Red Team Report

Hemavathy Alaganandam
Parvez Anandam
Jameel Alsalam
Yi-Kai Liu
Pravin Mittal
Elena Rodriguez-Vieitez
Santeri Voutilainen

University of Washington CSE P 590TU
UC Berkeley PP 190/290-009
UCSD CSE 291 (C00)

Christine Hartmann-Siantar
Professor Ed Lazowska
Stephen Maurer
Professor Stefan Savage
Professor Geoffrey Voelker

October 24, 2005

Table of Contents

Division of Labor

Section 1: Attacks Mounted
Elena Rodriguez-Vieitez
with technical consult by **Parvez Anandam and Santeri Voutilainen**
Section 2: Damage Estimates to Home, Corporate and Financial Systems
Parvez Anandam and Jameel Alsalam
Section 3: Feasibility and Strategic Value of Attack Technique to Terrorists
3.1 Cyber Attacks on Critical Infrastructure Scalability and strategic value: **Pravin Mittal**
3.2 Resources Needed to Execute a Cyber Attack: **Yi-Kai Liu**
3.3 Other Use of Cyber Attacks: **Yi-Kai Liu**
3.4 Conlusions, and the future of Cyber Security: **Pravin Mittal**
Section 4: Feasibility and Cost of Defenses for Home, Corporate and Financial Systems
Home & Corporate: **Hemavathy Alaganandam**
Financial: **Santeri Voutilainen**

1 Attacks Mounted

1.1 Description

The simulation involved three attacks to a target computer at UC San Diego. The three attacks exploited the buffer overflow vulnerability that allowed the attacker to gain root privilege on the machine. We will also refer later to other attack techniques such as worms, botnets, etc. A “buffer overflow” is an anomalous situation where a program writes data beyond the allocated end of a buffer (portion of memory where data is stored). Buffer overflows arise usually as a consequence of a bug (error in a computer program that causes the program not to work as intended). Particular kinds of bugs lead to security problems, for example a buffer overflow bug may allow a malicious user to execute other programs that are normally not allowed to run.

One consequence of the overflow is that valid data can be overwritten. Buffer overflows are a commonly exploited computer security risk. A program which takes advantage of a vulnerability to compromise another program's security is called an "exploit". A buffer overflow exploits work by feeding the program special input content that is designed to overflow the allocated data storage buffer and change the data that follows the buffer in memory. This has usually serious consequences, since program control data often sits in the memory areas next to data buffers.

Properly written programs should check the length of input data, to ensure that it is not larger than the allocated data buffer, but this is frequently overlooked, especially by inexperienced programmers.

The three exploit codes used against the UC San Diego computer are named splot1.c, sploit2.c and sploit4.c

Sploit 1 is a basic buffer overflow. The target copies a buffer of essentially unlimited size into a limited size buffer thus causing the overflow. The sploit code uses this to cause the return address, which is essentially a bookmark that indicates where the program came to this point, to be overwritten. With the return address overwritten the program is misdirected when back tracking to its original starting point and instead executes the attacker’s code.

Sploit 4 is similar to Sploit 1 in that it can overwrite an arbitrarily large section of memory. What makes this different from sploit 1 is that the target program actually attempts to limit the size of data it copies from the attacker. However, because it stores the size of the attacker’s data in a space that does not fit the full number, the size is truncated. When checking the size of the data to copy the program thus inadvertently compares the wrong values. It further compounds the problem by then using the actual size when copying the data to memory rather than the truncated value. These two programming errors allow too much data being copied to memory resulting in a buffer overflow.

Sploit 2 is more complex than 1 or 4 and is best explained using a travel analogy. Mr. X goes on a trip to visit multiple cities. In every city he keeps notes about the city. Whenever he arrives in a city he writes down the city he came from and the page number where he has the notes for that city. Once he reaches the final city he traces back his steps in reverse order. He looks at the notes for the current city to remember which city he came. He also finds the page number for that cities notes. He returns to that city and flips to that page in his notes. If anyone replaced any of the page number associated with a previous city’s notes, then Mr. X would return to the city correctly but refer to the wrong set of notes. He would refer to those wrong notes to decide which city to return to next. A malicious attacker could replace such a page number with a page that the attacker inserted into Mr. X’s notebook and thus cause him to go astray on this return journey.

