



LAWRENCE  
LIVERMORE  
NATIONAL  
LABORATORY

# **Taxonomies of Cyber Adversaries and Attacks: a Survey of Incidents and Approaches**

*Carol Meyers, Sarah Powers, and Daniel Faissol*

**April 2009**

This document was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor Lawrence Livermore National Security, LLC, nor any of their employees makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or Lawrence Livermore National Security, LLC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

# **Taxonomies of Cyber Adversaries and Attacks**

## **A Survey of Incidents and Approaches**

### **Abstract**

In this paper we construct taxonomies of cyber adversaries and methods of attack, drawing from a survey of the literature in the area of cyber crime. We begin by addressing the scope of cyber crime, noting its prevalence and effects on the US economy. We then survey the literature on cyber adversaries, presenting a taxonomy of the different types of adversaries and their corresponding methods, motivations, maliciousness, and skill levels. Subsequently we survey the literature on cyber attacks, giving a taxonomy of the different classes of attacks, subtypes, and threat descriptions. The goal of this paper is to inform future studies of cyber security on the shape and characteristics of the risk space and its associated adversaries.

## **I. Cyber Crime**

Cyber defense is a vast and growing problem in national security. According to the FBI, the annual loss due to cyber crime was estimated at \$67.2 billion for US organizations in 2005 (GAO, 2007). As opposed to traditional crime, cyber crime has the advantages of being able to target a vast number of victims, it can be executed quickly, and it is unhindered by the attacker's physical location or proximity.

In a survey of more than 8,000 businesses conducted by the US Department of Justice in 2005 (see Rantala, 2008), 67% of the companies reported detecting at least one cybercrime in the past year. Contributing to this number were the nearly 60% of respondents who discovered one or more types of cyber attack, 11% who identified cyber theft, and 24% who experienced other security incidents. The monetary losses for these businesses exceeded \$867 million, and system downtime totaled 323,900 hours. Two-thirds of all such incidents were targeted against companies in the US critical infrastructure, of which telecommunications firms suffered the greatest number of attacks (Rantala, 2008). These statistics conclusively demonstrate that cyber crime is a major problem for US businesses.

On an individual level, cyber crime can also be extremely destructive. The FBI-sponsored Internet Crime Complaint Center logs complaints of internet fraud and forwards relevant claims to federal, state, and local law enforcement agencies. According to the Internet Crime Report (ICCC, 2008), this website received 275,284 separate complaint submissions in 2008, a 33% increase over complaints in

the year 2007. The total dollar amount of these individual cases of fraud came to \$264.6 million, or \$931 per complainant referred to law enforcement. The top three categories of fraud complaints were non-delivered merchandise, internet auction fraud, and credit/debit card fraud. Email and webpages were the two primary mechanisms by which the fraud took place (ICCC, 2008).

Numerous products have been created to help mitigate the effects of cyber crime, from anti-virus and anti-spyware programs to intrusion detection/prevention systems to advanced application-level firewalls (Richardson, 2008). The US government also sponsors a number of organizations that manage and respond to cyber threats, most notably the United States Computer Emergency Readiness Team, or US-CERT. Among the publications of US-CERT are monthly activity summaries of general threat activities, as well as quarterly trends and analysis reports detailing the evolution of threats over the course of several months (US-CERT, 2008).

Given that cyber security is such a vast problem, it is essential in constructing a defensive architecture to know who the cyber adversaries are and what kinds of threats they are likely to attempt. This paper surveys the literature on cyber adversaries and attacks, presenting taxonomies of the different types of players and attack methods. In each case, we describe the relevant studies that have been performed as well as providing a detailed explanation of each of the entries in the taxonomy. Where possible, we give specific examples of the particular adversaries and attack types featured. Our goal is for this work to be used in future studies of cyber security.

## **II. Taxonomy of Cyber Adversaries**

### **A. History and Motivation**

The study of cyber adversaries was initiated in the early 1980's, when personal computers began to come into the mainstream and the term 'hacker' entered the lexicon as a person skilled at programming and manipulating operating systems. The early hackers were products of MIT and other top technical schools, who enjoyed programming and stretching the abilities of computers (Raymond, 2003; Walleij, 1998).

The use of the word 'hacker' to describe an individual engaging in malicious activity emerged several years later, after the widely publicized arrest of six teenagers known as the '414 gang,' who notably broke into 60 computer systems, including those of the Los Alamos National Laboratory (Murphy et al., 1983). Within the computer science community today, there are many who argue against the perceived misappropriation of the term 'hacker,' preferring the term 'cracker' to describe individuals engaging in malicious behavior and breaking into security systems (Lawson, 2001).

Notwithstanding the debate on nomenclature, by the mid-1980's there was a growing interest on the part of law enforcement in understanding who these cyber adversaries were and how to stop them (Sterling, 1994). The Comprehensive Crime Control Act of 1984 was the first attempt at addressing computer fraud, and the Computer Fraud and Abuse act of 1986 specifically defined breaking into computer systems as a crime (Eltringham, 2007). Profiling of cyber adversaries suddenly became important as a method of identifying these criminals and determining their motivations (Smith & Rupp, 2002). We now discuss several of the most prominent studies in this area, which have greatly influenced our own work.

### **Landreth (1985)**

One of the first attempts to define and describe the community of cyber adversaries was done by Landreth, an accomplished hacker himself (Gorman, 1986; Chapa & Craig, 1996). He proposed five categories of individuals within the hacking community:

- novices
- students
- tourists
- crashers
- thieves

The novices consisted of entry-level hackers, usually around ages 12-14, who engaged in petty mischief making. Individuals in this class got bored quickly and easily made mistakes. The students followed in the tradition of 1970's students at MIT, engaging in hacking primarily for the intellectual challenge, with minimal criminal motivation and the desire to simply gather information about infiltrated systems. The next category, tourists, engaged in hacking primarily for the thrill of being there. They felt the need to test themselves and experience a sense of adventure. By contrast, crashers engaged in destructive behavior and sought to intentionally damage information and systems. These adversaries enjoyed taking credit for their attacks and stroking their egos. Rarest of all the classes were the thieves: these individuals were true criminals, and usually profited off of their malicious activities. They were also the most dangerous and sophisticated of hackers, as they were often technically sophisticated professionals who researched their targets thoroughly in advance.

### **Hollinger (1988)**

A criminologist at the University of Florida, Hollinger interviewed several students who were convicted of gaining unauthorized access to the university's account management system and modifying or damaging a number of files. From these interviews, he determined that the hackers followed a progression from less skilled to more technically elite crimes. He proposed that these individuals fit into three categories:

- pirates
- browsers
- crackers

The pirates were the least technically sophisticated adversaries, primarily confining their activities to copyright infringements and the distribution of illegally copied software. This category also contained the greatest number of offenders. In addition to piracy, the browsers gained occasional unauthorized access to the computer accounts of others and browsed through private files. Individuals in this class possessed a moderate technical ability but were not necessarily malicious. The crackers were the most serious abusers, engaging in repeated modification or sabotage of others' files and programs. They were both the most technically sophisticated hackers and also the most malicious, seeking to crash entire computer systems.

