Taxonomy of Cyber Attacks and Simulation of their Effects

Ian M. Chapman
Defence Research and Development Canada
Centre for Operational Research and Analysis
Ian.Chapman@drdc-rddc.gc.ca

Sylvain P. Leblanc,
Assistant Professor
Computer Security Laboratory
Royal Military College of Canada
Sylvain.Leblanc@rmc.ca

Andrew Partington
Research Assistant
Computer Security Laboratory
Royal Military College of Canada

Keywords: Cyber attack, taxonomy, effects, command, control

Abstract

Due to an increasing level of reliance on computer network technology, military organizations are increasingly vulnerable to cyber attacks. Cyber attacks take a variety of forms and have a broad spectrum of effects. In order to facilitate military cyber operators' and defenders' understanding of the threats they face, we propose a taxonomy of cyber attacks based on the level of access required by the attacker to launch the attack. We also discuss a number of methods used to deliver cyber attacks to target systems. Finally, we propose methods to simulate the effects of several cyber attack types for use in simulation in support of training and experimentation.

1. INTRODUCTION

Recent events, such as the 2007 cyber attack on Estonia [1] and the 2008 cyber attack on Georgia [2], have shown the rising importance of computer network operations in an increasingly inter-networked world. Both civilian and military domains have become increasingly reliant on computer networks for communication, information management, utilities management, financial systems, air traffic control, and many more critical applications. It is becoming ever more apparent that cyber attacks have the potential to be extremely disruptive to a wired society.

1.1. Military Threat of Cyber Attacks

Militaries are not immune to cyber attacks. In fact, concepts such as Network Enabled Operations and Adaptive Dispersed Operations require increasing amounts of connectivity, thus increasing vulnerability to cyber attacks.

Cyber attacks come in many types, each with specific effects that may be observed by network operators and ordinary users. Given the increasingly digitized and networked nature of military organizations, it is important to explore the potential effects of these attacks through simulation in support of training and experimentation. Through these methods, we may begin to understand the effects that cyber attacks may have on military commanders' decision-making capabilities and thus on mission effectiveness.

1.2. Classifying Cyber Attacks

Because cyber attacks strike in a variety of ways at individual computers and computer networks, it is important to classify them to facilitate operators' and defenders' understanding of the threats they face. A descriptive taxonomy will allow military audiences, who may not have extensive experience dealing with cyber attacks, to communicate more effectively with their network operators and allow them to understand the potential effects and scope of these attacks. The taxonomical approach will also provide the military modeling and simulation community with the correct jargon for the cyber attacks they will be simulating.

Previous work in this field has included the development of taxonomies for specific attack types, such as computer worms [3]. These taxonomies tend to be very detailed, but narrow in focus. Other taxonomical work has focused on specific network environments, such as the 3G cell network [4]. The taxonomy of Kotapati et al (2005) is based on the access level (physical and system) to 3G network infrastructure required by the attacker to launch an attack. This approach is appealing, but is limited to the 3G environment. Other taxonomies of computer and network attacks have been created to classify specific attacks [5]. The taxonomy proposed by Hansman and Hunt (2005) is multi-dimensional, with categories for attack vectors, targets, vulnerabilities and payloads. This work allows for detailed characterization of a broad spectrum of attacks, but the purpose is to describe *specific* attacks, such as the Code Red computer worm.

In Section 2 we propose a taxonomy of cyber attacks, based on the level of access that the attacker requires to launch the attack, with prominent examples of cyber attacks in each level. The descriptions of the cyber attacks in Section 2 include examples of their potential effects on the target systems. The intent of this taxonomy is to facilitate military personnel's understanding of the cyber threats they

face. The inclusion of descriptions of the attacks' potential effects enables better representation of the attacks in simulation.

Along with the taxonomical approach to cyber attacks and their effects, it is important to consider the methods used to deliver the attacks to their targets. To enhance the training or experimentation audience's immersion in a simulation, it may be necessary to simulate the delivery of a cyber attack into the target systems. Thus, a number of cyber attack delivery methods are discussed in Section 2.