1.2 Estimated Difficulty

Buffer overflows are most easily exploited when the data buffer is in the program's function stack, since this can lead directly to an alteration of the program's execution path. Determining the exploitability of a buffer overflow vulnerability can be difficult, even for experience programmers, since it involves a lot of high and low level knowledge of the architecture internals and target program. Overflows of as little as a single byte beyond the end of the buffer have proven exploitable. Of course, it is easier to exploit buffer overflows with access to the source code to the target program as this reduces the need for some trial and error.

1.3 Cost and feasibility of defenses

To defend against future attacks, it is necessary to write more robust programs that don’t contain bugs. The computer software industry has put a great deal of effort into finding methods for preventing programmers from inadvertently introducing bugs while writing software, for example:

- Programming techniques: Since bugs often create inconsistencies in the internal data of a running program, programs can be written to check the consistency of their own internal data while running. If an

inconsistency is found, the program is halted so that the bug can be located and fixed. Techniques such as address space layout randomization can make any remaining buffer overflows harder to exploit.

- Various techniques have been used to make buffer overflows less likely, such as the "intrusion-detection software". Also useful is the "application firewall" which limits access to software and resources on the computer thus limiting the number of places where an attacker can find buffer overflows.
- Hardware improvements such as no-execute (NX) memory regions can cripple buffer overflow attacks by not allowing the attack code to be executed because it is in a memory region not legal for commands.

1.4 Recommended Policy Responses

It is important to point out those actions that would make the IT systems more resistant to cyber-attacks. This is important to prevent future attacks, since one of the techniques used by the terrorists is so-called "incremental terrorism" where relatively local attacks (like the ones described in this exercise) on banks, small businesses, hospitals, local government offices, etc., are repeated often so that the public confidence is undermined and significant economical and psychological disruption results. Using a similar analysis as that provided by the National Academies[i], a series of short-term actions appropriate for this relatively small-scale attack would be related to improving information and network security in public and private organizations, in particular:

- For users (home, small businesses): Have good updated information-security tools
- For larger corporations: Have good information-security tools and have unannounced red-team attack simulations of the IT systems, promptly fix problems and vulnerabilities, mandate use of strong authentication mechanisms, defense-in-depth in addition to perimeter defense

As for long-term recommendations: Increase overall robustness of the computer systems. This would be useful not only for relatively small-scale attacks like the one we are dealing with in this red-team exercise, but also for larger-scale attacks were cyber-attacks are combined with other physical operations. Invest in better:

- Authentication: Better ways of preventing unauthorized parties to access a computer and cause harm
- Detection of intruders
- Containment, so that the attack is of limited scope
- Recovery, which involves backup and decontamination
- Install fixes to take care of buggy codes. Better administration needed.

2 Damage Estimates to Home, Corporate and Financial Systems

The economic damage caused by an attacker who gains administrative access to a computer can be classified into four categories: 1) damage to the software and hardware of the computer, 2) theft or destruction of information stored on the computer, 3) leverage of other computers' trust in the compromised one, 4) impersonation of the computer's user to cause social harm.

It is useful to prepare for worst case scenarios, even though they are unlikely to actually occur, since they demand a series of fortuitous events. Worst case scenarios typically involve attackers who seek to maximize economic disruption to all parties rather than to directly profit from it.

Private home computers usually do not have a lot of valuable information stored, and no special access to external resources beyond what could be reached from any internet-connected computer. There are two caveats: that this computer is not used to store work related information and that this computer does not have access to a corporation through a virtual private network. The typical damage done by a brute-force attack is limited in magnitude to the value of the hardware and software, around $3,000 maximum. The information on the computer that is monetarily valuable is limited to the identity of the computer's user and to data on the user's bank, credit and brokerage accounts. Reaping such information is not guaranteed to the attacker, since the user would have to be computer savvy enough to store it electronically but not so sophisticated as to protect it with a password. Running keystroke loggers and screen scrapers would allow the attacker to capture account information in real time but this is a fairly inefficient way to conduct identity theft. Instead, phishing scams can be carried out quickly on a mass scale and allow this information to be organized without any human intervention. The "market rate" for a stolen identity record is $10 to $60[ii] but the damage to all parties concerned is clearly much greater. The realistic worst case damage occurs when the attacker gets a complete set of bank, credit card and brokerage account information for the user and goes on a shopping binge, either for themselves or to just spend the money. That worst case damage clearly depends on the finances of the owner of the computer but around $20,000 in liquid, readily-accessible assets seems reasonable.

