e-News: An 'Open' Portal Policy

By Robert B. Fried, BS, MS

Abstract

This paper will attempt to prove the notion that "threats combined with vulnerabilities and consequences produce risks". In order to accomplish this goal, a number of possible threats and attacks that could be launched against a web site offering its users a news service will be analyzed. The results of this analysis will be presented in order to determine a number of possible defense mechanisms. Ultimately, such an analysis will allow for a conclusion to be drawn regarding the relationship that exists between threats, attacks and defense mechanisms.

Introduction

The Internet provides a wealth of information and services. It is gradually emerging as an integral part of everyday life. In the days prior to the Information Age, most things were tangible. However, with the coming of the Digital Revolution, a majority of what we see and read is presented virtually. Forget about having to take a stroll down your driveway to pick up a dose of the daily news. Today, all one really has to do is simply take a trip into cyberspace from the comfort of their own home and they will find enough news to keep them busy for quite awhile.

Many web sites on the Internet, either to boost popularity or cater to their users' needs have added some types of news related links. Yahoo! and CNN are two web sites, which offer such a service. With all the traffic that continuously comes and goes on sites providing an up to date source of information, one may begin to wonder how companies such as these attempt to safeguard the integrity of the news they provide.

The Scenario

The online population is expanding tremendously with the passing of each day. People utilize the Internet for many different reasons. Some of the people like to check the headline news or stock markets at various points throughout the day. Others like to do research on a specific subject/topic that is of interest to them. Of course who can forget about the hours people spend chatting real time with friends or sending electronic mail messages. In other words, a lot of time can be passed online and a lot of people are doing just that. The founder of e-News, Robert Fried, has realized the potential of the World Wide Web and has decided to take advantage of the global market that exists online.

The news portal, e-News, was founded in August 2002. Owner and Chief Editor, Robert Fried envisions that e-News will emerge as a leader in news related web sites for netizens. The site offers its subscribers up to the minute news briefs in the following areas: US news, international news, finance, entertainment/arts, sports and technology. Profits are generated through a classified ads section and from online advertisements by several vendors/sponsors. The company consists of a chief editor, assistant editor, five staff writers, a web

designer, a systems administrator, database manager and receptionist or secretary.

The design of the e-News news service LAN is one, which is made up of a server that supports proxy operation and a mail server. Microsoft Windows NT Server 4.0 is installed on the proxy server along with Microsoft Proxy Server 2.0. TCP/IP is properly configured. The proxy server is connected to the e-News network via a CAT 5 cable and a network interface card. The proxy server is connected to the Internet Service Provider via a DSL router (tied into a DSL modem). The DSL router is connected to the proxy server by way of a CAT 5 cable and a network interface card.

Essentially, a proxy server is "a World Wide Web server that acts as the sole web server for your clients and the rest of the Internet" [1]. The systems administrator maintains the proxy server and the network. The network is configured to allow for all e-News employees to be granted access control from their own individual computer systems. Access control is granted by properly configuring each authorized employee's system to allow the proxy server to function as its Internet gateway [1]. Each client on the network is equipped with the Microsoft Windows 98 operation system and the same application software including a licensed copy of Panda Antivirus for MS Proxy Server. All clients are tied into the network through CAT 5 cables. Each client is password protected as well.

Furthermore, each e-News employee also has access to a personal e-mail account. The e-News computer network possesses a corporate portal. "Corporate Portals allow access to internal corporate information such as documents from a variety of sources. They are very clearly a document management system, along with a content, or written word, management system" [2]. With a corporate portal, staff members are given the benefit of being able to utilize news production tools and then store the news stories and other documents/papers they have written directly onto the company's network. The writers or e-News editors can then retrieve these stories at any time and publish them onto the web site.

The physical location of e-News is within a corporate plaza in Long Island, New York. The e-News office suite is on the second floor. The proxy server, mail server, DSL modem and router are stored within a locked room of the office suite. Only the Chief editor, the Assistant Editor and the Systems Administrator has access to this room. Furthermore only the Chief and Assistant Editor have keys to the suite.

Poossible Threats: Network / Information Security

Fried's vision of being amongst the best in online news sites requires that the news provided be up to the minute and of the highest integrity. Providing breaking news is simple. There are a lot of reputable news sources including the Associated Press, Reuters and BBC that provide the latest updates on the top news stories. The integrity of the news e-News provides is the most challenging and important requirement. One does not have to worry about the news sources; these sources are liable for the information they distribute. What companies like e-News have to worry about is the integrity of the information that they distribute to their subscribers. It is the news editors'

duty to ensure the quality of their staff writers' work. It is the duty of the systems administrator to ensure that the staff writer's stories are secure on the company's internal network and public web site. In order to evaluate the security/integrity level of stories residing on the e-News network, it is necessary for the systems administrator to analyze the current network setup for possible vulnerabilities and threats that may exist.

