Steven Stanek
PP190-Book Report

# Book Report: Secrets and Lies

Bruce Schneier's *Secrets and Lies: Digital Security in a Networked World* is a text primarily targeted at a technical and business audience dealing with digital security threats and mechanisms to help curtail them. However, the text also details several policy problems relating to cryptography, security and privacy. Schneier, a founder of a security company and an internet security consultant for large corporations, doubtlessly overstates some of the security threats to consumers and companies alike but there is no denying that computer security or lack thereof will have many policy, social and business implications in the years to come.

One main point of *Secrets and Lies* is the conclusion that as software complexity increases, more security holes appear as the increased size makes finding security problems in large amounts of code much more difficult. Unfortunately, the conventional forms of quality assurance in the software industry, beta testing and stress testing, do not find subtle security bugs because the programs appear to function perfectly on the surface. An attacker intent on breaching a program's safeguards can actively look for a single security flaws which allow him access. These flaws rarely surface during the beta testing process which is designed to insure functionality but not search for security bugs. Schneier's proposed solution, running software through rigorous testing by security experts such as himself is expensive and doesn't guarantee protection, it simply helps eliminates the obvious flaws, thus making attacks more difficult. For these reasons, it is doubtful that technology alone can solve computer security problems in the foreseeable future.

Schneier also stresses that security is a "process, not a program" and that "security is only as strong as the weakest link", these two principles indicate that many companies claiming to have "buzzword complaint" products, for example touting the new AES cryptographic system, are not necessarily secure. While a good degree of academic and government research goes into breaking cryptographic algorithms, these attacks are often very theoretical or require a unfathomable amount of data and computer time. Often much simpler attacks such as those exploiting buffer overflows or unsecured ports have the same net effect as breaking very secure cryptographic systems but are easy to accomplish on home computers. Since these attacks are subtle and are not reflected in marketing specifications, even a well informed purchaser would have difficulty deciding between seemingly identical products which in fact offer very different levels of security.

An additional threat to information technology lies in the people who program and use supposedly secure computers. Programmers are known to often leave intentional loopholes in security systems to allow themselves access in the future or as leverage for additional pay. Whatsmore, most end users of products, corporate and government employees or home users, are

not very vigilant. Schneier mentions that most people do not spend time reading the Secure Socket Layer (SSL) certificates that authenticate web commerce despite the fact that they are often indicative of a "man in the middle" attack (due to poor web site design). Many employees are a susceptible to a process known as social engineering, where a malicious individual is able to convince a well meaning employee to grant her access to sensitive systems. Likewise, after security flaws are discovered many system administrators never install the patches closing these holes. Without these patches, systems are open to incursions in the future.

Security holes and defensive design aside, Schneier argues malware, Trojan horses, worms and viruses, have already caused significant damage and will continue to do so in the future. Sometimes relying on security flaws, but often the actions of computer users to propagate, many of these pieces of software have caused data to be lost and networks to be saturated by traffic. Furthermore, Schneier claims that no widespread virus has yet attacked with a truly malicious payload (for example erasing all Microsoft Word documents on every computer it infects). Such a virus could have far more devastating financial repercussions than its predecessors. While antivirus products do exist, they are often only useful after a virus has struck and thus don't prevent damage during the first hours of attack. With the speed that viruses spread millions of dollars damage can occur in this interval, and even after the anti-virus updates are made available, many unprotected computers are easy to victimize. Stiffer penalties for virus writers coupled with technological solutions in searching for suspicious behavior may be the only possible preventative measures.

Security flaws allow computers to be attacked by a variety of parties, with different goals but all of whom are potentially damaging. These parties range from "common criminals" who seek wealth through fraud or blackmail, hackers and crackers who try to break into computers because of the technical challenges associated with the incursions to "Cyberterrorists" who see the Internet as a place to draw attention to their causes and government intelligence agencies and police forces such as the NSA, FBI and Defense Intelligence Agency which attempt to learn about foreign nations, their own citizens as well as criminals and terrorists. Of these groups really only the hacker and cracker group is unique to the Internet the rest are simply digital extensions of real world entities. While highly publicized, most of these groups have yet to cause significant damage online. Most of their actions have been electronic vandalism such as defacing web sites, or engaging in denial of service attacks against specific targets. While these are nuisances which are potentially costly none have yet caused irreparable damage or affected the lives of the majority of internet users.

Schneier claims that most modern computer security is focused around the concept of prevention but attempting to utilize "impenetrable" firewalls, secure servers and encrypted e-mail systems alone is insufficient. He advocates the increased use of monitoring tools known as Intrusion Detection Systems (IDS) to catch attackers in the act and that once their sorties are detected they

should be promptly responded to. This response portion of the problem is would seem to be mostly a matter for law enforcement but organizations policing the Internet are notoriously slow and overworked. Unfortunately, Schneier claims that law enforcement has been unable to cope with the problem at large but instead chosen to pursue specific targets. Schneier cites the long sentences given to hacker Kevin Mitnick and Melissa virus writer David Smith as "overcorrection", where police attempted to make an example of one or two well known figures while the majority of computer criminals go free.

Since law enforcement appears unable to dedicate the resources necessary to respond to the majority of computer crimes (especially the minor ones), Schneier sees the rise of private companies tasked to hunt criminals for clients who pay them for protection. He alludes to the Pinkertons who were legendary for their pursuit of train robbers after the robbers held up trains protected by the Pinkerton company. Unlike the Pinkertons, modern companies probably shouldn't be allowed to make arrests or break into private homes, but they could track attackers and provide that information to the appropriate authorities. Effectively such private firms would engage if the difficult process of finding criminals on the internet and then provide their physical whereabouts to legitimate police who would make the actual arrests. Alternatively, their information could be used civil suits against the offenders. If such enterprises become common, the government will need to both develop mechanisms for interacting with these firms and may need to implement restrictions on their powers.