1.3. Simulation of Cyber Attack Effects

Simulation is a valuable tool for training and experimentation in modern military organizations. Simulation of the effects of cyber attacks will enable a training audience to learn to identify and deal with these effects in a safe environment. Through experimentation, the effects of cyber attacks on mission effectiveness can be evaluated, and new methods of mitigating degradation can be investigated.

A full simulation of a cyber attack would require a red team (opposing force) to attack the exercise networks and systems, which would prove to be expensive. While this type of simulation would be useful to train "cyber warriors" to defend the network, we are more interested in investigating the effects of cyber attacks on a modern command post headquarters. Thus, the simulation can be limited to the *effects* of the cyber attacks on the systems used by the training or exercise audience. Section 3 of this paper presents several methods of simulating the effects of some common cyber attacks. The proposed methods are general in nature and will become more detailed in future work.

A survey of modeling and simulation implementations of cyber attacks and computer network operations (CNO) was conducted by the authors [6]. The results of this survey show that the modeling and simulation of cyber attacks has mainly focused on studying their network and economic effects, with little emphasis on effects a typical user would experience. Thus, the simulation of the user-level effects of cyber attacks in a military setting is a novel area of research.

It is vital that military audiences experience these effects in simulation in order to study their impact on mission effectiveness and to train for potential CNO. The methods of effects simulation proposed in Section 3 of this paper represent a preliminary step in presenting the effects of cyber attacks to military staff exercise audiences.

2. CYBER ATTACK TAXONOMY

Given the multitude of cyber attacks that have been observed, we propose a taxonomy that classifies them based on the level of access on the target system required by the attacker in order to launch an attack. In creating this taxonomy, we aim to facilitate military audiences' understanding of the language used to describe cyber attacks. We propose a 3-tier taxonomy, ranging from *no access* to *user access* to *root access* requirements. Each tier is described in its own subsection, with examples of the attacks and their potential effects provided. The taxonomy was designed to aid military network defenders in structuring their defence plans against the threats at each level. Through the taxonomy, military network users will also become more familiar with cyber attack jargon, and the penetration levels different attacks imply. Also, the taxonomy provides the military modeling and simulation community with a structure to base their methods on, when called upon to simulate the effects of a particular cyber attack.

The final part of this section discusses the various delivery mechanisms used to implant the attacks discussed in the 3-tier taxonomy.

The taxonomy presented in this section is by no means a complete treatment of the subject matter. New attacks arise every day with a volume and variety that are staggering. The examples we discuss are among the most common and thus are meant to be a starting point for investigating the modeling of cyber attack effects in simulation.

The reader should note that we are suggesting a taxonomy that is applicable to only a portion of potential cyber attacks. Sophisticated attackers, such as intelligence services or military forces of certain nation states, can mount precisely targeted attacks against very narrowly focused targets. The study of such targeted attacks is outside the scope of this paper. Instead, we concentrate here on more broad-based cyber attacks that have been observed in large computer networks such as the internet.

2.1. Tier 1: No Network or Computer Access

Tier 1 attacks require no special network or computer access privileges in order to launch. In fact, most of these attacks exploit the open nature of computer networks and the protocols they use for communication.

2.1.1. Denial of Service Attack

A Denial of Service (DoS) attack overwhelms a target computer's resources (such as processing time or memory) or its bandwidth, with the aim of making it incapable of responding to legitimate requests. A DoS attack can be launched directly through a computer network (usually through the internet). Attackers only need to know a target computer's Internet Protocol (IP) address in order to launch the attack.

There are several distinct types of DoS attacks that have been identified, but all share a common method of sending requests or data packets to the targeted computer [6]. The most common DoS attack, known as a *Flood Attack*,

overwhelms a target computer with a flood of requests that must be answered. This disrupts normal connection requests from being able to access the target computer in a timely fashion.

Another common DoS attack is known as a *Smurf Attack*. In a smurf attack an attacker spoofs, or impersonates, the target computer by sending requests to networked computers using the target's IP address. Each of the requests sent out requires a response to be sent to the sender's IP address, thus the target computer is flooded with messages from a number of computers. Again, this limits the ability of the target computer to handle legitimate traffic in a timely matter.