### **Chantler (1996)**

The goal of Chantler's work was to perform a large-scale ethnographic study of hackers. He argued that hacking behavior could be categorized along several different attributes, including knowledge, motivation, prowess, and length of time involved. His study was primarily qualitative in nature and drew upon surveys and interviews with 164 known hackers. Based on this research, he proposed three categories of hackers:

- losers and lamers
- neophytes
- elites

The losers and lamers demonstrated little intellectual ability, and were primarily motivated by greed and vengeance. Individuals in this group constituted 10% of the hacker population. Neophytes, the next most sophisticated group, were learners and followers and tended to pursue where the elites had been. They were also the largest component of the sample, at around 60%. The elites displayed a high level of technical ability and were motivated by achievement, excitement, and challenge. Members of this class constituted the remaining 30% of the population.

### **Rogers (1999, 2001, 2006)**

The most comprehensive study of cyber adversaries and their motivations is due to Rogers, who over the past decade has developed and refined several taxonomies of hackers, in addition to receiving coverage in the popular press (Glave, 1999). His earliest work (1999) was done as a companion to his PhD thesis (2001), which examined demographic and social characteristics associated with a sample of 66 cyber adversaries. In particular, he discovered that these cyber adversaries were:

- predominantly male (81.8% male; 18.2% female)
- Caucasian (72.7% Caucasian; 10.6% Asian; 10.6% not stated; 6.1% other races)
- single (56.1% single; 18.2% married; 13.6% divorced; 11.1% other or unknown)
- high-school educated (47.0% high school; 18.2% 9<sup>th</sup> grade; 4.5% college; 30.3% other or unknown)

He also found that hackers displayed high levels of moral disengagement (convincing oneself that ethical standards do not apply in certain contexts), as well as differential association (learning their behavior through the examples of others). A follow-on work discussed the applicability of psychological theories for explaining this behavior (Rogers, 2000).

The taxonomy of cyber adversaries that we propose at the end of this section is heavily drawn from the adversary taxonomies proposed by Rogers (1999; 2006); a more thorough discussion of this work ensues at that point.

### **Subgroup Studies**

Most of the other studies concerning cyber adversaries and their behavior have focused on a specific subgroup of adversaries, centered around their method of attack. Gordon (2000, 2006) has examined the subclass of virus writers, who compose the scripts that are used by themselves and others to infiltrate computer systems. She suggests that virus writers are primarily composed of four groups (adolescents;

college students; adults; ex-virus writers), of which only the adult group was shown to be ethically abnormal (possessing a lower than average level of ethical maturity). The first two groups were ethically average but showed little concern or responsibility for the results of their actions, and the last group cited a variety of reasons for leaving the “craft.”

Shaw, Ruby, and Post (1998) study a different subclass of adversaries, specifically those involved with insider threats. They provide a suite of psychological profiles associated with such insiders, as well as citing a number of specific case studies. They suggest that the key factors associated with a person becoming an insider adversary are: introversion, social and personal frustration, computer dependency, ethical “flexibility,” reduced loyalty, entitlement, and lack of empathy. These findings are elaborated and expanded upon in works by Post (1998) and Steele & Wargo (2007).

Other work has examined the characteristics of adversaries who write computer worms (Weaver et al., 2003), web spammers (Jennings, 2007), political ‘hacktivists’ (Denning, 2001), and the subset of hackers who engage in identity theft (Föttinger & Ziegler, 2004). While it is possible to probe with greater depth in narrowly focused studies such as these, the goal of our work is to provide a broad, macro-level description of cyber adversary behavior and motivations.

## **B. Proposed Adversary Taxonomy**

Our taxonomy of cyber adversaries is featured in Table 1. We draw heavily from the work of Rogers (2000, 2006), as well as several of the other studies mentioned in this section. For each of the adversary types, we list the corresponding skill level, maliciousness, motivation, and method. In what follows, we give descriptions of each of the adversary classes, in terms of increasing levels of skill and sophistication.

### **script kiddies, newbies, novices**

This is the least sophisticated category of adversaries, comprised of individuals with limited programming skills. They are new to hacking and rely on pre-written scripts known as ‘toolkits’ in their exploits; examples of these include NeoSploit, WebAttacker, and IcePack (Westervelt, 2007) . The primary motivation of these adversaries is boredom and thrill-seeking; they are often young and eager for acceptance from the hacker subculture. Though they are attracted to deviant behavior, their overall maliciousness level tends to be low, because of their limited skills. With the increasing sophistication of the available toolkits, their ability to pull off larger-scale attacks is on the rise, as in the case of the denial-of-service attacks perpetuated by ‘Mafia Boy’ in Canada (Rogers, 2006).

### **hacktivists, political activists**

These adversaries are different than the other classes in that they are motivated by a political cause rather than a form of personal gain. Their attacks consist primarily of denial of service and defacement attacks against the sites of rival organizations, though they have also been known to employ worms and viruses (Denning, 2001). Their maliciousness is highly focused against the targeted organizations, though it can still have broad-reaching consequences. Some examples of hacktivism include the ‘virtual sit-ins’ perpetuated by Electronic Disturbance Theater against the Pentagon and other agencies, in protest of perceived civil rights violations; email bombs used by the Internet Black Tigers throughout Sri Lanka to gain publicity for the Tamil Tigers; and worm propagation by WANK (Worms Against Nuclear Killers) on computers in NASA’s Goddard Space Flight center, protesting an upcoming launch (Denning, 2001).

| <b>Adversary Class</b>                  | <b>Skills</b> | <b>Maliciousness</b> | <b>Motivation</b>                       | <b>Method</b>   |
|---|---------------|----------------------|---|---|
| script kiddies, newbies, novices        | very low      | low                  | boredom, thrill seeking                 | download and run already-written hacking scripts known as 'toolkits'.                             |
| hacktivists, political activists        | low           | moderate             | promotion of a political cause          | engage in denial of service attacks or defacement of rival cause sites                            |
| cyber punks, crashers, thugs            | low           | moderate             | prestige, personal gain, thrill seeking | write own scripts, engage in malicious acts, brag about exploits                                  |
| insiders, user malcontents              | moderate      | high                 | disgruntlement, personal gain, revenge  | uses insider privileges to attack current or former employers                                     |
| coders, writers                         | high          | moderate             | power, prestige, revenge, respect       | write scripts and automated tools used by newbies, serve as mentor                                |
| white hat hackers, old guard, sneakers  | high          | very low             | intellectual gain, ethics, respect      | non-malicious hacking to help others and test new programming                                     |
| black hat hackers, professionals, elite | very high     | very high            | personal gain, greed, revenge           | sophisticated attacks by criminals/thieves; may be 'guns for hire' or involved in organized crime |
| cyber terrorists                        | very high     | very high            | ideology, politics, espionage           | state-sponsored, well-funded cyber attacks against enemy nations                                  |

**Table 1. A Taxonomy of Cyber Adversaries**

### **cyber punks, crashers, thugs**

Adversaries in this class have similar motivations but greater skills than those in the novice category. They are capable of writing their own (limited) scripts and engaging in malicious acts such as spamming, defacing, and identity theft. These hackers seek attention and prestige and are most likely to be featured in the media, often because they pick high-profile targets and come under the notice of authorities (Rogers, 2006). Occasionally such adversaries will go on to become internet security consultants, as in the case of Kevin Mitnick, who combined his hacking skills with social engineering to gain access to restricted systems (Mitnick, 2002; Rogers, 2006).

