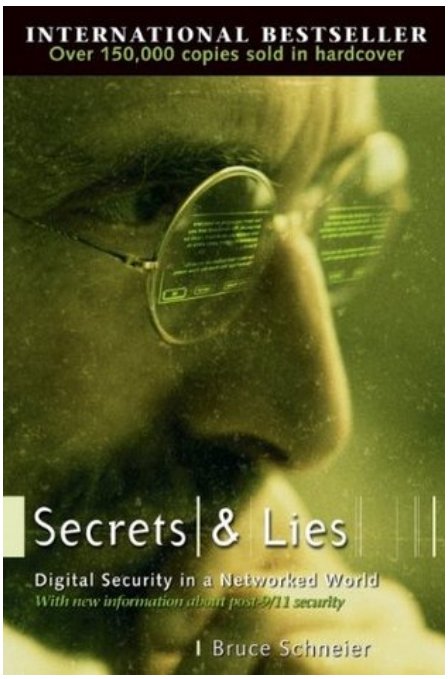

Secrets and Lies: Digital Security in a Networked World

Bruce Schneier

Secrets and Lies: Digital Security in a Networked World

Bruce Schneier

Secrets and Lies: Digital Security in a Networked World Bruce Schneier
Viruses. Identity Theft. Corporate Espionage. National secrets compromised. Can anyone promise security in our digital world?

The man who introduced cryptography to the boardroom says no. But in this fascinating read, he shows us how to come closer by developing security measures in terms of context, tools, and strategy. Security is a process, not a product – one that system administrators and corporate executives alike must understand to survive.

This edition updated with new information about post-9/11 security.

Secrets and Lies: Digital Security in a Networked World Details

Date	:	Published January 30th 2004 by Wiley (first published 2000)
ISBN	:	9780471453802
Author	:	Bruce Schneier
Format	:	Paperback 401 pages
Genre	:	Nonfiction, Science, Technology, Computer Science, Computers

From Reader Review Secrets and Lies: Digital Security in a Networked World for online ebook

Xing Chen says

I'm a technology end-user, deluged with acceleratingly frequent news reports of large corporations getting hacked, have recently been using my internet banking passcode generator, and occasionally placing basic htaccess security on my websites.

Thus, increasingly aware that security isn't to be left solely to experts who run the banking systems and data storage and transfer facilities- even casual users need an understanding of the premises on which they're built, and are responsible for correct implementation, otherwise we cut corners unwittingly and end up being the weakest link.

By training ourselves to examine the limitations of our security systems, we can spot vulnerabilities and uncover unsound assumptions about how secure they really are, and how to order our priorities.

Plenty of insights, too, into how the current systems evolved, and thus how we can learn from previous technological and society-wide breakthroughs, and allocate resources optimally.

It wasn't just digital security- this book made me think more analytically about protection of physical property, loopholes and real-world messiness. I greatly appreciate authors who put the realities of the situation at the forefront, and highlight limitations- how 'secure' something is depends on the context. Such books remind you of interconnections between their topic and everything else.

Bruce is a prolific, high-profile writer, particularly well-known for his criticism of ineffective, time-wasting measures that plague airports throughout the world.

Recently came across a fascinating article by Jeffrey Goldberg, describing how the patchwork of security checks (ID, boarding pass, online database searches) renders the system entirely penetrable to someone with an elementary knowledge of how it (doesn't) work.

Raj Makaram says

If you want a “crash course” on digital security this is the book. The author Schneier is well-respected security consultant, cryptographer and the author of Applied Cryptography - one of the most respected books on the subject. If you are a professional who knows the limitation of technology, but need solution then this book will interest you. For those who are still to realize this fact – Schneier opens this book by acknowledging the he was wrong when he said earlier, that cryptography is The Answer™ for security. He goes further to make his point that it is not the mathematics of cryptography, which is faulty, but his perception of security devoid of the people is faulty (i.e., it people who use and implement the security). So people are the weakest link in security. Let us appreciate the fact that an authority like Schneier acknowledges his mistake and shares with us. This is not a book if you are looking at just building firewalls, IDE, secure code or encryption algorithm. This book is all about understanding of the security risks and coming out with a practical solution to mitigate them

The core thesis of this book is –
1. There is nothing like “complete”, “air tight” secure product, and all those claims we hear on various secure products are all “buzzword compliant products” (pp 102-103) Because security comes from carefully crafted systems not mass produced products (pp 217)
2. Security is about managing risks. Security requirement is relative and contextual
3. Instead of going beyond a total secure system, it is better to have a mediocre security
4. The best methodology to build security into your product, is by collective analytical ability – that is provide unlimited access to people to review and critique the product design and implementation
5. Use Prevention, Detection and Reaction mechanism in tandem to counter security breeches

This book has facts on digital security that makes your reading hilarious and also scary because it removes the illusion that everything is safe and brings an awareness of the vulnerabilities with which we are conducting business in the “digital world”.