The final example of a DoS attack we will discuss is a *Malformed Packet Attack*. This attack is functionally different than the previous ones in that it does not use a flood of data to attack the target computer. Rather, this attack focuses on vulnerabilities in a computer's Transmission Control Protocol (TCP)/IP stack, which may be used to attack resources on the target computer and shut down processes, turn off network communication, or crash the target's operating system.

2.1.2. Distributed Denial of Service Attack

If a defender can identify the source of a DoS attack, it is easily defended against. A Distributed Denial of Service (DDoS) attack is very similar to a DoS, and yet much more powerful because the source of the attack is harder to pinpoint. DDoS attacks make use of a network of compromised computers, known as a *botnet*, to send in floods of data to the target computer [8]. The target is then overwhelmed and unable to handle the traffic. A sustained DDoS attack was the main tactic used by the aggressor in the 2007 cyber attack on Estonia.

Typically, the computers that make up the botnet used in a DDoS attack have been compromised earlier through various hacking and infection techniques. The attacker can then control all of the computers in the botnet by sending commands from his own location. Thus, DDoS attacks are usually difficult to attribute to any particular attacker since they make use of computers used by innocent bystanders who are unaware that their systems have been compromised.

DDoS attacks usually use the same strategies as DoS attacks, such as flood attacks and smurf attacks. However, since more computers are used to send requests, DDoS attacks can completely cripple the target system.

2.1.3. Stack-Based Buffer Overflow Attack

A buffer overflow attack takes advantage of poorly-written computer code to insert more data into a buffer than it has room for [9]. The overflow data is then written to the stack, a "last in, first out" data processor in the computer. By exploiting this weakness, an attacker can overflow a buffer in a program and pass malicious code on to the stack to be processed.

The code that can be processed by the stack is dependent upon the access level of the program that is attacked. Thus, attackers tend to focus on programs that have administrative level access, which will be passed to their malicious processes. The types of actions an attacker can take include extracting or deleting data, corrupting system files, crashing the program or operating system, etc.

Note that although this attack can be launched remotely, it is also effective if the attacker has a higher level of access to the computer or network (as discussed in Sections 2.2 and 2.3).

2.1.4. Phishing

Phishing is a common type of attack that makes use of social engineering techniques to get users to either reveal sensitive information or run malicious programs [10]. Mass email messages can be used to deliver messages that appear to be legitimate. A more sophisticated attacker may attempt to make the phishing message more attractive by personalizing it for the intended target in a refinement known as *spear phishing*.

Frequently, these messages contain attachments that, when run, deliver malware to the reader's computer system. A prominent, relatively benign example of this attack was the ILOVEYOU email worm that attacked millions of computers in 2000 [11]. Email messages arrived with the subject line of, "ILOVEYOU," and an attachment called, "LOVE-LETTER-FOR-YOU.TXT.vbs." Once opened, the attachment sent the same message on to all of the contacts in the readers' address books. While not particularly destructive, this attack demonstrated the relative ease of transmitting an infection through the phishing method.

Another type of phishing (general or spear) sends messages purporting to be from companies that the user may deal with, such as banks, social networks, or online email domains. These messages typically contain a link to a site that closely resembles the actual company's site, prompting the user for a username and password. In this manner, the attack can trick the user to provide their personal information. From this point more information can be stolen, money can be withdrawn from bank accounts, or access can be granted into the users' systems.

2.2. Tier 2: User Access with Limited Privileges

At this level, an attacker has access to a computer, but with limited privileges. Access can be gained remotely through the network, or locally if the attacker has physical access to the computer terminal. Essentially, at this level, the attacker can assume the role of a non-administrator user. Even though the privileges at this level are limited, there are still a number of attacks available to the attacker. Such user-level exploits are also important because they provide the

attacker with a foothold on the target system, from which the attacker can attempt privilege escalation which will give access to the exploits in Tier 3 (see Section 2.3).

