AU/ACSC/055/2001-04

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

ACTIVE COMPUTER NETWORK DEFENSE:

AN ASSESSMENT

by

Eric J. Holdaway, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Major John Glock

Maxwell Air Force Base, Alabama

April 2001

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

Illustrations

Page

Preface

Threats to the security of the DoD's networks have been the topic of much research and speculation, and concerns remain about the ability of present defenses to assure their availability. One of the options is "active defense", yet the concept is as yet poorly defined.

I wish to first thank my advisor, Major John Glock for his guidance throughout, and especially for providing the impetus often needed to keep my nose to the grindstone. I also wish to thank Major Lisa Onaga and Captain Mike Miller of the 39th Information Operations Squadron, and Colonel Richard Stotts of the Air Force Information Warfare Center, for pointing me to sources and making sure I could get access to them. Without their help, I could never have completed this paper.

Abstract

A Presidential Commission, several writers, and numerous network security incidents have called attention to the potential vulnerability of the Defense Information Infrastructure (DII) to attack. Transmission Control Protocol/Internet Protocol (TCP/IP) networks are inherently resistant to physical attack because of their decentralized structure, but are vulnerable to CNA. Passive defenses can be very effective in forestalling CNA, but their effectiveness relies on the capabilities and attentiveness of system administrators and users. There are still many measures that can be taken to improve the effectiveness of passive defenses, and one of these is active defense. It can be divided into three categories: preemptive attacks, counterattacks, and active deception. Preemptive attacks show little potential for affecting an adversary's CNA capabilities, since these are likely to remain isolated from the Internet until actually beginning their attack. Counterattacks show more promise, but only if begun early enough to permit all preparatory activities to be completed before the adversary's CNA is completed. Active deception also shows promise, but only as long as intrusions can be detected quickly and accurately, and adversaries redirected into "dummy" networks. Active and passive defense measures can work synergistically, to strengthen one another.

Chapter 1

Introduction

The United States is vulnerable to sneak attacks in cyberspace that could amount to a "digital Pearl Harbor," a top government official warned on Friday. Richard Clarke, who coordinates security and infrastructure protection at the White House National Security Council, said the next U.S. president must shield the economy from foreign cyber warriors.

—Reuters, December 8, 2000

Despite the United States armed forces' widely discussed dependence on their information systems infrastructure, called the Defense Information Infrastructure (DII), almost all defensive efforts have been focused on passive measures. While these efforts seem to have been sufficient up to this point, the numbers of reported computer security incidents and vulnerabilities have increased significantly, as shown in Figure 1.

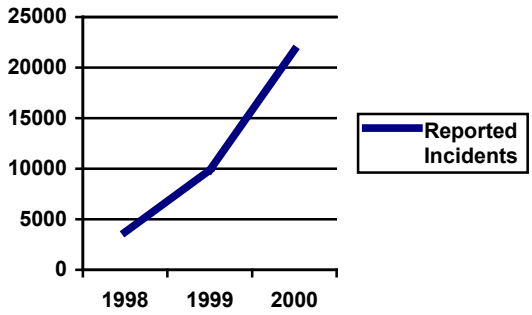

Figure 1 – Reported Computer Security Incidents, 1998-2000[1]

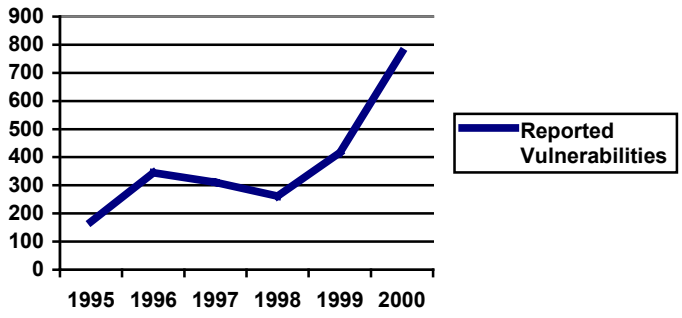

Figure 2 – Reported Vulnerabilities, 1995-2000[2]

There is, however, a growing school of thought which holds that passive measures alone cannot adequately protect the DoD's digital infrastructure from attack. This paper has two purposes. First, it intends to explore whether active defense is practical, and second, if information assurance efforts based on firewalls, encryption, and users' security awareness can be more effective with its support. Due to the attendant complexities, it will not address the legal issues surrounding computer network warfare. It will begin by defining some necessary terms and concepts, then describe the threat, discuss limitations of passive defenses, evaluate practicalities of counterattacks, preemptive attacks and deceptive measures, and conclude by synthesizing a recommendation for a synergistic employment of active and passive measures.

Definitions

Joint Vision 2020 mentions the information revolution in no fewer than three places, and identifies Information Superiority as a key enabler for victory in future warfare[3]. One of the key elements of Information Superiority is "the capability to collect, process, and disseminate an uninterrupted flow of information."[4] Information assurance is the activity that aims to create this part of information superiority, and computer network defense is one of its fundamental components. Most of these efforts center on passive defenses such as password protection, data

encryption, and firewalls, but recent events such as the October 2000 break-in to Microsoft's system, during which hackers may have succeeded in committing industrial espionage, have shown that these measures are far from perfect.[5]

So what exactly do we mean by "active defense", and what is its role in computer network defense? If we begin with a dictionary definition of active as "originating action; not merely passive or inert,"[6] we can broadly define it as any measures originated by the defender against the attacker. Because the purpose of any computer network defense is to protect information systems, these active measures must at least thwart any attack in progress, and ideally make further attacks more difficult. We can divide them into three broad categories: counterattack, preemptive attack, and active deception. A counterattack would be a CNA conducted against the attacker's information system during or immediately after the original attack. This is similar to a counterattack on the ground, where reserve forces are committed to attack the advancing elements of the adversary's force, with the minimum goal of creating a stable line of defense and preventing the adversary from getting loose in the rear area. Preemptive attacks would be CNA against the adversary's information systems infrastructure designed to prevent him from launching effective attacks against ours. One model for this would be US counterair doctrine, which holds that the best way to defend against an adversary air force is to attack it on the ground[7]. Another option might be to adapt Air Chief Marshall Sir Hugh Trenchard's theory of air superiority, that a strong offensive against an adversary's vital centers would soon force him on the strategic defensive[8], to information superiority. To paraphrase Trenchard[9], then, the gaining of information superiority will be incidental to this main direct offensive upon the adversary's vital centers sic and simultaneous with it. Lastly, we should consider active deception as a means to defend our information systems from attack. Similar to the concept of

judo, which uses the momentum of the attack to defeat it, active deception tries to channel an attack away from the defender's information system and into a virtual model of it. By doing so the defender leads the attacker to believe he or she is being successful, when in fact he or she is in fact neutralized.

