*(A version of this paper, "Lessons for Layering", appeared in the January 2010 issue of* Security Management *54(1), pp. 64-69.*

# Layered Security: Self Defense or Self Delusion?

Roger G. Johnston, Ph.D., CPP
Vulnerability Assessment Team
Argonne National Laboratory
9700 S. Cass Ave.
Argonne, IL 60439-4840
630-252-6168, rogerj@anl.gov, fax: 630-252-7323

## Introduction

Security in Depth is a good thing: 4 layers of security trumps 1 layer of security every time, right? Well, not so fast! Layered security can be a useful tool, but it also holds lots of hidden dangers.

Almost every vulnerability assessor is familiar with the following scenario, which the author has personally witnesses at least 2 dozen times (including at nuclear facilities): A security manager is shown a simple, successful attack on a security device or system, or a portion of the overall security program. Then he/she is shown an inexpensive counter-measure, or at least a partial fix that is relatively painless. The instant response: "Well, yes, that is all very interesting, but we have multiple layers of security, so a failure in one layer does not mean that our overall security has failed. Thus, we don't need to be concerned with this vulnerability, nor do we need to implement the recommended countermeasure(s)."

Is this the correct decision? Ultimately, maybe it is and maybe it isn't. But to knee-jerk the decision not to explore the possibility of improving a given layer or portion of a security program based solely on the idea that there are additional layers is certainly not the right response.

As we shall see, having multiple layers of security opens up a wide assortment of new problems, complexities, and vulnerabilities. If security managers aren't careful, security in depth can also lead to over-confidence, sloppy thinking, a flawed mindset, and lax security culture. Sometimes complex, multiple layers of security may be less secure than having a single layer that is carefully thought through, taken seriously, conscientiously maintained, and constantly tweaked to deal with new challenges, threats, technologies, and conditions.

## The Two Kinds of Layered Security

Layered security comes in two general flavors: serial and parallel. Most security programs, however, involve some mixture of the two.

Serial security is the most common type of layered security. It involves nested layers. A typical example might be a facility having a fence on the perimeter to keep out the general public. Within the fence (or at the gate) may be a guard to check credentials, or some kind of automated access control system such as a badge reader or biometric device. Deeper inside the facility there may be roaming guards, closed circuit television, safes and vaults, or even intrusion detectors. Typically, this kind of nested serial approach is designed with the idea that an adversary will encounter ever increasing levels of security (spatially and temporally) as he moves towards the interior of the facility where the most critical assets are kept.

Another example of serial layered security can be found on consumer tamper-evident packaging. Anyone opening an over-the-counter pharmaceutical, for example, may first need to open break open the box, then remove the frangible clear plastic film around the bottle cap, before opening the bottle and finding a foil seal. Hiding evidence of tampering may (ostensibly) require repairing all 3 levels: the box, the frangible film, and the foil seal.

The parallel approach to security in depth involves having multiple security measures all in the same general area. The theory here is that the adversary will confront multiple security challenges more or less simultaneously. Commercial access control devices, for example, often deploy parallel levels of security (though often not very effectively in the author's experience). Access control devices, for example, may require a badge plus a password, personal identification number (PIN), or biometric signature to grant facility access. The hardware may also employ a tamper-indicating or hardened cover, along with a mechanical tamper switch just inside the cover to sound an alarm should the device be opened. A human guard may also be overlooking the whole access control process. An adversary intent on defeating the access control must—at least theoretically—deal with all these security features more or less simultaneously (or at least some subset of them).

## The Dangers

So what pitfalls should we look out for when considering or using multiple layers of security?

Paralysis

The most common problem with layered security is the scenario described above where the mere existence of multiple layers automatically shuts down any attempt to improve any one layer (or the overall security program). Having multiple layers of security should never be an excuse for being satisfied with the *status quo*. Each layer must be taken seriously in its own right and optimized to the extent practical. And all layers should be constantly adjusted (or at least evaluated) in a holistic manner that takes into account new vulnerabilities discovered in any of the other layers, as well as changing conditions,

technologies, threats, and adversaries.

In the author's experience, sometimes the paralysis so often found with layered security programs may not be the fault of layered security *per se*, but rather is due to what psychologists call "cognitive dissonance"—an unwillingness to admit to one's self that there may be security problems. See sidebar. Security managers (or entire organizations) who have a cognitive dissonance problem often seem to pile on layers of security as a mental coping mechanism for dealing with their suppressed fears about the adequacy of their security. On the other hand, layered security does not *cause* cognitive dissonance, nor do security managers with tendencies towards cognitive dissonance necessarily always use layered security. Sometimes they instead place blind faith in a single security measure, rather than invoking layers. The important point is that layered security and cognitive dissonance tend to be strongly correlated, even if there is no absolute connection.

There seems to be another strong correlation between an organization having extensively layered security, and seriously ignoring or underestimating the insider threat to the organization. The reason for this connection is unclear, but it may simply be that most organizations use layered security AND most tend not to deal adequately with the insider threat.