The areas where I would like to see improvements in the second edition of this book are - editorial is bad, sentences are not phrased in a manner to understand easily, no references for further reading. There is no section numbers, which makes the flow difficult. How could anyone ever justify the cause of terrorism (pp 53)? – Is it because author and USA had not yet seen 9/11;-) There are sections that gives the felling that the author goes overboard to make a point! But definitely this is a must book to read, since gains to be achived by reading this book overweigh these issues(1) and in addtion difficult to put up with those repeated China, UK, and Microsoft bashing! - Is worth the effort ?

The 25 chapters in this book are organized into three main sections. The first section sets the context for security requirement in the current digital world; the second describes the various technologies and their limitations. Finally the third provides us the roadmap to mange for now with the current technology limitations.

The Landscape –. Schneier says cyber crime is very similar in motive to the real world, people haven’t changed and cyberspace is just yet another new place to “ply their trade” (pp 45). The motives are – financial gains, publicity, etc. (Chap 3) The threat in the digital world is the same as in the real world, but it gets a new perspective because of - speed of automation what would take hundreds of days in the real world can be done in minutes. Secondly prosecuting a cyber criminal is difficult because he/she may be sitting in New York and hacking a computer in St Petersburg, so neither the law of USA or Russia can apply. Finally “skill to hack” is just the need of the first person that break the system, later he/she can share with the rest of the world through the Internet (Chap 2) for others to follow. Schneier characterizes the adversaries of the digital world based parameters such as - the objective of their attack, how resourceful are they, how willing are they to tolerate risks, etc. Hackers, lone criminals, industrial espionage, national Intelligence are some of the adversaries described (Chap 4). Finally Schneier concludes this section discussing the various types of security needs, such as - Privacy, multiple levels of security, anonymity, authentication, integrity and audit (Chap 5)

Technologies – This section starts of stating that security is like “an onion”, with various layers – users being at the outermost and cryptography being the inner most layer in the security process/chain. Each of these layers is described, starting with the introduction to what cryptography is and its limitation and its context in computer security landscape (Chap 6-8). Symmetric encryption algorithm, message authentication code, one-way hash functions, types of protocol attacks, are some of the concepts introduced in this section. Various identification and authentication such as password, biometrics, and access token are described with their limitations (Chap 9). As per Schneier there are various ways a system/network can be attacked like -

malicious code (virus, worms, etc). Modular code due to the advent of modular programming, and proliferation of scripts such as Java scripts™ ActiveX™, plug-in in software, are all cause for security breach (Chap 10). He then goes to describe the vulnerabilities of network security and defense mechanisms, introducing to readers concepts on IP scoffing, Denial-of service attacks, firewall, demilitarized zone, VPN, IDE, vulnerability scanners, etc (Chap 11-12). Relationship between bugs/quality and security is described (Chap13). Various concepts of securing hardware such as - tamper proof tamper evident and tamper resistant concepts are introduced. Various means of side channel attacks such as through- timing, power, radiation etc are introduced (Chap 14). Digital certificates and their limitations are discussed. Schneier illustrates that certificates are not he some magic security elixir (pp 237). GAK, Database security, Steganography and other techniques are introduced in Chapter 16. Finally this section ends detailing the six aspects of human problems for digital security such as – people overestimate risk, people don't deal with things that happen very rarely, social engineering, etc

