

# The Maginot Line of Information Systems Security

Rick Forno  
March 1999  
Rforno@taoiw.org

*On ne passe pas* -- "they shall not pass", was engraved in the Maginot line, a military fortification designed in the early 1900s to prevent a future German invasion of France. Karl von Clausewitz, the brilliant Prussian military theoretician and instructor, wrote a hundred years earlier, "If you entrench yourself behind strong fortifications, you compel the enemy to seek a solution elsewhere." On 10 May 1940, General Erich von Manstein, a student of Clausewitz's writings, demurred at the thought of attacking the well-fortified line and slipped his German armor through the Ardennes forest.

The Ardennes was considered a poor place to deploy armor and without the Maginot Line it would have been the worst choice. But the strength of the line changed the dynamics of the situation and made the previously impenetrable Ardennes look like the most workable solution--underlining the veracity of Clausewitz's observation. And because the French had no strategic reserve to shield themselves from an attack from that direction they lost their territorial sovereignty in just ten days.

In the south where the Italians had no choice but to attack the line, seven French soldiers operating behind the controversial fortification, held up an entire enemy division for more than a week.

Wouldn't Maginot be an appropriate name for a firewall product or any company offering *only* technical solutions to communications security problems? Good firewalls and other purely technical solutions do their work effectively, but to a clever and determined attacker they are just obstacles to be either broken or side-slipped, whichever is most effective.

It is not just the financially motivated cyber-thief or teenage hacker that is testing the electronic Maginot lines of global corporations. Terrorists and states unsatisfied with the current balance of power are turning to what they consider to be low-risk, high-return cyber-strategies that avoid traditional types of military defense. According to George Tenet, Director of the Central Intelligence Agency and statute head of the United States intelligence community, "It is clear that nations developing these programs recognize the value of attacking a country's computer systems both on the battlefield and in the civilian arena." He pointed to telecommunications and banking as high-profile targets.

Technology, combined with the creative genius of military thinkers around the world, is leading to the development and application of new forms of warfare, and the innovative modification of traditional military practices. While the United States and its allies are the

source of much of this innovation, others are motivated by the dominant military position of the United States, and its demonstrated commitment to maintaining its military lead. This basic reality is forcing many of the nation's adversaries (current and potential) to seek other means to attack American interests. Lieutenant General Patrick Hughes, USA, Director of the Defense Intelligence Agency mentioned these (and several other) items in a recent Congressional testimony. With regard to this article, some of the more important vulnerabilities and opportunities are listed below:

- Information Warfare (IW) involves actions taken to degrade or manipulate an enemy's information systems while actively defending one's own. Over the next two decades, the threat to American information systems will increase as a number of foreign states and sub-national entities emphasize offensive and defensive information warfare strategies, doctrine, and capabilities. Current information on national vulnerabilities, and foreign intelligence initiatives in general, point to the following threats:

- Trusted insiders who use their direct access to destroy or manipulate the information or communications system from within.

- Modification of equipment during transport or storage.

- Physical attack of key systems or nodes, including the insertion of modified or altered hardware.

- Network penetration to include hacking, exploitation, data manipulation, or the insertion of various forms of malicious code.

- Electronic attack of various interconnecting links, sensors that provide data to the system, or other system components.

- Empowered agents including "sponsored" or individual hackers, cyber-terrorists, criminals, or other individuals who degrade, destroy, or otherwise corrupt the system. In the most advanced case, empowered robotic agents, embedded in the system, could be used to take autonomous (timed) actions against the host or remote systems or networks (cyber war).

- Cybernetic warfare (CYW) is a distinct form of information warfare involving operations to disrupt, deny, corrupt, or destroy information resident in computers and computer networks. One particularly troubling form of "war in cyberspace" is the covert modification of an adversary's data and information systems. This form of warfare will grow in importance as technology makes new methods of attack possible. Cybernetic warfare defies traditional rules of time and distance, speed and tempo, and the conventional or traditional military capabilities of the opposing elements.

- Transnational Infrastructure Warfare (TIW) involves attacking a nation's or sub-national entity's key industries and utilities – to include telecommunications, banking and

finance, transportation, water, government operations, emergency services, energy and power, and manufacturing. These industries normally have key linkages and interdependencies, which could significantly increase the impact of an attack on a single component. Threats to critical infrastructure include those from nation-states, state-sponsored sub-national groups, international and domestic terrorists, criminal elements, computer hackers, and insiders.