Notes

[1] Computer Emergency Response Team (CERT) Coordination Center, *CERT/CC Statistics, 1998-2000*, Carnegie-Mellon University, available at http://www.cert.org/stats/cert_stats.html

[2] *ibid*

[3] Director for Strategic Plans and Policy, J5; Strategy Division, *Joint Vision 2020*, June 2000, 4

[4] *ibid.*

[5] Reuters. *Microsoft Break-in. O*ctober 27, 2000. Available at http://www.zdnet.com/intweek/stories/news/0,4164,2645864,00.html

[6] *The Concise Oxford Dictionary*, 9th ed. (Oxford: Oxford University Press, 1995), 14

[7] Department of the Air Force. *Air Force Doctrine Document 1: Air Force Basic Doctrine.* Maxwell AFB, Alabama. September 1997, 46

[8] Trenchard, Sir Hugh, *Memorandum on the War Object of an Air Force*, cited in Chaliand, Gerard, editor, *The Art of War in World History: From Antiquity to the Nuclear Age* (Berkeley and Los Angeles, California, The University of California Press, 1994), 907

[9] *ibid.*

Chapter 2

The Threat

> *IW attempts to beat the enemy in terms of promptness, correctness, and sustainability, and electrons are capable of reaching out and touching someone a long way away. It thus makes complete sense to put a significant effort into developing an information-based capability in both the civilian and military sense.*
>
> —Timothy L. Thomas, Foreign Military Studies Office

Unlike previous military technologies such as cannon or the airplane, civilian exploitation of the Internet now leads rather than follows that by the military. As a by-product, the emergence of the hacker subculture has produced something unprecedented in past Revolutions in Military Affairs, namely a glimpse of how the future may look. Both their activities and efforts by systems administrators to counter them help us sketch out the "virtual terrain" over which the CNA battle is likely to be fought. The first characteristic is the potential for espionage, as demonstrated by the hackers who managed to infiltrate Microsoft's servers in October 2000[1]. Second is the potential for inducing delays into the DII. Even in a best-case scenario, where the compromised system could be restored from backups, have its security holes plugged, and be reconnected, the attacker has managed to deprive users of its services for several hours at least. Just like the delays communications jamming can cause to command and control, this effect could be useful to an attacker. So even if the "Electronic Pearl Harbor" itself does not occur, successful espionage and harassment carried out through CNA might enable an adversary to carry out a real Pearl-Harbor-like surprise attack.

This section will first address the fundamentals of how communication occurs over the Internet, and will describe characteristics of various cracking techniques and the vulnerabilities that they exploit, along with the effectiveness of passive defenses against each. In addition to helping define the threat, describing these techniques will provide the knowledge necessary to assess their utility in a preemptive or counterattack. It will then summarize the capabilities and limitations of passive defenses to defeat these attacks, and will conclude with an overview of the entities which might pose a threat to the DII.

TCP/IP Fundamentals

Two of the primary communications protocols used on the Internet are the Transmission Control Protocol (TCP) and the Internet Protocol (IP); taken together with the other protocols used, they are called the TCP/IP Suite. IP allows data to be broken up into "packets" for transmission, each packet containing a header which identifies the address of its origin and the address to which it's going, and a body which contains the actual data being transported. TCP is the protocol that creates the "handshake" between the two communicating computers, allowing IP data packets to be sent and received. Each computer assigns an address, or port, to each application, through which another computer may connect.[2] Open ports are necessary for communicating between computers, but if hackers can gain access to a system through them, they are also potential vulnerabilities.

Players

Both state and non-state players have the potential to pose a threat to the DII. Several states have shown interest in developing CNA capabilities, and the relative low cost of entry means that states will not enjoy anything like a monopoly on CNA techniques and technology. The

next two subsections will attempt to describe state and non-state CNA that have already happened, and try to give a general picture of the nature of each.

State Actors

Some sources believe Russia may have been the first state to undertake a CNA against the US DII. In the so-called "Hannover Hackers" case in the early 1980s, the Soviet KGB employed German hackers in the city of Hannover to gain access to US DoD computers.[3] Some form of CNA efforts apparently carried through the demise of the Soviet Union, as the Moonlight Maze investigation reveals.[4] China and Taiwan also have demonstrated significant interest in information warfare capabilities. As early as 1995, Senior Colonel Wang Baocun and Li Fei of the Chinese Academy of Military Science wrote:

> Information offense means attacking enemy information systems. Its aims are: destroying or jamming enemy information sources, to undermine or weaken enemy C^2 capability, and cutting off the enemy's whole operational system. The key targets of information offense are the enemy's combat command, control and coordination, intelligence, and global information systems. A successful information offensive requires three prerequisites: 1) the capability to understand the enemy's information systems, and the establishment of a corresponding database system; 2) diverse and effective means of attack; and 3) the capability to make battle damage assessments [BDA] of attacked targets.[5]

In response, Taiwan began planning for information warfare as early as 1998 and publicly activated its first information warfare unit on January 1, 2001[6]. Discussion has also surfaced in Pakistan over the need to develop both defensive and offensive information warfare capabilities.[7] Any country with a sufficient base of knowledge in information technology can be assumed to be working on some form of computer network warfare, even if only defensive in nature. The Taiwan example indicates, however, that any country seeing a rival show interest in CNA may itself be spurred to develop the capability. State actors will have relatively large amounts of resources to devote to IW. Even a modest investment (by government standards) will allow

them to develop tools and techniques, build virtual models of the networks they intend to attack, and test tools and techniques against the models under controlled conditions, all sealed off from the Internet until they are ready to use them. They will, of course, need some prior knowledge of the victim network, and computer network exploitation (CNE) efforts to gain that information may well provide advance warning of which networks might be targeted. Provided they can get this information, the testing will allow them to adjust their tools and techniques to maximize effects against the intended target(s), to better conceal their efforts, and to minimize collateral effects. State actors that are concerned with the physical security of CNA assets may be more likely than non-state to originate an attack from within their own country or that of an ally. However, an aggressive CNA effort is likely to involve state agents travelling to a neutral or (to them) hostile state to originate an attack, with the object of disguising its true source. If the attacker uses the Internet to gain access to a network, he or she is likely to hack through several intermediate networks to make it more difficult to ascertain the origin of the attack. Finally, despite the relatively low cost of a CNA capability, the vastly greater resources of states *vis a vis* independent hackers indicates that the former will be able to develop CNE and CNA tools and techniques far beyond those yet encountered. Administrators may very well find that defenses that are highly effective in the peacetime environment are entirely inadequate to prevent, or even detect, CNE and CNA by a state-sponsored attacker.

