

# Secure From Whom?

By Tim Maletic

Every security practitioner knows that you must anticipate your enemy. Keeping that axiom firmly in mind, however, is easier said than done. During the last few weeks I have run across several examples of common but faulty infosec reasoning. Beneath each bad argument was the same oversight: the failure to consider the nature of the attacker.

## The Determined Hacker

Here's a classic:

Antagonist: "Don't bother implementing security feature X (strong passwords, say—or the Microsoft patch *du jour*), because there's no such thing as 100% security. A determined attacker will get in anyway."

This is partially correct. A determined attacker *will* get in anyway. But chances are, of all your attackers, the determined ones are a small minority. This leads to the following response.

Protagonist: "Security feature X may not protect against a determined attacker, but it *will* help against all the other ones. We'll thwart the determined attacker as best we can, but there is no excuse for letting the casual attacker get through."

## Different Kinds of Enemies

The appropriateness of a security feature cannot be accurately assessed without consideration of the nature of anticipated enemies.

You should anticipate many different kinds of enemies. For the purposes of classifying attackers of information systems, three characteristics are particularly important: targeting vs. untargeting, sophisticated vs. unsophisticated, and external vs. internal. Most (but not necessarily all) worms and viruses are untargeting attackers. An untargeting attacker may aim for certain platforms, applications, or classes of users, but they don't target a specific person or organization. Many unsophisticated human attackers (for example, script kiddies) are also untargeting—they are trolling for victims, instead of targeting someone specific. The "determined" attacker referred to by our antagonist above is, according to this schema, a "targeting, sophisticated and external" attacker. By drilling into this level of detail, it becomes obvious that this kind of attacker is only one kind among many. Our defenses must take all kinds into account.

## The Herd Mentality

Consider this argument:

Antagonist: "WEP is good enough for your wireless security, since hackers already have their hands full exploiting the unencrypted WLANs."

This reminds me of an expression I've heard from hikers in bear country: "You don't have to be the fastest runner in the group—just don't be the

slowest." If your WLAN defense assumes that your only attackers are untargeting, then this "defense-via-the-herd" may actually get you somewhere. Unfortunately, none of us are justified in making such an assumption. Maybe you don't have competitors. And no disgruntled employees, either. You still cannot assume that you have no enemies partial to you.

This herd mentality is a significant driving force in today's infosec community, though it doesn't advertise itself as such, and its implications are subtle. Think about how much time you spend monitoring and responding to alerts issued by US-CERT, Microsoft, the anti-virus vendors, and other infosec news organizations. Now factor in the bandwidth consumed by our infosec vendors in general, where the message is almost always that security is gained through properly configured hardware and software. These two sources alone—alerts and vendor information—inundate us with the security-via-products message. And of course there are many more sources: product reviews, white papers, conference proceedings, certification exams, you name it.

## The Focus on Products

Each of these venues encourages us to focus our efforts on products. Why? That is a long story. For starters, think about why US-CERT will never issue a bulletin concerning a hole found in common computer security training procedures. Next, consider one of our laudable efforts at information-sharing and consensus-building, such as the Center for Internet Security's Operating System Benchmarks. The CIS cannot hope to help every company defend against their own personal targeting or internal attackers. And since untargeting attackers tend to also be unsophisticated (sophisticated attackers having better things to do with their time), these collaborative efforts are naturally addressing the ever-popular "untargeting, unsophisticated, and external" attacker, otherwise known as viruses, worms and script kiddies. And this in turn encourages defenses via products.

Trying to obtain security through products is one manifestation of the herd mentality. If we could just stay on top of the patch treadmill and install the latest intrusion prevention tools, then maybe the next worm outbreak will hit our neighbors instead of us.

This isn't to say that the security-via-products concept is a bad thing. It is a good thing. It increases the overall reliability of the Internet. It fosters good 'Net stewardship. It allows for greater information sharing, since the products provide a common language for the community. (Or to look at it another way: perhaps products are stressed within the community *because* the vocabulary they provide is a least common denominator within our conceptual repertoire—it's like talking about the weather.) And most importantly, by keeping pace with the herd and its focus on products, we protect ourselves not just from worms and viruses, but from many other less predictable forms of attack.

But for better or for worse, security-via-products is just one part of our job. It must find its place alongside security through policies, procedures,

education, training, risk management, forensic analysis, incident response capabilities, and many others. If only it could find its place. The overwhelming attention paid to products yields more negative side effects than merely eclipsing the other aspects of security. It contributes to the hard-on-the-outside/soft-on-the-inside situation that plagues most of our local area networks. And it distorts our perception of the enemy.

It leads to statistics that show that many infosec managers list viruses and worms as their number one problem.<sup>1</sup> It leads to discussions of the window between vulnerability disclosure and exploit code that completely ignore the issue of zero-day exploits. (And it leads to the mainstream infosec press assuming that zero-day exploits rapidly spread through the hacker underground.<sup>2</sup> Shouldn't we be more concerned about zero-day exploits that are known only by a select few?) Yes, these untargeting attacks must be defended against—you cannot be connected to the Internet and not do so. But if you're spending the bulk of your time on this one project, your security program needs a reevaluation.


## Less Security?

Here is one last faulty argument that is different from the previous examples in two ways. It is based on a mistake regarding sophistication, not targeting, and the correct view is toward less security, not more.

Antagonist: "Shouldn't you escalate installing that OpenSSH patch on the internal servers as well? After all, studies show that most hacking is perpetrated by insiders."

Most breaches of your security may indeed be perpetrated by insiders. But while your insider may know your system like the back of her hand, that doesn't imply that she is technically sophisticated. (Here I'm using "sophistication" to connote what it is that makes expert hackers experts.) The kind of knowledge that she has to breach your security is not the same kind of knowledge needed to hack OpenSSH. The antagonist has mistakenly assumed that all attackers are equally sophisticated. Does this mean you shouldn't patch your internal servers? Of course not. You just may be unfortunate enough to have some sophisticated, internal attackers lurking in your midst. (All else being equal, the larger your organization, the more likely this will be.) But it does mean that you should place a different level of urgency on patching the internal servers.

## Conclusion

Our profession will someday mature to the point where all of this is passé. Then studies of attackers will be more informative. Instead of concluding that "72% of attackers are insiders," they will break the concept of attacker into many more variables. They might go on to say that "of the attackers that are insiders, 3% are technically savvy." Similarly, alerts won't merely classify vulnerabilities as "low," "medium," "high," and "critical." They may actually tell us something (up front—without 20 minutes of analysis) about who can exploit them. 

---

*Tim Maletic, CISSP, is the IS Security Officer for Priority Health and co-founder and current president of the Grand Rapids Chapter of the ISSA. Prior to focusing on security full-time, he spent 10 years as a Unix System Administrator.*

<sup>1</sup> CompTIA, cited in "By the Numbers," Information Security, Vol 7 No. 3 (March 2004), p. 24.

<sup>2</sup> searchSecurity.com's definition of "zero-day exploit," [http://searchsecurity.techtarget.com/sDefinition/0,sid14\\_gci955554,00.html](http://searchsecurity.techtarget.com/sDefinition/0,sid14_gci955554,00.html)