child pornography, victim testimony and police operations.

Johnny Long's last book sold 12,000 units worldwide. Kevin Mitnick's last book sold 40,000 units in North America. As the cliché goes, information is power. In this age of technology, an increasing majority of the world's information is stored electronically. It makes sense then that we rely on high-tech electronic protection systems to guard that information. As professional hackers, Johnny Long and Kevin Mitnick get paid to uncover weaknesses in those systems and exploit them. Whether breaking into buildings or slipping past industrial-grade firewalls, their goal has always been the same: extract the information using any means necessary. After hundreds of jobs, they have discovered the secrets to bypassing every conceivable high-tech security system. This book reveals those secrets; as the title suggests, it has nothing to do with high technology. • Dumpster Diving Be a good sport and don’t read the two “D” words written in big bold letters above, and act surprised when I tell you hackers can accomplish this without relying on a single bit of technology (punny). • Tailgating Hackers and ninja both like wearing black, and they do share the ability to slip inside a building and blend with the shadows. • Shoulder Surfing If you like having a screen on your laptop so you can see what you’re working on, don’t read this chapter. • Physical Security Locks are serious business and lock technicians are true engineers, most backed with years of hands-on experience. But what happens when you take the age-old respected profession of the locksmith and sprinkle it with hacker ingenuity? • Social Engineering with Jack Wiles Jack has trained hundreds of federal agents, corporate attorneys, CEOs and internal auditors on computer crime and security-related topics. His unforgettable presentations are filled with three decades of personal "war stories" from the trenches of Information Security and Physical Security. • Google Hacking A hacker doesn’t even need his own computer to do the necessary research. If he can make it to a

public library, Kinko's or Internet cafe, he can use Google to process all that data into something useful. • P2P Hacking Let’s assume a guy has no budget, no commercial hacking software, no support from organized crime and no fancy gear. With all those restrictions, is this guy still a threat to you? Have a look at this chapter and judge for yourself. • People Watching Skilled people watchers can learn a whole lot in just a few quick glances. In this chapter we’ll take a look at a few examples of the types of things that draws a no-tech hacker’s eye. • Kiosks What happens when a kiosk is more than a kiosk? What happens when the kiosk holds airline passenger information? What if the kiosk holds confidential patient information? What if the kiosk holds cash? • Vehicle Surveillance Most people don’t realize that some of the most thrilling vehicular espionage happens when the cars aren't moving at all!

In this critically acclaimed novel, Harry Rent finds himself young and single and lost after the passing of his wife. Although numbed by his life's unexpected turn, Harry becomes fixated on Molly, an obsidian-haired, twenty-two-year-old waitress. Meanwhile, Harry is forced to fend off Clare, his sister-in-law, who is convinced that Harry is somehow responsible for her sister's untimely death. At once deeply moving and darkly comedic, Harry, Revised is an extraordinary novel about the measure of a man's worth by a wonderful, emerging talent.

The “engrossing” sequel to The Crocodile kicks off an Italian crime fiction series by the author of the bestselling Commissario Ricciardi novels (Publishers Weekly). They’ve made a fresh start at the Pizzofalcone precinct of Naples. They fired every member of the investigative branch after they were found guilty of corruption. Now, there’s a group of detectives, a new commissario, and a new superintendent. The new cops immediately find themselves investigating a high-profile murder that has the whole town on edge. Heading the investigation is Inspector Lojacono, known as “the Chinaman,” a cop with a checkered past who is currently riding a reputation as a crack investigator after having captured a serial killer known as “The Crocodile.” Lojacono’s partner is Aragona, who wants to be known as “Serpico,” but the name doesn’t stick. Luigi Palma, a.k.a. “Gigi,” is the commissario, Francesco Romano, known as “Hulk,” is the slightly self-deluded lieutenant. Lojacono, Aragona, Palma, and Romano are joined by a cast of cops portrayed by bestselling author Maurizio de Giovanni with depth and intimate knowledge of the close-knit world of police investigators. De Giovanni’s award-winning and bestselling novels, all set in Naples, offer a brilliant vision of the criminal underworld and the lives of the cops in Europe’s most fabled, atmospheric, dangerous, and lustful city. “Colorful, fully drawn characters and several intriguing subplots help propel the plot to a satisfying resolution.” —Publishers Weekly “De Giovanni provides satisfyingly logical answers to every riddle . . . Despite the Neapolitan setting, the crew of mismatched cops may remind you of similar teams in Sweden, New York, or Hollywood. Not that there’s anything wrong with that.” —Kirkus Reviews

