WHITE PAPER

The Silent Battlefield:

America's Alarming Vulnerability to Cyber Attack

Rob Rachwald
Director of Product Marketing
rrachwald@fortify.com

The Silent Battlefield:

America's Alarming Vulnerability to Cyber Attack

Table of Contents

3 **The Threat**

6 **The Challenge**

8 **Technological Responses to Attacks**

10 **An Effective Technological Countermeasure**

11 **Technology Is Not Enough: Awareness Is Paramount**

11 **About Fortify**

The Threat

Browse a news Web site or open a newspaper and every day headlines proclaim the threat of cyber attack on the United States:

- A single attack in the summer of 2007 disabled a reported 1,500 Pentagon computers.
- According to the Pentagon, the Defense Department detects 3 million unauthorized "scans"—or attempts by would-be intruders to access official networks—on its computers *every day*[1].
- Experts claim China, North Korea and others are escalating their use of cyber warfare techniques and are actively training new hackers.
- A recent coordinated attack on Estonia's cyber infrastructure was thought by some to be the result of a disagreement with Russia and was termed "Web War I" by Estonia's Deputy Minister of Defense.
- A 2007 Defense Department report to Congress states that the Chinese Army sees computer network operations "as critical to achieving 'electromagnetic dominance'."
- Cleaning up cyber attacks on the National Defense University, Naval War College and Fort Hood each cost $20 to $30 million.
- In 2007, reports confirmed that attacks emanating from the Chinese military had penetrated the Pentagon, the German Chancellery and England's Whitehall.

There's also the real possibility that a cyber attack could disable defense command systems, bring down power grids, open dam floodgates, paralyze communications and transportation, create mass confusion and hysteria: Any or all of which could be the precursor to land, sea and air conventional and nuclear military attacks.

The problem is only growing.

An increased reliance on computers for communication and management makes the U.S. government ever more vulnerable to cyber attacks.

What is the goal of these attacks? Any attack can have serious and expensive results, whether it be targeted toward individuals, small businesses or corporations. Intellectual property can be compromised, personal and business information can be stolen, normal business operations can be disrupted and major financial losses can occur.

More seriously, attacks on the U.S. Government carry the increased threat of the theft of government and military secrets. There's also the real possibility that a cyber attack could disable defense command systems, bring down power grids, open dam floodgates, paralyze communications and transportation, create mass confusion and hysteria: Any or all of which could be the precursor to land, sea and air conventional and nuclear military attacks.

Whatever the origin or method of attack, the rate of attack is growing fast. The Department of Defense has seen a 46 percent increase in attacks on its Web site since 2005, and the Department of Homeland Security received 37,000 reports of attempted breaches on government and private systems in fiscal year 2007, up 54 percent from 24,000 in 2006.

The Danger of Unpreparedness and Complacency

Unfortunately, in both the private and public sectors, unpreparedness and naiveté have enabled cyber attackers to score major wins. Hundreds of millions of dollars to cleanup cyber attacks on American military bases and institutions already have cost the American taxpayer.

In other cases, the ultimate costs of the attacks are still to be discovered. In May 2005, the Air Force Assignment Management System (AMS) was hacked. AMS, an online program used for assignment preferences and career management, contains career information on officers and enlisted Airmen, as well as personal information, such as birth dates and Social Security numbers. In all, 33,000 personnel records were downloaded. This breach was made public, including coverage in many major news outlets such as the *Washington Post*.

A corollary of these Web attacks is that any all intrusion attempts must be taken seriously. Whatever the intent—vandalism, mischief or military intrusion, attacks can appear similar in method. Modern anonymizing techniques make source identification difficult. Even if an attack can be tracked to an IP address in a specific country, it's extremely difficult to prove that a hacker or agency in that country was responsible.

The only answer is preparedness and vigilance. America can't afford to be surprised by a major cyber attack that leaves it scrambling to create new systems and new defenses that are too little and too late.

The only answer is preparedness and vigilance. America can't afford to be surprised by a major cyber attack that leaves it scrambling to create new systems and new defenses that are too little and too late.

Who Is Responsible for Defending Against Attacks?