Non-state Actors

These might be employed by states or might act independently. Plenty examples already exist of relatively independent hackers targeting web sites in support of one or another side during a conflict. For example, in the current conflict between Israelis and Palestinians,

> An online battle between Israeli and Palestinian vandals escalated this week with the theft and public posting of a database containing the personal information of

> 700 members of the American Israeli Public Affairs Committee on Wednesday and the posting of information by Israeli-affiliated hackers regarding Palestinian communications.[8]

The conflict need not even be an armed one: during a meeting of the World Economic Forum in Davos, Switzerland in January 2001, hackers opposed to globalization obtained and posted private information about attendees.[9] What is certain is that, much like the privateers of the 17th and 18th centuries, web vigilantes will be difficult to control, even by those who lead the cause they are acting to support. The availability of scripts and their ease of use imply that technical know-how is no longer the barrier to entry into CNA that it once was.[10] The sharp rise in web page defacements in rtecent years correlates very closely with the easy availability of scripts:

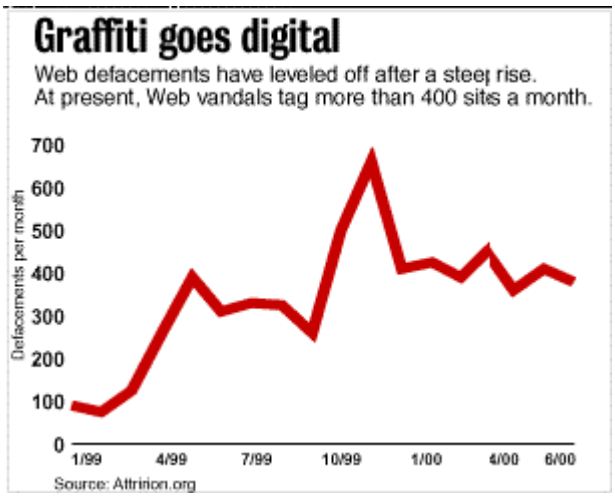

Figure 3 – Web Defacements 1999-2000[11]

The source of the attack might easily be within the United States, or a neutral or even friendly nation, and as with state actors, the attacker is likely to hack through several networks in several countries before attacking the ultimate target.

Notes

[1] Reuters, *Microsoft Break-in. O*ctober 27, 2000. Available at http://www.zdnet.com/intweek/stories/news/0,4164,2645864,00.html

[2] . For example, if the server receives a TCP request to connect through port 25, it knows the requesting ("client") machine wants to establish an e-mail connection using the Simple Mail Transfer Protocol (SMTP). If it receives a request to connect via port 80, it knows the request is for the hypertext transfer protocol (http), which is used by web browsers.

[3] Coale, John C., *Fighting Cybercrime*, Military Review, March-April 1998, available at http://www-cgsc.army.mil/milrev/english/MarApr98/coale.htm

[4] Bierbauer, Charles, *Senate Report: Nation at Risk of Y2K-related Terrorism*, CNN, September 22, 1999, available at http://www.cnn.com/TECH/computing/9909/22/cyberterror.y2k/index.html

[5] Baocun, Wang and Fei, Li, *Information Warfare*, excerpted from The Liberation Army Daily, June 13 and June 20, 1995. Available at http://www.fas.org/irp/world/china/docs/

[6] Hsu, Brian, *First Information Warfare Group Put Into Service*, The Taipei Times, January 3, 2001. Available at http://www.taipeitimes.com/news/2001/01/03/story/0000068206

[7] Amir Husain, Syed M., *Pakistan Needs an Information Warfare Capability*, Defence Journal, July 1998. Available at http://www.defencejournal.com/july98/pakneeds1.htm

[8] Lemos, Robert, *'Hacktivism': Mideast Cyberwar Heats Up*, ZD Net News, February 6, 2001, available at

[9] Carolan, Matt, *Vigilantism Online*, Interactive Week, February 7, 2001

[10] Scripts allow people with limited technical knowledge to threaten network security. See Appendix A for more information.

[11] Lemos, Robert, *Script Kiddies: The Net's Cybergangs*, ZD Net News, July 12, 2000, available at http://www.zdnet.com/filters/printerfriendly/0,6061,2602573-2,00.html

Chapter 3

Passive Defenses

> *[D]efense has a passive purpose: preservation, and attack a positive one: conquest…in order to state the relationship precisely, we must say that the defensive form of warfare is intrinsically stronger than the offensive.*
>
> —Karl von Clausewitz

Firewalls, anti-virus software, access control (with or without encryption), updates (patches) to software to correct security vulnerabilities, and adaptive response tools currently constitute the majority of defenses against CNA. Not only are these passive measures an important component of information assurance, should active defenses be employed in a preemptive or counterattack role, such defenses are likely to be encountered on hackers' systems. For this reason, we will now examine the main types of passive defenses.