It is equally interesting to consider the compromised private home computer not as a single isolated entity but as one of the bots in a botnet. Botnets are largely responsible for covert, spam, phishing and denial of service attacks. The economic damage due to this type of attacks was estimated[iii] at around $300 billion for 2004. An estimate of the number of computers worldwide that are part of a botnet is speculative at best. Let us assume that it is 10% of all broadband-connected computers. The number of broadband lines was about 150 million in 2004[iv]; this gives us a crude estimate of about 15 million computers within botnets (or a thousand-odd useful-sized botnets). This means that each botnet computer is responsible for $20,000 in damages on average. Assuming that the economic damage grows faster than the number of needed botnet computers (e.g. because of society's greater reliance on the Internet on one side and the increase in broadband speeds on the other), the damage per compromised computer will continue to rise into the tens of thousands of dollars, unless some strong counter-balancing forces are applied in the coming years. Therefore, the damage caused by a compromised private computer is in many cases greater to society as a whole than directly to the individual in possession of the computer.

A word-processing computer used by the high-level Walmart VP is unlikely to have direct access to any Walmart operations control, but probably does contain time-sensitive information and have access to the company network. The information could be exploited in many ways. First, if it were published, it would have serious public relations implications for Walmart. Second, if files are deleted, an attacker could hinder important negotiations; for example, emails from contacts overseas could be selectively deleted without revealing that the computer has been compromised. Third, if the attack were a case of corporate espionage by a Walmart competitor, that competitor could use the tactical information to buy similar goods or ink deals with suppliers before Walmart does. Fourth, if the attacker is one of Walmart's suppliers, that supplier may find out the price Walmart is willing to go to and hold out on the negotiations with Walmart till that price point is reached. In addition to stealing information, the ability to impersonate the VP allows an attacker who is trying to obtain specific information to request it from other Walmart employees; that ability could also be used to misrepresent Walmart to outsiders. The greatest financial damage arises when the attacker uses the information to affect Walmart's sales for the quarter, even by a tiny fraction. Competitors and vendors are the most likely candidates to cause a dip in revenue. A 0.1% change in Walmart's quarterly revenue[v] is about $75 million; this is a reasonable worst case damage.

A computer on the trading floor of Schwab is most valuable for its ability to manipulate clients' funds - to buy and sell stock with no controls outside of the trader sitting at his computer, although sign-offs by several individuals may be necessary for large trades. With such a computer, there could well be many other identity safeguards that would ensure that root access to an individual terminal would be insufficient to obtain the ability to conduct trades - a strong authentication token specific to the trader is likely to be necessary. If the attacker is able to bypass such checks (e.g. using a real-time keystroke logger), the compromise of a computer with this level of control over external resources during trading hours would have a large economic impact on Schwab and possibly provide large financial opportunities to the attacker. If a good amount of clients' money is either stolen or misused in the markets, or even immobilized during an important shift in the markets, then customer confidence could be severely shaken. Furthermore, if Charles Schwab attempts to "take back" any trades executed from the compromised computer, the New York and the NASDAQ Stock Exchanges' trust in Schwab comes into question. Trust by customers and trust by the exchanges are the entire foundation of Schwab's business. If 10% of Schwab's customers get jittery by the apparent lack of security at the company and pulled their money out within the year, Schwab's annual revenue[vi] would suffer by $400,000 million. If fear spreads to customers of other brokerage firms, and they pulled out some of their money to stash it into safer investments such as FDIC-insured CDs, that could cost the brokerage industry a few billion dollars.

3 Feasibility and Strategic Value of Attack Technique to Terrorists

We examine cyberattacks from the perspective of a terrorist organization. Section 3.1 argues that cyberattacks on critical infrastructure are unlikely to cause major damage, and thus have limited strategic value to terrorists. Section 3.2 gives some estimates of the resources needed to carry out different kinds of cyberattacks. Section 3.3 discusses some other possible uses of cyberattacks; section 3.4 concludes and discusses the future of cybersecurity.

3.1 Cyber attacks on critical infrastructure – scalability and strategic value

Before we delve into whether cyberspace can be used as a strategic weapon for terrorism, we will try to get a precise semantic meaning of the word “Cyber terrorism.” The most widely accepted and unambiguous definition was put forward by Dorothy Denning, a professor of Computer Science, on the subject before the House Armed Services Committee in May 2001, which states: “Cyber terrorism refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or

its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not."[vii]

We should now look from the perspective of a military strategist to define what is the threshold of damage from cyber-attacks will help them to achieve their aforementioned goals, given that hundreds of systems which provide critical infrastructure routinely fail without paralyzing or affecting the public psyche.[viii] So it is reasonable to think from a strategic military level for terrorist to make political statement or to inflict psychological damage that the scale of cyber-attacks should go beyond routine disruptions.