Hackers

When something new comes about, people want to learn more about it. Hackers can be characterized as "people who enjoy using computers and exploring the information infrastructure and systems connected to it" [3]. In the beginning phases of operation, e-News will utilize different tactics in order to attract possible subscribers. Site information and keywords will be submitted to search engines to help get e-News positioned on the cyberspace map. Animated web banners will also be placed on popular search engines to help grab the attention of possible subscribers. Although these tactics will help draw netizens to the e-News web site, they may also attract hackers.

Hackers are individuals who generally want to learn how information systems work. They do not necessary intend to do anything malicious while exploring the information systems they come into contact with [3]. However, hackers "tend to gather and exploit tools that open holes to other attackers" [3]. If e-News attracts the attention of a hacker, the hacker's curiosity may cause him to want to find out a little more about the company. A Hacker may be interested in how the e-News network is designed and what security measures are in place for preventing outsider intrusion. Hackers may also want to study the network in order to determine possible vulnerabilities or security holes that exist with any of the security policies that are in effect.

Crackers

The threat posed by crackers is similar to that of hackers. However, there is some difference. Essentially, crackers are individuals who "maliciously break into information systems and intentionally cause harm in doing so" [3]. These individuals are usually not as skilled or knowledgeable as hackers are and their motivation lies in the fact that they want to cause their intended target a little bit of chaos [3]. Crackers are definitely a threat to the e-News network. Crackers may want to possibly exploit vulnerabilities within the e-News network. Furthermore, crackers may also utilize the tools they have access to in order to cause damage to the e-News network or web site in some way, shape or form [3].

Professional Thieves

Professional thieves are characterized as "people who make their living from stealing things" [3]. In life, people must always be aware of the threat that thieves pose. Throughout history, people have always found ways to steal from others. Thieves may steal things that are tangible; however, they may steal things that are intangible, such as ideas. Not

only does a company like e-News have to protect against thieves breaking in and stealing their office furniture, computer hardware and the like, e-News also has to safeguard the stories of its employees. A thieve may simply want to steal a copy of an article that a e-News staff writer had written that has not yet been published. Although, this type of situation may in reality, never actually happen, the threat is always there.

Maintenance People

Every office-building owner offers its clients some sort of maintenance crew option. This option may be included within the lease of the office space. However, sometimes this option is an extra charge. Maintenance people are "people who typically have access to physical locations in order to do routine maintenance tasks" [3]. Many individuals who lease office space usually prefer to hire a maintenance crew to tidy up the place once everyone leaves for the night. Does e-News utilize the services of a maintenance crew? If they do, are there any safeguards in place in order to prevent these maintenance people from getting onto the network or grabbing hard copies or e-News' sensitive data? Do employees leave their work or files on or near their desks in plain view? Are all the computers in the office turned off at the end of the business day? Furthermore, what type of rubbish is generated throughout the day by e-News employees and is it placed in trash receptacles? If computers are left on and hard copies of documents, files and stories are left out in plain view for all to see, most likely the maintenance crew who enters will see it. If the documents and such on employee's desks contain sensitive information and it is left for all to see, including the maintenance crew, then it is safe to assume that in this scenario maintenance people can be viewed as a threat.

Insiders

Sensitive information should never be in the wrong hands. Insiders could pose a serious threat to e-News. Insiders are characterized as "employees, board members, and other internal team members who have legitimate access to information and/or information technology" [3]. According to Raytheon, a global technology leader, "84 percent of network threats can be expected to come from inside an organization" [4]. Although, e-News is a relatively small company, its employees have access to stories that have not yet been published/released to the public. Can the employees of e-News be trusted with stories, articles or information that has not been fully released to the general public? Furthermore, imagine the threat insiders could pose if an employee of e-News left to work for another web based news service? This former employee can tell their new employer all about e-News' operations and computer network configuration.

There is always the question of what methods/tactics Fried utilized in building his work force. Did he just look at their skill sets and not their background? How much did he invest in looking into his employees past to verify previous employment and schooling? From a security standpoint, is it a good idea to allow all employees to have access to the e-News network? These are all good questions to consider when considering how serious a threat insiders are to e-News.

Crackers for Hire

Crackers for hire are usually individual recruited/hired by an individual or corporation to cause harm to another's computer system(s). The reward if and when they are successful is either by way of money or another form of payment. Such individuals pose a great threat to e-News. For example, let's say that another new web site wanted to intentionally harm e-News' computer network. Essentially, all a competitor would have to do is pay a cracker for hire to break into the e-News computer network to make a few harmful manipulations, which may cause e-News to shut down operations.