Strategies – This section goes into solving security problems in a planned way. Schneier emphasizes that - security is not a pile of defenses: adding firewalls, IDS, etc will not bring in a secure system (pp 272). The three steps to counter security vulnerabilities are by – protection, detection and reaction. These three steps need to work in tandem to secure a system. On the contrary the people in the digital world think that protection is the only way to protect - this fallacy as per Schneier attributes to the bulk of security breech (pp 281). The solution/success to effective digital security is good engineering and effective understanding of the threats and designing countermeasures (pp 303). The process of understanding threats or in other words threat modeling is not a one-time activity; it needs to be done/revisited at regular intervals. Since "secure system" has different meaning depending upon the context, for e.g. the anti-theft mechanism for expensive cars was to disable hotwiring. But this would take the threat model from one level to another aka from stealing a car from a parking lot to a more dangerous one of carjacking (pp317). So it is an iterative procedure of threat modeling and risk assessment
Ultimately the Schneier three steps for designing a secure system is -
1. Threat modeling – Chapter 21 describes a formal method to model threat using method called as "attack trees"
2. Security policy to defend against the threats - is the one which unifies the threats and countermeasures
3. Design counter measures
On testing for security, Schneier says there is no way functional testing can discover security flaws, since security is a function of probability (pp 257). As on date the best bet for identifying security flaws is through full disclosure – the philosophy being share the design, implementation with the general community to test and review the system. In this method, bugs would have gone through the normal sequence of getting logged and closed making the system "secure" over a course of time (Chap 22). On the question of whether we will ever achieve the "100% secure system anytime in the near future", Schneier's advice is – make system simple and use "good enough" security assuming complexity is inevitable (Chap 24). Technology is changing for the better, but the fundamental issues like unreliable software, people not able to remember long passwords, social engineering, etc, are there to stay and torment digital security (pp 353). Finally in Chap 24, the author gives us the process for a security assuming it is realistic to always think that security can be broken. Compartmentalize, secure weakest link, Fail-safe, Detection & Response, Counter attacks and outsourcing security are some of the steps suggested as part of this security process.

James Taylor says

Security consultant, cryptographer and author, Bruce Schneier basically gives the reader a history lesson on

Digital Security. Some reviewers state the book is “a bit dated”, which is only valid in the sense there's no discussion on post 2001 era computing. However, history is history, and the discussed concepts are still relevant today. There's a few references early on in the book which he just names and doesn't explain, so there's a few examples which were meaningless without doing a small bit of research. I think there are a few sections that cut be trimmed down somewhat, and there's a slight bit of repetition, but overall, it's a good book.

Aku says

An excellent overview of what digital security is all about. Many people equate it with firewalls and encryption, based on poor news stories among other things, but that's only a small facet of what real security is. This book covers security from a much larger perspective.

What most surprised me, while reading this in 2013, is how prescient this book turned out to be. Originally written between 1998 and 2000, it anticipated the numerous challenges our industry has faced since then. It feels very ominous and bleak at times, but given this year's NSA & GCHQ scandals, it was probably not bleak enough.

The content is written so that laypersons can understand it, and it does not go into detail all that much, but it's definitely good reading for everyone in the field. More than a decade later, security still does not get the respect and resources it needs to, despite the massive proliferation of attacks and the following media coverage.

Zeeshan says

Secrets and Lies is a non-technical , non-mathematical book that deals with the "social" , & practical day-to-day aspects of hacking and security breach and violations. The book explains the hows and whys of hackings and its consequences. It explains the different types of cyber crimes i.e. identity thefts, ATM thefts, etc. and explores the causes of each in a different viewpoint than just code flaws or weak algorithms. It focuses specially on the Social Engineering aspect, the fallibility of the human integrity and proves a valid case winningly that human beings are the weakest and easily the most gullible link in a wired world, and no matter how strong the encryption algorithm is, it can always fail if it falls in wrong hands or is wrongly implemented. A non-mathematical, less technical & a really enjoyable book, must for techies and nerds, and highly suggested for people who want to know about cyber crimes, and want to safeguard themselves from it.

Alis Franklin says

The INFOSEC book by *the* INFOSEC guy. Also pretty accessible to people outside the field, so if you've got even a passing interest in all this computer security stuff, this is the place to start.

?Misericordia? ~ The Serendipity Aegis ~ ?????? ✺✲❤❣ says

Q:
In any case, the future does not look good. (c)

Vidyadhar says

Simply put one can make career out of this book, if used wisely. This book gives a glimpse of the entire landscape, the past, present and future, of digital security in the networked world.

Marie says

Slightly dated, but still a very good book that gives a reader who is uninitiated/unfamiliar with information security a clear idea about what information security actually is, how it affects us all (as a generation of humans connected by internet), how to protect information systems and tactics criminals use to break those systems (from malware to social engineering). The book is written in language the average person can understand and really provides an eye opening look at the role cryptology plays in security/encryption products (like password encryption standards, firewalls, anti-virus, etc..), and the limits of those products when they are used improperly. Another important topic that is covered in this book is that of social engineering; how easily people fall victim to it, how criminals get away with it, and how to prevent against it. If you are the slightest bit interested in hacking, cyber crime, social engineering, information security, or computer security in general - this is a must read that will give you a broad sense of how prevalent cyber crimes are, and how rapidly the industry is evolving.

Jirka says

Despite the fact our industry is changing with incredible pace Schneider was able to well describe and also predict many possibilities of attacks and risks. He also provides the reader with explanation of main technologies and approaches to tackle the risk.

Well recommended.