Types of Passive Defenses

Firewalls

A firewall is either a combination of software and hardware, such as the PIX Firewall 4.1 supplied by Cisco to work with its routers, or a software application by itself, such as Norton Personal Firewall. By analyzing incoming packets of data it tries to prevent unauthorized users from accessing a network, and can be configured to do so in very specific ways. First, a firewall can screen users by point of origin; for example, DoD restricted unclassified networks use a

firewall configuration that allows only users from a recognized .mil domain to have access. It can also be configured to allow only certain classes of users to access certain applications, e.g., the firewall might allow access to a database of bomb competition scores only to members of the Wing Weapons shop. Third, a firewall can screen content; for example it can be "taught" to recognize and exclude executable code such as Java, or even a known attack signature.[1] Lastly, some firewalls such as Sun Microsystems' SunScreen, can "hide" unused ports from scanners. Configuring a firewall involves striking a balance between security and usability; i.e., the more restrictive the configuration, the less the ability to communicate freely through the network and/or between the network and the Internet. One way to work around this dynamic is to allow free access from systems known to be controlled by reputable administrators. This is called a "trust relationship", and it allows efficient communication without needlessly compromising security as long as the trusted network is itself not compromised. Should that happen, though, the attacker can exploit that trust relationship to bypass the firewall. Effective firewall configuration also requires updates to ensure it can recognize and exclude newly discovered threats. For these reasons, a firewall is only as good as the system administrator who runs it. Once it's penetrated, as was done to Microsoft's, it is no longer defending the network.

Antivirus Software

Perhaps the most pedestrian of security measures, effective use of antivirus software can be the crucial second line of defense for a network. Viruses are simply self-replicating files, and two particular subsets of the virus family, trojans and worms, can be used to compromise a network's security. Both contain code that will execute upon receipt of an external trigger, for example a date or a command sent by the attacker (for more details about viruses, trojans, and worms, see Appendix A). Regular updates to virus signature lists (which identify threats by the

length and structure of their code) and regular scans are probably the best way to detect trojans and worms that may have infiltrated a network. Antivirus software can also complement a firewall by being configured to scan all incoming e-mail for known virus signatures. The increasing prevalence of centrally controlled operating systems in DoD (such as Windows NT/2000) makes it much easier for system administrators to automatically download and install updated virus signatures, and to schedule automatic virus scans, on every machine in the network.

Access Control

The simplest and longest running way to defend a network is through access control. Users are assigned different levels of permissions, which determine which directories and files they may or may not access, and may or may not alter. The most powerful access is "root" access, which has permission to access and alter any directory or file on the network. "User" access has the least permissions, and is typically restricted to those functions needed by the average account holder, for example, e-mail, web browsing, certain shared applications such as office automation, and a private directory where files he or she has created may be stored. Varying intermediate levels may exist, such as "superuser", to allow the system administrator to delegate specific routine tasks. Access to an account is typically protected by a password, which creates a vulnerability; e.g., if any account password can be cracked, a hacker can use various tools to then crack the root account and gain access to the entire network[2]. Passwords that are easy to remember are also easy prey for password crackers; conversely those that are difficult to guess offer increased security, but users are more likely to write them down because they are also difficult to remember, thus increasing risk of compromise. One experiment by Daniel Klein of the Software Engineering Institute at Carnegie-Mellon University revealed the relative ease with

which a hostile party could gain access to a network. Using 15,000 actual passwords supplied by systems administrators, he applied various common cracking programs, and within 15 minutes cracked 368 passwords. After the first week of testing, the number rose to nearly 3,000 passwords, 21% of his sample.[3]

System administrators can ensure effective password security only by encouraging users to choose passwords that are easy for each of them to remember but which are not made up of common words or phrases, and by regularly running their own password crackers to identify weaknesses. Once again, password security is only strong as long as the system administrator has the time, energy, and clout to enforce it.

Patching Known Vulnerabilities

Of the 10 most common Internet security vulnerabilities identified by the SANS Institute in January 2001, nine had been identified in 1999 and one in 1998.[4] Patches and/or measures are available to correct all ten, yet they continue to be the most often exploited security flaws. As the SANS report states, "attackers are opportunistic…[t]hey count on organizations not fixing the problems, and they often attack indiscriminately, by scanning the Internet for vulnerable systems."[5] System administrators report "that they have not corrected these flaws because they simply do not know which of over 500 potential problems are the ones that are most dangerous, and they are too busy to correct them all."[6]

Intrusion Detection and Adaptive Response Tools

Intrusion detection software scans application logs and processes, looking for abnormal activity (the system administrator configures the software to define "abnormal"). It can then alert a system administrator to take action. Adaptive response tools are the most recent development. They mate intrusion detection software with automated responses, allowing a

network to "defend itself" against attacks. Is uses case-based reasoning to compare what it presently senses to past "experience", and "decides" how to respond to the possible intrusion, for example, by denying further access to a user it has determined is carrying out unauthorized activity.[7]

Passive Defenses: A Summary

Sun Tzu wrote: "if he [the enemy] does not know where I intend to give battle, he must prepare in a great many places."[8] The problem of passive defense is that it is only as strong as its weakest part: a hacker needs to find only one exploitable vulnerability to gain access to a system. According to the SANS Institute, the problem is not that these are hidden holes -- only a few security flaws account for the majority of security incidents, and these are already well known. It is commonly accepted that hackers don't target specific servers so much as they look for those which have weak security[9], which would suggest that a targeted CNA is unlikely. However, the successful penetrations of Microsoft and SecurityFocus indicate that with sufficient preparation, and either laxness on the part of even one employee or a very well-concealed CNA tool, the former is certainly possible. Adaptive response tools show promise but for the most part passive defenses are only as good as the system administrators and users who participate in them, and in any case they cede the initiative to the hacker.

Notes

[1] Anonymous, *Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network,* 2nd ed. Indianapolis: Sams Publishing, 1998, 274-275

[2] Klein, Daniel, *"Foiling the Cracker": A Survey of, and Improvements to, Password Security*, (Pittsburgh: Software Engineering Institute, Carnegie Mellon University, 1993), 3-4. Available at http://remus.prakinf.tu-ilmenau.de/Reif/Publications/CT9509/security-sokol.html

[3] *ibid.*

Notes

[4] SANS Institute, *How To Eliminate The Ten Most Critical Internet Security Threats*, January 18, 2001, available at http://www.sans.org

[5] *ibid.*

[6] *ibid.*

[7] Kenyon, Henry S., *Adaptive Response Tool Targets Hacker Intrusion*, Signal, August 1999

[8] Sun Tzu, *The Art of War* (Oxford: Oxford University Press, 1963), 98

[9] SANS Institute, *loc cit.*

Chapter 4

Active Defense

> *Japan is preparing to use electronic weapons to destroy the computers of hackers trying to infiltrate the country's defence systems. The move follows raids on government computer systems.*
>
> —London Daily Telegraph, October 24, 2000

Whether or not the "electronic weapons" described above exist, the appearance of the story does show some of the frustration system administrators feel when dealing with CNA. Passive defenses not only cede the initiative to the attacker, they also fail to contain within themselves any immediate threat of counteraction. We will now describe different potential active defenses, consider the prerequisites required for each, then determine possible outcomes.