Extortionists

When the Internet is the primary medium in which you conduct business, it is extremely vital that your information is secure. If your not careful about this then let's just say that you can quickly see your way offline and out of business. Extortionists are "people who extort money or goods by threatening harm if not paid off" [3]. If they are skilled enough, have the proper resources and motivation, they can be a major threat. If for example, somebody accessed the e-News network and stole a few news stories written by e-News staff writers, then demanded money for their return, this can be viewed as extortion. Being that e-News, is in the business of journalism and the stories produced are vital to keeping the company up and running, it is important that e-News be aware of the threat extortionists pose.

Industrial Espionage Experts

It is safe to assume that the threat of industrial espionage experts on a small business such as e-News is very minimal. Industrial espionage experts are essentially, "people who specialize in harming companies to the benefit of other companies" [3]. Such individuals would rather target a large corporation that posses a more serious threat than a small, newly established company such as e-News. Industrial espionage experts would probably want to help Oracle spy on Microsoft. Unless e-News was to really become a success and attract enough attention to get noticed by the major competitors, who would in turn feel threatened and hire industrial espionage experts to "take care of some business for them", this threat is possible, but in reality unlikely.

Other Possible Threats:

Fraudsters

Fraudsters are characterized as "individuals who defraud others" [3]. These individuals can easily pose a threat to e-News through advertising on the e-News web site or through placing an ad in the e-News classifieds section. Fraudsters are usually motivated by greed in their desire to deceive others [3]. By placing an advertisement or classified ad on the e-News web site, these individuals have the potential to reach a large target audience. They can place ads, which look, appealing and legitimate. However, in reality, these ads are meant to deceive. If being tricked into believing and following up with

such ads victimizes subscribers or visitors of e-News, then e-News can possibly lose the subscriber as well as find itself liable. It is very important that e-News carefully chose their advertisers. They should properly screen potential advertisers and check the legitimacy of the opportunity or products being offered. Many fraudsters are making their way to cyberspace these days and e-News should be full aware of the threats they pose to the Internet community.

Competitors

Like any new company trying to get its feet on the ground, e-News will be faced with the challenge of providing a service that will be able to stand tall amongst its competitors. Competitors are characterized as "other individuals or companies in the same or similar businesses and who stand to gain from your loss or who can gain economic advantage by taking advantage of you" [3]. Companies in direct competition for subscribers to their news service will probably be intimidated by e-News venturing into cyberspace. Although this threat is minimal because the e-News has to establish a reputation and a large list of subscribers, competitors may still decide to come along and attempt to intimidate e-News. The tactics will be discussed in greater detail at a later point.

Vandals

Vandals are "people who damage things for the fun of it" [3]. These individuals pose no direct threat to e-News. However, if for example, an individual who possessed enough of a skill set wanted to deface the e-News web site or post unauthorized messages or the site, then from this stand point it is safe to say that vandals do pose some sort of a threat. Furthermore, if an e-News staff writer was to write a story on a sensitive subject that offended a vandal with the proper skill set to vandalize the e-News web site, this can be seen as a direct threat.

Activists

Activists are individuals who "believe in a cause to the point where they take action in order to forward their ends" [3]. It is quite possible that activists can pose a threat to e-News. In the journalism industry it is very easy to write something that either inspires its readers or offends them. If an e-News editor or staff writer publishes a story, which offends an individual or a group of people, activist can possibly join together to support or reject the staff writer's point of view. Therefore activists can bring both good and bad. Good, in that if many agree a writer's point of view, positive publicity for e-News can be generated. However, if many readers reject the writer's view, e-News may get a bad reputation and lose many subscribers. This is not a very serious threat, however, it should be viewed as a possible threat.

Possible Attacks on Vulnerabilities: Network /Information Security

Spoofing and Masquerading

The e-News computer network is vulnerable to many different forms of attack. The attack referred to as spoofing and masquerading refers to the creation of "false or misleading information in order to fool a person or system into granting access or information not normally available" [5]. A hacker who is interested in exploring the e-News network can attempt to spoof or masquerade his way in. Essentially, all a hacker would technically have to do is change the connection settings within his/her web browser (Microsoft Internet Explorer or Netscape Communicator) so the proxy address matched that of e-News. The hacker would automatically gain trust from the system and find his way into the e-News internal network and make all sorts of changes (including the content of news stories) and possibly even insert viruses or Trojan Horses into the network. This form of attack is viewed as very simplistic, clever and disturbing [6].

Data Diddling

Data diddling is a form of attack that involves the "modification of data through unauthorized means" [5]. From the standpoint of information security and integrity, this form of attack should be taken very seriously.