Rick Howard says

Read full review at my blog: http://terebrate.blogspot.com/2014/05...
See Cyber Security Canon Candidate List: http://terebrate.blogspot.com/2014/02...

"Secrets and Lies: Digital Security in a Networked World" is the perfect book to hand to new bosses or new employees coming in the door who have not been exposed to cyber security in their past lives. It is also the perfect book for seasoned security practitioners who want an overview of the key issues facing our community today. Schneier wrote it more than a decade ago, but its ideas still resonate. He talks about the

idea that “security is a process, not a product.” With that one line, Schneier captures the essence of what our cyber security community should be about. He explains that even though we have advanced technology designed to specifically find cyber break-ins, people are the still the weakest link. He describes how cyber risk is not a special category. It is just another risk to the business. He highlights the ludicrous idea that software vendors have no liability or selling buggy code, and he was one of the first thought leaders to characterize the adversary as something more than just a hacker. He makes the case for things that the cyber security community still needs in order to make the Internet more secure, things like strengthening confidentiality, integrity, and availability (CIA); improving Internet privacy and Internet anonymity; and challenging the idea that security practitioners must make the Sophie’s Choice between better security or more privacy in terms of government surveillance. Finally, he anticipates the need for a Bitcoin-like capability long before Bitcoin became popular. The content within Secrets and Lies is a good introduction to the cyber security community, and Schneier tells the story well. Because of that, Secrets and Lies is candidate for the cyber security canon, and you should have read it by now.

Shelleybindon says

Great book, but I don’t think it can take one more update. How about starting from scratch on this topic?

Peter House says

This book came to me well recommended and after making my through it, I understand why. The author takes the reader through the sweeping expanse of digital security with aplomb. Rich with fascinating stories, candid observations, and good technical detail Secrets and Lies is a fairly exhaustive introduction to security.

At the end (not really a spoiler here), the author confesses to have had to pause writing the book because of a certain level of hopelessness and it shows through at times. As the book winds its way through the myriad forms of insecurity and attacks, I found myself at times wondering if the author felt there was any way forward. And I found myself questioning that perspective, after all, we seem to be making our way yet still today. The author does recover.

I really enjoyed reading this book and I recommend it.

Jonathan Katz says

time to update my review given that i am now finished!

one thing that slightly annoyed me while i was reading the book was that it did not appear that schneier was offering any solutions to the problems that he was presenting in information security. but, after a certain point, that is when i realized: there really are no clear-cut solutions. as schneier emphasizes throughout the book, security is a process, not a solution. there is no generally algorithm for applying a security process; it really must be performed on a case-by-case basis.

i did like how schneier admitted that it took him longer to write the book than he thought because he could not provide hope to the reader based on all the issues in information security today, until his big epiphany.

many of the issues he presented in 1999 are still relevant today (2007), but a lot of it comes down to the thought process that not only an information security expert has, but even just a non-technical person using technology in the information age.

in the end, i am glad i read this book, it was definitely an interesting read, and i would recommend it to people who are not only interested in computer-related security, but also those who may be involved with the liability issues should a breach in security occur.

Ed Holden says

I've wanted to read a Bruce Schneier book for a long time and this particular one was well rated. I might have confused it with the similarly named *Liars and Outliers*, which came out much more recently. What I didn't realize when I bought *Secrets and Lies* it is that Schneier published it in 2000, so it's both an insightful look at computer security practices and a trip down foggy memory lane.

Most of the advice in this book is still perfectly valid, like the importance of intrusion detection in a world where perfect prevention is impossible. But some of it feels dated. It's especially enlightening to read what people were worried about 13 years ago. For example, do you remember that the US federal government spent most of the 1990s advocating legislation that required encryption key escrow? You'd have had to register your private keys (or some other backdoor keys) with Uncle Sam or an independent agency so that law enforcement could access your data when necessary if you wanted to use any sort of encryption. The policy makes no sense because it's basically unenforceable, and its popularity in political circles is a distant memory because of the idea's technical flaws.

But on the other hand Schneier has virtually nothing to say about later security issues like e-mail spam. If he'd published this book a mere three years later he'd probably have devoted a whole chapter to spam, not to mention to phishing attacks that he hints at but doesn't describe in depth -- certainly not with the inevitable references to Nigeria a mid-decade book would have had. Same goes for spyware and other browser-vulnerable malware that would so inundate Windows XP (pre-SP2) users due to the craptastic security architecture of Internet Explorer 6 (may it be deleted with extreme prejudice).

Still, an interesting read. The best bits are where he talks about Windows NT/2000 security: he really lets loose, and with ample justification.