Many analysts[ix] believe a cyber-terrorist may hack into the water supply infrastructure, take control of dams and floodgates to use them to cause widespread havoc in terms of life and property. This is not an easy task given that United States has 54,064 separate water systems serving an uneven spread of the population[x]. Most of them run on a diverse set of network technologies making it even harder for the terrorists. Also, many of these supplies get routinely disrupted without causing terror or paralysis, as a lot of redundancy is built into these systems[xi]. So a terrorist will need to simultaneously disrupt hundreds of these for a longer period of time to be of any strategic value.

Similarly, the U.S. electrical power grid consists of 3,000 electrical power providers, private and public, using a variety of different technologies to operate them. To effectively undermine them it will need vast group of hackers and identify different vulnerabilities as it is a heterogeneous system which is a very difficult task. This is supported by congressional testimonies by NERC[xii] and an independent study on risk assessment done by Task force of National Security Telecommunications Advisory Committee[xiii].

Another cyber-threat scenario which has been bought forward by many analysts[xiv] is hackers taking control of air traffic systems and aircraft. This is not feasible as aircraft are not controlled by remote computer systems. Again, the Federal Aviation Authority does not solely depend on computer networks to control air-traffic or its communications. Now given the context that it is normal for 15000-20000 flights to be delayed or cancelled every month, small intrusions if occurs will provide no strategic incentive for terrorists.

Although the Internet infrastructure has a few points of failure, internet protocols like packet switching allows rerouting of communications even if some nodes on the network are eliminated. This war-game dubbed "Digital Pearl Harbor," sponsored by U.S. Naval War College in July 2002, was carried out by well-known government hackers and security analysts. The hackers failed to crash the internet. Officials concluded that such an attack would require a vast amount of resources including $200 million and would need at least five years of preparation. This is quite an evidence of the limited likelihood of any successful cyber-attacks by terrorists on internet infrastructure.

3.2 Resources needed to execute a cyber attack

A cyber attack requires substantial technical skills, but only modest financial resources. Computer security is a rapidly changing field--attacks and defenses are becoming more sophisticated, and a software vulnerability can be discovered, exploited and patched all within a span of one year[xv] [xvi]. As a result, attackers must work to "stay current" with new vulnerabilities and defenses. Financial resources, on the other hand, can be quite modest--desktop PCs are becoming commodity products, and high-speed internet access is fairly common. Human labor (i.e., programming the attack) is probably the most "expensive" component.

Here we analyze two main possibilities: large-scale attacks on unprotected home PCs, and specialized attacks on well-defended corporate and government systems.

First, we consider attacks on low-end targets, such as home PCs with well-known vulnerabilities and no defenses. Each individual PC is not very valuable, so the emphasis of this attack is on massive scalability using automated attack tools. The usual approach is to spread a worm or Trojan horse, or assemble a botnet and use it to do a distributed denial-of-service (DDoS) attack. For example, the Code Red worm infected more than 250,000 hosts within 9 hours on July 19, 2001.[xvii] There are also anecdotal reports of botnets with 50,000 machines.[xviii] Botnets may be especially attractive to an attacker, since they are multipurpose tools that can do anything from DDoS attacks to sending spam [xix].

The technical requirements of this attack are fairly low, since it makes use of already-known vulnerabilities. Documentation, exploit code and network scanners are all freely available (tools such as Nmap are dual-use, having legitimate uses in "red team" penetration testing). More overtly malicious tools, like worms and DoS agents, can be obtained with moderate effort; this may be inferred from the fact that "script kiddies" with limited technical ability have been implicated for releasing worms into the wild, as well as a significant fraction of DoS attacks[xx] [xxi]. We estimate that an attack of this kind could be carried out by 5 moderately skilled programmers in a few weeks.

Alternatively, the whole operation might be outsourced to a criminal organization. Judging from the costs of recent "cyber-extortion" cases, we estimate that such a job might cost a few hundred thousand dollars.[xviii]

One caveat is that a terrorist group would need to mount an exceptionally large attack, in order to distinguish itself from criminals and hackers. This is a bigger challenge, but it is hard to estimate. As an extreme case, it may be possible to design a worm that would spread throughout the Internet within minutes; alternatively, a worm could spread surreptitiously, eventually infecting 10,000,000 hosts.[xxii] However, such an attack would require much greater technical skill, and a much deeper understanding of the functioning of the Internet as a whole.