As stated previously, a hacker can easily gain access to the e-News network by masquerading and spoofing his way in. Once in, this hacker can engage in data diddling. For example, let's say an e-News staff writer had recently finished an article that was getting ready for its last stage of review by the chief or assistant editor. This article would most likely be stored on the e-News network in a location that allowed for the article to be easily retrieved by both the writer as well as the editor. If an intruder were to infiltrate the network, he would be able to access files on the e-News network. The intruder could possibly get a hold of this article as well as others on the network and manipulate the text or illustrations within the article. Furthermore, the intruder while he had access could even decide to make changes to the network configuration if his heart so desired.

Viruses

Computer viruses are continuously growing in number and complexity. Viruses are characterized as "programs that reproduce and possibly evolve" [5]. Viruses are usually transmitted through e-mail attachments or via computer programs. When considering the threats involved, viruses should definitely be considered a priority due to the amount of viruses that are continuously appearing on the Internet.

There are many ways that viruses can wind up on a system. Among the easiest of ways for someone to obtain a virus is by downloading a program or opening an e-mail attachment from an unreliable source. That's not to say that one should not be leery of trusted sources.

All employees of e-News have been granted access to both the Internet and e-mail. Viruses can be found in the following sources: "public domain software, bulletin boards, the Internet, computer club software, a friend or colleague's diskette, or commercial packages that have been tampered with" [7]. With e-News employees having access to the Internet and e-mail, the possibility of the network being infected with a

virus significantly increases. All an e-News employee really has to do is download a program from the Internet onto his/her computer, or simply open an attached file contained within an e-mail message. Its that simple!

Based on the current configuration of the e-News network, it was shown that an intruder could easily gain access to the system through masquerading or spoofing. Once in, an intruder can easily introduce a virus into the network. The reality is that, there are many ways in which viruses can be find their ways onto networks. What they do once they are active and inside the network is another story. Viruses can do all sorts of things. However, the scariest effect that viruses could have on a network is that they have the ability to self-replicate. If gone unnoticed, the virus could eventually cause all computer systems on the network to cease operation.

Trojan Horses

The Trojan Horse is a heavily weighed attack when considering the threats involved. Essentially, Trojan Horses are "unintended components or operations are placed in hardware, firmware, software, or wetware causing unintended and/or inappropriate behavior [5]. A majority of the Trojan Horses circulating today are either available for download via a web site or they arrive as executable attachments in the mailbox of an e-mail management program.

All employees at e-News have both Internet access and e-mail capabilities. Anyone who has ever surfed the Internet is well aware that there is an enormous amount/variety programs available for download. It is quite possible that employees of e-News may download programs of interest onto their computers in the office. How does one know if this program does what it says it will do? One cannot assume that all programs available on the Internet are safe and free from vulnerabilities. However, most people don't think twice when they click twice. If an employee of e-News were to download a program, which in fact contained a Trojan Horse, a lot of damage to the network could take place.

As stated previously, Trojan Horses can also arrive in e-mail messages. E-News employees are able to check both their company e-mail as well as personal web-mail accounts (i.e. Yahoo! and Hotmail). Many people open e-mail messages from people that they don't even know. Of course, we have all gotten our share of spam/junk e-mail. This type of e-mail is a nuisance, hence one of the reasons why we are so thankful our keyboards are equipped with a "delete" key. However, there are still people who are curious to read all the e-mail they receive. Unfortunately, these are the same category of people who download and execute all the e-mail attachments that appear in their e-mail messages. What these people don't realize is that their actions are very risky. It's no surprise why so many Trojan Horse programs are still infecting millions of computer systems.

Once a Trojan Horse infects a person, many unusual things can start to occur on that individual's computer system.

Some of the most common symptoms of a Trojan Horse infection include:

1. The CD-Rom drawer mysteriously opens and closes.

2. The computer screen flips upside down or inverts

3. Microsoft wallpaper or background settings change by themselves.

4. Documents or messages print to a printer by themselves.

5. Internet web browser goes to an unfamiliar web site.

6. Microsoft Windows color settings change by themselves.

7. Microsoft Windows screen saver settings change by themselves.

8. Mouse buttons reverse functions.

9. Mouse pointer disappears.

10. Mouse moves by itself.

Trojan Horses can also do damage to by way of deleting essential system files or changing user names or passwords within system programs [8].

From a security standpoint, the insertion of a Trojan Horse program into the e-News network could be devastating. A Trojan Horse could have the potential to make all sorts of changes to the network configuration. Furthermore, Trojan Horse programs are now becoming even more sophisticated. For example, a Trojan Horse SubSeven, allows for its users to gain remote access an intended target's computer system [9]. If e-News loses control of its own network, then the integrity of all the data stored within the network could be compromised.