· Asymmetric warfare – attacking an adversary’s weaknesses with unexpected or innovative means while avoiding his strengths – is as old as warfare itself. In the modern era, many forms of asymmetric attack are possible – to include the forms of warfare outlined above, terrorism, guerilla operations, and the use of Weapons of Mass Destruction (WMD.) As a result of the dominant American military position on the world stage, it is very likely to be the focus of numerous asymmetric strategies as weaker adversaries attempt to advance their interests while avoiding a direct engagement with the United States on its own terms. If forced into a direct conflict with the United States, those same adversaries are likely to seek ways of "leveling the playing field" to maximize their chances of success.

· Asynchronous warfare involves a preselected, or delayed (timed) attack on an adversary, taking advantage of the passage of time to develop a strategic opportunity or to exploit a future vulnerability. In a preselected attack, the operation has a latent effect on the adversary. Human or technical assets are strategically placed well before – sometimes years before – the actual confrontation. In a delayed attack – often carried out as an act of reprisal months or even years later – the operation is conducted after an opponent has lowered his guard.

Essentially, in the Age of Information Warfare, one is either a target or a victim. In other words, a target has defenses against attackers while victims are defenseless. On a national, strategic level, there are a number of intriguing target possibilities, including:

Electronic Switching Systems (ESS) - Nationwide systems that manage all telephone communications. Consider the consequences if the nation could not communicate via the telephone or dial-up Internet access.

Global Positioning System (GPS) – US-developed constellation of geosynchronous satellites that provide excellent navigational data for civilian aircraft, ships, and handheld units used by campers. Provides precise information to US military units and attack systems.

Internet - the communications backbone of science, industry, and society.

Commercial Operating Systems and Applications – This is an accident waiting to happen. What about commercial off-the shelf operating systems that run major networks for large government agencies and companies? Who knows what lives inside these "untrusted binaries" in such widespread use around the world? Users and administrators must be on constant alert to the almost-weekly announcements of a new vulnerability in these

systems and be prepared to implement corrective action immediately to avoid potential threats to the integrity of their data and networks. The same can be said for financial and other business-critical applications that are used in conjunction with these untrusted operating systems.

One serious vulnerability not discussed in many circles is the sad but true fact that the mission-critical systems and infrastructures (financial, power, and most business or government systems) of the United States and elsewhere are run by commercial operating systems and software applications purchased *with the assumption that such products are secure as shipped from the manufacturer*. Unfortunately, this is not the case, and numerous vulnerabilities have been discovered in systems that were marketed as allegedly "secure" to industry or government specifications. Why? Some software companies are more concerned with profit, market share, and putting competitors out of business than they are with producing a quality software product that provides reasonable levels of security and acceptable levels of risk to the user. Granted, total security is as real as the Tooth Fairy, but stronger quality assurance must be taken on these products the world is now relying on.

Today, unfortunately, slipshod products are rushed to market quickly, being driven by their competitor's schedule or their own internal marketing efforts. This effectively turns the consumer and corporate markets into expanded, "beta" testers who, instead of *being paid* to examine a piece of software for quality, *pay* the manufacturer for the privilege to own a license for an untested product and stand a good chance of having to absorb the costs of securing, recovering, or restoring their systems and data resulting from issues arising from a shoddy product nobody outside of the vendor has examined! During their use or "examination" of such products, systems routinely crash, data gets lost, or other issues arise that comes from implementing such untested software. While not an "external" attack to information systems like a hacker or cracker, such untested software applications are an equal threat to the sanctity of corporate data and information resources and the infrastructures relying on such products.

It was rumored that the Microsoft Windows 95 operating system installed by the consumer masses, shipped with over " 5,000 *known* bugs." Not unexpectedly, corporate and consumer clients complained about the quality of the new operating system when it shipped amongst much fanfare in August 1995. After several "service fixes" to the product, an upgraded operating system, Windows 98, was rushed to market in late June 1998 to spite an ongoing United States government court case, and reportedly fixed "about 3,500 *known* bugs in Windows 95." *A quality product?* Sure, if the company considers the world consumers to be unpaid "quality assurance" or "continuing beta testers" for such software. In the same vein, the auto industry recalls vehicles with defects in them and fixes such defects at no charge to the "owner"...but the software industry requires that its "users" / "owners" fork over money to get such defects and dangers to their data fixed. However, as of January 1998, even with two "service packs" and a few "patches" to the operating system, Windows 98 is still not Y2K-compliant. At this late date, a quality product must – by definition – not fail on 1 January 2000. To be fair, the Windows 98 product is more stable and robust than its predecessor, although it ships with

several controversial features seemingly placed in the product for product placement than end-user utility.