Next, we consider a second major class of attacks, targeting PCs and other systems that have been patched to fix known vulnerabilities, and are protected by network defenses. These can be found in corporate and government settings. The emphasis of this attack is on penetrating security in order to disrupt operations or gather information.

The technical requirements of this attack are substantial. The attacker may need to identify new vulnerabilities and develop new exploits; moreover, because of countermeasures such as intrusion detection systems, the attack itself will be more complicated. Some information may be available from hackers, but each attack must be tailored to a specific target--thus, insider information is helpful. We estimate that such an attack could be carried out by a team of 5 people, with experience in systems and network programming, over a period of 6 months to one year.

A special case of this attack occurs when the target is an uncommon or one-of-a-kind system, such as a router, a mainframe or an embedded control system (e.g., SCADA). These may be found in critical infrastructure. Often, information about these systems is not publicly available, so the attacker will have to actively investigate, or obtain cooperation from an insider. Developing an attack will likely require technical expertise, creativity and sustained effort. On the other hand, many of these systems were not designed with security in mind, and may have serious (but little-known) vulnerabilities.[xxiii] Moreover, in the case of critical infrastructure, a successful attack can have catastrophic consequences.

3.3 Other uses of cyber attacks

While cyber attacks are unlikely to cause mass destruction and casualties (and thus do not constitute terrorism in the strict sense of the word), we believe they can be used in other ways to achieve terrorists' aims. The ultimate goal of terrorism is to influence public opinion and cause a change in government policy. In this context, cyber attacks can be used as a psychological tool.

Many people rely on computers and the Internet in their daily lives, while having only a minimal understanding of computer technology and security. A cyber attack has the potential to create irrational fear among people who simply feel exposed, but do not understand the nature of the threat. Also, because of their novelty, such attacks tend to get extra news coverage. Terrorist groups may see this as a way to get attention, show off their capabilities, and make themselves more credible.

Yet another possibility is that terrorists would use the Internet as a communications medium. The equivalent of an al Qaeda video might be a worm that downloads a terrorist manifesto onto every computer it infects. Terrorists might find this attractive because, unlike television and radio, the Internet lets them communicate directly with their audience.

Finally, cyber attacks have certain advantages for international terrorist organizations. First, cyber attacks do not require personnel to live and operate in the target country; al Qaeda's experiences have shown that learning English and living in the U.S. can be major stumbling blocks. Also, operating from a friendly foreign country shields attackers from law enforcement; cyberspace is international, so there is no clear governmental authority, and fewer constraints on malicious activities. Lastly, cyber attacks can help with other aspects of terrorism, such as propaganda and recruitment, and these attacks can be self-financing through criminal enterprises such as identity theft and cyber-extortion.

3.4 Conclusions, and the future of cyber security

The primary aim of terrorists is to coerce the government or public opinion by inflicting psychological and physical damage on the target. In our report, we distinguish cyber-terrorism from common cyber-crimes. The scale of cyber-threats that can be launched was viewed in the context of routine disruptions that occurs commonly in these critical infrastructures. We are of the view that, for a cyber attack to be of any strategic value to terrorists, it needs to go beyond routine disruptions to paralyze or create psychological terror.

From the scenarios we analyzed, it appears that most cyber-attacks against critical infrastructure have a very limited chance of causing widespread damage. It would be also fair to say that the fears of the cyber-terrorism have been exaggerated by mass media. [viii] [ix] which unfortunately has failed to distinguish between cyber-terrorism and cyber-crimes.

Nevertheless, we cannot deny or ignore the future risks of cyber terrorism. Many scholars (Verton) have argued that Al-Qaeda has shown a great penchant to acquire modern technology. Osama Bin Laden, in an interview published in an Arabic newspaper, claims to have the support of "hundreds of Muslim scientists were with him who would use their knowledge…ranging from computers to electronics."

Moreover, the dependence of our critical infrastructure on computer networks is not static, as it is getting more inter-twined and ubiquitous. Also, there seems to be momentum for adopting more standardized versions of network protocols as this provides greater cost advantage over maintaining propriety standards and protocols. Finally, several states, including the U.S. and China, are now developing information warfare capabilities. All these factors may make future cyber-threats more viable than they are now. It is essential that we put enough resources into research efforts which will make network infrastructure more secure, robust and resilient to future cyber-attacks.