Modification / Observation in Transit

Imagine what could/would happen if an intruder was able to access the e-News network. The attack known as spoofing and masquerading clearly illustrates how easy one could infiltrate the network. Once access to the network is gained, one could easily modify or observe data in transit across the network.

One engages in "modification of information in transit so as to modify communications as desired" [5]. On the other hand, "observation in transit refers to "the examination of information in transit" [5]. Both of these attacks should be great concern to e-News.

If an intruder can easily gain access to the e-News network, then this individual can just as easily observe and or modify data that in transit across the network. If such attacks were to occur, an individual can gain access to and manipulate all sorts of data; including news stories and other important documents and such. This can have a significant impact on e-News.

Shoulder Surfing

Have you ever had someone glance over your shoulder while you were diligently typing/starring away at your computer? Most people who

utilize computers outside the comfort of their own houses often find that they have an audience near by. Shoulder surfing involves "watching over peoples' shoulders as they use information or information systems" [5]. Although, this may seem like a minimal concern, when dealing with sensitive information and maintaining the integrity of data, this issue could be of great concern.

This type of attack can be applied to e-News in several ways. Let's say that for example that one staff writer is curious to see what another staff writer is typing into his computer system. However, the staff writer who is doing the typing does not want the other staff member to see what he is doing. The technique/attack known as shoulder surfing could be utilized to help the curious writer grab a quick peek. Essentially, all this curious individual would have to do is gain a strategic position over the secretive writer and either glance at the individual's keystrokes or computer monitor and attempt to interpret what is being typed.

Another example in which shoulder surfing could be utilized within the e-News office would be if someone wanted to gain unauthorized access to a co-worker's system. Essentially, the curious employee would have to strategically place himself/herself in a position where he/she could easily see the targeted co-worker's keystrokes when entering the password needed to access the computer system. The curious individual may want to gain access to the computer of a co-worker of equal or higher status. If the intended target is someone of higher status - then the curious employee may want to see some of the files on the chief or assistant editor's computer; maybe there are some e-mails that this curious employee wants to see; maybe there is a story that the chief or co-editor is reviewing that the curious employee wants to read or manipulate.

Password Guessing

Much of our sensitive or confidential data is protected by passwords. However, passwords can often be broken – by a fairly simple method known as password guessing. Essentially, password guessing occurs when "sequences of passwords are tried against a system or password repository in order to find a valid authentication". If an intruder wanted to somehow break into the e-News network - sure enough, if the network was password protected - the first thing the intruder would do is guess.

It's sad to note, but "users frequently chose very predictable passwords: their names, addresses, birth dates, phone numbers or Social Security numbers; the names of their family members, friends or pets; the names of favorite artists, authors or sports figures. Therefore, many hackers simply guess a few dozen of the most common password choices; all too often, they hit a match" [10].

So, the question becomes, what can an intruder do once a password is obtained? "If someone guesses or steals your password, he or she will have access to your files, your e-mail, your computing funds, your personal information and more. The intruder will be able to modify or delete your files, send e-mail threats in your name, or subscribe to unwanted services for which you may have to pay. A knowledgeable intruder also can use your account as a stepping stone to gain access

to other accounts and systems, increasing the likelihood that they will do further damage" [10].

From the standpoint of e-news, an attack such as password guessing should be of minimal concern. There are so many ways in which someone can actually obtain a password without even having to guess at it. Many programs are available on the markets that help one to reveal all the passwords for every machine residing on a LAN.

It is known that each of the e-News staff writers have passwords associated with their computer. Some of the files, documents, news articles and such on their computers may be confidential. If password guessing is attempted on these machines, it is quite possible that the password can be "guessed" without the use of any other tools other than the intruder's intuition and logic. If in fact, a password can be revealed this easily, than the integrity of the data stored on those machines, as well as the network needs to be questioned. Furthermore, who knows what methodology the systems administrator used in helping to determine a password for the e-News server? Can it be easily guessed?

Distributed Denial of Service Attack

There are many ways in which an intruder can gain access to a network. All one essentially has to do is seek out the vulnerabilities within the network's infrastructure and be able to exploit them. A Distributed Coordinated Attack (DCA) is a form of attack that allows one to fully exploit systems tied into a network. Essentially, DCAs occur when "a set of attackers use a set of vulnerable intermediary systems to attack a set of victims" [5].

This type of attack is of minimal concern. However, the possibility of such an attack being implemented with the utilization of e-News' network is not impossible and therefore, should not be overlooked.