The installation of and subsequent reliance on such systems that have not undergone peer review or independent analysis is an accident waiting to happen. While items like UNIX (an open operating system that "runs" most of the Internet), Pretty Good Privacy (the *de facto* Internet encryption tool), and Netscape Navigator (the first, and some would say *only* reputable Web browser) have released their source code to the world for public analysis, disclosure, and discussion, many of the world's largest operating system and applications vendors - particularly Microsoft - do not, citing "proprietary trade secrets." In these cases where software has undergone worldwide peer review, the result is that user concerns and quality control issues are addressed *before* the product hits the open market, not after, where a considerable user base exists and is potentially threatened by bad code. Further, users have the opportunity to see how the programming code will interact with existing applications, much like checking a medical prescription for any potential drug interactions or side effects. Software that has been examined by "independent third parties" stand a better chance of being accepted as indeed "secure" and "stable" than products where the vendors announce "our product is secure...trust us!" In this case, an objective, third-party "Software Underwriters Laboratory" for instance, would not be a bad thing.

An example of the user community's reluctance to sleep well and rely on untested proprietary software is found in government circles in the early 1990s when the National Security Agency and National Institute of Standards and Technology attempted to create a standard encryption system for the United States to replace the antiquated Data Encryption System (DES). "Use it," they said in official reports, "but the encryption algorithm is classified TOP SECRET and not available for independent review." While the implication was "trust us, we're the government" -- the product flopped and was declassified in mid-1998. Some would argue that the reason why UNIX, PGP, and Navigator became *de facto* user products in the computing community was that the software was reviewed by outside experts who certified the products, algorithms, or software code were robust, stable, and worked as advertised or intended.

While lucrative for security professionals, the increase in known vulnerabilities associated with such "proprietary" systems is disheartening. Where is the product security, stability, and reliability for the "good of the customer base"? Recently, under tremendous pressure from the deep-pocketed software industry, new copyright laws passed in 1998 prohibiting reverse-engineering and analysis of computer software without the express consent of the vendor. After much wrangling from the security community, Congress finally inserted provisions for academics and security professionals to be legally able to analyze software for security or academic purposes only. If the industry continues to develop insecure, untested, programs and operating systems -- and

prohibits independent testing and analysis – the future for truly secure operating systems – and systems in general -- is fading rapidly from reality.

In July 1998, news surfaced that the Navy's first Commercial-Off-The-Shelf ship, the Aegis vessel *Yorktown*, had a systems failure only hours after departing Norfolk. The ship's Windows NT network crashed conducting a mathematical calculation and rendered the vessel unable to continue its mission. Why? Who knows what applications interacted with the NT software to cause the crash? Can the Navy dissect the NT operating system to find the flaw like they can in UNIX? Not a chance. The hacker and quality assurance communities had a field day with this latest blunder, dubbing Windows NT as "Needs Towing" and an operating system that certainly "Needs Tweaking." Yet the Navy is going ahead with plans to standardize fleet information systems to this allegedly "secure, stable, and robust" operating system, most certainly out of user familiarity with its interface that is nearly identical to many home computers. In true military fashion and typical government lock-step, the Marine Corps is following the Navy's IT-21 Project and standardizing the Corps on Windows NT as well as most of the Department of Defense and United States government. Of course, any product or operating system requiring several hundred-megabyte "Service Packs" should raise an eyebrow or two

Given the move toward "information systems security" in the federal information infrastructure, is it wise to develop a networked infrastructure on such untested, crash-prone, bloated, and difficult (not to mention costly) operating systems? The three components of information security (INFOSEC) are Confidentiality, Integrity, and Availability. This rush to standardize on NT given the number of recent hacks, cracks, and attacks -- coupled with the infamous "Blue Screen of Death" -- certainly challenges these fundamental INFOSEC principles. An opening of the NT code to allow third parties to witness its inner workings and potential fallacies will go a long way in reassuring security administrators that NT is the "way to go" compared to glitzy public relations (some would say "disinformation") campaign by Microsoft.