In February 2003, the Department of Homeland Security released *The National Strategy* to Secure Cyberspace. This policy set a priority to secure the federal government's cyberspace. Not long afterwards, the United States Air Force expanded its mission from protecting land, sea and air, to include cyberspace, and the Air Force has taken the lead in developing methods and tools to protect both Department of Defense (DoD) and non-DoD agencies.

Everyone agrees that all attacks must be taken seriously. The only effective defense against the increasing wave of cyber attacks is an active offense that uses a range of techniques to render the attacks ineffective.

The only effective defense against the increasing wave of cyber attacks is an active offense that uses a range of techniques to render the attacks ineffective.

In the recent past, it was sufficient to hire software security experts and leave the problem to them. Today, it has become apparent that cyberwarfare is here to stay and will become one of the major battlefields of the future. The job of preparing for these battles belongs not only to the troops in the field—CIO's, CSO's, QA testers and the like—but to the generals, admirals and secretaries of defense to make the policy and provide direction.

The Air Force has a tradition of engaging first in new arenas of warfare, and was itself created due to the Army's growing need for air power. The Air Force has taken the federal government's mandate to establish cyber security to the next level by expanding a tactical, perimeter-based approach to a strategy of *building in security*.

Organizationally, the Air Force is the only branch to have established a cyber command to prepare for the cyber battlefield. It will do this by defending national computer networks running critical operations as well as by offensively neutralizing adversaries' hacking capabilities. The Air Force now operates a Provisional Cyberspace Command at Barksdale Air Force Base in northwest Louisiana.

The Challenge

What's Being Attacked?

The DoD is arguably the largest Internet user on the planet, with more than 11 million users. These systems are often a major target for hackers, both domestic and international.

Custom-Built Applications Are Often the Weakest Link

Like many civilian and commercial sites, DoD sites use Java and .NET applications, and methods of attack and exploits are largely the same as are used in attacks on non-governmental sites. To a lesser extent, legacy and internally facing applications such as COBOL and C/C++ applications also are vulnerable.

Unlike civilian and commercial sites, however, custom-built applications for the DoD handle essential defense systems, such as weapons systems, including tank coordination and missile guidance. They also include human resources systems that contain sensitive information, such as rank and Social Security number for officers and enlisted men.

All of these applications are vulnerable and targeted by cyber attackers who are looking to disrupt operations, steal information or gather intelligence to aid in coordinated assaults on American defenses.

Methods of Attack

Bot Storming

The most common method is ***bot storming***. This method employs disguised software delivered through the Web or e-mail that takes over an unprotected computer and turns it into a zombie computer under the command of the hacker. The attack is not targeted at specific networks or computers: The probes are cast throughout the Internet and seek out vulnerable systems through wide dispersal and sheer force.

Experts estimate that millions of computers worldwide could have been incorporated into these bot networks. Bot networks can be used to mount DOS (denial of service) attacks, create or misuse SMTP mail relays for SPAM delivery, perpetrate click fraud, or steal application serial numbers, login IDs and financial information, such as credit card numbers.

Google Hacking

Another common method is ***Google hacking,*** which refers to the technique of creating complex search-engine queries in order to filter through large amounts of search results for information related to computer security. In its malicious format, it can be used to detect Web sites that are vulnerable to numerous exploits and vulnerabilities as well as locate private, sensitive information about others, such as credit card numbers, Social Security numbers and passwords.

Both bot storming and Google hacking can result in an attack on a specific system, but their initial use is to find any vulnerable computer or network.

Directed Attacks

The third method, and the most dangerous, is the ***directed attack.*** The directed attack targets a specific Web site and has a human controlling the attack, even if that person is using an automated mechanism. These attacks are less frequent, but they are much more sophisticated and dangerous to the application under attack.

In its malicious format, it can be used to detect Web sites that are vulnerable to numberous exploits and vulnerabilities as well as locate private, sensitive information about others, such as credit card numbers, Social Security numbers, and passwords.

