

Editor's Comments

This is the first issue of *The Journal of Physical Security* (JPS) hosted by Argonne National Laboratory. We'd like to thank Argonne for their support.

JPS will continue to be a scholarly, peer-reviewed, multidisciplinary journal devoted to physical security research, development, modeling, and analysis. Papers from both the technical and social sciences are welcome.

As always, the views expressed by the editor and authors in JPS are their own and should not necessarily be ascribed to Argonne National Laboratory, the United States Department of Energy, or the United States Government.

This issue contains an eclectic mixture of topics. The first two papers are about the emerging issue of Open Sourcing for physical security. Open Sourcing has long been a common practice for software, but is relatively rare for security hardware. The remaining papers discuss a design basis threat approach to protecting a radiological source in a hospital, when and how to disclose physical security vulnerabilities, and a discussion about business confidentiality and protecting sensitive information.

In the last issue, I offered some fairly cynical Security Maxims that were intended to be only partially tongue-in-cheek. These were general rules of thumb that I believe apply about 90% of the time to physical security programs and applications. They have proven to be wildly popular based on the feedback I have received from several hundred people. Curiously, most of these people work in cyber security, not physical security. I'm not sure what that says about the two communities, or the two fields.

At any rate, I present below an updated list of maxims based on additional thinking about these issues, as well as suggestions and input from other security professionals. The newest ones are in red.

Whether you agree with any, all, or none of these, I hope they provide food for thought.

Thank you for reading our journal, and please consider submitting a manuscript, and encouraging your security colleagues to do so as well.

--Roger Johnston, Argonne National Laboratory, June 2009

Security Maxims

While these security maxims are not theorems or absolute truth, they are typically valid ~90% of the time for physical security, and may have applicability to cyber security as well.

Infinity Maxim: There are an unlimited number of security vulnerabilities for a given security device, system, or program, most of which will never be discovered (by the good guys or bad guys).

Comment: This is probably true because we always find new vulnerabilities when we look at the same security device, system, or program a second or third time, and because we always find vulnerabilities that others miss, and vice versa.

Thanks for Nothin' Maxim: A vulnerability assessment that finds no vulnerabilities or only a few is worthless and wrong.

Arrogance Maxim: The ease of defeating a security device or system is proportional to how confident/arrogant the designer, manufacturer, or user is about it, and to how often they use words like “impossible” or “tamper-proof”.

Be Afraid, Be Very Afraid Maxim: If you're not running scared, you have bad security or a bad security product.

Comment: Fear is a good vaccine against both arrogance and ignorance.

So We're In Agreement Maxim: If you're happy with your security, so are the bad guys.

Ignorance is Bliss Maxim: The confidence that people have in security is inversely proportional to how much they know about it.

Comment: Security looks easy if you've never taken the time to think carefully about it.

Weakest Link Maxim: The efficacy of security is determined more by what is done wrong than by what is done right.

Comment: Because the bad guys typically attack deliberately and intelligently, not randomly.

Safety Maxim: Applying the methods of safety to security doesn't work well, but the reverse may have some merit.

Comment: Safety is typically analyzed as a stochastic problem, whereas the bad guys typically attack deliberately and intelligently, not randomly. For a discussion of the reverse problem, see RG Johnston, *Journal of Safety Research* **35**, 245-248 (2004).

High-Tech Maxim: The amount of careful thinking that has gone into a given security device, system, or program is inversely proportional to the amount of high-technology it uses.

Comment: In security, high-technology is often taken as a license to stop thinking critically.

Dr. Who Maxim: "The more sophisticated the technology, the more vulnerable it is to primitive attack. People often overlook the obvious."

Comment: Tom Baker as Dr. Who in *The Pirate Planet* (1978)

Low-Tech Maxim: Low-tech attacks work (even against high-tech devices and systems).

Comment: So don't get too worked up about high-tech attacks.

Schneier's Maxim #1 (Don't Wet Your Pants Maxim): The more excited people are about a given security technology, the less they understand (1) that technology and (2) their own security problems.

Too Good Maxim: If a given security product, technology, vendor, or techniques sounds too good to be true, it is. In fact, it probably sucks big time.

Schneier's Maxim #2 (Control Freaks Maxim): Control will usually get confused with Security.

Comment: Even when Control doesn't get confused with Security, lots of people and organizations will use Security as an excuse to grab Control, e.g., the Patriot Act.

Father Knows Best Maxim: The amount that (non-security) senior managers in any organization know about security is inversely proportional to (1) how easy they think security is, and (2) how much they will micro-manage security and invent arbitrary rules.

Big Heads Maxim: The farther up the chain of command a (non-security) manager can be found, the more likely he or she thinks that (1) they understand security and (2) security is easy.

Huh Maxim: When a (non-security) senior manager, bureaucrat, or government official talks publicly about security, he or she will usually say something stupid, unrealistic, inaccurate, and/or naïve.

Voltaire's Maxim: The problem with common sense is that it is not all that common.
Comment: Real world security blunders are often stunningly dumb.

Yippee Maxim: There are effective, simple, & low-cost counter-measures (at least partial countermeasures) to most vulnerabilities.

Arg Maxim: But users, manufacturers, managers, & bureaucrats will be reluctant to implement them for reasons of inertia, pride, bureaucracy, fear, wishful thinking, and/or cognitive dissonance.

Show Me Maxim: No serious security vulnerability, including blatantly obvious ones, will be dealt with until there is overwhelming evidence and widespread recognition that adversaries have already catastrophically exploited it. In other words, "significant psychological (or literal) damage is required before any significant security changes will be made".

