3 page(s) will be printed.

Back

Record: 1

Title:	SECRETS & LIES AND THE NEW AES STANDARD.
Source:	Boardwatch Magazine, Dec2000, Vol. 14 Issue 12, p164, 2p, 2c, 1bw
Author(s):	Wang, Wallace
Thesaurus Term(s):	COMPUTER security
Product(s):	SECRETS & Lies (Book)
Abstract:	Focuses on the book 'Secrets and Lies,' by Bruce Schneier. Book's discussion of topics relating to computer security; Exploration of cryptography; Ways in which people have attacked encrypted data; Explanation of the creation of attacks that defeat or circumvent protective technologies; Ways in which hackers defeat biometrics.
Full Text Word Count:	1505
AN:	3884373
ISSN:	10542760
Database:	Business Source Premier

Section: Notes From the Underfround

SECRETS & LIES AND THE NEW AES STANDARD

If computer security has taught you anything, it should be that you're going to wind up doing a lot of reading just to keep up with the latest advancements in the field. Computer security professionals are already overwhelmed by information streaming out from the hacker underground community in the form of zines, Web sites and Usenet newsgroups, but also through their peers publishing books and magazine articles.

Although there are many useful and interesting computer security books available, one of the first books you should read is Secrets & Lies by Bruce Schneier.

SECRETS & LIES

Bruce Schneier wrote the classic Applied Cryptography book, so anticipation was naturally high for a follow-on book. Originally intended for publication in 1998, Secrets & Lies was only recently released. The delay reflects Schneier's change of heart in relation to cryptography. Unlike the extremely technical discussion of cryptography in Applied Cryptography, Secrets & Lies focuses on the more general topic of computer security, why it will never be 100 percent secure and why it doesn't have to be.

Secrets & Lies covers a wide range of topics peppered with interesting tidbits of trivia, such as stories about how the National Security Agency (NSA) eavesdropped on Soviet leader Kruschev's car phone, how someone issued a fake Bloomberg report to shoot the market price of PairGain Technologies stock up 30 percent and how voters in Dodge County, Georgia, tried to sell their votes in 1996.

Although Secrets & Lies does discuss cryptography, the book provides far fewer technical details than

Applied Cryptography. If you're expecting to see C source code and mathematical equations, you won't be happy with Secrets & Lies. But if you're a manager who needs to know more about computer security and what it can do rather than how the technical details work, you're the type of audience Secrets & Lies is aiming for.

The first few chapters discuss cryptography and the different ways people have attacked encrypted data ranging from brute-force attacks to password stealing. For every protective technology created, Schneier explains how others have created attacks that defeat or simply circumvent those defenses altogether.

For example, biometrics has been touted as nearly infallible because everyone has a unique set of fingerprints. Yet it can be defeated if an attacker simply captures the digital representation of a person's fingerprint and inserts that digital information into the targeted computer. As far as the computer knows, there is no difference between an authorized user pressing a finger to a sensor that sends the fingerprint data to the computer, and an attacker sending that identical data to the computer without once having touched the fingerprint sensor.

Similarly, digital signatures face the same problem. It's difficult to accurately forge another person's signature, but it's trivial to copy and use that digital signature over and over again, essentially forging another person's identity.

Related to digital signatures is the digital signing of code such as ActiveX or Java applets. Unfortunately, while the technical details are hard to forge, this system ignores the real problem. Most people don't have the slightest clue when to trust and when not to trust an ActiveX control Since nine times out of 10, most users are not going to have a problem, they will simply trust every ActiveX control they see, whether it's been digitally signed by any self-proclaimed trusted entity or not.

And that's the main theme of Secrets & Lies. Technology can only solve technical problems; it can never solve security problems that rely on human gullibility and trustworthiness to keep systems secure. Despite the tone of impending doom that permeates most of the book as Schneier explains each security problem, discusses how specific solutions are supposed to work and then explains how easily each solution has already been defeated, the book actually offers a final message of hope.

Rather than getting caught on the endless treadmill of technological advances, Schneier's latest book suggests that we use risk management. In other words, accept that computer security will inevitably fail, but that as long as a security system provides sufficient protection for a company to make a profit, that security system is secure.

Perhaps more convincing than any of the book's theoretical arguments is the admission that Bruce has shifted the focus of his company (Counterpane Labs) away from computer security and more toward intrusion detection and response (Counterpane Internet Security). Car alarms fail because they go off and nobody cares, and computer intrusion attacks are likewise often ignored.

Secrets & Lies suggests that the future of computer security lies in detection, response and, ultimately, prosecution. The reason hackers run rampant through the Internet isn't because the Internet is inherently insecure or that there aren't enough firewalls to stop them. Instead, the reason so many armies of hackers exist at all is that cracking is one of the few forms of attacks that can be conducted anonymously over long distances, practically guaranteeing that detection and prosecution will be nearly impossible.

That's why you don't see armies of burglars going from house to house, checking for open doors. Someone might see them doing this and call the police to come out and catch them. As Secrets & Lies suggests, this same threat of detection and prosecution can drastically reduce the number of crackers and script kiddies, who are responsible for causing many of the more irritating attacks today. Once crackers realize they can and will be caught, the threat to security could plummet overnight.

Secrets & Lies is easy to read and provides a gentle introduction to a wide range of security technologies from public-key encryption to encrypting data on smart cards. In retrospect, much of what Bruce Schneier says sounds like the obvious, but that's exactly why such a book is important for any security professional to read. When a book makes something seem obvious in retrospect, there's an important message in its pages that everyone needs to hear.