4 Feasibility and Cost of Defenses for Home, Corporate and Financial Systems

4.1 Current protection incentives

Financial Incentives

The most important financial incentive for home users is to prevent exposure of sensitive or personal information/Identity Thefts - Unauthorized people may be able to access financial or medical data or other personal information. Other incentives are to prevent cost to replace or repair their machine and to prevent financial losses when their home based business is crippled. One last incentive is to prevent fines or late charges due to their inability to submit their e-bill payments on time.

For Corporate the most important financial incentive is to retain their Customers and Business partners. Security, from the technology provider's perspective, is becoming more of a contra expense than a revenue opportunity. Security is a way for companies to save money by lowering operating costs. Every time a corporation such as Microsoft release security patches it costs a lot of money. Security is necessary to maintain companies franchise - For Microsoft, which has witnessed more than 80 million Firefox downloads and the emergence of countless papers arguing that open source is more secure than Windows, security isn't going to be a way to make more money—instead, it will be a way to protect the company's core franchise. By securing their system they could avoid damages caused by tampering of data or exposure of sensitive corporate information or losses incurred due to data lost beyond replacement. Other incentives for Corporate are to prevent stock market losses, losses incurred to repair and the hassle of dealing with lawsuits from compromised customers or partners.

While many of the same existing incentives to provide defenses for home and corporate systems also apply to financial systems, unique or amplified incentives also apply to them. A leading incentive is the far greater financial liability from damages caused by an attack, which are composed not only of the trades lost due to an attack, but any fraudulent trades executed by the attacker and financial judgments brought under applicable laws.

Both government and stock exchange regulation, although not directly directed at protection levels, are also significant incentives. An attack or even a disclosed vulnerability exposes the financial firm to sanctions, and even expulsion, under the stock exchanges rules governing responsibilities and requirements in financial transactions. Similarly government regulations establishing protection requirements for data such as the Gramm-Leach-Bliley Act and the Sarbanes-Oxley Act are incentives for upgrading defenses.

Non-Financial Incentives

All incentives for corporate are directly or indirectly financial incentives. But for home users some of the non-financial incentives to secure their machines are 1) to prevent slowness in their computer - attacks can cause a significant amount of traffic over the network and relies on certain processes on your computer 2) To prevent Loss of Communication – they would be cut off from communicating from their friends or family 3) To prevent the hassle of getting their computer fixed and the inconvenience. 4) To prevent loss of credibility – if the user unknowingly infects other friends then they will be wary in trusting the e-mails from the user in future resulting in loss of credibility 5) In order to prevent frustration in being unable to complete their work. 6) To prevent unnecessary spamming. This might also make parents restrict their children from accessing the computer

4.2 Adequacy of Incentives

For home computer users I should say that that the incentives are not adequate enough. For computer educated users the above incentives are good enough to protect their machines. For the common users, they don't realize the magnitude of damage their negligence to protect their machine could cause them or to others if their

machines is used as part of the rogue network. Several seniors for whom being able to use the computer is an achievement in itself are not confident in ensuring that their computer is update with the patches and security updates. Home Sector could benefit from enticing benefits from Government or Corporate which would in the very least motivate people to keep their machines up to date.

For Corporate the incentives are not adequate. It is adequate for a Corporation whose business is hugely tied with software but not for smaller non-software companies. For companies like Microsoft it will be a way to protect the company's core franchise. But for others implementing security will add up to fewer features, inconvenience and additional costs. Unless Government enforces strict policies and places liabilities on firms or provide attractive incentives, corporate sector has a long way to go.

In reality for the financial industry, the existing incentives may not be as significant as they appear, because damages from minor attacks can easily be absorbed by the financial corporation. Additionally, the likelihood of large scale attacks is low enough that extra defenses are not viewed as cost effective. Corporations can easily absorb minor damages through write-offs or passing the cost to customers. Damages are also limited by the difficulty of assigning cause to the corporation; courts generally do not allow customers to bring Tort Law actions when the damages are purely economical.[xxiv] Although Contract Law is one viable option, it does not apply to cases where no contract exists.

The ability to absorb minor damages combined with the unlikely occurrence of major attacks results in more reactive than proactive upgrade behavior. For the incentives to be adequate, they should result in corporations looking at defenses for emerging threats a couple years ahead.

4.3 Cost Efficiency of Additional Protection

There are several free security products and upgrades that available in the market. Also these days the Internet service providers bundle basic security services into their products. Most OS come with security features such as firewall. Of course what you pay for is what you get. But even the products that you have to spend extra money is a cheap price to pay for the benefits that come along. But there is the overhead of upgrading the products constantly. For home users it more about the awareness than about the costs as there are free options to keep their machine protected.