Types of Attacks

Attacks typically fall into the following categories:

- SQL injection
- Cross-site scripting
- Buffer overflows
- Other

SQL Injection

A SQL injection occurs when user input is formed in such a way as to be passed to the database layer of an application and unexpectedly (to the application) executed. The exploit can occur when the user input is not strongly typed or is incorrectly filtered for string escape characters embedded in the SQL statement.

Cross-site Scripting

Cross-site scripting, or XSS, refers to a method of injecting malicious HTML or scripting code into an otherwise benign Web page without the user's or Web site host's knowledge. This exploit circumvents the "same-origin policy" of Web browsers in which code that originates from a location other than the current Web page should not be trusted. Using this method allows an attacker to gain elevated access privileges to sensitive page content, session cookies or other objects. Mitigation of this exploit can include limiting or denying the use of client-side scripting, or more commonly to filter or encode user-supplied HTML to avoid its misinterpretation as HTML or script.

Buffer Overflows

A buffer overflow occurs when a process stores data beyond the boundaries of a fixed-length buffer, writing data or instructions to a potentially vulnerable memory location. This condition can be avoided by implementing strict bounds checking, either in the code, the compiler or the runtime.

Other Types of Attacks

Other exploits exist, with names such as 'command injection, HTTP response splitting, log forging and path manipulation'. There are many more. All take advantage of the Achilles heel of application security: trusting or not filtering user and outside input, enabling unvalidated metacharacters, alternate encodings and numeric representations to get through and wreak havoc on applications and networks.

Technological Responses to Attacks

What Are the Standard Responses?

There are standard responses to attacks on Web applications, and, applied rigorously, they have their place in the arsenal of defenses. These measures include source code analysis, application firewalls and intrusion prevention systems. However, the battlefield is constantly evolving, and keeping abreast of new exploits requires constant vigilance, study and regular updating of methods and defenses.

Limitations of Standard Responses?

As exploit methods evolve, those responsible for defense against them must incorporate new tactics into their arsenal. This requires continual customizations of firewalls and external fortifications against intrusion. Regular and rigorous examination of source code can reveal flaws, but the process is timely and, all too often, schedules don't allow for the time and effort involved for this method to be effective. Additionally, an inability to discern attacks from regular Internet traffic can lead to an inefficient and mistargeted use of valuable defensive resources, both in technology and human power and time.

Outside-in methods, such as firewalls, intrusion prevention systems and network monitors with no specific knowledge of the applications they are protecting, can display the weaknesses common to any defense with a "black box" mentality, i.e., if the exploit has a greater knowledge of its target than the defense protecting that target, the exploit has the advantage.

Moreover, an ineffective response to attacks can be more dangerous than no response at all for the simple reason that misplaced use of resources leads to complacency. A common human mindset is to believe that one is smarter, working harder and more prepared than the enemy, but the cyber battlefield is evolving more quickly than any battlefield in history. Today's supposed state-of-the-art fortification against cyber attack can overnight become a medieval trebuchet facing a modern breech-loading, rifled cannon.

A More Effective Response

What would be the most desirable characteristics in an effective response to the threat of cyber attacks?

While individual analyses—static code analysis, for example—can help discover vulnerabilities in one environment or during specific operations, tools that are used in isolation run the risk of not discovering problems that are apparent only when the application is run, or when subjected to business logic during interaction with other components. QA groups are typically unprepared and untrained in the intricacies and specialized knowledge of security attacks, so specialists with specialized tools are employed to probe for problems. A solution must be usable by QA testers during standard QA testing to ensure that rushed schedules, limited resources or the unavailability of specialists don't limit its effectiveness.

Fortify's family of security tools provide 360 degrees of protection, in the key areas of static, dynamic and real-time analysis.

All too often, the first sign of a problem is when a running application, network or Web site is compromised by an attacker and the damage has been done. An effective response should protect against both known and unknown attacks, so that it's always ready for new threats. It should be able to work before the application is deployed, during testing and after deployment, in real-time, to ensure that all challenges are met. Any response that requires initial or ongoing customization will always lag behind new threats, so as little customization as possible is desirable. The response should be able to identify which part of the application is being attached, and by whom, to order to address vulnerabilities and prepare for future intrusions.