Preemptive Attacks

As stated in Chapter 1, Air Force doctrine holds that the most effective means of neutralizing an adversary's offensive aerospace potential is by attacking his aerospace forces and their support structures. Alternatively, should an adversary's CNA assets not be vulnerable to preemptive action, effective attacks on his information infrastructure might either prevent or disrupt his CNA efforts. By examining both the prerequisites for a successful CNA and the likely outcomes, we can determine whether either of these models of preemptive attack is a practical option. Since preemptive attack is by definition a hostile act, command authorities are likely to approve it only for use against already defined hostile state and non-state actors, and

even then only if they have reasonable guarantees the attack's effects can be restricted to the hostile actor's network.

The primary assumptions underlying preemptive attack doctrine are that the adversary's offensive forces and/or their support structures can be located and either disabled or destroyed before they can be effectively used. Locating an adversary's CNA forces itself presents a difficult problem. Since the "weapons" themselves are the software applications, and are contained and used in computer networks similar to those that exist in corporate offices and bureaucracies, physical signatures are irrelevant. CNE carried out through the Internet might discover a potential attacker's offensive "weapons", but since there is no need to connect them to the Internet until ready to attack, this is unlikely. One better option might be to attack any scanners, sniffers, and password crackers found operating on adversary networks. Since these are also defensive tools, such preemptive attacks will also advance friendly offensive efforts, and may in fact already be underway as part of friendly CNA activities. A thorough exploration of the adversary's networks might reveal these assets, but this must be able to defeat all his defenses if it is to provide a complete answer, and this will be very time consuming. Detection and tracing of his efforts to scan our networks might more rapidly and accurately identify them, although there is no guarantee it will discover the true source of the attack. The network that appears to be the source of an attack might in fact be only an intermediate link used by the hacker to disguise the true origin, since hackers possess tools which can erase evidence of their activities, such as utclean.c and tlnthide.c.[1] Alternatively, the attacker may be running his CNE effort from a neutral or even friendly network that he has already compromised. In the former case attacking his CNE tools is at best problematic and at worst impossible for diplomatic if not technical reasons, and in either case the defender can deny one CNE capability but still has not

managed to harm his adversary's own network. Second, while authorities in neutral and friendly countries may be willing to acquiesce to probing of their networks to support law enforcement, they may be less willing to do so in support of a preemptive CNA. Should any part of the adversary's force be located, a CNE of the adversary's passive defenses is needed to map out the adversary's network and allow a successful preemptive attack to be planned. This will take additional time, and if the target for preemptive attack was found by tracing an adversary CNE effort, the adversary's attack may begin soon, or even be underway. For a more complete discussion of targeting considerations in planning CNA, see *"Operationalizing" Information Operations* by Major John Glock.[2] An important caveat comes into play if the network which contains the target for the preemptive attack does not belong to the hostile entity, as is especially likely when the adversary is a non-state actor: CNA against a network residing in a neutral or friendly country is something of command authorities are likely to be very wary, even if such an attack is ruled to be allowable under national and international law.

If the adversary's CNA forces themselves are not locatable or vulnerable, another option might be to rely on the offensive against the adversary's information infrastructure to forestall his CNA. A successful effort there will likely make it more difficult to launch attacks from in-place assets, however the portability of CNA "weapons", which can be loaded from off-line intranets to laptops, means this is far from a complete answer. Military or civilian agents can take the capability with them to third countries to launch their attacks, and may in fact be prepositioned prior to initiation of hostilities. In the case of non-state actors, the networks on which they rely will likely belong to commercial ISPs or universities, and US command authorities are unlikely to allow widespread targeting of such networks.

Counterattacks

Since the source and characteristics of an adversary CNA are unlikely to be apparent until it is actually in progress, another option for active defense is counterattack. While prerequisites for counterattacks are similar to those for any other CNA (including preemptive attacks), the conditions under which they must be accomplished are different.

As for preemptive attacks, the source of the attack must be located and scanned for vulnerabilities, IPB performed, and the attack carried out. Unlike preemptive attack, though, all these tasks must be completed before the attacker ends his attack and removes the network hosting his "weapons" from the Internet. First, a counterattack will require tracking the original attack back to the source, just like tracking adversary probes in support of preemptive attacks, with many of the same pitfalls including the chance a network might be misidentified as the source. While friendly countries are likely to take a much more favorable view of tracking hackers through their networks once an attack is underway, there is no guarantee neutrals will. Furthermore, while international agreements facilitate tracking hackers through other countries' networks for law enforcement purposes, similar agreements for military purposes will exist only between the US and friendly nations. Second, even if the source is reliably located, the time available for probing and IPB is unlikely to be sufficient. Once the CNE has been accomplished, the actual attack takes relatively little time, and since by definition the attacker is someone who should know the time required for preparing an effective attack, it is unlikely he will take longer than that to execute his own. While it is possible to reduce the preparation time by beginning it as soon as a probe is detected, an adversary who probes from one network and attacks from another automatically negates this counterattack. While counterattacks on the attacker's CNE capability is unlikely to prevent an attack, since the latter is likely to begin long before the

defender's IPB is even partially complete, it can forestall subsequent attacks. Lastly, a full-scale CNA on an adversary's information infrastructure may deny any indigenously based CNA and CNE efforts the access to the Internet they need, but will not affect any teams already deployed outside the hostile country. Furthermore, a capability can be reconstituted relatively rapidly, since the CNA and CNE tools and personnel can easily be deployed to other nations where they can regain access.

Effects of Successful Preemptive or Counterattacks

Assuming a preemptive or counterattack can be successfully launched, what are the effects likely to be? Destroying or damaging the computers from which an adversary plans to launch an CNA is likely to have only a temporary effect, since the computers themselves are relatively cheap in the context of governments' (or even terrorist groups') military expenditures, and damaged software (including "weapons") can be quickly replaced from backups. The real center of gravity is the hacker's knowledge. Deceptive efforts are likely to be more effective; successful preemptive attacks and/or counterattacks to alter an adversary's CNE capabilities can effectively "blind" his CNA forces, as long as the alteration is not discovered. Once it is, the adversary can rapidly restore his capability from backup sources and carry on as before, but at the cost of lost time.