Something that is often overlooked in information systems security is the potential for back-doors left inside applications by their programmers. This is predicated on the fact that the majority of commercial software and services are produced by American companies, many of which are written by foreign nationals employed by the software companies working on visas in America or back in their home nations. This is a major concern to government organizations who try to monitor personnel with critical access to systems and information. How easy might it be to co-opt a programmer in India to place some small backdoors for the Indian government to have secret access to any Windows NT server? Given the poor quality assurance measures by many software companies today, our guess is very easy. Suppose these Indian programmers inserted some malicious lines of code into NT as a way of "getting back" at the US after it imposed economic sanctions on their country after their recent rounds of nuclear testing in early 1998? Not a pleasant thought, but a very real vulnerability. A good number of programmers and consultants working the Year 2000 issue are foreigners who are granted nearly unlimited, unfettered, and unmonitored access to the mission critical systems of our largest

corporations and government organizations without any criminal background checks. Need we say more?

There are hidden programs, routines, and "Easter eggs" such as small flight simulators and pinball games hidden inside such products by their programmers, which perhaps adds to the size, complexity, and problems running the software. *Do we really need to play a flight simulator while viewing financial data on a spreadsheet? Will the Navy or the rest of the world know what evil or "treats" lie in the 40- million-plus lines of programming code that constitutes Windows NT, Internet Explorer, or Word?* Probably not. *Will we still run the software and put up with the crashes, hiccups, and reboots associated with these products?* Sure...it's a "feature" and a seemingly acceptable level of risk to the world. Unless the NT server crashes and the famed Blue Screen of Death appears while targeting a Harpoon missile, that is.

Sadly, most policymakers, flag officers, and corporate executives are not products of the Communications Revolution. They do not understand programming code, the critical value of information, or the inherently "virtual" way the world works, not to mention the vulnerabilities inherent with the growing reliance on information infrastructures. Everyone plans for the major military offensive through the procurement of high-profile and glitzy weapon systems, but no one is planning for the critical defense of our less visible - but equally critical - interior vulnerabilities, the "Soft Underbelly" of the country. Technology such as firewalls and encryption alone will not provide adequate security for information.

While a great deal of press attention has been focussed on the teenage hacker and the egomaniacal programmer gone wrong, these are actually the least threatening intruders as their motives are childish. The acts of these people can range from bravado to destruction, but they are most often aimed at getting attention or simple greed.

Terrorists and state-sponsored programmers are less likely to want attention guaranteed to stimulate defenses. They prefer to attach themselves like parasitic organisms to government and corporate systems either to create wider security breaches or simply create long-term taps into strategic information. This style of attack can be more insidious than a destructive attack, as stolen or corrupted information (which should be backed up anyway) never actually disappears from its owner. In human terms, each day the victim gets sicker, but never knows why until it is too late.

It does not take a genius to develop tools or applications to effectively bring down one of today's mission critical, commercial-off-the-shelf systems. Indeed, there are numerous free "hacker tools" and several legitimate diagnostic tools that can be used for both good and evil. In short, **the greatest vulnerability is uncertainty regarding the content and integrity of programs and operating systems that drive our commerce and protect our national security and corporate secrets.** Coupled with this is a considerable amount of technical and common-sense ignorance in administering and implementing information technology regarding security implications and vulnerabilities. Technology alone will not provide good information security -- it must be coupled with common

sense and awareness of the threats and vulnerabilities inherent with not only the installed systems but the security tools and technologies used to protect them as well. Blind and ignorant reliance will not work.

While some may scoff at the likelihood of large-scale attacks on corporate and government infrastructure through the medium of commercial software, remember how the best military experts prior to World War II considered the Ardennes to be an impractical axis of attack. In the security business, the very act of dismissing the possibilities of an attack raises the chances of its ultimate success. Without knowing the enemy's activities and routes into the fortress, the inherent risks to one's organization are present. Ignoring it will not make it go away.

The attack will come. A strong defense will be necessary.

---

Article Copyright © 1998-99 Richard Forno. All Rights Reserved. Author biography and Book Information (The Art of Information Warfare) available at <http://www.taoiw.org>.