The cost effectiveness for Corporate depends hugely on how big or small the firm is. Few firms seem willing to incur the additional costs. For huge firms such as Walmart or Microsoft being secure is the way to survive in the market and so for them any additional protection is cost effective. Whereas for smaller business it is not cost-effective. The software department of such firms is a small/minor/non-profitable component of the firm. The costs of maintaining a software department with the overhead of regular maintenance and upgrades is not something that they would be willing to spend on unless something drastic happens.

The cost efficiency of acquiring additional defenses is determined by comparing amount of direct damages prevented to legal and financial liability exposure reduced. Traditionally, this has been determined by comparing the cost of protection to the level of potential damage multiplied by the likelihood of an attack. This comparison breaks down at the level of a stock market trading system. A single attack, however unlikely, can cause immeasurable damage not only to the financial corporation attacked but also to the stock market and the economy in general. This leads us to conclude that protection against nearly any full breach attack whose likelihood is above zero should be considered cost efficient. The traditional analysis should be used for attacks that can not cause fundamental damage – a denial of service attack will cripple the system for a given period but does not affect the system at its roots.

4.4 Lowest Cost Providers for Protection

There are several free options for protecting home computers: ZoneAlarm firewall, Ad Blocker(WebWasher Classic), Anti-Sypware (Spybot, Ad-aware), anti-virus (AVG Antivirus), E-mail Encryption (Pretty Good Privacy). Norton Security Suites is a good paid option which offers most of the above as a package. For corporate good solutions for different layers of protection comes with a cost but all equivalent products are priced at the same range. It hugely depends on the size and the requirements of the firm. Norton, McAfee, e-trust Internet security suites all cost roughly the same and provide equivalent protections. Utility software runs the gamut, but prices tend to hover in the $50 to $100 range per license. There is no best solution but just different ways and layers of how it can be made difficult for the attacker.

Financial systems are by their very nature vast and widely connected. Such an environment contains many points of vulnerability, making it very nearly impossible to determine a single lowest cost provider for upgraded defenses for the system. The lowest cost would exist in all parties working together to provide the necessary multiple layers of protection. Each can address its areas of the system in the most efficient manner.

The difficulty of using a single provider is that in a large system a single component can not guarantee full protection for the entire system. Strong encryption can protect communications but the encryption keys need also be protected and encryption can not protect against router based attacks.

4.5 Policy Levers

One suggested policy is to give tax breaks to people and organizations that use networked computers in a properly secure way or to obtain cyber-security insurance. In practice, of course, we can't afford to do a security evaluation on each taxpayer so we would instead give the break to those who meet some formalized criteria. Designing these criteria so that they correlate well with the right kind of security, and so that they can't be gamed, is the toughest part of designing the program. Also along the same lines government could give tax breaks to companies that develop security technologies. Mandatory Basic Computer Security course educating users on the vulnerability and various available options of protecting themselves for all fields of study is a good option to widen awareness.

As far as liabilities goes there are different way of approaching this 1) Increase the exposure of software and system vendors and system operators to liability for system breaches and mandated reporting of security breaches. Mandatory disclosure law requiring companies holding computerized personal information of users to take steps either to encrypt this personal information will be effective 2) Shifting liability to another party that has the capability to prevent computer security breaches or mitigate the harm caused. This strategy places liability on actors with indirect control over Internet security. But then the strategy would assign liability to computer owners whose insecure property serves as an attractive intermediary for computer criminals. 3) Another proposal is to place liability on Internet service providers that permit their users to attack computer security elsewhere. It would likely be extremely costly and intrude on the privacy of the internet users.

For the financial industry several policy levers are available to the government that would provide additional incentives for financial corporations to proactively upgrade IT protection. Mandatory cyber attack insurance would be a strong financial incentive for proactive protections because insurance would not be available at reasonable prices, if at all[xxv], for corporations without top notch protection in place. Public disclosure of protection activity – such as required by the SEC for Y2K[xxvi] – and penetrations would result in public pressure to maintain protections. This is similar to California's public disclosure requirements when private information is disclosed.. Changing Tort law to apply to cyber attacks in addition to making cyber protection a legal obligation for companies would increase the financial incentives to avoid court actions by maintaining proper protection. Establishment of regularly updated industry-wide standards has a similar effect; a corporation not meeting those standards exposes itself to claims of negligence.

These incentives reinforce each other. Exposing a corporation to legal action will likely increase the pressure from insurance providers for corporations to provide greater levels of protection in order to keep premiums reasonable due to the greater risk of claims.