### **insiders, user malcontents**

This group of adversaries represents arguably the greatest risk to companies, and yet is often the least publicized (Rogers, 2006; Gelles et al., 2008). Insiders are most frequently motivated by revenge, usually in response to a negative work-related event; this frustration leads them to deliberately attack their own company (Kowalski et al., 2008). The scope of insider damage can be extremely large, as these individuals are often very familiar with the systems that they are attacking and often hold elevated access privileges. Insiders often seek to sabotage systems, as in the case of Michael Lauffenberger, who planted a logic bomb to delete data in a system that he designed and envisioned subsequently coming to ‘rescue’ his company (Shaw et al., 1998).

### **coders, writers**

Adversaries in this category are primarily involved in writing the codes and exploits that are used by others, especially those in the novice category. Their motivation is power and prestige: they see themselves as the mentors to the younger hackers and like feeling important (Rogers, 2006). There is a continuum of ability within individuals in the category, and it has been suggested that many such writers eventually ‘age out’ of this behavior (Gordon, 2006). In general, such writers can be quite dangerous, as their software can be widely distributed and acquire a life of its own.

### **white hat hackers, old guard, sneakers**

Individuals in this category consider themselves ‘purists’ and ascribe to the flavor of hacking initially popularized at MIT in the early days of computers. They are not malicious hackers and do not wish to cause damage, though they often show a lack of regard for personal privacy (Rogers, 2006). White hat hackers are primarily motivated by the intellectual challenge of testing security systems and creating new programming. They are often hired as security analysts, paid to test a company’s defenses by trying to break into their system and assessing its response (Barber, 2001). The National Security Agency even offers certification in such ‘ethical hacking’ activities (Taylor et al., 2006). Although these individuals probably should not be considered “adversaries,” we include them in our treatment for the sake of completeness.

### **black hat hackers, professionals, elite**

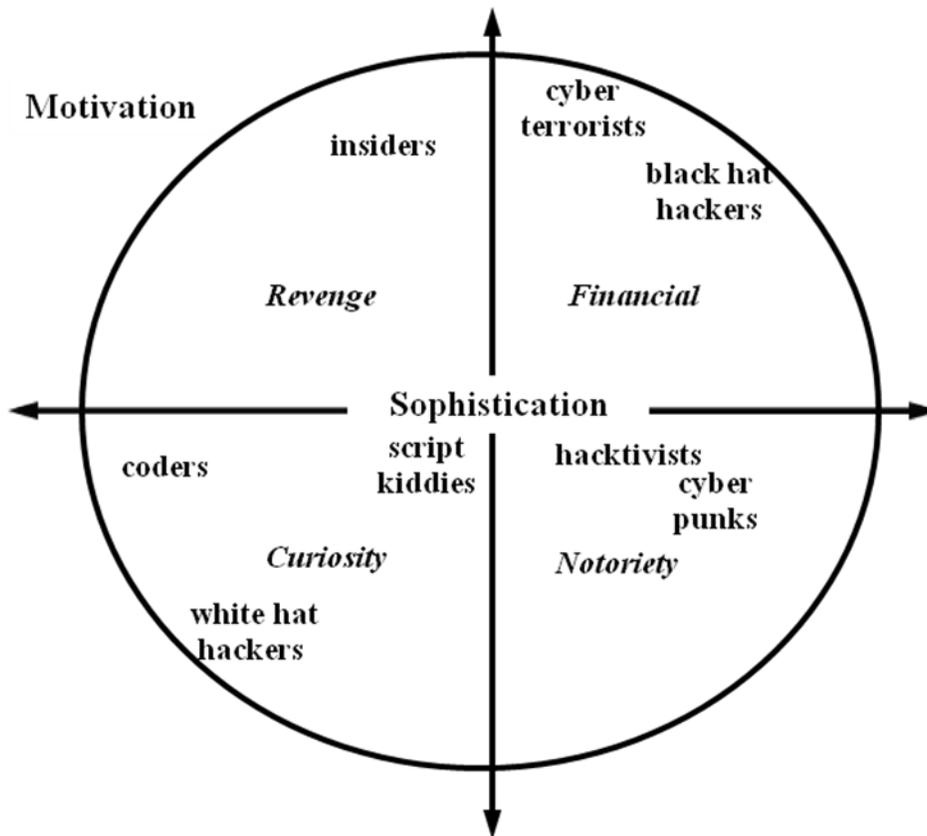
The adversaries in this category are professional criminals, who use their technical skills in pursuance of their criminal activities. Similar to criminals outside the cyber domain, they are motivated by money and greed. Rather than seeking fame, they prefer to lay low and evade authorities (Rogers, 2006). These hackers are both rare and very dangerous, as they have strong technical skills and are often able to support themselves through their criminal exploits. Such adversaries are often employed by organized crime, and

can be described as ‘guns for hire’. Although this is one of the most dangerous types of cyber adversaries, it is also the one about which the least is known (Rogers, 2006).

**cyber terrorists**

The most dangerous and skilled of all cyber adversary classes, cyber terrorists engage in state-sponsored information technology warfare. Their job is to conduct attacks that destabilize, disrupt, and destroy the cyber assets and data of an enemy nation or government organization (Rogers, 2006). Attacks by cyber terrorists are typically well-funded and highly secretive; individuals engaging in such activities have extremely high skills and are motivated by ideology. One of the best known examples of such terrorism occurred in Estonia in 2007, following the removal of a Russian World War II monument; a massive denial of service attack crippled the websites of Parliament, several national newspapers, and the central bank (Landler & Markoff, 2007). A similarly crippling DDoS attack preceded the conflict between Russia and the Republic of Georgia in 2008 (Markoff, 2008). Such attacks are hard to prosecute, which makes them even more dangerous, and guarding against these attacks has become a top national priority.

In Figure 1 we give a two-dimensional circumplex representation of the cyber adversary types described in this paper. This is reproduced from the work of Rogers (2006), with some small modifications. Motivation of the adversary types is represented along the circumference of the circle, and the sophistication level is measured along the radii. For example, the ‘insider’ label indicates that insiders are primarily motivated by revenge, though finance is a factor, and they have a solid technical ability.



**Figure 1. A circumplex depiction of the adversary types in this paper (following Rogers, 2006).**

### III. Taxonomy of Cyber Attacks

#### A. History and Motivation

The formal study of cyber security began in the mid-1970's, when computers first became prominent in the government and universities. The earliest studies were primarily mechanical in nature and focused on the formal verification of the security of computer operating systems. As early as 1975, researchers at UCLA attempted to design, implement, and verify a security kernel for UNIX (Popek & Kline, 1975). Other work sponsored by the Air Force at MITRE and Case Western University focused on the construction of prototype security kernels and formal models of computer security (Walter et al., 1975; Bell & La Padula, 1976). Landwehr (1981) reviews the state of cyber security in the 1970's and the progress of these and other early efforts.

Most of this early work in cyber security did not explicitly consider the different types of attacks that might be perpetuated. The first studies of cyber attacks in particular arose in the early to mid-1980's, around the same time that cyber adversaries first entered the public eye. Stoll (1986) describes the methods a German hacker used to break into computer systems at Lawrence Berkeley National Lab, and how researchers there used the hacker's activities to track him. The Computer Emergency Response Team (CERT) was founded by DARPA in 1988, after a high-profile crippling of the internet via the Morris worm (Scherlis, 1988; Kehoe, 1992).