If the attack of masquerading and spoofing has allowed one to easily infiltrate the e-News network, then one could easily utilize the systems on the network to perform a DCA. Essentially, all one has to do is install a Trojan Horse program such as SubSeven onto one of the networked computers. Once such a program is installed, the intruder can gain access/control to/of the e-News network at any time. When the intruder has gained access/control to/of a large number of computers, then the intruder can launch a DCA. DCAs have the potential to cause a denial of service.

“In a denial of service attack, the user sends several authentication requests to the server, filling it up. All requests have false return addresses, so the server can't find the user when it tries to send the authentication approval. The server waits, sometimes more than a minute, before closing the connection. When it does close the connection, the attacker sends a new batch of forged requests, and the process begins again – tying up the service indefinitely" [11].

Other Possible Attacks Based On e-News Vulnerabilities:

Dumpster Diving

Do you ever wonder what happens to all the trash you generate? It winds up in a landfill or recycling plant somewhere; right? Actually, not all of what you throw away makes it to these sites or facilities. Some of what you throw away may actually come into the hands of an individual known as a "dumpster diver". Dumpster diving, is an activity in which "waste product is examined to find information that might be helpful to the attacker" [5].

Dumpster diving is a form of attack that e-News staff members should be aware of. E-news is very vulnerable to this type of attack.

Dumpster diving should be of great concern due to the fact that some of the documents and stories produced by e-News staff writers might not have been released to the public. For example, what if a e-News staff member threw away a draft copy of a story that was going to be published on the web site in the next few weeks? If this draft copy winds up in a dumpster, it may be found by one who is willing to dive in to get it.

Furthermore, if hard copies of data, such as registered subscriber lists are thrown away, a dumpster diver could potentially grab a hold of this information and possibly use it to commit fraud or another illegal act. Imagine what could happen if a competitor gets his or her nose dirty sifting through the e-News dumpster and discovers a subscriber list; the results could be devastating.

"Increasingly, criminals are winning at the dumpster simply by obtaining personal information such as credit card numbers, social security numbers, signatures and bank statements from garbage cans across the nation. The government can't stop them; the U.S. Supreme Court, in effect overturning the 1974 Privacy Act, stated that garbage left at a curb for pick-up is public domain and subject to inspection and seizure by anyone. This 'anyone' could include criminals and corporate competitors" [12].

Get a Job / Fictitious People

The attack referred to, as "Get a Job" is quite interesting. As its name clearly suggests, occurs when "an attacker gets a job in order to gain insider access to a facility" [5]. Although this attack is not regarded as the most serious, in the case of a small company suchas e-News it should cause some concern.

Let's say for example, a competitor such as Yahoo! News wants to find out some information about e-News; wouldn't it be clever for Yahoo! to have one of their own join the ranks of e-News? Well, this thought can become a reality. Essentially, Yahoo! could hire an individual to apply for a job at e-News. The person hired by Yahoo! To apply for a position within e-News, may in fact be so inclined as to use his or her real name; however, this individual may also fact decide to assume a fake identity. The utilization of a fake identity to try and get a job within e-News can be viewed as an attack. This attack, referred to as "fictitious people" occurs when "impersonations or false identities are used to bypass controls, manage perception, or create conditions amenable to attack" [5]. If in fact, this "fictitious" individual does get offered a job and accepts, e-News is in for a little bit of trouble. This person, once in the door, can serve as a spy for Yahoo!.

This spy could leak secrets about e-News back to Yahoo! Furthermore, this individual could tamper with data on the e-News network. Many possible consequences can occur.

Defense! Defense!

Now that we have ripped everything about e-News' network apart, let's try to put it back together - in working order. In order, to do so, it is imperative that some of the best defenses - suitable for the situation at hand to be implemented. It's not a good idea to leave a network in such a vulnerable state. Based on the vulnerabilities that are known to exist, many new defense mechanisms will be introduced into the e-News environment.

The following defenses were selected based on the scenario at hand:

Behind Door #1: Alarm

First things first; e-News must realize that security begins with the front door. It is very important that e-News protect itself from outside intrusion. One of the ways to help deter people from entering into areas in which they are unauthorized is to simply install alarms. Alarms are essentially "used to indicate detected intrusions [13]". With regard to the e-News' physical location, it is absolutely essential, especially when dealing with sensitive information, to invest in something a little more than a lock on a door. If an intruder has the desire to get past the lock on the front door he/she will. Let's not forget, doors can be kicked or preyed open utilizing only a minimal amount of force. Having an alarm installed within the e-News' office suite, the intruder may be surprised to find something behind door #1 - a nice piercing sound and possibly the scare of a lifetime.

