Sun Tzu : The Art of Cyber Warfare

By Ashish Banerjee, www.Ashish.Banerjee.name, 12 May 2005.

We needed a framework for thinking and designing security for mission critical geographically distributed banking application over a wide area network.

Our goal was to provide the financial transactions, databases and computing infrastructure with highest possible security.

What does security mean in terms of information domain?

Information security must address Authenticity and Confidentiality. Authenticity involves data integrity and non repudiation. Data Integrity means that we are assured that the information is not tampered with and data packets have not been re-transmitted (or replayed) with malicious intent. Non repudiation means that the author of the record is not able to deny its originality, it mainly involves public key based digital signature. Confidentiality involves the assurance that no one is able to snoop on the communication and only authorized persons within the organization can access the information.

We found that the warfare paradigm suited us the best.

Sun Tzu, an ancient Chinese general in 6th century BC, wrote the Art of Warfare over 2000 years ago and yet its principles are still used in modern warfare as well as in management thinking. Sun Tzu 's central doctrine is: *To win without fighting is the best*. We have adopted this doctrine for our security framework.

By thinking about security as a transformation of warfare into cyberspace, enables us to get the best of the two prevalent security models namely: the asset centric security and the perimeter centric security.

In the asset centric model, the assets like servers and databases are protected while in the perimeter based model, the focus is on protecting the corporate boundary. But in our framework, we model the Information Infrastructure Security as a manifest of warfare in virtual reality. Thus we are able to cover both the assets as well as the boundary.

Understanding the warfare terrain is the highest responsibility of the general, and it is imperative to examine them: Sun Tzu.

In our security framework we first define three concepts:

- Terrain
- Domain
- Territory

The warfare Terrain encompasses all the network space from where the attack can be launched on our domain. Domain encompasses our territory as well as all the networking pathways, not owned by us, through which our data flows. The Territory encompasses all our computing assets, databases and networking infrastructures owned by us. The aim is to keep or domain secured and protect our territory.

Thus Terrain in a superset of Domain, which is a superset of Territory.

Imagine that you are a baron owning two castles and you need to transport foodstuff from one of your castles to another. You do not own the road connecting the two, as it passes through a friendly neighboring fiefdom. The roads passes through a valley surrounded by high mountains, not owned your neighbor nor yourself. In this analogy the two castles are your Territory. The road and the castles your Domain. And, the Terrain would constitute the high mountains, the valley, the road and the castles.

You may ask, why is castles included in the warfare terrain? Well, to protect ourselves from the enemy within. A study found that nearly 70% of the attacks are launched by insiders having intimate knowledge of the system's internal security.

Making armies able to take on opponents without being defeated is a matter of unorthodox and

orthodox methods: Sun Tzu.

This brings us to face the enemy. Enemy is any entity who intends to attack our territory. In order to plan our defenses, we need to profile our potential enemies and chart out their motives.

A non exhaustive list of enemy profiles and their motives are:

A disgruntled current or ex employee, whose motive may be to harm the company.

A greedy employee out to make a quick money.

A hacker wanting to hold your data hostage for extracting a ransom.

A teenager out to prove herself a wise crack.

A customer wanting to gain an unfair advantage by fudging your accounts.

A competitor wanting an access to your trade secrets or your customer databases.

You can add more to this list. Also there are situations where the above profiled may collaborate to achieve their ends.

Invincibility is a matter of defense, vulnerability is a matter of attack: Sun Tzu.

Having profiled our potential attackers, lets see what are the types of attacks they can launch:

- Denial of Service attack: the network or a server is rendered unusable by flooding it by spurious traffic.
- Trojans: A program has trap doors built in to compromise the system, but sending information out or letting people in.
- Facade: A dummy resource erected to fool the legal users to give out secret information. For example, a dummy ATM machine was setup by attackers to collect the credit card PIN numbers!
- Spy wares: These are malicious program, usually get in through emails or rouge web sites, monitor your desktop for password typing and send back this information.
- Man in the middle: In this type of attack, the communication is intercepted and modified for malicious reasons, by getting into and becoming a part of the communication channel.
- Phishing: a type of social engineering attack, where official looking emails are send to harvest passwords and access codes.
- IP Masquerading: A machine or a router is reprogrammed within the network of an service provider to redirect traffic to another computer.
- DNS spoofing: The DNS server, which resolve the IP address for a domain name, is hijacked to resolve a trusted site name to a malicious computer.
- Hack in: software venerability or a weak password is exploited by the attacker to break into the system.
- Snooping: The attacker access the communication, many a times, the security authorities have hooks into the public IT infrastructures; this authority can be misused by an agent.
- Authority misuse: An authorized internal person, misuses his access to manipulate the system to their advantage. A programmer had once programed to drop the rounded off change to his bank accounts!

Again the above list is not exhaustive and newer methods are always being invented.

It is hard to know as the dark; its movement is like pealing thunder: Sun Tzu.

We not come to the point of planning our defenses. There are three situations in defense:

- Preemptive : This is the best situation to be in, we have not been attacked and yet be are prepared for it. Erecting a firewall and venerability testing are the two most common plans for

this situation.

- Under Attack: Here we have been attacked and need to respond to the situation. Fighting a DOS (Denial of Service) attack is one of the most challenging example.
- Postmortem : This situation arises after our security have been compromised. This is the worst situation of the three to face. We need to trace the intruder, sanitize the resources to remove any Trojans or spy wares also we need to inform and co-operate with legal agencies and collect the log files as evidence to trace and book the offender. An offender who goes Scott-free is likely to attack again.

Armies must know there are adaptations of the five kind of fire attacks, and adhere to them scientifically: Sun Tzu

In the warfare paradigm software tools, algorithm and programs become the weapons. Weapons, are technology tools and can be both used for defense as well as attacks.

There are many such tools available and since this is a general white paper, we shall come out with a detailed paper on specific tools applicable within our security framework. However many security sites like www.insecure.org and linux.org list many security tools in use.

One who is good at martial arts overcome other's forces without battle: Sun Tzu.

One of the strategies is to shrink the terrain. The optimum being domain being equal to the terrain. This can be achieved in multiple ways. One of them being, taking a VPN (Virtual Private Network) from a single vendor, having MPLS and IPSec protocols running over IPv6.

The maximum security you can get is to shrink the domain into your territory. That is you own all the networking as well as computing infrastructure. This scheme is however, not practical for most of the real life financial domain applications. For example, most of the financial transactions including ATM traffic in USA is routed over Internet!

So it is said that victory can be made: Sun Tzu.

Reference: The Art of War by Sun Tzu, translated by Thomas Cleary. ISBN 1-56957-100-7, Published by www.Shambhala.com