---

[i] "Information technology for counterterrorism: Immediate actions and future possibilities" National Research Council of the National Academies, 2003, J. L. Hennessy, D. A. Patterson, H. S. Lin (Eds.)

[ii] Keeping an Eye on your Identity, CBS News, http://www.cbsnews.com/stories/2005/06/08/earlyshow/contributors/raymartin/main700481.shtml

[iii] Yearly economic damage estimates - All Attacks, mi2g, http://www.mi2g.com/cgi/mi2g/press/ged2004.pdf

[iv] World broadband statistics: Q4 2004, Point Topic, http://www.point-topic.co.uk/content/dslanalysis/World+Broadband+Statistics+Q4+2004.pdf

[v] Wal-Mart Reports Record Second Quarter Sales and Earnings, Walmart, http://investor.walmartstores.com/phoenix.zhtml?c=112761&p=irol-newsArticle&ID=743493&highlight=

[vi] Key Statistics for Charles Schwab, Yahoo! Finance, http://finance.yahoo.com/q/ks?s=SCH

[vii] Gabriel Weimann, "Cyberterrorism: How real is the threat?," United States Institute of Peace, December, 2004

[viii] James A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Threats," Center for Strategic and International Studies, December, 2002

[ix] Barton Gellman, "Cyber attacks by al Qaeda feared: Experts: Terrorists at threshold of using Web as deadly tool," The Washington Post, June 27, 2002

[x] DeNileon, Guy, "The Who, What Why and How of Counter-terrorism Issues," American Water Works Association Journal, May 2001, Volume 93, No. 5, pp. 78–85

[xi] Scott Berinato, "Debunking the Threat to Water Utilities," CIO Magazine, March 15, 2002, http://www.cio.com/archive/031502/truth_sidebar2.html
[xii] Testimony of Michehl R. Gent Before the Senate Government Affairs Committee, May 8, 2002, ftp://www.nerc.com/pub/sys/all_updl/docs/testimony/mrg-testimony-SenateGovernmentalAffairs-5-08-02-(final).pdf
[xiii] Information Assurance Task Force of the National Security Telecommunications Advisory Committee, http://www.aci.net/kalliste/electric.htm
[xiv] Larissa Paul, "When Cyber Hacktivism Meets Cyberterrorism," SANS Institute, February 19, 2001 "Examples of cyber terrorist actions can include hacking into an air traffic control system that results in planes colliding…"
[xv] CERT Coordination Center, "Overview of Attack Trends," manuscript, 2002. Available at http://www.cert.org/archive/pdf/attack_trends.pdf (accessed 10/21/05).
[xvi] W.A. Arbaugh, W.L. Fithen and J. McHugh, "Windows of Vulnerability: A Case-Study Analysis," IEEE Computer Magazine, Dec. 2000.
[xvii] CERT Advisory CA-2001-23, "Continued Threat of the 'Code Red' Worm," July 26, 2001. Available at http://www.cert.org/advisories/CA-2001-23.html (accessed 10/23/05).
[xviii] E. Ratliff, "The Zombie Hunters," The New Yorker, Oct. 10, 2005.
[xix] SwatIt, "GT Bot," web page. Available at http://swatit.org/bots/gtbot.html (accessed 10/22/05).
[xx] C. Thompson, "The Virus Underground," New York Times Magazine, Feb. 8, 2004.
[xxi] D. Moore, G.M. Voelker and S. Savage, "Inferring Internet Denial-of-Service Activity," USENIX Security Symposium, 2001.
[xxii] S. Staniford, V. Paxson and N. Weaver, "How to 0wn the Internet in Your Spare Time," USENIX Security Symposium, 2002.
[xxiii] D. Matthews, "Hardware Bus Security in Embedded Systems," The Fifth HOPE (Hackers on Planet Earth), New York City, July 9-11, 2004.
[xxiv] "Critical Information Infrastucture Protection and the Law: An Overview of Issues" The National Academies, 2003. Stewart D. Personick and Cynthia A. Patterson (Eds.)
[xxv] Gaudin, Sharon. "Managing Digital Risk with Cyber Insurance" eSecurityPlanet.com February 16, 2005. Retrieved October 21, 2006 < http://www.esecurityplanet.com/trends/article.php/3483736>
[xxvi] "Third Report on the Readiness of the United States Securities Industry and Public Companies To Meet the Information Processing Challenges of the Year 2000". SEC. July 1999. Retrieved October 20, 2006 < http://www.sec.gov/news/studies/yr2000-3.htm>