With regard to detecting an intrusion, software programs are available both on the Internet for download as well as on store shelves, that alerts a systems administrator when someone is attempting to infiltrate a network. Due to the sensitivity of the data on the e-News network, such software should be installed onto the network.

Behind Door #2: Firewall

If one were to legally enter the e-News office suite, they would find a room filled with a network of computers. These computers, as we are well aware, are all on the Internet. It is quite obvious that the Internet can be a very scary place. So, to prevent any of the bad stuff from coming into the e-News-networked environment, it would seem effective/ logical to install a firewall at the network's entry point. Essentially, "a firewall is the first program or process that receives and handles incoming network traffic, and it is the last to handle outgoing traffic. A firewall must be positioned to control all incoming and outgoing traffic. If some other program has that control, there is no firewall" [14].

Filtering Devices

Packet (an amount of data) filtering can also serve as an effective form of defense from harmful data that may come across the e-News

network. "Filtering consists of examining incoming or outgoing packets and allowing or disallowing their transmission or acceptance on the basis of a set of configurable rules, called policies" [14].

Packet filtering policies may be based upon any of the following:

· Allowing or disallowing packets on the basis of the source IP address

· Allowing or disallowing packets on the basis of their destination port

· Allowing or disallowing packets according to protocol [14].

Packet filtering can be utilized within the e-News network to filter incoming and outgoing e-mail. Each e-News employee is issued an e-mail account. Attachments can be sent along with e-mail addresses. To prevent any unwanted e-mail or attachments within, the systems administrator can utilize a packet filter to accept or refuse the data.

Feed False Information: Let's Install a Honeypot

So, let's say someone still tries to get in or still wants to get in! A clever way to detect if someone is attempting to infiltrate a network is to "catch him or her in the act". Honeypots help to do just that. Essentially, "a 'honeypot' refers to a computer designed to look like an unprotected machine with which to trap unsuspecting hackers. The honeypot can do several things. It can sufficiently distract someone who plans to cause damage to other systems on your Network. It also tracks hacking attempts and alerts the appropriate persons in your company that a hack or unwelcome intrusion is in progress" [15]. Honey pots could definitely deter hackers who may want to infiltrate the e-News network. Although such computers may be somewhat costly, in the case of e-News, it is imperative that the integrity of the data on their network is not compromised. Therefore, a honey pot, (alongside an intrusion detection software program) may be worth the investment.

Encryption

As stated previously, it is imperative that the integrity of the data on e-News' network remains intact. One way to effectively prevent the data on the network from being compromised is through the utilization of encryption. When encryption is utilized "information is transformed into a form which obscures the content so that the attacker has difficulty understanding it" [13]. If the intruder cannot interpret it, there is no sense trying to steal it! The e-News system administrator should chose the data resident on the network that is most sensitive and using his judgment, with the help of the Chief and Assistant editors, decide what data is a candidate for encryption and what data is not.

Hard to Guess Passwords

Although passwords are in place throughout the e-News network, how do we know these passwords are adequate? Therefore, it is important to ensure that all employees know how to chose an effective password - one that is not able to be easily guessed.

Passwords should:

· have a mixture of uppercase and lowercase letters and numbers

· be easy to remember, but difficult to guess

· be at least 8 characters in length be changed at least once every 60 days

You should not use passwords that consist of:

· any permutation of your name

· any personal details about yourself, such as the registration number of your car, your spouse's name or your children's names

· jargon associated with any profession or trade

· famous names or places

· birth dates

· taxfile or bank account numbers

· credit card or Medicare card numbers

· simple keyboard patterns such as qwerty or aabbccdd

· proper nouns

· old passwords

· digit substitution of letters on correctly spelled words [16].

Known Attack Scanning

Computer viruses and Trojan Horses are critters that can be a nuisance. Many computer viruses and Trojan Horse programs can be dangerous. In order to try and protect any viruses from infecting the e-News system, known attack scanning software is used. Although, the proxy server has Panda Antivirus for MS Proxy Server installed, it is important to have an alternative Antivirus software program on the system. Furthermore, in order to make sure all the client systems are protected, licensed copies of Norton Antivirus 2002 will be installed onto each of these systems. A daily scan for viruses will be performed. Furthermore, a periodic full scan of each system's hard-drive a will be conducted as well. It is imperative that anti-virus software be constantly updated. Therefore, an up to date scan engine as well as the latest virus definitions will be sought frequently from the vendor.

Fight Waste Examination: Waste Data Destruction

People hardly wonder about what happens to the trash they generate. In the case of e-News, hard copies of sensitive material/document

have to be made on occasion. So, the question becomes, how can one destroy that material/document. The most effective and logical way to do so is by way of a paper shredder. "Shredding makes your personal information unavailable for the taking" [12]. According to William Britt, chief of the C.I.D of the I.R.S.'s Atlanta, Georgia office suggests "the shredding of all documents prior to disposal. Crumple something up, tear it in half, and dumpster divers will gladly put it back together. Shred it, and it is gone for good" [12].

