Why Do Hackers Have the Advantage?
The Problem with a One-Dimensional Security Approach
Brent Stackhouse

Modern computing is increasingly marked, or marred, depending on your viewpoint, by conflict. Along with more pleasant terms like "groupware," "chat rooms," and "virtual communities," the general public is becoming more familiar with terms like "hacker," "virus," and "attack" in relation to computing ("hacker" will be used here in the conventional, and incorrect, manner throughout this essay to indicate users of modern technologies, including computer and telecommunications, with malicious intent[1]). For those who have, or are attempting to gain, experience in the area of information security, understanding terms like "compromise," "threat environment," and "vulnerability," is critical for performing their jobs. So on the one hand, the Internet is seen as a great tool for communicating, building community, and, perhaps more cynically, making money. On the other, it is seen as a basically unfriendly, or even hostile, environment that requires great care to navigate safely. The reality is that there is a contest in cyberspace, with basically two opposing parties. In this contest, there are analogies to classic warfare, or even sport, for that matter. There are opposing sides with different strengths and weakness, strategies and tactics, and philosophies and styles of combat or play. However, there is one huge difference between the current state of hackers vs. security professionals and conventional engagements: one set of combatants is limited in its involvement to primarily one dimension, which is defensive. In most sports, and certainly in war, the standard approach is to have both offensive and defensive capabilities. In fact, a common American phrase that is applicable to both sports and war alike is, "The best defense is a good offense." How does this imbalance affect the overall dynamic of information security and can or should it be changed? The ultimate assertion of this essay is that it is critical that security personnel, and society at large, become more active in examining and employing offensive capabilities to correct the current imbalance of information warfare.

Given the current imbalance of cyberwar, let us examine the advantages that attackers typically enjoy over their targets. While we do so, it is important to understand these advantages and the appropriate analogies to conventional war because, ultimately, both forms of conflict involve human beings and human nature does not change merely because the medium within which we conduct battle has changed[2]. Some of the primary advantages that hackers enjoy are:

- Relative mobility
- High level of knowledge-sharing
- Intensity
- Relative lack of assets
- General complacency on the part of ISPs and software vendors
- Advantages of attack (potential for surprise, economy of effect)

Each of these points is important and deserve some discussion.

First, relative mobility is the wonderful ability to present a moving source of attack or target in the sense that hackers do not create fixed, long-term bases of operation like companies, educational institutions, or governments do. It's generally not possible to go to a fixed point, so to speak, in cyberspace to find the bad guys. Whereas in meatspace, if a conventional attack is carried out by Russian armed forces, we are pretty confident that the country of Russia has not moved and we therefore have numerous targets at which to respond. Perhaps an adequate analogy might be to the Vietnam Conflict where the North Vietnamese forces emphasized mobility, among other things, thus diminishing the success of our bombing efforts[3]. The bottom line is we cannot stop an adversary we cannot find.

Next, the hacker community is very accomplished at sharing real-world knowledge of hacking and creating easy-to-use tools to accomplish same. IRC and other Internet technologies all lend themselves to semi-anonymous information-sharing and community-creation and hackers put them to great use. There is also a loosely-defined hacker code of ethics that encourages not only hacking itself but a larger social environment that can create a sense of belonging for normally anti-social people[4]. Contrast that with security professionals whose only common bond, many times, is the negative one of stopping hackers. That leads to our next hacker advantage, intensity.

While a short discussion of Michael Jordan may seem rather inappropriate in the midst of a discussion on cyberwar, he is a great example of intensity. There is no question that over his career, Mr. Jordan showed extreme athleticism. His aerobatics led to his nickname, "Air Jordan." However, one of his most underestimated traits that sets him apart from most other professional athletes, let alone other basketball players, is his intensity[5]. His ability to play year after year through sickness and other adversity, with such consistency and passion, and win so many championships, is a testimony to his intensity. Many professionals in other sports, even those who win championships, win one or maybe two over the span of their career. Those who are consistently excellent are extremely rare (Wayne Gretsky, for example). Why does this matter? Intensity, or desire, is that extra, non-quantitative factor that often makes the difference between victory and defeat in both sport and war, for that matter. Hackers clearly have the desire to spend many more hours per day than most security professionals. They often exhibit passion in their work that is sorely lacking in many working environments. The result is that even though hackers are underfunded and undereducated compared to systems administrators, their dedication, passion, and patience often make up for that lack.