One of the major issues in studying cyber attacks is that the notion of an "attack" itself is quite broad: it can encompass attack vectors, operating systems, hardware and software targets, access schemes, attacker objectives, specific implementation and design vulnerabilities, and the attack payload (Howard, 1997; Hansman & Hunt, 2005). It is practically infeasible to encompass all of these aspects in a single taxonomy, as the associated length would be overwhelming. In the next sections, we review some of the literature that attempts to tackle pieces of this larger problem, followed by our own attack taxonomy. It should be noted that in our taxonomy, we will focus primarily on attacks in terms of their associated attack vectors—specifically, the general class of methods and exploits that the attack uses. This high-level treatment of the attack space allows for a much more tractable representation.

#### **Landwehr et al. (1994)**

Drawing from a number of widely documented cyber security incidents in the 1970's and 1980's, Landwehr et al. presented a taxonomy of computer security flaws. Their taxonomy consisted of three major components, according to the nature of when and where a given flaw was introduced. These were:

- flaws by genesis (*how* a flaw arises: maliciously, non-maliciously, or inadvertently)
- flaws by time of introduction (*when* a flaw is introduced: development, operations, or maintenance)
- flaws by location (*where* a flaw is located: software or hardware)

Each of these three major components contained several sub-components; for instance, malicious flaws were broken down into trojan horses, viruses, trapdoors, and logic/time bombs. Likewise, the category of software flaws was decomposed by operating system, support, and application. The most novel contribution of this work consisted of the authors' detailed classification of 50 real security flaws into this framework. This was accompanied by a description of each of the flaws and their justification for the categorization of each flaw within the taxonomy.

### **Howard (1997); Howard and Longstaff (1998)**

One of the most comprehensive studies of computer security incidents was performed by Howard, as the basis for his Ph.D. thesis at Carnegie Mellon University. In this work and a companion paper the following year, he executed a detailed analysis of data collected by CERT/CC consisting of over 4,500 security incidents between 1989 and 1995. Based on this data, he proposed a network and attack taxonomy for classifying and comparing such incidents. This taxonomy contained five primary components:

- attackers (hackers, spies, terrorists, corporate raiders, professional criminals, vandals)
- tools (scripts, autonomous agents, toolkits, user commands, data tap)
- access (implementation/design vulnerabilities, authorized/unauthorized access, processes)
- results (corruption/disclosure of information, theft of service, denial of service)
- objectives (challenge, status, political gain, financial gain, damage)

This taxonomy was very general and did not go into further detail. The objective was to provide a broad scheme within which different incidents could easily be placed. He proceeded to classify many of the security incidents into this framework, though at a (necessarily) lower fidelity than that of Landwehr et al (1994). The value of this work in particular lay in the large sample size, which made it possible to obtain a reasonable probabilistic description of the attack space.

### **Hansman and Hunt (2005)**

Hansman and Hunt have provided the most thorough taxonomy of network and computer attacks to date. Their work extended that of earlier taxonomies by introducing multiple tiers of threats, with a greater exposition of levels and description within each category. Specifically, they classified attacks on four main dimensions:

- attack vectors (the main means by which the virus reaches the target)
- target(s) of the attack (hardware/software/etc.)
- specific vulnerabilities and exploits that the attack uses (security flaws)
- payload of the attack (outcome and effects, possibly beyond the attack itself)

These dimensions were decomposed based on the specificity of detail. Target categories consisted of six levels, ranging from generic descriptors (level 1: hardware versus software) to very precise (level 6: specific versions of specific programs). Altogether this gave a very thorough picture of the attack space and available methods. They demonstrated how 15 well-known attacks could be classified on the dimensions of this taxonomy, from generic to specific levels of detail in each instance.

### **Kjaerland (2005, 2006)**

The work of Kjaerland was notable for adding a *quantitative* component to the classification of network attacks. In particular, her work sought not only to classify the attacks, but also to determine which factors were most likely to co-occur in an attack. Her analysis was based on a sample of 2,755 reported incidents to CERT/CC, from the years 2000-2002. She classified the incidents based on four categories:

- source sectors (com, gov, edu, intl, user, unknown)
- method of operation (misuse of resources, user/root compromise, social engineering, virus, web compromise, trojan, worm, denial of service)

- impact (disrupt, distort, destruct, disclosure, unknown)
- target services (com, gov)

After categorizing each of the reported incidents along these dimensions, she performed a smallest space analysis (SSA) to determine which of these factors were most likely to happen together. Her results showed, among other things, that “individual user” and “web compromise” were likely to occur together; conversely, “educational source” and “trojan” were not likely to co-occur. Although this analysis did not determine the causality of these incidents, this sort of correlative study is very useful in understanding the characteristics of the threat space.

### Other Work

A larger body of literature can be found on cyber attacks as compared to that of cyber adversaries. With regards to taxonomies and classification, a number of studies focus on attacks in a specific area. These include Weaver et al. (2003), who gave a taxonomy of different kinds of computer worms, including propagation methods, payloads, and attacker motivation. Worms were also studied by Collins et al. (2006), within the context of opportunistic network exploits. Rutkowska (2006) gave a categorization of different kinds of malware, and Lough (2001) gave a taxonomy of attacks with a particular focus on applications to wireless networks. Specht and Lee (2004) and Wood and Stankovic (2004) both gave classifications of distributed denial of service attacks, addressing both the different kinds of attack and the countermeasures that can be used against such attacks.

There is also a great deal of work on mapping the prevalence of different cyber attacks (see the section on ‘Cyber Crime’), including viruses (Bridwell, 2005) and malware websites (Keats, 2008). Lipson (2002) provides an excellent summary of cyber attacks over time, as reproduced in Figure 2.

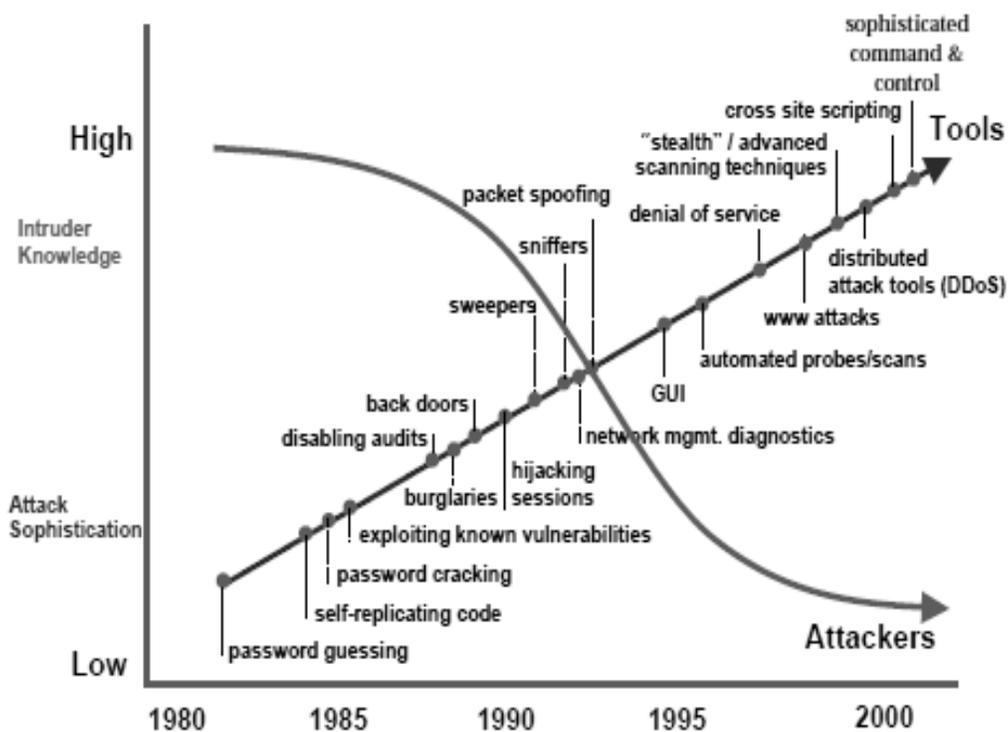


Figure 2. Sophistication of Cyber Attacks and Attackers over Time, from Lipson (2002)

