The Application Security Pyramid - Introduction

Posted At : April 6, 2006 11:34 AM | Posted By : Mark Kruger
Related Categories: Security

> CF Muse Reader Asks:
> How do I educate my employer on the concepts of application security? How do I get them past the "We have a firewall and a DMZ, we're secure!" mentality? Specifically, in the past, I've tried using info from owasp.org to help, but they got "lost". Thanks Mark!

My first piece of advice is to never ever direct a non-geek to an open source project. You might as well be directing them to a site broadcasting Shakespeare in Hellenistic greek. Open source projects have a wealth of information, but the information usually isn't written very good... er... well (although I found this owasp.org site to be ok). Geeks use acronyms like Samuel L Jackson uses the F-bomb - often and gratuitously. Of course you can try to summarize what you learned - and it sounds like that is what you did. The owasp.org site starts at the application code level however, and is going to be difficult for *any* non-programmer to grasp - at least without some groundwork. Even though you are trying to get them beyond that "first level" of security in your discussion, you may still need to address it. So let's lay some groundwork.

- Part I
- Part II
- Part III
- Part IV

Recently we worked with a very large company employing dozens of IT staff and developers. They had lots of hoops for us to jump through to be a preferred contractor. We had to sign forms and be issued credentials. Policies were crafted carefully to insure that we would not have access to anything out of scope. Finally we were ushered into the holy of holies and we were allowed to access the code.

We promptly found out that the code was rife with unchecked variables being passed to queues and databases. Since they were using numeric pins for login I was able to muster a very simple SQL injection attack that allowed me to log right in. I put something like "5555 OR 1 = 1" in the password field and it let me right in just like Ali Baba saying "open sesame".

This illustrates the most common misconception about security. It is not what you keep out that is usually the most dangerous. It is the things you are already letting in that wreak havoc on your security. Part of the reason for this is that the metaphors we use when dealing with security are inadequate.

I realize that metaphors are only aids to understanding things that are more concrete, but they have a surprising impact on our viewpoint. For example, the Bears and the Cubs are both sports teams from the rough and tumble midwestern town of Chicago. Neither team has a reputation for greatness. Except for 1 shining year in 1985 the bears have had decades of mediocrity. The cubs have had moderate success to abject failure for nearly a century.

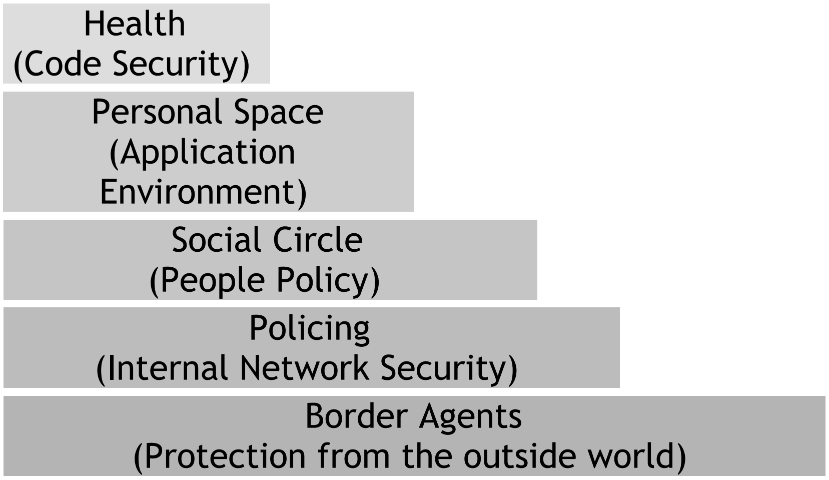
Yet one of these teams has the reputation for being tough and grizzled and "grind-it-out" persistent, while the other team has the reputation as the "lovable losers". Can you guess which is which? You guessed it, the bears are the ones with the reputation for "smash mouth football", while the erstwhile cubs are universally beloved in spite of languishing in the National League Central Cellar for 80 years. At least part of the formula for that sentiment is the adorable "cubbie" logo - who can resist a little bear cub. Sure, they grow up to rip your face off and eat your lawn furniture, but when they are small they are so darn cute!

So it is with security. We choose metaphors that come from a by-gone era and make sense to us. We think in terms of a bank vault - strong, impenetrable steel walls with a stern guard at the door eyeing everyone who enters. But what if you had all the permissions you needed to get into the bank vault? Better still, what if you did not need to actually remove the contents of the vault to cause mischief? What if you could do it by simply singing in the corridor or reading hamlet in the lobby? What if the bank *allowed everyone* to access the vault but restricted them to using only the finger and thumb of one hand, or required blind-folds?

You can see the problem with comparing security on the Internet to security at a bank. The truth is that the Internet lets people in. And you want those people in - at least the ones with which you are doing business. You want them to be able to use your applications legitimately. You are not interested in placing burdensome restrictions and requirements on them that makes doing business with you more challenging.

Many business owners, CIOs and CTOs opt for the bank metaphor, and fail to take it any further. They install watchdogs at the perimeter. All of the security is facing outward looking for threats and blocking them before they get into the network. This is important stuff to be sure. It would be foolhardy indeed to run your network without a firewall - just as it would be foolish to paint a big sign on your house that said "door unlocked and plasma screen inside". But the metaphor fails at that point. Keeping people out is like the first level of Maslow's pyramid of self actualization. Sure, you need food and shelter, but they don't make you healthy and happy (unless the food is pina coladas and the shelter is a seaside cottage in Tahiti). If your network is ever going to be self-actualized it has to move up the pyramid.

I propose a different metaphor for security. It is based on the safety, not of valuable items, but the safety of personhood. Or more appropriately, it asks the question what does it take for you to feel secure. Let's start on the outside and work our way backward just like Maslow.



Health
(Code Security)

Personal Space
(Application
Environment)

Social Circle
(People Policy)

Policing
(Internal Network Security)

Border Agents
(Protection from the outside world)

For the next few Posts I'll attempt to address each of these topics. When I'm finished I will try to bundle them into a podcast. Stay Tuned.