The Application Security Pyramid - The Border

Posted At : April 8, 2006 2:01 PM | Posted By : Mark Kruger
Related Categories: Security

In my **Previous Post** I introduced a new metaphor for thinking about security. The purpose of this metaphor is to give us a framework for discussing the topic with stakeholders who have a cavalier attitude toward security, or who have fallen into the habit of relying on mere network security to keep them safe. We discussed how current metaphors that are physical in nature don't do enough to encompass the whole realm of security when it comes to addressing a specific application. A new metaphor is needed. I came up with a model based on Maslow's hierarchy of self-actualization (it sounds pompous but hey - it works for me). If you want to know more, read on.

- **Intro**
- **Part II**
- **Part III**
- **Part IV**

The model looks like this:

Basic needs are at the bottom and "ideal" needs at the top. Today we are going to start at the bottom and work our way up 1 post at a time. Even though this is a series on *application security* it is important that we address the network first.

Border Agents - Your Country Must Be Safe

It doesn't take a genius to recognize that the integrity of your country has a bearing on your actual security. In the US the armed forces protect us from hostility of nations, the INS protects us from those awful aliens who want to rob us of our unwanted low paying jobs in order to feed their families and the FDA protects us from food - at least food that doesn't meet a certain health standard. I should mention that your view of these agents of government may vary wildly depending on your political orientation and whether you live in California. Still, it's safe to say that the civil structure that defines us as a country is part of what makes us feel safe.

In the same way you must have *border agents* protecting your network. This is really what most people think about when they talk about *network* security. Your network should be protected with a firewall, you should have an organizing principle that

segments network traffic (a DMZ for example), and you should have monitoring or auditing that enables you to react when something is amiss.

For most networks the border agents consist of network design that centers around hardware devices. A packet filtering firewall is a good example. It monitors packets and ports on your network and tests traffic against rules that you set up. Certain things are allowed in, certain things are allowed out, and everything else is denied. In the old days these devices were set up as a denial service. Everything was allowed unless you specifically blocked it. Surprisingly, there are still many networks that use this approach. When something becomes a problem they block it, otherwise everything is open. Typically though, a modern firewall blocks all ports and protocols unless they are specifically enabled.

Modern firewalls also use something called "stateful inspection". That means the firewall is concerned about more than just the individual packets. It is also aware of the session or "state" of the connection in question. In other words, a computer gaining access through a port for one purpose (let's say FTP) cannot take over that port for a different purpose. The "stateful" firewall monitors connections, not just packets. For that reason it is often referred to as "stateful packet inspection".

Other border agents exist for specific protocols. Devices like Barracuda Networks Spam Firewall for example, examine a specific kind of traffic (SMTP) and protects you from words like v*i*a*g*r*a and c1al1s. Devices like ISA server - a security product put out by Microsoft (no snickering please, this is a serious article) - do double duty as a caching/acceleration server and a packet monitoring firewall for http and https traffic.

These devices work on a very low level and they are very sophisticated. Unfortunately they are often badly configured. For example, Cisco reckons that the most egregious and persistent security problem with it's own security conscious devices is that network engineers often leave them configured with the default username and/or password. That means another engineer (or someone who can read documentation) can log in by researching how the device comes from the factory. In my own neighborhood there are at least 2 wireless networks using Linksys routers and the default settings.

I know this because I also own a Linksys router and one day when I was troubleshooting my *own* router I couldn't get in for some reason. I reset the router back to the factory defaults and got right in. Then I realized I was on *somebody else's router*. Sure, that happens with little SOHO routers you say, but nobody would configure a corporate network like that - would they? Oh yes they would. Human nature is both lazy and optimistic. When dealing with network security that is a bad combination of attributes. When setting up new devices people often say "I'll change the password later" or "It's inside, noone will notice" or "I think I saw the 'hot now' sign at Krispy Kreme - I have to run".

So the first thing is - configure the firewall correctly!! You might have a 5000 dollar firewall, but it doesn't do any good to wear Armani if your fly is open. Some firewalls are better than others, but all of them are crap if you don't know what you are doing. Start by asking the question, what do we want to allow into the network and what are we going to allow out of the network. Make your initial firewall provisions very strict and modify them as you experience any difficulty. When modifying your rule set resist the temptation to simply "open everything up" to solve a problem. Get used to reading documentation and searching through forums.

If you are using Cisco and the Cisco EOS is beyond your capability you might try one of the many firewall devices that offer higher ease of use and a lower learning curve. I've heard good things along those lines about SonicWall and WatchGuard. While I like Cisco their usability standard is constructed to maintain the high rate of pay of Cisco engineers. You simply cannot adequately configure a PIX without using the command line.

So, now that your country is secure what else does it take to make you feel "safe" - answer, internal policing. Next time on Coldfusion Muse (film at 11:00).