## Throw in the Kitchen Sink Syndrome

When security in depth is viewed as the automatic approach to security, there is a risk that some security managers will begin throwing all kinds of strategies, products, hardware, and technology into the various layers with minimal thought. This can lead to wasting large amounts of money, chasing after the latest overly-hyped technology or security product, confusing and discouraging security personnel and regular employees, and creating such a complex and confusing environment that little critical and skeptical thinking about security can take place.

Even if the security program is cautious in its approach to piling on layers of security, hardware, and the latest technology, splitting funding and attention between many layers of security may mean that none of them is funded or overseen at a threshold level sufficient to make them effective. At the very least, security programs that have many layers of security typically have problems figuring out where to intelligently spend extra funds to gain the greatest marginal increase in security per dollar spent. With only one or a small number of layers, in contrast, it can be much easier to spot where to spend extra money, or focus additional attention.

## When Your Backup isn't a Backup

Security managers who proclaim the advantages of layered security often view each layer as a "backup" or redundancy measure, for either serial or parallel layering. But in fact, many times the various layers have such completely different purposes that they can't reasonably be considered as backups for each other. For example, many government facilities have a security fence and also use tamper-indicating seals for critical assets

stored inside the facility. But the fence does not "backup" the seals, or vice versa. The purpose of the fence is to delay or discourage unauthorized outsiders from entering the facility. The purpose of the seals is typically to detect theft or tampering with critical assets by insiders—the very people who are granted authorized access through a gate in the fence on the basis of possessing a security badge, PIN, or other credentials.

Similarly, guns, gates, and guards do not typically backup (1) a two-person rule for writing company checks, (2) financial audits to detect and prevent (insider or outsider) embezzlement, (3) software security measures for countering external computer hacking, or (4) employee fitness-for-duty checks. Just because each layer in an overall security program is intended to provide some sort of security does not guarantee it will somehow automatically compensate for the weaknesses of all the other layers that serve completely different security functions, have utterly dissimilar attributes, and that are meant to counter very different kinds of threats.

## The Orthogonality Problem

Security planners and security managers sometimes think that their various layers of security are not redundant at all, but rather "orthogonal". This means the different security layers have completely dissimilar functions and characteristics, and are each meant to counter very different threats. Unless an effective, independent, and skeptical vulnerability assessment has been performed, however, there is a great risk that the various layers just superficially appear to be orthogonal, and that they instead share related, serious vulnerabilities. For example, it may be possible for an adversary to bribe a security guard to turn off facility electrical power briefly, thus shutting down all the supposedly orthogonal electronic security layers.

## The Wrong Focus

In many layered security programs or devices, the focus tends to be on each layer alone and in isolation, not in how all the layers interact to provide overall security. Understanding the interactions is extremely important because easy-to-exploit vulnerabilities in security often exist at the interfaces. It is important as well to understand how the various security layers complement each other, but also how they get in each other's way.

Another potential danger inherent in spatially serial layers is that they tend to focus our attention on the "inner sanctum" and the physical assets stored there, deep within the nested layers. Too often, however, security programs are overly focused on protecting tangible physical assets located in the inner sanctum, when they should probably be more concerned about protecting much more important (and spatially distributed) assets such as people, buildings, intellectual property, trade secrets, private information about vendors and customers, the reputation of the organization, and its ability to stay in business. These kinds of assets can't necessarily be hidden deep within nested layers of security in the high-security inner sanctum.

It is also important to recognize that the volume inside a secure building or facility that is at the center geographically, or that has the greatest number of nested security layers

around it, is not automatically the volume that needs the most protection. Threats and consequences should drive how the security layers are configured; the spatial layout of the layers themselves should not determine what we most protect. For example, an organization's CEO, key technical or financial people, or important IT equipment may be the most critical assets for keeping the organization in business during times of crisis, but these assets may well not be located anywhere near the center.

Complexity

Layered security tends to be complex, and complexity is usually not conducive to good security, especially in large or bureaucratic organizations. Complexity complicates effective communication, training, and metrics. It creates many different modes for failure, opening up opportunities for the bad guys and distracting the good guys. This is one of the reasons why low-tech methods can so often defeat high-tech security. [See RG Johnston and JS Warner, "The Dr. Who Conundrum: Why Placing Too Much Faith in Technology Leads to Failure", *Security Management* **49**(9), 112-121 (Sept 2005).]

Even more dangerous is the fact that the complexity inherent in layered security often makes it much easier for "Groupthink" to set in. This is a type of bureaucratic, wishful-thinking mentality where no one individual is willing to step up and ask the necessary hard, skeptical questions, or challenge the entrenched view of things. Indeed, complex systems can be very difficult to keep nimble, which is essential in our rapidly changing world.

Bad Security Mindsets & Bad Security Culture

This is probably the greatest potential hazard with layered security, other than Paralysis. Too often, the idea that we have multiple layers of security leads to a mental mindset that no one layer of security is all that important because, after all, "we have lots of other layers." When security mangers and practitioners start taking any one layer for granted, it is not much of a stretch to begin taking all layers for granted. This can lead to a lazy and lackadaisical attitude towards security in the organization, and may create a general lack of personal accountability on the part of security professionals and regular employees. Security guards or even regular, non-security employees, for example, who observe unfamiliar personnel engaging in questionable activities may become hesitant to challenge them because they believe somebody else or some other security layer will probably deal with the issue. They don't take seriously the contribution that their own layer—that is, themselves—can make. This invariably leads to bad security.