Being underfunded, in fact, has one huge advantage: you have very little to lose. If a company has a large investment in online services, including e-commerce, having their web server(s) DOS'd may cost them a great deal of money. Many times, the only hit hackers take is the loss of a cheap dial-up account if they violate their ISP's Acceptable Use Policy. In "real-world" warfare terms, there is no point bombing an opponent who has nothing worthwhile to bomb. Thus, even if we can find the hackers, our ability to disable or destroy their assets is extremely limited.

The next advantage, general complacency on the part of ISPs and software vendors, ensures that network and software vulnerabilities continue to be created[6,7]. As long as there is no major disruption in service, ISPs tend to be lax in either preventing or following up on security incidents. This may be partially due to a lack of security knowledge and partially due to a lack of apparent benefit for doing so. The general state of the industry is that making money is not seen as having an obvious connection with adequate security implementations, even though they ultimately protect the overall investment. Software companies, including OS vendors, continue to push out programs with more lines of code per program, thus raising the possibility of bugs, including security-related bugs. Also, security tends to be a low priority in the approach of many application programmers, even though it is through their coding errors that many security vulnerabilities arise[8,9,10].

Finally, the advantage of attack versus defense is multifaceted. There is the element of surprise, even when it is limited by a defender's expectation of an attack. Over time, complacency can set in for any defense, virtual or physical, thus limiting its effectiveness. Attacking is also economical in the sense that a defender has to defend every possible point of entry whereas the attacker can focus his efforts on a short list of targets. All told, professional security personnel are at a grave disadvantage on many levels but the most profound limitation is the inability to balance attack versus defense. What can be done to change this imbalance?

Simply, professional security personnel need to incorporate offensive capabilities in their overall security approach. There are three main arenas that need addressing to enable effective offensive capabilities: legal, cultural and technical. Because most systems administrators live in countries of law and order, random or haphazard attacks on hackers without the support of law will not be viewed kindly. In fact, law enforcement may begin to see the good guys as the bad guys, if proper procedures are not followed. In America, there are well-established legal precedents or actual laws dealing with property, both physical and intellectual. These can and should be extended to cyberspace, as appropriate. Lawmakers need to be educated about cyberspace and the importance of information security to the prosperity and security of the whole country[11].

Also, there needs to be a cultural change on the part of security professionals, law enforcement, and the general public regarding information security and offensive capabilities. Security pros need to be willing to add offensive elements to their approach instead of merely waiting for the newest virus or buffer overflow in Sendmail. Those who enforce the law need to elevate their technical understanding of cyberspace, or else pursuit, apprehension, and prosecution of criminals will be much more difficult. Finally, the general public needs to be supportive of the punishment of cybercriminals. If all of these shortcomings are not addressed, hackers will continue to have the upper hand.

Lastly, technical tools are needed to properly track and disable hackers and their capabilities. Tools are already on the market that improve the ability to track hostile adversaries[12]. As these tools improve, the imbalance between hackers and systems administrators will stabilize and the ability to peacefully exist in cyberspace will improve dramatically. Much of the difficulty in targeting the hackers is due to the inherent lack of security in Internet technology, including TCP/IP itself. Security has largely been an afterthought in computing, which obviously has helped malicious users. The next version of the Internet Protocol (IP), version 6, has significantly more security features built in[13].