## **B. Proposed Attack Taxonomy**

Our taxonomy of cyber attacks is featured in Table 2. A description of the attack classes is given as well as a listing of the different subtypes of each attack vector. This taxonomy is primarily inspired by the work of Hansman and Hunt (2005), though it draws from the other references mentioned in this section as well. In what follows, we give a portrayal of each of the featured attack classes. We note that many recent incidents have employed more than one of these attack methods, so they should not necessarily be viewed as mutually incompatible alternatives.

### **viruses**

A computer virus is a program that can copy itself and infect system files without knowledge of the user. Viruses are transferred when their host is connected with the target system, either via a computer network, the internet, or a form of removable media. The spread of viruses is dependent on user interaction, in particular in the execution of the corresponding virus code; for this reason many viruses are attached to legitimate program executables. The term ‘computer virus’ was first used in 1983 by Frederick Cohen, who likened the spread of the program to a biological system (Highland, 1997). Possibly the most destructive virus to date is the ILOVEYOU virus, a visual basic scripting virus that originated in the Philippines and caused 10 to 15 billion dollars of damage worldwide in the year 2000 (Jones, 2006).

### **worms**

A computer worm is a self-replicating program that uses a host network to send copies of itself to other computers on the network. As opposed to viruses, worms do not need to attach themselves to existing programs and can be spread without any user interaction; moreover, they seek to infect the network infrastructure rather than individual files. Worms spread primarily by exploiting vulnerabilities in operating systems, most often striking unupdated systems after a major security patch. Commonly, worms install a ‘backdoor’ on infected systems to allow remote control; using this, the Sobig worms were able to create a massive ‘botnet’ of systems dedicated to sending spam (Levy, 2003). Worms can spread very quickly, as in the case of SQL Slammer, which shut down all of South Korea’s online capacity for 12 hours after its launch in 2003 (Jones, 2006).

### **trojans**

Much like the mythical Trojan horse, trojan attacks function by concealing their malicious intent. They masquerade as a piece of software that performs a desired function, while secretly executing malicious content. Users can be fooled into installing the trojan via one of many vectors, most often online downloads or email links. The most common types of trojans install a ‘backdoor’ on infected systems to allow remote access, or engage in data destruction. As opposed to viruses and worms, trojans do not self-replicate and rely entirely on the distribution of their host program to propagate. The earliest trojan horse dates back to 1975, when the computer game ANIMAL housed the subroutine PERVADE, which copied itself into every directory in which the user had access (Walker, 1996). More recently, in 2008 the Chinese password-collecting trojan Mocmex was found housed in digital photo frames (Soper, 2008).

### **buffer overflows**

In programming, a buffer overflow occurs when a program writes more information into the buffer (temporary memory storage) than the space allocated to it in memory. During a buffer overflow attack,

| <b>Attack Class</b>                  | <b>Subtypes</b>   | <b>Description</b>   |
|--------------------------------------|---|--|
| viruses                              | file infectors, system/boot record infectors, macros  | self-replicating program that replicates through infected files; attached to an existing program |
| worms                                | mass mailing via botnets, network aware   | self-replicating program that replicates through networks or email; no user interaction required |
| trojans                              | remote access, data destruction   | program made to appear benign that serves a malicious purpose                                    |
| buffer overflows                     | stack-based overflows, heap-based overflows   | process that gains control or crashes another process via buffer overflowing                     |
| denial of service                    | host (resource hogs, crashers), network (TCP, UDP, ICMP flooding), distributed                  | attack that prevents legitimate users from accessing a host or network                           |
| network attacks                      | spoofing, web/email phishing, session hijacking, wireless WEP cracking, web application attacks | attack based on manipulating network protocols, against users or networks                        |
| physical attacks                     | basic, energy weapon (HERF gun, EMP/T bomb, LERF), Van Eck                                      | attacks based on damaging the physical components of a network or computer                       |
| password attacks/<br>user compromise | guessing (brute force, dictionary attacks), exploiting implementation                           | attacks aimed at acquiring a password or login credential  |
| information gathering                | packet sniffing, host mapping, security scanning, port scanning, OS fingerprinting              | attacks in which no damage is carried out, but information is gathered by attacker               |

**Table 2. A Taxonomy of Cyber Attacks**

malicious users exploit this property by forcing a buffer overflow to overwrite local variables and alter program execution, forcing the process to execute malicious code introduced by the user. Such techniques are well-documented and most often used to gain control of host systems (Levy, 1996). This buffer overflow technique may be used as a method of enabling other attacks such as worms to be executed on a system. This method was used in both the Code Red and SQL Slammer worms, which exploited overflow vulnerabilities in Microsoft's Internet Information Services and SQL server respectively (Chen & Robert, 2004).

### **denial of service**

A denial of service attack functions by making a computer network or resource inaccessible to legitimate users. Most often this is accomplished by "flooding" the target with data, so that it is overloaded with such requests. Common targets of these attacks include network routers (resulting in very slow network performance), DNS servers (resulting in an inability to access websites), and email accounts (resulting in a "mail bomb" deluge of spam). In a distributed denial of service attack, multiple systems combine to flood the bandwidth and resources of the target. The first widely publicized distributed attack occurred in 2000, when numerous high-profile websites (including Amazon.com, Yahoo, eBay, and CNN) were crippled for several hours (Garber, 2000). Such attacks can also have political overtones, as in the bombardment of Georgian government websites shortly preceding conflict with Russia (Markoff, 2008).

### **network attacks**

Within our taxonomy, a network attack is one in which network protocols are manipulated to exploit other users or systems. Examples of such attacks include IP spoofing, in which the source IP address is falsified (Heberlein & Bishop, 1996); web/email phishing, in which a legitimate website or email is reproduced by a hacker (Emigh, 2005); session hijacking, in which the theft of a session cookie leads to exploitation of a valid computer session (Xia & Brustoloni, 2004); and cross-site scripting attacks, in which malicious code is injected into web applications (Di Lucca et al., 2004). These attacks are often used in conjunction with other attacks in the taxonomy, such as denial of service attacks. They can also be quite costly: an estimated \$1.2 billion were lost in phishing attacks in the year 2003 (Emigh, 2005).