Active Deception

Active deception takes an alternate approach to passive defense. Instead of attempting to keep intruders out of the network, it will want to redirect them into a false network, fully populated with the same sort of data and network resources that would exist on a real one, that exists solely to deceive them. Active deception has its own set of prerequisites, each of which

will be addressed below. While it cannot cause actual damage to the attacker's system, it does force him to expend effort for no gain, and allows the defender to observe his techniques and possibly capture his tools, and therefore provides the time and knowledge to create defenses against them. Furthermore, by creating the false impression that the attack has been successful, active deception further distorts the adversary's mission analysis of the effectiveness of his CNA effort.

Prerequisites for Active Deception

An effective active defense must be able to differentiate between attackers and legitimate users. The simplest way to do this is to provide an exploitable vulnerability ("trap door") which will lead him into the virtual dummy network, for example, an undefended port or a user account with a password vulnerable to a password cracker. Another means might be to install a patch for a known vulnerability, then use an adaptive response tool that recognizes the signature of the attack that exploits it, and allows the attacker into the false network. To be really effective the trap door will have to be altered regularly, because once it is recognized as such, it is no longer useful and the attacker will concentrate on finding real vulnerabilities.

Second, like all deception efforts, the false network will have to yield information that makes the attacker's efforts appear to be effective. At a minimum it should contain made-up user accounts, complete with randomly updated user files containing false but plausible information along with enough true information to lend credibility to the deception, and common network applications. It should be made up of several subcompartments, each with its own set of imaginary users and planted data. Once an attacker's TTP is recognized, each time he recognizes he's being deceived, backs out, and tries to hack into the real network, he could be redirected into a different subcompartment.

Active and Passive Defense Interaction

A common prerequisite for both preemptive and counterattack forms of active defense is time to prepare an adequate attack. Passive defenses and active deception are both methods that can delay the success of an adversary's CNA, and thus should contribute to the success of any preemptive or counterattacks. Similarly, any attack on an adversary's network that reduces his ability to scan friendly networks will in turn increase the effectiveness of passive defenses. For these reasons, active defense should be considered along with passive defenses rather than independent of them.

Notes

[1] Anonymous, *Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network*, 2nd Edition (Indianapolis: Sams Publishing, 1998), 412

[2] Glock, John. *"Operationalizing" Information Operations*. Montgomery AFB, Alabama: Air Command and Staff College, 2000. Available at http://

Chapter 5

Recommendations

> *Anciently the skillful warriors first made themselves invincible and awaited the enemy's moment of vulnerability. Invincibility depends on one's self; the enemy's vulnerability on him.*
>
> —Sun Tzu

These recommendations are doctrinal rather than technical in nature, and as such they are based on TTP that should be possible rather than on those that exist. It is apparent that there is an advantage to undertaking active defense efforts in support of passive defenses vice in lieu of them, and but that there is still room for improvement in the latter. Specific recommendations will first address augmentation of present passive defenses, followed by recommendations for preemptive and counterattacks.

Recommendations for Passive Defenses

This paper's brief survey of passive defense measures and the effectiveness of each shows a consistent requirement for system administrators to pay close attention to their status, particularly by periodic intervention to test system security. It also indicates that they must not only adequately train users in proper security practices, but must also ensure those practices are being followed. Since evidence from the SANS Institute and Internet security firms shows system administrators are not consistently implementing even readily available security patches,[1] DoD should streamline the process of patching software to close security vulnerabilities. This

will reduce their workload while simultaneously improving network security. Current access control relies on simple passwords, which are highly vulnerable to compromise. DoD must replace this with some form of one-time passwords (OTP) as soon this is practical.

Active Defense: Preemptive Attack

Considering the relatively low expectation of producing results that might forestall or prevent attacks on friendly networks, there is no reason to recommend any separate preemptive attack effort as part of active defense.

Active Defense: Counterattack

Once CNA is underway, counterattack is possible only if the attacker is foolish enough to stay connected long enough for active defense personnel to locate his network, probe it for vulnerabilities, conduct sufficient CNE to allow successful attack, and launch the counterattack. Should an attacker's probes of a friendly network be detected and accurately traced back to their source, it may be possible to launch a counterattack against the probe itself to forestall follow-on attacks by denying the attacker further information about friendly defenses. Once a target for counterattack has been identified, the tasks that must be performed to make it successful should be no different from those required for any other CAN. This will include approval from the appropriate command level, which may be restricted to the NCA. For this reason, personnel in units already trained and equipped for CNA must be the ones to carry it out. Only they will have the training and command and control connectivity needed to ensure the counterattack neither undermines theater and national strategy nor violates agreements and LOAC. Furthermore, since communications personnel are already overtasked maintaining up-to-date passive defenses, once a hostile CNA is underway they will have their hands full, and will not be able to undertake any

other tasks without seriously compromising the network's security. As soon as they've detected a possibly hostile probe of their network, they should immediately hand off any counterattack tasks to properly constituted CNA units.

Active Defense: Active Deception

Active deception shows immense promise, both for strengthening passive defenses and for enabling CNA against adversaries' offensive potential. Communications personnel should give high priority to efforts to develop defenses of this type. They should be prepared to conduct these operations since doing so will allow them to maintain constant awareness of hostile action directed against their networks.

Summary

While passive defenses cannot shed their essential weaknesses, that they cede the initiative to the adversary and that they rely on fallible human activity to maintain them, there is still much that can be done to strengthen them before resorting to active defense. Active deception and counterattacks carried out by properly constituted units can contribute significantly to the defense of the US DII. The US IO community should explore development in these areas to help ensure information superiority in all future conflicts.