An anthology of short stories that originally appeared in "Playboy" magazine presents tales by Isaac Bashevis Singer, Nadine Gordimer, Gabriel Garcia Marquez, Bernard Malamud, John Updike, Tom McGuane, T. Corraghessan Boyle, and others

Il presente volume è finalizzato al raggiungimento di diversi obiettivi: operare una ricostruzione critica e unitaria del fenomeno degli hackers; superare le concezioni sensazionalistiche e superficiali che lo hanno travisato; analizzarne gli aspetti involutivi ed evolutivi mettendo in luce i profili giuridicamente rilevanti; valutare il contributo degli hackers e della loro etica alla costruzione della società contemporanea; studiare il ruolo della disobbedienza civile e dell’hacktivism alla luce della crisi delle moderne democrazie rappresentative e della società globalizzata; delineare alcune possibili prospettive del fenomeno. Una simile indagine, che abbraccia problematiche diverse, ha richiesto una considerazione unitaria ed interdisciplinare dell’hacking. Caratterizzato da un’etica dirompente, è espressione dell’agire di un uomo che vuole essere artefice del proprio destino e che può contribuire anche a migliorare quello altrui grazie alla condivisione delle proprie idee. In una società caratterizzata da molteplici elementi critici, soprattutto in ambito informatico-giuridico, ciò non è tuttavia facile. Gli effetti della rivoluzione tecnologica hanno infatti modificato la società contemporanea rendendo problematica l’attività di legislatori e magistrati, in un mondo in cui i confini tradizionali fra gli stati sono sempre più labili e quelli digitali quasi inesistenti; in esso sorgono nuovi soggetti che pretendono di far sentire la propria voce e di esprimere consenso e dissenso non solo nel proprio stato e verso i propri rappresentanti ma anche nella società globale. Tuttavia, l’interazione, a diversi livelli, è spesso virtuale e posta in essere mediante strumenti informatici e reti telematiche, in comunità reali e virtuali (inclusi i siti di social network). Il sensazionalismo che caratterizza nuovi e vecchi media ha tuttavia portato a travisare la figura degli hackers, soggetti ben distinti dai criminali informatici ma ad essi normalmente parificati, nonostante la loro etica sia basata su principi che richiamano quelli democratici. Un recupero di tale etica può assumere una fondamentale importanza nella Società dell’informazione, ove molti fenomeni, sinora legati alla materialità della realtà fattuale, assumono valenze nuove in seguito allo sviluppo delle tecnologie informatiche: basti pensare alla disobbedienza civile elettronica, che può diventare una forma assai efficace di espressione del dissenso. In tale quadro, compiutamente analizzato nel presente volume, gli hackers, oggi più che in passato, possono fornire un prezioso apporto nello sviluppo di una società che cambia forse troppo in fretta e contribuire al rispetto di quei principi di democrazia e libertà troppo spesso proclamati e contestualmente violati.

Documents how a troubled young computer hacker seized control of a massive international computer fraud network in 2006, tracing the efforts of FBI and Secret Service agents as well as an undercover operator to locate and arrest him. Reprint.

At its heart, mathematics is about numbers, our fundamental tools for understanding the world. In Professor Stewart's Incredible Numbers, Ian Stewart offers a delightful introduction to the numbers that surround us, from the common (Pi and 2) to the uncommon but no less consequential (1.059463 and 43,252,003,274,489,856,000). Along the way, Stewart takes us through prime numbers, cubic equations, the concept of zero, the possible positions on the Rubik's Cube, the role of numbers in human history, and beyond! An unfailingly genial guide, Stewart brings his characteristic wit and erudition to bear on these incredible numbers, offering an engaging primer on the principles and power of math.