### **physical attacks**

Some of the most frightening cyber attacks are physical in nature, such as those using electromagnetic radiation waves to disrupt or damage the electrical parts of a system or decode its signals. A high-energy radio frequency (HERF) gun blasts a high-power electromagnetic pulse capable of physically destroying a computer's motherboard and other components (Schwartau, 1996). Similar to this but even stronger is the electromagnetic pulse transformer (EMP/T) bomb, which can generate a thousand times the damage of HERF (Schwartau, 1996). Using a different mechanism, in a Van Eck attack the electromagnetic signals of a computer can be hacked to reveal the signal's data content, using equipment costing as little as \$15 (Van Eck, 1985). The US government's TEMPEST component standards are designed to mitigate the risk of all these kinds of attacks, but they do not eliminate the problem (Russell & Gangemi, 1991).

### **password attacks/user compromise**

Password attacks have the objective of gaining control of a particular system or user's account. There are three basic kinds of such attacks: guessing, based on knowledge of the user's personal details; dictionary attacks, which loop through a list of dictionary words and try to find a match; and brute force attacks,

which loop through sequences of random characters. In a recent study of MySpace passwords, fully 4% consisted of dictionary words, and another 12% were a word followed by a single number (Evers, 2006). In a user compromise attack, the implementation of a system or program is exploited to gain access to sensitive information, such as credit card numbers. Hackers Ian Goldberg and David Wagner found such a problem in the random number generator used for secure sockets layer (SSL) transactions in Netscape 1.1, allowing for easy decoding of encrypted communications (Goldberg & Wagner, 1996).

### **info gathering/resource misuse**

The last category of attacks is not inherently malicious, but is often found as a precursor or component of other attacks. These attacks are used to gather information about the target in an attempt to exploit its defenses and learn more about the system. A mapping exploit is used to gain information on the hosts in a network, including what programs are running and what operating system is used. Security scanning is similar, but involves testing the host for known vulnerabilities in the hardware or software it is using. A packet sniffer is designed to intercept and log traffic on a network, which can potentially be decoded later (Hansman, 2003). Worms such as Sasser, Slammer, and Code Red also use scanning as a method of determining vulnerable hosts to compromise (Kikuchi et al., 2008).

## **IV. Conclusions**

We have surveyed the literature on cyber adversaries and attacks, providing a broad taxonomy of the relevant players and methods in each area. Whenever possible we have attempted to give illustrative examples for each of the particular adversary and attack types featured. It is our hope that this work can be used to inform further studies in adversary modeling and cyber security, particularly those that deal with adversarial threat response.

A natural question for future research would be whether we can *correlate* the kinds of adversaries with the types of attacks they perform. In our survey we did not come across any such literature, which is probably due to a couple of reasons: first, such data would be necessarily difficult to come by, as it would likely be the result of criminal proceedings; and second, the majority of cyber attacks are very difficult to trace back to their originator. Still, as the body of research on cyber adversaries grows, it may be possible to do some sort of a probabilistic analysis in the future.

## **Acknowledgements**

The authors wish to thank Tony Bartoletti for many helpful technical discussions and for suggesting we study this subject area. We would also like to thank Bill Hanley for overall guidance and support.

## References

1. R. Barber. Hackers profiled: who are they and what are their motivations? *Computer Fraud and Security*, 2(1):14-17, 2001.
2. D. Bell and L. La Padula. Secure computer system: unified exposition and multics interpretation. Technical Report MTR-2997, MITRE Corporation, 1976. Accessed at <http://csrc.nist.gov/publications/history/bell76.pdf>.
3. L. Bridwell. ICSA labs 10<sup>th</sup> annual computer virus prevalence survey. Technical Report, ICSA Labs, 2005. Accessed at <http://www.icsa.net/icsa/docs/html/library/whitepapers/VPS2004.pdf>.
4. N. Chantler. *Profile of a Computer Hacker*. Infowar, 1996.
5. S. Chapa and R. Craig. The anatomy of cracking. Online Publication, University of Texas, 1996. Accessed at <http://www.actlab.utexas.edu/~aviva/compsec/cracker/crakhome.html>.
6. T. Chen and J. Robert. Worm epidemics in high-speed networks. *Computer*, 37(6):48-53, 2004. Accessed at [http://ieeexplore.ieee.org/xpls/abs\\_all.jsp?arnumber=1306386](http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1306386).
7. M. Collins, C. Gates, and G. Kataria. A model for opportunistic network exploits: the case of P2P worms. In *Proceedings of the Fifth Workshop on the Economics of Information Security*, Cambridge, England, 2006. Accessed at <http://weis2006.econinfosec.org/docs/30.pdf>.
8. D. Denning. Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy. Chapter 8 of *Networks and Netwars: the Future of Terror, Crime, and Militancy*, Rand Monograph MR-1382, 2001. Accessed at [http://www.rand.org/pubs/monograph\\_reports/MR1382/index.html](http://www.rand.org/pubs/monograph_reports/MR1382/index.html).
9. G. Di Lucca, A. Fasolino, M. Mastroanni, and P. Tramontana. Identifying cross-site scripting vulnerabilities in web applications. In *Proceedings of the Sixth International IEEE Workshop on Website Evolution*, pages 71-80, Benevento, Italy, 2004. Accessed at [http://ieeexplore.ieee.org/xpls/abs\\_all.jsp?arnumber=1410997](http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1410997).
10. S. Eltringham (editor), Computer Crime and Intellectual Property Section, US Department of Justice. *Prosecuting Computer Crimes*. Office of Legal Education Executive Office for US Attorneys, 2007. Accessed at <http://www.usdoj.gov/criminal/cybercrime/ccmanual/index.html>.
11. A. Emigh. Online identity theft: phishing technology, chokepoints, and countermeasures. Technical Report, Infosec Technology Transition Council, Department of Homeland Security, 2005. Accessed at <http://www.cyber.st.dhs.gov/docs/phishing-dhs-report.pdf>.
12. J. Evers. Report: net users picking safer passwords. *ZDNet News*, December 16, 2006. Accessed at [http://news.zdnet.com/2100-1009\\_22-150640.html](http://news.zdnet.com/2100-1009_22-150640.html).
13. C. Föttinger and W. Ziegler. Understanding a hacker's mind- a psychological insight into the hijacking of identities. Technical Report, Danube University, Krems, Austria, 2004. Accessed at <http://www.safetybelt.at/download/danubeuniversityhackersstudy.pdf>.
14. L. Garber. Denial-of-service attacks rip the internet. *Computer*, 33(4):12-17, 2000. Accessed at [http://ieeexplore.ieee.org/xpls/abs\\_all.jsp?arnumber=839316](http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=839316).
15. M. Gelles, D. Brant, and B. Geffert. Building a secure workforce: guard against insider threat. Technical Report, Deloitte Federal Consulting Services, 2008. Accessed at <http://www.deloitte.com/dtt/article/0,1002,cid%253D226369,00.html>.