The following are a sample of the attacks available at Tier 2.

2.2.1. Password Hacking

Password hacking is, quite simply, attempting to discover passwords of legitimate users through a number of methods. Most of these methods use a hacking application that automates the process [12].

For most computers, passwords are encrypted with a one-way encryption algorithm and then stored on the host in the form of password hashes. Typically, and attacker will extract the password hashes and copy it to his own computer, where the hacking application is installed. Most password hacking applications operate in different modes including *rainbow tables*, guessing potential passwords from a dictionary, or attempting all possible password combinations (known as *brute force*). In all cases, the password attempt is encrypted using the same algorithm used in the target system, and then compared with the captured password hash.

Once a password is hacked, the attacker can then access the computer, locally or remotely, by impersonating the user whose credentials were discovered. Depending on the access privileges of the user, this can potentially give a hacker varying levels of access on the computer. The access level of the user determines the types of further malicious activity the attacker can engage in. For example, data can be corrupted or deleted, malicious software might be installed, or users' passwords changed to prevent their access to the system.

2.2.2. Sniffing

Sniffing is a form of cyber attack aimed at collecting information from a computer network. Once access has been gained to a target computer with limited privileges, the attacker installs a sniffer program which can read and store data that passes through the network for transmission or later physical retrieval. Typically, sniffers work as background processes, and an attacker need not stay in operation of the infected computer once the program is in operation [13].

Sniffing can reveal sensitive information as it travels through a computer network. Potentially, an attacker can collect usernames, passwords, and email messages if they travel through the network unencrypted.

A more aggressive attack that can arise out of sniffing (as well as password hacking) is called *session hijacking*. Using sniffing to obtain a user's name and password, an attacker can also make use of IP spoofing to take over a legitimate user's session. Once a hijacking occurs, an attacker can use DoS techniques to use up bandwidth on the network or to break the connection between the legitimate user and the network.

2.2.3. Nuisance Attacks

After gaining limited access to a computer an attacker can perform a number of actions that, while not necessarily catastrophic, are a nuisance to the legitimate users of the computer or network it is attached to. Examples of these nuisance attacks include: sending emails from the legitimate user's account, stealing data, deleting files, filling the hard drive with data, changing data or documents, changing the user's passwords, running large numbers of processes (consuming all memory available), and spamming the network with communications from the target computer. Many more actions can be taken which are only limited by the imagination of the attacker and the access level on the target computer.

What is seen as a nuisance attack on civilian computer systems can have greater effects on military networks. In fact, an attacker who gains access to a military networked computer system can use user level access for disinformation, which can have serious effects on operations.

2.3. Tier 3: Root Access/Administrative Privileges

Users with administrative privileges to a computer or network are said to have *root access* (from the name of the Unix/Linux administrative account). This level of access gives an attacker complete freedom to act on the computer, changing settings and installing software at will. Typically, once gaining root access, an attacker will install a backdoor (see Section 2.3.1) on the target computer and then seal the security vulnerability that allowed him access in order to prevent other attackers from gaining access to the target [1].

The following subsections describe various attack techniques that can be used after gaining root access.

2.3.1. Backdoor

After an attacker gains root access to a computer, he will often attempt to guarantee his future access to the computer by installing a backdoor. This will prevent an interruption to the attacker's access to the computer if the legitimate user patches the security exploit used to gain access.

A backdoor usually consists of a server and a client program. The server resides on the attacker's computer and the client is installed on the target computer. The client, which resides on Tier 3 on the target computer, executes the commands sent to it from the attacker's server. In this manner, the attacker can bypass the password/login system on the target system.

2.3.2. Rootkit

Rootkits are designed to alter or replace system components on the target computer [1], such as the common UNIX functions: `login`, `du`, `find`, `ifconfig`, `ls`, and `ps`. This gives the attacker's malicious process an opportunity to act every time one of the compromised system calls is executed.

Because rootkits are designed to mimic the actual look and operation of real system commands, they are difficult to detect and remove.