Any good defense must be able to distinguish between what is malicious and what is regular Internet traffic. Good security can't rely on a single-detection algorithm, so multiple, easily updated algorithms must be employed.

Any good defense must of course meet key software security requirements, such as Payment Card Industry (PCI) Data Security Standards, OWASP Top Ten, HIPAA, FISMA and more.

Finally, overhead should be kept to a minimum for efficiency and not interfere with regular network and application operations.

An Effective Technological Countermeasure

While other providers offer tools in one or maybe two of the key areas of software security —static code analysis, dynamic execution analysis and real-time analysis —only Fortify offers a multi-level solution combing best-of-breed solutions in *all* key security areas.

Fortify 360 Static Code Analyzer (SCA) identifies vulnerabilities in an application's source code before it's deployed. Every aspect of the application is tested for a comprehensive list of vulnerabilities early in the software development lifecycle, when they are least expensive to fix and before they get out into an operational environment.

Fortify 360 Program Trace Analyzer (PTA) tests an application at run-time, when it's deployed. PTA identifies weaknesses that only manifest themselves during deployment, such as those that depend on the application's environment and configuration. Fortify PTA integrates seamlessly into QA testing, without requiring QA testers to become security experts.

Fortify 360 Real-Time Analyzer (RTA) works inside an application and can detect not only attacks coming into the application but also vulnerabilities in the application itself. RTA works like an application firewall, providing protection during execution, with the unique ability to see problems as they arise while an application is running. With access to business logic, RTA also is able to identify attacks that are typically more difficult to detect, such as fraud.

This integrated solution enables users of Fortify 360 to see and understand the big picture of threats to their applications and networks. Information from each key area is correlated with results from the others to prioritize vulnerabilities, while at the same time eliminating time-consuming false positives.

Fortify's family of security tools provide 360 degrees of protection, in the key areas of static, dynamic and real-time analysis.

Only with an integrated approach to system security can security administrators hope to stay ahead of today's savvy and aggressive hacker forces. Success on the cyber warfare battlefield will go to those who are best prepared with the most effective tools and methodologies.

> "Fortify's solutions address an enormous problem for the U.S. Air Force. What we required was a comprehensive solution that made software self protecting at the code level during development, as well as providing the ability to determine how our applications were getting attacked and by whom. Fortify's solutions meet those objectives."
>
> **Lieutenant General**
> **Charles L. Johnson III**
> **U.S. Air Force**

WHITE PAPER

Technology Is Not Enough: *Awareness Is Paramount*

Even before tools and counter forces are deployed, awareness of the severity of the threat among all users and clients must be a priority. Informed vigilance—a result of education, training and constant reinforcement—is required to ensure protection against current and future exploits. Even with the best tools and systems in place, the greatest danger is that our critical systems and computers are vulnerable due to complacence or simple ignorance.

Whenever there is a major transition from the old to the new, from old battlefields to new ones, the risk is that enemies will exploit weaknesses and vulnerabilities before people wake up to the challenge and prepare themselves for the coming threat.

Software security applications, such as those from Fortify and others, are necessary and essential, but are only part of the solution. Real-world initiatives that include policy, leadership, processes, education and funding, go hand in hand with technological solutions. Only with that combination will future threats be met with the strong, aggressive defense they require.

About Fortify

Fortify Software's Business Software Assurance solutions protect companies and organizations from today's greatest security risk: the software that runs their businesses. Fortify reduces the threat of catastrophic financial loss and damage to reputation as well as ensuring timely compliance with government and industry mandates. Fortify's customers include government agencies and Global 2000 leaders in financial services, healthcare, e-commerce, telecommunications, publishing, insurance, systems integration and information technology. For more information, please visit us at *www.fortify.com*.

FORTIFY SOFTWARE INC.

MORE INFORMATION IS AVAILABLE AT WWW.FORTIFY.COM

2215 BRIDGEPOINTE PKWY.
SUITE 400
SAN MATEO, CALIFORNIA 94404

TEL: (650) 358-5600
FAX: (650) 358-4600
EMAIL: CONTACT@FORTIFY.COM