Good Hiring Practices / Background Checks

In order to maintain the integrity of the data residing on the e-News network, a level of trust must be established between the upper management and their staff members. Companies such as e-News require the right type of people - with the right type of attitude and outlook. Sometimes people seeking employment have ulterior motives. In order to ensure that the e-News workforce is made up of the right people - background checks and reference checks will be required and requested by each applicant.

Other Defense Mechanisms:

Digital Signatures

Many analysts in the computer security industry are discussing the effectiveness of digital signatures. Digital signatures, "which are based on a technology that makes a signature invalid if the content is changed after it is sent" may be effective for e-News [17]. However, many people argue that digital signatures are costly and add to the complexity of a network.

Summary, Conclusions, and Further Work

In an ideal world everything would be simple to understand. We must all realize that there can be many answers to the same question. It's all a matter of interpretation. Many threats and vulnerabilities exist. Furthermore, there will always be attacks that are formulated to exploit known/hidden vulnerabilities within a system. Ultimately, one must rationalize a set of defense mechanisms to counter these threats and attacks. There is only one problem. Sometimes it's hard to identify all the risks, threats and vulnerabilities associated with a specific system. Again, it's all just a matter of interpretation. Based on how one analyzes and evaluates a given set of threats will determine how that individual goes about predicting possible threats and establishing some sort of defense mechanism. There is no set way to go about doing this. Conclusions can be drawn, based on trial and error, evaluation, analysis and interpretation.

Hopefully by now, it has become obvious that not every threat, attack and defense can be predicted. "Absolute security is an unrealistic goal. A natural disaster or an adversary with sufficient resources and ingenuity is enough to compromise even the most secure systems. The optimum security system balances the cost of implementing protective mechanisms with the reduction in risk achieved" [7].

References

[1]. Internet Access Control Using Proxy Servers:
http://www.cedpa-k12.org/databus-issues/v36n1/proxy.html

[2]. What is a Portal?
http://www.shavlik.com/whatIsPortal.asp

[3]. The All.Net Security Database: Threat Cross Reference
http://fc@all.net/

[4]. Benner, Jeffrey. "Nailing the Company Spies".
Wired.com: March 1, 2001.
http://www.wired.com/news/business/0,1367,41968,00.html

[5]. The All.Net New Security Database: Attack Cross Reference
http://fc@all.net/

[6]. Strom, David. "Time to Secure Your Web Site".
ITWorld.com: Oct. 3, 2001.
http://www.idg.net/english/crd_in_712045.html

[7]. Latest Scams and Alerts from RCMP Economic Crime Branch
http://www.rcmp-grc.gc.ca/scams/ccprev.htm

[8]. A List of Trojan Infection Symptoms
http://www.lockdowncorp.com/trojansymptoms.html

[9]. Trojan Horse Demo
http://www.lockdowncorp.com/trojandemo.html

[10]. Hofer, Theresa. "Passwords Being Tested for Vulnerability".
http://www.umich.edu/~urecord/9798/Jan14_98/pass.htm

[11]. "How A 'Denial of Service Attack' Works. Feb. 3, 2000.
http://news.cnet.com/news/0-1007-200-1546362.html

[12]. "Protect Against 'Dumpster Diving' With Shredder
http://www.b4-u-buy.com/09c4700.htm

[13]. The All.Net New Security Database: Detection Cross Reference
http://fc@all.net/

[14]. What is a Firewall?
http://www.nwinternet.com/~pchelp/security/firewalls.htm

[15]. Nutter, Ron. "Intrusion Detection Software and Honeypots".
http://www.nwfusion.com/columnists/2001/1105helpdesk.html

[16]. How Can I Create An Effective Password?
http://www.scg.qut.edu.au/passwords/effectivepass.shtml

[17]. Bergstein, Brian. "Hacker Changes Yahoo Articles".
The AP: Sept. 24, 2001.
http://www.canoe.ca/CNEWSTechNews0109/24_yahoo-ap.html

About the Author

Robert Fried holds a B.S. and an M.S. in Forensic Science with a concentration in Advanced Investigation. He also holds Certificates in Law Enforcement Science, Forensic Computer Investigation, and Information Protection and Security from the University of New Haven and SEARCH. Fried has extensive knowledge of forensic science, however, most recently he has worked extensively in the developing field of "digital forensics" and has published in this area by organizations such as the SANS Institute. He is also a member of the NorthEast chapter of the High Technology Crime Investigation Association (HTCIA).