Rootkits can function very similar to backdoors if they are used to replace the normal `login` file. In this case, a false version of `login` will allow legitimate users to login to the computer as normal, while allowing the attacker to login with full access privileges using a backdoor password. Legitimate users would not know their system had been compromised, as the false `login` function would appear exactly as the real version did.

Another function that is commonly replaced in a rootkit is `inetd`, which controls FTP, telnet, and other communication protocols [1]. The attacker can thus disguise the communications between the target and attacking computers. The attacker can also exploit this function to discover passwords and usernames for other computers that connect through the network.

2.3.3. Kernel-Level Rootkit

A kernel-level rootkit is a more dangerous version of a standard rootkit, and more difficult to detect and to remove. This type of rootkit can perform the same types of functions as a standard one, except instead of replacing system files it alters part of the target computer's kernel (the central component of the operating system).

The use of kernel-level rootkits is very similar to the standard rootkits described previously; however, operating at the kernel level allows corrupted files to be hidden more effectively from scanners and allows the attacker to mask his malicious processes and communications through the network ports. Thus, administrators have a difficult time detecting this type of rootkit.

2.3.4. Spyware and Keyloggers

Spyware is a type of malicious software that is used to invade a legitimate user's privacy. After being installed on the target computer, spyware programs collect data from the legitimate user based on their use of the computer. For example, the attacker can collect usernames and passwords for email accounts, online banking, and other programs on the computer. Spyware can also be set to record and transmit sensitive information, such as classified documents or trade secrets.

A keylogger is a type of spyware that records all keystrokes made on the keyboard of a target computer. The keylogger can also record the time and date of each keystroke, which program was in use at the time, and even periodically take screenshots to send back to the attacker. Again, the collection of this information will provide the attacker with sensitive information about the legitimate user of the computer.

2.3.5. Adware

Adware is a similar type of attack to spyware, but with a goal of putting advertising messages in front of the user as opposed to stealing information. The symptoms of an adware infection can vary, but some common effects include: a slow operating system, slow web browsing, pop-up ads on the desktop or within programs, and redirection of web browsers to advertisements for specific pages. Adware tends to be more irritating than destructive, especially since it often requires special programs to remove it.

2.3.6. Various Malicious Attacks

In addition to the attacks described previously, a number of other attacks can be accomplished relatively easily once root access has been gained. Examples of common attacks include, but are not limited to, removing administrative privileges of legitimate users, reconfiguring system settings to make computers difficult to use, and ending computer processes in order to crash the system.

Another common attack type is known as a *logic bomb*. These attacks are set to be triggered by specific events on the target computer, such as at specific times or when a certain program is opened or closed. The logic bomb, when triggered, can end system processes, crash the computer, or destroy data through deletion. Often, logic bombs are accompanied by messages that attempt to extract payment from the user in order to prevent the trigger from detonating the bomb. This is known as a *ransomware attack*, and has proven to be a moderately successful method of criminal extortion.

2.4. Delivery Methods

Many cyber attacks depend on some level of access to the target computer (see Sections 2.2 and 2.3). This means that the attack mechanism must somehow be delivered to the target computer. Some of the attacks described in Section 2.1 can be used to deliver code into a target system that will be used for a future attack; however, they tend to be tightly controlled by the attacker. The delivery methods discussed in this section require far less direction from the attacker, and their spread is often self-sustaining and self-directed.

2.4.1. Trojan Horses

A Trojan horse, or "Trojan", is a program which offers legitimate and useful functionality in order to entice a computer user to download and install it. However, the actual purpose of the program is to install harmful code on

the user's computer, thus mirroring the story of the Trojan horse from Greek mythology.

Many Trojans are made available through the internet, and are advertised as useful programs such as a video codecs (computer programs to encode and decode video data streams), internet browser toolbars, games, or other free applications. By including software with attractive functionality, the Trojan can be installed without the user becoming suspicious.

Trojan horses can be used for a variety of attacks, including many of those discussed in Sections 2.2 and 2.3. Trojans are difficult to remove, as they often change system settings and registry entries, and these must be fixed even after the software has been removed from the system.