One of the major hurdles all purchasers of software face is the lack of accurate information regarding security products. Schneier notes that unlike other industries where evaluation of products by organizations such as *Consumer Reports* is welcome, companies promising security often take steps to hide the flaws in their products. The United State Government attempted to set up a organization for receiving reports of security bugs called the Computer Emergency Response Team (CERT) which would notify manufacturers of valid security problems in their products. The manufacturers were then supposed to fix the reported bugs and CERT could publish the details of the problems and encourage users to apply the appropriate fixes. Unfortunately, manufacturers feared that negative publicity would be created by public knowledge of their products' bugs and for the most part the flaws went unfixed so that CERT would never publish them.

The failure of CERT lead many bug finders to publicly contact the press or post details of attacks on news groups and mailing lists which were read by fellow researchers and hackers alike. By making their discoveries public, through a process known as "full disclosure" these bug finders attempted to shame the manufacturers responsible for the products into patching them. Unfortunately, by making public announcements, full disclosure makes the flaws available to crooks as well. Since it takes the manufacturers time to patch bugs and many system administrators never actually apply the patches, these public announcements can open the way

for attacks. Such announcements have often resulted in public denials of the bugs and the use of the legal system to attempt to gag those who found flaws through provisions of the Digital Millennium Copyright Act (DMCA) and the Uniform Computer Information Transaction Act (UCITA).

Since preventing public announcements does nothing to prevent other malicious hackers from independently discovering the same flaws, the practice of hiding security defects doesn't make a company's products more secure and leaves holes that should have been closed open to attack. Schneier claims that since these glitches would remain, full disclosure by bug fixers and its associated problems are more desirable than keeping these problems quiet. He also claims that holding companies legally liable for the flaws in their products in the same manner as car manufacturers and food producers will decrease the number of products making false claims of security and increase the overall quality of software products. Unfortunately, Schneier admits that his and other security companies have quite frequently allowed flawed products onto the market despite their best efforts at making them secure. If the best experts in the field are unable to secure software before it goes to market, it is very doubtful that any degree of legal liability will be able to single handily radically improve security.

Perhaps a better alternative can be coupled with another of Schneier's suggestions. He suggests that the corporations could purchase hacking insurance from insurance companies which could gave their clients a discount on their premiums if they were to install products which were known to be more secure. Although Schneier warns of the dangers of laboratory tests in which a certain suite of attacks is mounted against a particular product, surely an independent testing organization such as Underwriters' Labs could evaluate security products and rate their security by actual testing, not technical (buzzword complaint) standards such as the US Government's Orange Book. Even companies which are not insured would have access to the laboratory rating of products, providing better information to all parties so they can make intelligent product choices.

Another possible method of improving security would be to strengthen CERT's authority to force bug corrections. CERT could be given the power to fine or publicly chastise companies that did not promptly correct reported bugs. CERT could also rate companies based on the number of actual vulnerabilities reported and total deployment (you don't want the popular products to be attacked most and thus have the worst ratings). The latter might encourage companies to evaluate their competitor's products for signs of weaknesses and spend extra time evaluating their own in hopes of improving their relative CERT ratings, thus driving up the security of all software.

Also, Schneier claims that a major security flaw exists in the present Secure Socket Layer (SSL) electronic commerce protocol. SSL is used to allow buyers and sellers to securely transfer credit card numbers and personal purchasing information over the internet to facilitate sales. For this

protocol to work, the seller sends a certificate signed a certificate authority (CA) to the buyer. The buyer is able to authenticate the CA's signature, telling him that the merchant is "trusted". Unfortunately, often the protocol doesn't ensure that signed certificates are from legitimate businesses and not criminals intent on stealing a credit card number who were able to someone acquire a signed certificate. While changes in the protocol could partially correct this flaw, CAs could also be legally forced to issue certificates to trustworthy merchants and penalized when their certificates are abused.

In some states these same CAs are attempting to make digital signatures have the same power as a written signature in that they are nonrepudiatable, that is these signatures cannot be claimed to be false. These laws are quite troubling since private keys used for digital signatures are stored on local hard disks, Trojan Horses or viruses could break into them and begin signing documents without the computer's owner ever knowing. Since the signature is cannot be repudiated, all of the documents would legally be signed by the owner of the private key. Even if the private key was password protected, modern hardware allows most passwords to be broken in a matter of hours. Clearly laws affecting digital signatures will need to be revised should either digital signatures or attacks on them become common place.

As the number of complex but vital systems in the world increases so does the number users who can be affected by their potential failures. The increased value of these systems will make them larger targets for criminals, terrorists and hackers who seek wealth, a cheap forum for airing their messages or who see their breaking security as a difficult problem. Schneier tells us that complexity, made possible by Moore's Law, hurts security by increasing the number of possible holes through which attackers can enter a system. He also tells us that some modern systems are very flawed. Near the end of his book, he estimates that nearly twenty times as much credit card fraud occurs on the internet as in physical "brick and mortar" stores. Mechanisms for responding to and prosecuting these e-criminals, establishing standards to audit security products and enforcing secure commerce will probably not be possible without new laws and policies.