Notes

[1] SANS Institute, *How To Eliminate The Ten Most Critical Internet Security Threats*, January 18, 2001, available at http://www.sans.org

Appendix A

CNA Tools

Scanners

Perhaps the most straightforward cracking tool is a scanner, which is a program used by system administrators to detect weaknesses in their own networks, but can also be used by a hacker for the same purpose. The way a scanner works is to query each of the target server's TCP/IP ports to determine which are open, and which of these open ports might allow the hacker access to vulnerable parts of the system. It will also tell the user whether a given service supports anonymous login (anyone can access) or if it requires authentication, usually by password.[1] Scanners are fairly simple to write, and many are available for download, some for free.[2]

Password Crackers

Should a hacker need to access a system that is password-protected, he or she might use a password cracker to gain access. Passwords are typically encrypted to prevent their interception and use by unauthorized parties, however, recent events have shown that the currently accepted standard, DES (short for data encryption standard) is vulnerable.[3] For the near future, there's good news and bad news. The good news is that a new, stronger encryption standard is on the way[4], but the bad news is that a password cracker doesn't need to decipher a password to crack

it. It takes either a list of common words and phrases which it assumes at least one account will have for a password, or rapidly combines strings of letters and numbers, and encrypts each possibility using the DES algorithm. Then runs each combination for matches; if a user has a common word or phrase as a password, the hacker will in all likelihood find it. System administrators can (and often do) also run password crackers, then they can notify a user when his or her password has been cracked, and help that person select a better one. Password crackers take a lot of time, but if the system administrator does not take steps to detect bad passwords and to educate users on password selection, they can be effective.[5] According to one administrator, "[g]enerally we find 30 percent of passwords on previously unsecured systems."[6] In this sense, passive defense against password crackers is only as good as the system administrator.

Sniffers

Sniffers are typically used to analyze network traffic; in fact, our own communications personnel use them to prevent unauthorized use of DoD computers. They intercept individual IP packets in order to help analyze network usage and performance. However, in the wrong hands, a sniffer can be used to steal passwords or simply steal data that is being communicated through the system. Unauthorized sniffers can be detected and removed, but only by running an application designed specifically to find them. A better option is to use encrypted sessions, where data is encrypted at the terminal, as is done with secure Internet browser connections.

Trojan Horses and Worms

The term Trojan Horse, or trojan for short, is applied to any program that contains unauthorized code that performs a function unknown to the user, or to the unauthorized code

itself.[7] Trojans are usually employed to steal information from a system, to cause damage to the system itself, or to launch attacks on other systems. An example of the last is “Sub-Seven”, which opens a port to allow the hacker access to the server. Unlike a conventional trojan, a worm replicates and spreads itself from computer to computer.[8] The most famous of these are Melissa and I Love You, the latter having infected and caused software damage to millions of machines in May of 2000.[9] Five months later an already well known worm was discovered to have been used to penetrate Microsoft’s corporate system. Despite the fact Microsoft is keenly aware it is perhaps the most popular private-sector target for hackers, its corporate security was unable to prevent the worm from penetrating its firewall and propagating itself within. When executed it made its way to the server, stole passwords, and sent them to the originator in St. Petersburg, Russia, who then used them to gain system access.[10] Even the security experts can be victims, as happened in late January 2001 when SecurityFocus, the firm which operates the Bugtraq security site, unwittingly posted a trojan posing as a security tool and thereby helped infect over 30,000 machines. Not only was SecurityFocus fooled, "[i]t seemed like legitimate code," said Elias Levy, chief technology officer for SecurityFocus. "It was given to us late last night. We sent a copy to (security software maker) Network Associates, and they said it looked OK."[11] The repeated success of trojans, even against companies like Microsoft, SecurityFocus, and Network Associates, which have the most security-aware employees in the computer business, indicates passive defenses are not impenetrable to hackers.

Scripts

Scripts are essentially self-contained cracking code, which require little if any technical knowledge to use. So-called “script kiddies” download them, then use them to deface – tag – systems with lax security. While most script kiddies lack the ability to seriously exploit any

break-in, the mere existence of scripts makes the break-in itself much easier, and with it the training of CNA specialists. Furthermore, time and energy spent chasing down high profile incidents of web defacement is no longer available for fighting more dangerous security vulnerabiliies.

Notes

[1] Anonymous, *Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network,* 2nd ed. Indianapolis: Sams Publishing, 1998, 182

[2] For example, Nessus, a simple TCP port scanner is available for free download at ftp://ftp.nessus.org/pub/nessus/nessus-1.0.7a/

[3] DES uses a 56-bit variable to encrypt data, which means the variable can be any number between 2^1 and 2^{56}. However, in October 2000 it was announced that a team of Swedish computer enthusiasts had cracked a cipher using a 512-bit variable, using immense amounts of computing power. While this technique is not practical for the average hacker, it does demonstrate the vulnerability of DES. Reuters, *Cracked: World's Toughest Security Code Broken*, October 12, 2000.

[4] Berinato, Scott, E-Week, *'Rijndael' Proposed As Government Encryption Standard*, 9 October 2000

[5] Anonymous, *op cit.*, 204-212

[6] Feldmeier, David and Karn, Philip R., *UNIX Password Security – Ten Years Later*,

[7] Anonymous, *op cit.*, 236-237

[8] Virus Terminology, Symantec Antivirus Research Center, http://www.symantec.com/avcenter/virus.backgrounder.html

[9] Lemos, Robert, *Top 10 Security Stories of 2000,* ZD Net News, December 24, 2000

[10] Reuters, *Microsoft Break-in*, 9:25 EST October 27, 2000, accessible at http://www.zdnet.com/intweek/stories/news/0,4164,2645864,00.html

[11] Lemos, Robert, *Beating the Experts: Hackers Infiltrate Bugtraq Security List*, ZD Net News, February 1, 2001

Glossary

AFDD	Air Force Doctrine Document
BDA	Battle Damage Assessment
C^2	Command and Control
CNA	Computer Network Attack
DDoS	Distributed Denial of Service
DII	Defense Information Infrastructure
DoD	Department of Defense
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
II	Information infrastructure
IO	Information Operations
IP	Internet Protocol
IW	Information Warfare
JP	Joint Publication
OTP	One time password
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
TTP	Tactics, techniques, and procedures

access control. Any means, device, or technique that allows an administrator to selectively grant or deny users access to a given resource; e.g., a file, directory, network, or process.

administrator. The individual who controls, and is responsible for security of, a network. Also a level of access which allows the possessor to control a network.

authentication. The process of identifying a user and determining whether or not the user is authorized access to a network, file, directory, or process.

client. A computer which is part of a network, but whose access is controlled through a server.

code. The lines of text that make up a computer program. Often used interchangeably with the latter.

computer. An electronic machine that performs high-speed mathematical or logical calculations or that assembles, stores, correlates, or otherwise processes and prints information derived from coded data in accordance with a predetermined program.