2.4.2. Viruses

A computer virus is a digital analogue of a virus in the biological world. Instead of corrupting a host organism's cells with viral DNA, a computer virus injects its code into applications installed on a computer. When a computer user activates the infected program the computer virus then attempts to infect other systems. Biological viruses use the cells' organelles as a factory to produce many copies of themselves that go on to infect other cells, while computer viruses use active applications to spread from computer to computer.

Because a computer virus uses compromised target computers to attack new computers, it is an efficient way for an attacker to infect many computers with little requirement for oversight. Viruses tend to spread through email or network resources such as shared drives or subnets. Once activated, viruses use the compromised computer's knowledge of other computers to propagate. Viruses can also take advantage of portable digital media such as USB flash memory and writable CDs to infect new computers.

The effects of viruses vary depending on their programmed functionality and on the access privileges of the software they attack. Some viruses are fairly innocuous, only propagating without doing real harm, while others have other effects such as crashing programs, installing backdoors, and extracting data.

2.4.3. Worms

Worms are somewhat similar to viruses in that they propagate through a network with no direction from the attacker. However, unlike viruses, worms require no user interaction to activate their attempts to spread. Because no user interaction is required for the worm to spread, these infections expand rapidly through network vulnerabilities.

The effects of worms vary, much like the effects of viruses. Worms often discover network topographies automatically and spread through any security vulnerabilities they can find.

2.4.4. Scareware

Scareware makes use of social engineering techniques to convince computer users to download malicious software onto their computers [14]. Commonly, scareware originates as a pop-up window during internet browsing. These pop-ups often resemble system setting windows or anti-virus software reports that show an infection on the computer. The user is then prompted to install a fix, which involves authorizing a download from the internet. This download contains the malicious code that, once installed, will go on to attack the target computer.

3. SIMULATING CYBER ATTACK EFFECTS

Simulation is often used by military organizations for training and experimentation. In a training role, simulation familiarizes soldiers with phenomena they will experience on the battlefield and provides safe, repeatable opportunities to learn how to deal with them. In a military context, the main role of experimentation is to investigate the effects of some particular issue or technology on mission effectiveness.

As mentioned in Section 1.3 and detailed in [6], simulation of the effects of cyber attacks is a novel subject, especially in a military setting. The methods discussed in this section are focused on simulating the effects of a number of cyber attacks from the taxonomy, especially within the context of a Command Post Exercise (CPX) which can be used for either training or experimentation. For each effect discussed, a general method of simulation is proposed, leaving the details to be developed in future work.

The cyber attacks discussed in this section were selected because they presented the effects that are most visible to the computer user. Further methods of simulation for the remaining cyber attack effects are currently under investigation.

3.1. DoS and DDoS

The effects of DoS and DDoS attacks (Sections 2.1.1 and 2.1.2, respectively) include slowed or overloaded network communications, isolation of target computers from the network, and potential application or system crashes. Operational networks are often simulated in CPXs and thus the exercise controllers often have a great deal of control over the network.

To simulate sluggish network communications, controllers can throttle network traffic in much the same way that internet service providers reduce data rates to customers downloading particular types of traffic such as streaming video or audio. Some DoS attacks can actually isolate the target computer from the network, and this can be simply simulated by disconnecting (physically or virtually) a computer from the exercise network. To simulate application or computer crashes, exercise controllers can

reconfigure affected systems (at the terminal or remotely through the network). Although slightly more intrusive, the same effect could be achieved by giving participants notes, or passing them instant messages over the exercise networks, informing them about what effects to replicate by shutting down software or computers. Programs and computers thus affected would have to remain shut down until the cyber attack is deemed to have ceased or to have been mitigated.

3.2. Phishing

A phishing attack (Section 2.1.4) begins with a social engineering attack, convincing a user to open a file or provide sensitive information. During CPXs, there are often a number of injects that arrive to move the scenario forward through various means. One of these is through the participants' email inboxes. In this manner, exercise controllers can simulate a phishing attack by including a phishing message with some of their inject traffic. A logging system could be used to determine if any participants had responded to the phishing attack, and these victims would then be passed notes or instant messages instructing them on the effects on their systems, although this would let the users know that they had been hit by an attack. Alternatively, exercise controllers can create some of these effects administratively through the exercise network.