Perhaps not surprisingly, the military has been quick to understand the dangers and possibilities of information warfare and they have been aggressively pursuing offensive as well as defensive capabilities. Though under very different restrictions, and with very different objectives, civilian information security specialists need to also develop a balanced approach to protecting information assets. Despite huge hurdles to overcome in the areas of immature cyberlaw, an uneducated populace, and the lack of effective offensive tools themselves, a concerted push must be made to begin disrupting hacker operations closer to where they originate and raise the legal and social penalties for hacking. Groups like SANS and CERT, among others, should be encouraged to take the message to legislators and law enforcement. And tools and protocols should be developed to help track and defeat hackers before their attacks are successful. When these actions are taken, hacking will be seen as a much less viable hobby for the classic, underfunded hacker and our information infrastructure will be much more secure from well-funded attackers as well.

Footnotes:

1 Raymond, Eric. "The Jargon Dictionary." Version 4.2.0. 1/31/2000.
URL: http://www.netmeg.net/jargon/terms/c/cracker.html (4/10/2000).

2 Wilson, Michael. "Hardwar, Softwar, Wetwar - Operational Objectives of Information Warfare." 1995.
URL: http://www.fas.org/cp/eprint/96/hswwar.htm (4/12/2000).

3 Meyers, Barton. "Vietnamese Defense against Aerial Attack." 4/19/1996.
URL: http://www.ttu.edu/~vietnam/96papers/meyers.htm (4/12/2000).

4 Unknown, not attributed. "Hacker Ethic." Unknown Date.
URL: http://www.thefuturesite.com/catman/faq/hacketh.html (4/12/2000).

5 Wilbon, Michael. "Jordan, the Definition of Focus and Intensity." 12/30/1999.
URL: http://www.quokka.com/9912/30/QCMa4aofc_s_jordan_WFC.html (4/12/2000).

6 Censor, Alex. "How To Secure Cable Modems." 8/9/1999.
URL: http://planetit.com/techcenters/docs/desktop_computing/expert/PIT19990801S0002 (4/12/2000).

7 Egelhof, James. "America Online Security?" Final Build - 1995 - 1996 Reference.
URL: http://www.aolsucks.org (4/12/2000).

8 de Mes, Arjan. "Jargon 4.2.0" 1/31/2000.
URL: http://www.science.uva.nl/~mes/jargon/b/bufferoverflow.html (4/12/2000).

9 CERT Coordination Center Staff. "CERT Coordination Center , 1999 Annual Report (Summary)." 1/31/2000.
URL: http://www.cert.org/annual_rpts/cert_rpt_99.html (4/12/2000).

10 Festa, Paul. "RealNetworks says RealPlayer bug won't sting." 4/4/2000.
URL: http://news.cnet.com/news/0-1005-200-1639271.html (4/13/2000).

11 Pethia, Richard. "Removing Roadblocks to Cyber Defense." 3/28/2000.
URL: http://www.cert.org/congressional_testimony/Pethia_testimony_Mar28-2000.html

12 Unknown.
URL: www.recourse.com (4/13/2000).

13 Unknown. "Advantages over IPV4."
URL: http://www.ipv6.com/advantage.html (4/13/2000).

Other Relevant Links:

The Center for Strategic and International Studies, Global Organized Crime Project Task Force on Information Warfare. "Information Warfare/Information Assurance."
URL: http://www.csis.org/goc/taskinfo.html (4/12/2000).

Widnall, Sheila and Fogelman, Ronald. "Cornerstones of Information Warfare."
URL: http://www.af.mil/lib/corner.html (4/12/2000).

Unknown. "Army Vision 2010, Information Superiority." Last Update, 11/16/1996.
URL: http://www.army.mil/2010/information_superiority.htm (4/12/2000).

Venzke, Ben. "Information Warrior." 08/1996.
URL: http://www.wired.com/wired/archive/4.08/schwartau_pr.html (4/12/2000).

McClure, Stuart and Scambray, Joel. "Security Watch." 3/1/1999.
URL: http://www.idg.net/crd_security_68309.html (4/13/2000).