Computer Network Attack. Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves. [JP 3-13]

cracker. Someone who, with malicious intent, unlawfully breaches the security of a computer and/or network.

encryption. The process of scrambling data so it is unreadable by unauthorized entities. Most computer encryption schemes require a password to de-scramble the data.

firewall. A passive defense measure used to deny unauthorized users from accessing a network. It can be a standalone computer, router, or some sort of proprietary hardware, or an application residing on the computer itself.

hacker. Someone interested in operating systems, software, security, and technical aspects of the Internet. Often used interchangeably with **cracker**.

hole. See **vulnerability**.

Hypertext Transfer Protocol. The protocol used to transmit hypertext across the Internet, and which therefore underlies the World Wide Web.

Information Assurance. I[nformation] O[perations] that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. [JP 3-13] In simpler language, information assurance is everything done to ensure our information systems are available for use by authorized users, that they work the way they're designed to, and that only authorized users are able to use and get information from them.

Information Operations. Actions taken to affect adversary information and information systems, while defending one's own information and information systems. It has both offensive and defensive aspects, and it includes, but is not limited to OPSEC, PSYOP, military deception, EW, and physical attack/destruction, and could include C[omputer] N[etwork] A[ttack]. [JP 3-13] Because IO is also defensive, JP 3-13 includes information assurance (IA) as part of IO.

intrusion detection. The process of using automated procedures to detect attempts to breach a network's security.

network. A chain of interconnected computers, machines, or operations.

one time password. A pseudo-random password generated by a challenge-response exchange between server and client. Such passwords are generated using a predefined algorithm, and because a new one is generated for each session they are extremely secure.

read access. The access permission which allows a user to read (but not alter) a file.

server. A computer which controls the operation of a network.

session. The duration of a client's logged-on connection to a server.

sniffer. A program that surreptitiously captures data being transmitted across a network. It can be used by administrators to assess the security of their networks, or illegitimately by crackers looking to steal passwords.

trojan. Code that hides within another program and which, unknown to the user, carries out another (unauthorized) task. Trojans are usually used to breach security and/or to cause damage to a network.

virus. Self-replicating and/or propagating code that attaches itself to other programs or files (such as e-mail).

vulnerability. Any weakness in a system that allows unauthorized intruders to gain unauthorized access to a system and/or process.

worm. A program that self-replicates, spreading itself from computer to computer through one or more networks. Worms can be used to overwhelm a network's resources and/or breach network security.

write access. The access permission which allows a user to read and alter a file.

Bibliography

Amir Husain, Syed M. *Pakistan Needs an Information Warfare Capability*. *Defence Journal*, July 1998. Available at http://www.defencejournal.com/july98/pakneeds1.htm

Anonymous. *Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network,* 2nd ed. Indianapolis: Sams Publishing, 1998

Baocun, Wang and Fei, Li, *Information Warfare*, excerpted from *The Liberation Army Daily*, June 13 and June 20, 1995.Available at http://www.fas.org/irp/world/china/docs/

Berinato, Scott. *'Rijndael' Proposed As Government Encryption Standard.* E-Week, 9 October 2000

Carolan, Matt. *Vigilantism Online. Interactive Week*, February 7, 2001. Available at http://www.zdnet.com/intweek/stories/news/0,4164,2682652,00.html

Computer Emergency Response Team (CERT) Coordination Center, *CERT/CC Statistics*, 1998-2000, Carnegie-Mellon University, available at http://www.cert.org/stats/cert_stats.html

The Concise Oxford Dictionary, 9th ed. Oxford: Oxford University Press, 1995

Department of the Air Force. *Air Force Doctrine Document 1: Air Force Basic Doctrine*. Maxwell AFB, September 1997

Director for Strategic Plans and Policy, J5; Strategy Division. *Joint Vision 2020.* Washington D.C., June 2000

Feldmeier, David and Karn, Philip R. *UNIX Password Security – Ten Years Later*. Available at http://www.alw.nih.gov/Security/first-papers.html#Password

Glock, John. *"Operationalizing" Information Operations*. Montgomery AFB, Alabama: Air Command and Staff College, 2000.

Hsu, Brian. *First Information Warfare Group Put Into Service. The Taipei Times*, January 3, 2001. Available at http://www.taipeitimes.com/news/2001/01/03/story/0000068206

Kenyon, Henry S. *Adaptive Response Tool Targets Hacker Intrusion. Signal*, August 1999. Available at http://www.us.net/signal/Archive/August99/adaptive-aug.html

Klein, Daniel, *"Foiling the Cracker": A Survey of, and Improvements to, Password Security*. Software Engineering Institute, Carnegie Mellon University, 1993. Available at http://remus.prakinf.tu-ilmenau.de/Reif/Publications/CT9509/security-sokol.html

Lemos, Robert, *Beating the Experts: Hackers Infiltrate Bugtraq Security List. ZD Net News*, February 1, 2001. Available at http://www.zdnet.com/zdnn/stories/news/0,4586,2681343,00.html

_____. *'Hacktivism': Mideast Cyberwar Heats Up. ZD Net News*, February 6, 2001. Available at http://www.zdnet.com/zdnn/stories/news/0,4586,2650300,00.html

_____. *Script Kiddies: The Net's Cybergangs*, ZD Net News, July 12, 2000, available at http://www.zdnet.com/filters/printerfriendly/0,6061,2602573-2,00.html

_____. *Top 10 Security Stories of 2000. ZD Net News*, December 24, 2000. Available at http://www.zdnet.com/zdnn/stories/news/0,4586,2668051,00.html

Reuters. *Microsoft Break-in*, 9:25 EST October 27, 2000, accessible at http://www.zdnet.com/intweek/stories/news/0,4164,2645864,00.html

SANS Institute. *How to Eliminate the Ten Most Critical Internet Security Threats.* January 18, 2001. Available at http://www.sans.org

Sun Tzu. *The Art of War.* Oxford: Oxford University Press, 1963

Trenchard, Sir Hugh. *Memorandum on the War Object of an Air Force*, cited in Chaliand, Gerard, editor, *The Art of War in World History: From Antiquity to the Nuclear Age.* Berkeley and Los Angeles, California: The University of California Press, 1994

Virus Terminology. Symantec Antivirus Research Center. http://www.symantec.com/avcenter/virus.backgrounder.html