3.3. Nuisance Attacks

Most of the nuisance attacks mentioned in Section 2.2.3 involve changing data or user privileges on the target computer. Because exercise control has full privileges on the exercise network, any of the attacks mentioned can be simply affected by an exercise controller.

As briefly discussed in Section 2.2.3, nuisance attacks can have more serious consequences on military networks. It is likely that an adversary would try to change or delete data in an operational database or change user passwords to prevent users from accessing their computers. Exercise controllers could affect these changes remotely, over the exercise network, if such events are included in the exercise's master events list. Running additional processes may be difficult to accomplish, however, the effect of crashing a computer can be simply simulated by instructing a user to restart their computer (or administratively restarting it remotely without telling the user what happened).

3.4. Spyware and Keyloggers

Spyware and keyloggers (Section 2.3.4) are most often used as data gathering tools by attackers. The effect of these attacks is that sensitive information can be leaked from an otherwise secure network, alerting adversaries to the military forces intent. Thus, if it is determined that a certain computer has been infiltrated by spyware, an exercise controller can pass sensitive information, such as intelligence reports or orders, on to the controller of the opposing force. The opposing force can then act on the information they receive, potentially altering the balance of power in the simulated conflict. This effect would not necessarily alert the command post staff that their information security had been compromised at the time of the leak, but the effect can be highlighted during exercise after-action reviews.

Frequently, information leaks result in media coverage that portrays the military in a poor light. These incidents often affect military operations by turning the local populace's anger against the military force. CPXs often include a simulation of media coverage of the operation and an information leak effect can be simulated by releasing negative news reports that include protected information. This has the advantage of alerting the staff that their information security has been compromised before the after-action review.

3.5. Adware

The main noticeable effects of adware (Section 2.3.5) are redirection of web browsers, pop-up windows, and slower operation or crashing of the target computer. If the CPX makes use of dedicated webpages in their operation, an exercise controller can cause automatic browser redirection through the addition of some minor code into the webpage. This can in turn cause new windows to pop-up, taking the users to simulated sites off the exercise network.

Slowed computer operation would be more difficult to simulate. However, as we have discussed previously, crashing computer can be simulated by instructing exercise participants to periodically restart their computers or by restarting them remotely.

3.6. Various Malicious Attacks

Some of the effects of the malicious attacks mentioned in Section 2.3.6 are similar in nature to those discussed in Section 2.2.3. These effects can be simulated using the same methods as proposed in Section 3.3.

The attacks that are more malicious in nature, such as logic bombs, can have devastating effects on the target computer and on information in the network. Some logic bomb effects can render a computer useless until it has been repaired by a technician. To replicate this, the user of a targeted computer could be instructed (via note or instant message) to shut down their computer for an indefinite period of time. Depending on the length of the CPX, the user may be able to turn his computer back on if sufficient time has passed to simulate a repair. Other effects, such as filling hard drives with data or deleting massive amounts of data can be simulated by exercise controllers through the network.

4. CONCLUSION

As militaries grow increasingly reliant on network technology to accomplish their missions, they become increasingly vulnerable to broad-based cyber attack. The taxonomy presented in this paper divides cyber attacks into three tiers (*no access, user access/limited privileges, and root access/administrative privileges*) and describes several examples in each. This taxonomy provides the military modeling and simulation community with a structure to understand cyber attacks and their effects. It also provides military audiences with the language they need to describe cyber attacks (as well as information about the level of penetration required to launch them), and a structure to facilitate understanding the potential impacts that these attacks may have on military operations. We have also discussed a number of delivery methods that can cause computer infection consistent with attacks from all three tiers. Because of the volume and variety cyber attacks, this taxonomy is merely the starting point for further investigation. Furthermore, the taxonomy is not designed to cover targeted cyber attacks.