16. J. Glave. Cracking the mind of a hacker. *WIRED Magazine*, January 20, 1999. Accessed at <http://www.wired.com/science/discoveries/news/1999/01/17427>.
17. I. Goldberg and D. Wagner. Randomness and the Netscape browser. *Dr. Dobb's Journal*, January 2006. Accessed at <http://www.cs.berkeley.edu/~daw/papers/ddj-netscape.html>.
18. S. Gordon. Virus writers: the end of the innocence? In *Proceedings of the 10<sup>th</sup> International Virus Bulletin Conference*, Orlando, FL, 2000. Virus Bulletin.
19. S. Gordon. Understanding the adversary: virus writers and beyond. *IEEE Security and Privacy*, September 2006, 67-70.
20. T. Gorman. The cracker cracks up? *Phrack Magazine*, December 21, 1986. Accessed at <http://www.phrack.com/issues.html?issue=11&id=11>.
21. Government Accountability Office (GAO). Cybercrime: public and private entities face challenges in addressing cyber threats. Technical Report GAO-07-705, US Government Accountability Office, 2007. Accessed at <http://www.gao.gov/products/GAO-07-705>.
22. S. Hansman. A taxonomy of network and computer attack methodologies. Master's Thesis, University of Canterbury, New Zealand, 2003. Accessed at [http://nzcsrsc08.canterbury.ac.nz/research/reports/HonsReps/2003/hons\\_0306.pdf](http://nzcsrsc08.canterbury.ac.nz/research/reports/HonsReps/2003/hons_0306.pdf).
23. S. Hansman and R. Hunt. A taxonomy of network and computer attacks. *Computers and Security*, 21:31-43, 2005. Accessed at <http://linkinghub.elsevier.com/retrieve/pii/S0167404804001804>.
24. L. Heberlein and M. Bishop. Attack class: address spoofing. In *Proceedings of the National Information Systems Security Conference*, pages 371-377, Baltimore, MD, 1996. NIST. Accessed at <http://seclab.cs.ucdavis.edu/papers/spoof-paper.pdf>.
25. H. Highland. A history of computer viruses- introduction. *Computers and Security*, 16(5):412-415, 1997. Accessed at <http://linkinghub.elsevier.com/retrieve/pii/S0167404897822456>.
26. R. Hollinger. Computer hackers follow a Guttman-like progression. *Sociology and Social Research*, 72:199-200, 1988. Accessed at <http://www.phrack.com/issues.html?issue=22&id=7>.
27. J. Howard. An analysis of security incidents on the internet, 1989-1995. Ph.D. Thesis, Carnegie Mellon University, 1997. Accessed at <http://www.cert.org/archive/pdf/JHThesis.pdf>.
28. J. Howard and T. Longstaff. A common language for computer security incidents. Technical Report SAND98-8667, Sandia National Laboratories, 1998. Accessed at [http://www.cert.org/research/taxonomy\\_988667.pdf](http://www.cert.org/research/taxonomy_988667.pdf).
29. Internet Crime Complaint Center. 2008 Internet crime complaint report. Technical Report, Internet Crime Complaint Center, 2008. Accessed at <http://www.ic3.gov/media/annualreports.aspx>.
30. R. Jennings. A (partial) spammer taxonomy. *Computer World*, June 21, 2007. Accessed at <http://blogs.computerworld.com/node/5720>.
31. G. Jones. The 10 most destructive PC viruses of all time. *VARBusiness Magazine*, July 7, 2006. Accessed at <http://www.crn.com/it-channel/190301109>.
32. S. Keats. Mapping the mal web, revisited. Technical Report, McAfee Inc., 2008. Accessed at [http://www.siteadvisor.com/studies/map\\_malweb\\_jun2008.pdf](http://www.siteadvisor.com/studies/map_malweb_jun2008.pdf).
33. B. Kehoe. *Zen and the Art of the Internet: a Beginner's Guide*. Prentice Hall, 1992. Accessed at [http://www-rohan.sdsu.edu/doc/zen/zen-1.0\\_toc.html](http://www-rohan.sdsu.edu/doc/zen/zen-1.0_toc.html).

34. H. Kikuchi, M. Terada, N. Fukuno, and N. Doi. Estimation of increase of scanners based on ISDAS distributed sensors. *Journal of Information Processing*, 16:100-109, 2008. Accessed at [http://www.jstage.jst.go.jp/article/ipsjip/16/0/16\\_100/\\_article](http://www.jstage.jst.go.jp/article/ipsjip/16/0/16_100/_article).
35. M. Kjaerland. A classification of computer security incidents based on reported attack data. *Journal of Investigative Psychology and Offender Profiling*, 2:105-120, 2005. Accessed at <http://doi.wiley.com/10.1002/jip.31>.
36. M. Kjaerland. A taxonomy and comparison of computer security incidents from the commercial and government sectors. *Computers and Security*, 25:522-538, 2006. Accessed at <http://linkinghub.elsevier.com/retrieve/pii/S0167404806001234>.
37. E. Kowalksi, D. Cappelli, and A. Moore. Insider threat study: illicit cyber activity in the information technology and telecommunications sector. Technical Report, National Threat Assessment Center, United States Secret Service, 2008. Accessed at <http://www.secretservice.gov/ntac.shtml>.
38. M. Landler and J. Markoff. Digital fears emerge after data siege in Estonia. *The New York Times*, May 29, 2007. Accessed at <http://www.nytimes.com/2007/05/29/technology/29estonia.html>.
39. B. Landreth. *Out of the Inner Circle: a Hacker's Guide to Computer Security*. Microsoft Press, 1985.
40. C. Landwehr. Formal models for computer security. *Computing Surveys*, 3(13):247-278, 1981. Accessed at <http://portal.acm.org/citation.cfm?id=356852>.
41. C. Landwehr, A. Bull, J. McDermott, and W. Choi. A taxonomy of computer program security flaws, with examples. *ACM Computing Surveys*, 26(3):211-254, 1994. Accessed at <http://chacs.nrl.navy.mil/publications/CHACS/1994/1994landwehr-acmcs.pdf>.
42. L. Lawson. You say cracker; I say hacker: a hacking lexicon. *Tech Republic*, April 13, 2001. Accessed at [http://articles.techrepublic.com.com/5100-10878\\_11-1041788.html](http://articles.techrepublic.com.com/5100-10878_11-1041788.html).
43. E. Levy (under alias Aleph One). Smashing the stack for fun and profit. *Phrack Magazine*, November 8, 1996. Accessed at <http://www.cs.wright.edu/people/faculty/tkprasad/courses/cs781/alephOne.html>.
44. E. Levy. The making of a spam zombie army: dissecting the Sobig worms. *IEEE Security and Privacy*, 1(4):58-59, 2003. Accessed at [http://ieeexplore.ieee.org/xpls/abs\\_all.jsp?arnumber=1219071](http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1219071).
45. H. Lipson. Tracking and tracing cyber attacks: technical challenges and global policy issues. Technical Report CMU/SEI-2002-SR-009, Carnegie Mellon University, 2002. Accessed at <http://www.sei.cmu.edu/pub/documents/02.reports/pdf/02sr009.pdf>.
46. D. Lough. A taxonomy of computer attacks with applications to wireless networks. Ph.D. Thesis, Virginia Polytechnic Institute, 2001. Accessed at <http://scholar.lib.vt.edu/theses/available/etd-04252001-234145/>.
47. J. Markoff. Before the gunfire, cyberattacks. *New York Times*, August 12, 2008. Accessed at <http://www.nytimes.com/2008/08/13/technology/13cyber.html>.
48. K. Mitnick. *The Art of Deception: Controlling the Human Element of Security*. Wiley, 2002.
49. J. Murphy, P. Elmer-Dewitt, and M. Krance. The 414 gang strikes again. *TIME Magazine*, August 29, 1983. Accessed at <http://www.time.com/time/magazine/article/0,9171,949797,00.html>.
50. G. Popek and C. Kline. A verifiable protection system. *ACM SIGPLAN Notices*, 10(6):294-304, 1975. Accessed at <http://portal.acm.org/citation.cfm?id=390016.808451>.