Modern cars are more computerized than ever. Infotainment and navigation systems, Wi-Fi, automatic software updates, and other innovations aim to make driving more convenient. But vehicle technologies haven’t kept pace with today’s more hostile security environment, leaving millions vulnerable to attack. The Car Hacker’s Handbook will give you a deeper understanding of the computer systems and embedded software in modern vehicles. It begins by examining vulnerabilities and providing detailed explanations of communications over the CAN bus and between devices and systems. Then, once you have an understanding of a vehicle’s communication network, you’ll learn how to intercept data and perform specific hacks to track vehicles, unlock doors, glitch engines, flood communication, and more. With a focus on low-cost, open source hacking tools such as Metasploit, Wireshark, Kayak, can-utils, and ChipWhisperer, The Car Hacker’s Handbook will show you how to: –Build an accurate threat model for your vehicle –Reverse engineer the CAN bus to fake engine signals –Exploit vulnerabilities in diagnostic and data-logging systems –Hack the ECU and other firmware and embedded

systems –Feed exploits through infotainment and vehicle-to-vehicle communication systems –Override factory settings with performance-tuning techniques –Build physical and virtual test benches to try out exploits safely If you’re curious about automotive security and have the urge to hack a two-ton computer, make The Car Hacker’s Handbook your first stop.

The first guide to planning and performing a physical penetration test on your computer's security Most IT security teams concentrate on keeping networks and systems safe from attacks from the outside-but what if your attacker was on the inside? While nearly all IT teams perform a variety of network and application penetration testing procedures, an audit and test of the physical location has not been as prevalent. IT teams are now increasingly requesting physical penetration tests, but there is little available in terms of training. The goal of the test is to demonstrate any deficiencies in operating procedures concerning physical security. Featuring a Foreword written by world-renowned hacker Kevin D. Mitnick and lead author of The Art of Intrusion and The Art of Deception, this book is the first guide to planning and performing a physical penetration test. Inside, IT security expert Wil Allsopp guides you through the entire process from gathering intelligence, getting inside, dealing with threats, staying hidden (often in plain sight), and getting access to networks and data. Teaches IT security teams how to break into their own facility in order to defend against such attacks, which is often overlooked by IT security teams but is of critical importance Deals with intelligence gathering, such as getting access building blueprints and satellite imagery, hacking security cameras, planting bugs, and eavesdropping on security channels Includes safeguards for consultants paid to probe facilities unbeknown to staff Covers preparing the report and presenting it to management In order to defend data, you need to think like a thief-let Unauthorised Access show you how to get inside.

The latest Web app attacks and countermeasures from world-renowned practitioners Protect your Web applications from malicious attacks by mastering the weapons and thought processes of today's hacker. Written by recognized security practitioners and thought leaders, Hacking Exposed Web Applications, Third Edition is fully updated to cover new infiltration methods and countermeasures. Find out how to reinforce authentication and authorization, plug holes in Firefox and IE, reinforce against injection attacks, and secure Web 2.0 features. Integrating security into the Web development lifecycle (SDL) and into the broader enterprise information security program is also covered in this comprehensive resource. Get full details on the hacker's footprinting, scanning, and profiling tools, including SHODAN, Maltego, and OWASP DirBuster See new exploits of popular platforms like Sun Java System Web Server and Oracle WebLogic in operation Understand how attackers defeat commonly used Web authentication technologies See how real-world session attacks leak sensitive data and how to fortify your applications Learn the most devastating methods used in today's hacks, including SQL injection, XSS, XSRF, phishing, and XML injection techniques Find and fix vulnerabilities in ASP.NET, PHP, and J2EE execution environments Safety deploy XML, social networking, cloud computing, and Web 2.0 services Defend against RIA, Ajax, UGC, and browser-based, client-side exploits Implement scalable threat modeling, code review, application scanning, fuzzing, and security testing procedures