Being able to simulate the effects of broad-based cyber attacks is important in order to train military forces on how to react to them, as well as to study the impacts cyber attacks have on mission effectiveness. As it becomes increasingly likely that cyber attacks can affect military command posts, it is necessary to teach staff officers how to spot and deal with their effects. Simulation of the effects of cyber attacks is a novel area of research and a number of simple methods to simulate these effects during a CPX have been discussed. These methods have been presented generally and continue to be developed by the authors.

Future work being considered by the authors includes the production of a detailed handbook of instruction for simulating the effects of cyber attacks, insertion of cyber attack injects in CPX activities, and an investigation of the effects of cyber attacks on mission effectiveness and commanders' trust in their information systems.

References

[1] Lesk, M. "The New Front Line: Estonia Under Cyberassault," *IEEE Security & Privacy* 5(4) (2007): 76-79.

[2] Markoff, J. "Before the gunfire, cyber attacks," *The New York Times*, August 13, 2008.

[3] Weaver, N., Paxson, V., Staniford, S., and Cunningham, R. "A Taxonomy of Computer Worms," *Proceedings of the 2003 workshop on Rapid malcode (WORM 2003)* (2003): 11-18.

[4] Kotapati, K., Liu, P., Sun, Y., and LaPorta, T. "A Taxonomy of Cyber Attacks on 3G Networks," *Lecture Notes in Computer Science* 3495 (2005): 129-138.

[5] Hansman, S. and Hunt, R. "A taxonomy of network and computer attacks," *Computers and Security* 24(1) (2005): 31-43.

[6] Leblanc, S.P., Chapman, I., Partington, A., Bernier, M., "An Overview of Cyber Attack and Computer Network Operations Simulation" *Proceedings of the 2010 Military Modeling and Simulation Symposium (MMS'11)*, (2011).

[7] Skoudis, E. *Counter Hack.* New Jersey: Prentice Hall PTR, 2002.

[8] Kjaerland, M. "A taxonomy and comparison of computer security incidents from the commercial and government sectors," *Computers & Security* 25(7) (2006): 522-538.

[9] Radosavac, S., Seamon, K., and Baras, J.S. "bufSTAT – a tool for early detection and classification of buffer overflow attacks," *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks* (2005): 231-233.

[10] Yu, W.D., Nargundkar, S., and Tiruthani, N. "A phishing vulnerability analysis of web based systems," *IEEE Symposium on Computers and Communications* (2008): 326-331.

[11] Jagatic, T., Johnson, N., Jakonsson, M., and Menczer, F. "Social Phishing," *Communications of the ACM* 50(10) (2010): 94-100.

[12] Potter, B. "A Review of 10phtcrack 6," *Network Security* 2009(7) (2009): 14-17.

[13] Ansari, S., Rajeev, S.G., Chandrasekar, H.S. "Packet sniffing: a brief introduction," *Potentials, IEEE* (2003): 17-19.

[14] Giles, J. "Scareware: the inside story," *The New Scientist* 205(2753) (2010): 38-41.

Biography

Ian Chapman is a defence scientist with the Defence Research and Development Canada Centre for Operational Research and Analysis in Ottawa, Canada. Mr. Chapman's work has included analytical support to a number of modeling and simulation activities at the Canadian Army Experimentation Centre and he is now working with the Canadian Cyber Task Force to determine the impacts of cyber attacks on military mission effectiveness.

Sylvain (Sly) Leblanc is an Assistant Professor at the Royal Military College of Canada (RMCC). He obtained his Master's of Engineering in Software Engineering from RMCC in 2000, where he is also a doctoral candidate. Sly was a Canadian Army Signals Officer for over 20 years, where he developed his interest in computer network operations. His research interests are in computer security and computer network operations.

Andrew Partington is in the final year of a Bachelor of Engineering in Mechatronics program at the University of Canterbury, New Zealand. He participated in a university exchange program at Queen's University in Canada in 2010. On the exchange he worked at RMCC researching computer network operations and simulations.