51. J. Post. The dangerous information systems insider: psychological perspectives. Technical Report, George Washington University, 1998. Retrieved from an archive of <http://www.infowar.com>.
52. R. Rantala. Bureau of Justice Statistics special report: Cybercrime against businesses, 2005. Technical Report NCJ 221943, US Department of Justice, 2008. Accessed at <http://www.ojp.usdoj.gov/bjs/abstract/cb05.htm>.
53. E. Raymond. *The Art of Unix Programming*. Addison-Wesley Professional Computing Series, 2003. Accessed at <http://www.faqs.org/docs/artu/>.
54. R. Richardson. 2008 CSI computer crime and security survey. Technical Report, Computer Security Institute, 2008. Accessed at [http://www.gocsi.com/forms/csi\\_survey.jhtml](http://www.gocsi.com/forms/csi_survey.jhtml).
55. M. Rogers. A new hacker taxonomy. Technical Report, University of Manitoba, 1999. Accessed at <http://homes.cerias.purdue.edu/~mkr/hacker.doc>.
56. M. Rogers. Psychological theories of crime and hacking. Technical Report, University of Manitoba, 2000. Accessed at <http://homes.cerias.purdue.edu/~mkr/crime.doc>.
57. M. Rogers. A social learning theory and moral disengagement analysis of criminal computer behavior: an exploratory study. Ph.D. Thesis, University of Manitoba, 2001. Accessed at <http://homes.cerias.purdue.edu/~mkr/cybercrime-thesis.pdf>.
58. M. Rogers. A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation*, 3:97-102, 2006.
59. D. Russell and G. Gangemi. *Computer Security Basics*. O'Reilly, 1991.
60. J. Rutkowska. Introducing stealth malware taxonomy. Technical Report, COSEINC Advanced Malware Labs, 2006. Accessed at <http://www.invisiblethings.org/papers/malware-taxonomy.pdf>.
61. W. Scherlis. DARPA establishes computer response team. Press Release, Defense Advanced Research Projects Agency (DARPA), 1988. Accessed at <http://www.cert.org/about/1988press-rel.html>.
62. W. Schwartau. *Information Warfare: Cyberterrorism: Protecting Your Security in the Electronic Age*. Thunder's Mouth Press, 1996. Accessed at <http://www.winnschwartau.com/resources/IW1.pdf>.
63. E. Shaw, K. Ruby, and J. Post. The insider threat to information systems: the psychology of the dangerous insider. *Security Awareness Bulletin*, 2:1-10, 1998. Accessed at <http://www.pol-psych.com/sab.pdf>.
64. A. Smith and W. Rupp. Issues in cybersecurity: understanding the potential risks associated with hackers/crackers. *Information Management and Computer Security*, 10(4):178-183, 2002. Accessed at <http://www.emeraldinsight.com/Insight/viewContentItem.do?contentType=Article&contentId=862828>.
65. M. Soper. Digital picture frames- now with free malware! *MaximumPC Magazine*, February 16, 2008. Accessed at [http://www.maximumpc.com/article/digital\\_picture\\_frames\\_now\\_with\\_free\\_malware](http://www.maximumpc.com/article/digital_picture_frames_now_with_free_malware).
66. S. Specht and R. Lee. Distributed denial of service: taxonomies of attacks, tools, and countermeasures. In *Proceedings of the 17<sup>th</sup> International Conference on Parallel and Distributed Computing and Systems*, pages 543-550, Cambridge, MA, 2004. ACTA Press. Accessed at <http://palms.ee.princeton.edu/PALMSopen/DDoS%20Final%20PDCS%20Paper.pdf>.
67. S. Steele and C. Wargo. An introduction to insider threat management. *Information Systems Security*, 16(1):23-33, 2007. Accessed at [http://www.infolocktech.com/download/ITM\\_Whitepaper.pdf](http://www.infolocktech.com/download/ITM_Whitepaper.pdf).
68. B. Sterling. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. Bantam Books, 1993. Accessed at <http://www.mit.edu/hacker/hacker.html>.

69. C. Stoll. Stalking the wily hacker. *Communications of the ACM*, 31(5):484-497, 1988. Accessed at <http://pdf.textfiles.com/academics/wilyhacker.pdf>.
70. C. Taylor, J. Alves-Foss, and V. Freeman. An academic perspective on the CNSS standards: a survey. In *Proceedings of the 10<sup>th</sup> Colloquium for Information Systems Security Education*, pages 39-46, Adelphi, MD, 2006. Springer. Accessed at <http://www.cisse.info/colloquia/cisse10/proceedings10/pdfs/papers/S02P01.pdf>.
71. United States Computer Emergency Readiness Team (US-CERT). Quarterly trends and analysis report, Volume 3, Issue 4. Technical Report, US-CERT, 2008. Accessed at [http://www.us-cert.gov/reading\\_room/](http://www.us-cert.gov/reading_room/).
72. W. Van Eck. Electromagnetic radiation from video display units: an eavesdropping risk? *Computers and Security*, 4:269-286, 1985.
73. L. Walleij. *Copyright Does Not Exist*. Online Book, 1998. Accessed at <http://home.c2i.net/nirgendwo/cdne/>.
74. J. Walker. The ANIMAL episode. Technical Report, Fourmilab Switzerland, 1996. Accessed at <http://www.fourmilab.ch/documents/univac/animal.html>.
75. K. Walter, S. Schaeen, W. Ogden, W. Rounds, D. Shumway, D. Schaeffer, K. Biba, F. Bradshaw, S. Ames, and J. Gilligan. Structured specification of a security kernel. *ACM SIGPLAN Notices*, 10(6):285-293, 1975. Accessed at <http://portal.acm.org/citation.cfm?id=390016.808450>.
76. N. Weaver, V. Paxson, S. Staniford, and R. Cullingham. A taxonomy of computer worms. In *Proceedings of the 2003 Workshop on Recurring Malcode*, pages 11-18, Washington, DC, 2003. ACM Press. Accessed at <http://www.icir.org/vern/papers/taxonomy.pdf>.
77. R. Westervelt. Cybercriminals employ toolkits in rising numbers to steal data. *Search Security*, September 6, 2007. Accessed at [http://searchsecurity.techtarget.com/news/article/0,289142,sid14\\_gci1271024,00.html](http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1271024,00.html).
78. A. Wood and J. Stankovic. A taxonomy for denial-of-service attacks in wireless sensor networks. Chapter 32 of *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, CRC Press, 2004. Accessed at <http://www.cs.virginia.edu/~adw5p/pubs/handbook04-dos-preprint.pdf>.
79. H. Xia and J. Brustoloni. Detecting and blocking unauthorized access in wi-fi networks. In *Proceedings of the Third International IFIP-TC6 Networking Conference*, LNCS 3042, Athens, Greece, 2004. Springer. Accessed at <http://www.springerlink.com/content/xbq6gt5uypnrabm5/>.