## When does layered security makes sense?

Simply because layered security has serious potential pitfalls and there are many bad examples of layered security does not mean layering should never be deployed. There is, after all, the very real possibility that—after carefully analyzing the security threats, adversaries, vulnerabilities, probabilities, and consequences, as well as the resources available to you—layered security offers the best protection. Just don't choose it by mindless default, and always be cognizant of its potential hazards.

There are also other situations where layered security may be a very prudent strategy. Sometimes it is the best choice when we lack a sophisticated understanding of a new security application. Having several layers in place may buy us some time while we study the security issues in greater detail, or we observe how the various layers perform.

Layered security can be useful, too, when we intend to only temporarily activate certain layers when on heightened alert status, or when unusual (but temporary) situations occur. Layered security can also be useful as a bluff for intimidating potential adversaries. If it looks to them like they will have to defeat many unrelated levels of security to succeed in an attack (even if it's not true), they may be reluctant to even try. Also, multiple layers of security can readily dramatize for employees, vendors, contractors, and visitors the importance of security, or the fact that the organization is taking security seriously. Indeed, different levels of (largely symbolic) security can be very effective for so called "Security Theater", sometimes called "Ceremonial Security", i.e., security measures that are largely for show. Having many levels of security can also slow down employees and visitors, giving security personnel a chance to interact with them on a personal level, and perhaps detect suspicious behavior or attitudes.

Sometimes security managers can get funding for a new layer of security, but not for upgrading existing security in an optimal manner. It may make sense to accept the funds in hopes the money can eventually be utilized in a manner that leads to better security, not just piling on another questionable layer that may actually cause disruptions.

Finally, layered security may be all that we can fall back on when our current security measures are poor. This is probably the case with most tamper-evident packaging and product anti-counterfeiting tags. Current techniques are so easy to defeat (and so little serious research and development is going on in these areas) that throwing on multiple layers of security may be all we have to work with.

## Conclusion

The old adage that security is only as good as the weakest link has some merit. Layered security ("security in depth") often makes sense, but each layer must be taken seriously in its own right and optimized to the extend practical while understanding how it interacts with all the other layers. Layered security must never be used as a lazy cop-out, motivation for over-confidence, or an excuse to avoid improvements. It certainly does not

grant us permission to stop thinking critically, creatively, and skeptically about security.

To borrow an analogy from safety: Your car probably has multiple safety features including seat belts, air bags, a tempered windshield, headrests, and a crash resistant body. That doesn't mean you shouldn't get your brakes fixed.

---

**Sidebar: Cognitive Dissonance**

When security managers are highly resistant to security improvements or the idea that their security might have vulnerabilities, whether they use layered or security or not, the reason is often a phenomenon that psychologists call "cognitive dissonance". Psychologists Carol Tavris and Elliot Aronson do a wonderful job of explaining the concept of cognitive dissonance to the general reader in their fascinating 2007 book, "Mistakes Were Made (But Not by Me)." Gary Marcus also discusses reasoning errors in his 2008 though-provoking book, "Kluge: The Haphazard Construction of the Human Mind". And historian Barbara W. Tuchman focuses on the problems caused by cognitive dissonance throughout history—which she calls "wooden-headedness"—in her classic 1985 book, "The March of Folly: From Troy to Vietnam".

Cognitive dissonance does not necessarily cause deliberate fraud or dishonesty, but rather motivates the self-delusional, ego-saving, wishful thinking, coping mechanisms that people frequently employ to deal with unpleasant or inconvenient realities. These can include *self-justification* (self-serving rationalization and excuse making), *paralysis* or *stagnation* (failure to confront serious problems or take necessary actions), *confirmation bias or motivated reasoning* (unduly dismissing ideas, arguments, evidence, or data that might call into question our current viewpoints, strong hopes, or past decisions). Cognitive dissonance is a huge problem for people in business, government, politics, academia, religion, sports, medicine, and the military, so there is no reason it shouldn't also plague security managers.

In the case of security managers, it can be very difficult to accept the idea that there are problems with your security when you have devoted your life and career to sincerely trying to protect people, your organization, and its important assets, and when you fervently hope that your security will be up to the challenge. The best indicators that cognitive dissonance may be a problem for a security manager are high levels of emotion about, and excessive pride (or arrogance) in his/her security. The best weapons against the dangers of cognitive dissonance are perspective, humility, skepticism, pragmatism, flexibility, and a sense of humor (or at least not taking yourself overly seriously). It is also crucially important to constantly remember that (1) security is a very difficult challenge at best and perfection is never going to be possible, so having security vulnerabilities is not evidence of negligence or some kind of character flaw, and (2) it is far easier to fool yourself than anybody else.