Are Laws Sufficient?

Computer crime continues to be defined within our legal system. This article examines the effectiveness of current law in our global environment. Included is a recommendation for future laws to specifically embrace technical solutions.

Within Europe, there is a large organization of computer hackers known as the Chaos Computer Club. During the late 80s, this club successfully attacked computers owned by the National Aeronautics and Space Administration [1]. At that time, West Germany, where the attacks were launched, did not outlaw hacking. With the advent of the Internet, how effective are US laws in deterring computer crime by non-US countries?

Recently, one hacker from a group calling itself *Global Hell*, was arrested following a several month FBI investigation [2]. In a more sober alleged incident, hackers may have seized control of a British satellite and demanded a ransom [3]. Obviously money and fame will continue to motivate hackers. However, there are indications of a more serious threat.

During the latest arguments between China and Taiwan, cyber attacks were directed at opposition computers [4]. There are suggestions that the Governments of both China and Taiwan may have sanctioned the attacks. Arguably, there are a number of countries, such Iraq and Yugoslavia, that are openly hostile to the United States. These countries most certainly would not abide by US law. To explore the ramifications of state sponsored cyber war, its worth reviewing references of US activities.

Computer viruses have been described as mechanisms to launch electronic warfare [5]. To this end, the US Army has been researching computer viruses for use in cyber war [6]. More recently, reports indicate the CIA was given the OK to “diddle with Milosevic’s bank accounts” [7]. We are also the recipient of cyber attacks. According to Deputy Secretary of Defense, John Hamre, referring to Russian state sponsored Internet attacks, “we’re in the middle of a cyberwar,” [8].

Today, software is rolling out with varying degrees of quality. The current offerings of compiled programs offer opportunities to hide malicious code [9]. As the application size increases, the frequency of exploitable errors increases. Therefore, it is important to properly protect computing resources. Unfortunately, many organizations do not exercise due care when it comes to computer security. This is compounded by the uncertainty of what is allowable security under US law.

The uncertainty of approved encryption has caused commercial vendors to use inadequate strength encryption [10]. The FBI has expressed concerns that if strong encryption is used, it will be difficult if not impossible to wire tap. Similarly, the FBI proposed reducing the security in digital telephone equipment to ease wire tapping [11]. While the intent of the law enforcement and intelligence communities is understandable, any statutory effort to reduce security should be strongly discouraged. Fortuitously, the Administration is reversing its previous stand on encryption [12]. However, the Attorney General offered the following rebuttal to the revised encryption policy” "will result in greater availability of encryption, which will mean that more terrorists and criminals will use encryption" [13]. Consequently, statutory and regulatory efforts to reduce the security in commercial products will continue.

Summary:

New cyber threats are redefining the electronic landscape. Hopefully, you will agree that improved security within commercial off the shelf products is important. We have already experienced problems with commercial software defaulting to a non-secure mode of operation. The risk of mandating lax security in commercial products is too great. Hopefully, we can convey this warning to the requisite parties.

References:

[1] *Computers at Risk*, National Research Council, pages 61-62, National Academy Press, 1991.

[2] Suro, Robert, “The Hacker Who Won’t Quit,” *Washington Post*, page A01, September 1, 1999.

[3] “Did Hackers Hijack a British Military Satellite?,” *Time Daily*, March 1, 1999.

[4] Laris, Michael, “Chinese Web Warriors,” *Washington Post*, Page A15, September 11, 1999.

[5] Cramer, Myron L., “Computer Viruses as Electronic Warfare, page 689, ” *14th National Computer Security Conference*, 1991.

[6] Waller, Douglas, “Onward Cyber Soldiers,” *Time Magazine*, Volume 146, Number 8, August, 1995.

[7] Vistica, Gregory L, “Cyberwar and Sabotage,” Newsweek, Issue 22_99a, 1999.

[8] Vistica, Gregory L., “We’re in the Middle of a Cyberwar.” Newsweek, Issue 12_99b, 1999.

[9] Davis, Russell, “Exploring Computer Viruses,” *4th Aerospace Computer Security Conference*, IEEE, 1998.

[10] Stiener, Richard C., GAO Testimony before the Committee on the Judiciary, November 4, 1993

[11] Communication Privacy, GAO/OSI-94-2, GAO, November, 1993

[12] “Administration Announces New Approach to Encryption,” Statement by the Press Secretary, The White House, September 16, 1999.

[13] Focus - US Relaxes Encryption Export Limits, Reuters, September 16, 1999.