Book Review

Secrets & Lies: Digital Security in a Networked World

By Bruce Schneier
John Wiley & Sons, New York, 2000; 412 pages

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

So sayeth Bruce Schneier, the guru in security systems circles. His statements are often blunt but he certainly backs them up with the right credentials. He authored one of the classic texts on cryptography ***(Applied Cryptography)*** and BLOWFISH, one of the most frequently used encryption algorithms used in business systems today. BLOWFISH is the algorithm used in the PRIMAR Security System. Although Schneier's first book, ***Applied Cryptography***, is a hefty tome packed to the brim with algorithms and more than most would ever want to know about the world of secret coding, this new book is eminently readable by the non specialist. It is definitely a worthwhile read for anyone interested in, or concerned with, some of the unique security challenges being raised in this new evolving networked world. And, if one is to believe Schneier, there is plenty to be concerned about.

Having said that, Schneier is quick to point out early in this new volume that his previous work had been naïve in its presumption that mathematics would solve all security problems. In fact, he points out, security is really more a people issue than a technical one. That revelation can come as a shock to many people who see digital security as some bolt-on process, commercially available and easily installed. Security, Schneier reminds us, is a risk management proposition. Getting people to understand that risk and prepare appropriately for it, is his mission.

Digital systems raise many security challenges for a number of reasons. Systems are complex with thousands of components; they interact to form larger, more complex systems; they have emergent properties with unanticipated effects on their users. Most importantly, they have bugs causing the system to perform in unexpected and peculiar ways. All these characteristics make it difficult to make systems secure. It calls for a different approach.

The usual method for treating complex problems is to break them down into well-defined components. This is the appeal of cryptography in security systems. Cryptography is well defined, manageable and implementable. Software fixes like cryptography and hardware fixes like firewalls are seen as bolt-on solutions. They can initially make people feel safer, but in the end add little defence against any serious attack.

Is your house safe just because you bought a good door lock ? Will a thief spend hours trying to pick the lock or just put a brick through your window or jack the door open with a crow bar ? Experience shows attackers always take the easy route and simply side step security devices. For example, many security systems employ encryption with long key lengths in a superficial attempt at more security. In theory this is a good idea as longer key lengths are indeed more difficult to crack. In practice however, access to the secret key is protected by a password – often a user-defined password. Thus the security hinges not on the key, but on the user's password. And password protection is notoriously weak. A freeware program available over the Internet will crack almost all passwords through a so-called dictionary attack in a few seconds on a standard PC. Actually it's worse that that as many users, fearing they will forget their password, will write it down nearby, some on a post-it note on the underside of the keyboard - the equivalent of hiding the key for that new, state-of-the-art lock, under the porch mat. So longer key lengths, just like more door locks, don't necessarily give you more security.

Schneier is a great believer in threat modelling and risk assessment. Threat models can be made by using a technique called Attack Tree Analysis. Attacks against a system are graphed in a tree like fashion with the attack goal as the root and the different ways to attack as the stem and leaves. All possible attacks are drawn out and values associated with each attack such as possible/impossible, probable/improbable, cost of attack, need for special equipment, etc. Evaluating the various options in the Attack Tree will show the most likely threat area. Knowing the threats allows the organisation to develop an appropriate Security Policy that lays out the goals and objectives of the system. It outlines the motivation for the security, leading the way to the most appropriate set of countermeasures. For example protection against amateur pirates, where basic countermeasures will normally suffice, is a much simpler problem than developing a security system to protect against the determined professional.

The book is laid out into three main themes; Landscape, which details the existing threats; Technologies, that gives the state-of-the-art in security technology and Strategies, that lays out the process to follow in evaluating and then acting upon security threats. There is also an extensive chapter devoted to product testing and validation of security products. Other chapters deal with the human factor, firewalls, biometric devices, smart cards, authentication, digital watermarking, coming security problems associated with new networked devices like photocopiers, the effects of more teleworking, mail bombing and denial of service attacks, email viruses, and perhaps one of the biggest problems of all – security bugs in our everyday system software.

This is an excellent book written for the non-security specialist. It is written in an easy-to-read, almost chatty style. It provides a process for the non-specialist to follow in evaluating security risks, actions and possible consequences. I highly recommend it.

Book reviewed by M.J. Casey