I Just Work Here Maxim: No salesperson, engineer, or executive of a company that sells or designs security products or services is prepared to answer a significant question about vulnerabilities, and few potential customers will ever ask them one.

Bob Knows a Guy Maxim: Most security products and services will be chosen by the end-user based on purchase price plus hype, rumor, innuendo, hearsay, and gossip.

Familiarity Maxim: Any security technology becomes more vulnerable to attacks when it becomes more widely used, and when it has been used for a longer period of time.

Antique Maxim: A security device, system, or program is most vulnerable near the end of its life.

Payoff Maxim: The more money that can be made from defeating a technology, the more attacks, attackers, and hackers will appear.

I Hate You Maxim 1: The more a given technology is despised or distrusted, the more attacks, attackers, and hackers will appear.

I Hate You Maxim 2: The more a given technology causes hassles or annoys security personnel, the less effective it will be.

Colsch's (Keep It Simple) Maxim: Security won't work if there are too many different security measures to manage, and/or they are too complicated or hard to use.

Shannon's (Kerckhoffs') Maxim: The adversaries know and understand the security hardware and strategies being employed.

Comment: This is one of the reasons why open source security makes sense.

Corollary to Shannon's Maxim: Thus, "Security by Obscurity", i.e., security based on keeping long-term secrets, is not a good idea.

Comment: Short-term secrets can create useful uncertainty for an adversary, such as temporary passwords and unpredictable schedules for guard rounds. But relying on long term secrets is not smart.

Gossip Maxim: People and organizations can't keep secrets.

Plug into the Formula Maxim: Engineers don't understand security. They tend to work in solution space, not problem space. They rely on conventional designs and focus on a good experience for the user and manufacturer, rather than a bad experience for the bad guy. They view nature as the adversary, not people, and instinctively think about systems failing stochastically, rather than due to deliberate, intelligent, malicious intent.

Rohrbach's Maxim: No security device, system, or program will ever be used properly (the way it was designed) all the time.

Rohrbach Was An Optimist Maxim: No security device, system, or program will ever be used properly.

Insider Risk Maxim: Most organizations will ignore or seriously underestimate the threat from insiders.

Comment: Maybe from a combination of denial that we've hired bad people, and a (justifiable) fear of how hard it is to deal with the insider threat?

We Have Met the Enemy and He is Us Maxim: The insider threat from careless or complacent employees & contractors exceeds the threat from malicious insiders (though the latter is not negligible.)

Comment: This is partially, though not totally, due to the fact that careless or complacent insiders often unintentionally help nefarious outsiders.

Fair Thee Well Maxim: Employers who talk a lot about treating employees fairly typically treat employees neither fairly nor (more importantly) well, thus aggravating the insider threat and employee turnover (which is also bad for security).

The Inmates are Happy Maxim: Large organizations and senior managers will go to great lengths to deny employee disgruntlement, see it as an insider threat, or do anything about it.

Comment: There is a wide range of well-established tools for mitigating disgruntlement. Most are quite inexpensive.

Troublemaker Maxim: The probability that a security professional has been marginalized by his or her organization is proportional to his/her skill, creativity, knowledge, competence, and eagerness to provide effective security.

Feynman's Maxim: An organization will fear and despise loyal vulnerability assessors and others who point out vulnerabilities or suggest security changes more than malicious adversaries.

Comment: An entertaining example of this common phenomenon can be found in "Surely You are Joking, Mr. Feynman!", published by W.W. Norton, 1997. During the Manhattan Project, when physicist Richard Feynman pointed out physical security vulnerabilities, he was banned from the facility, rather than having the vulnerability dealt with (which would have been easy).

Irresponsibility Maxim: It'll often be considered "irresponsible" to point out security vulnerabilities (including the theoretical possibility that they might exist), but you'll rarely be called irresponsible for ignoring or covering them up.

Backwards Maxim: Most people will assume everything is secure until provided strong evidence to the contrary—exactly backwards from a reasonable approach.

You Could've Knocked Me Over with a Feather Maxim 1: Security managers, manufacturers, vendors, and end users will always be amazed at how easily their security products or programs can be defeated.

You Could've Knocked Me Over with a Feather Maxim 2: Having been amazed once, security managers, manufacturers, vendors, and end users will be equally amazed the next time around.

That's Why They Pay Us the Big Bucks Maxim: Security is nigh near impossible. It's extremely difficult to stop a determined adversary. Often the best you can do is discourage him, and maybe minimize the consequences when he does attack.

Throw the Bums Out Maxim: An organization that fires high-level security managers when there is a major security incident, or severely disciplines or fires low-level security personnel when there is a minor incident, will never have good security.

Scapegoat Maxim: The main purpose of an official inquiry after a serious security incident is to find somebody to blame, not to fix the problems.

A Priest, a Minister, and a Rabbi Maxim: People lacking imagination, skepticism, and a sense of humor should not work in the security field.

Mr. Spock Maxim: The effectiveness of a security device, system, or program is inversely proportional to how angry or upset people get about the idea that there might be vulnerabilities.

Double Edge Sword Maxim: Within a few months of its availability, new technology helps the bad guys at least as much as it helps the good guys.

Mission Creep Maxim: Any given device, system, or program that is designed for inventory will very quickly come to be viewed—quite incorrectly—as a security device, system, or program.

Comment: This is a sure recipe for lousy security. Examples include RFIDs and GPS.

We'll Worry About it Later Maxim: Effective security is difficult enough when you design it in from first principles. It almost never works to retrofit it in, or to slap security on at the

last minute, especially onto inventory technology.

Somebody Must've Thought It Through Maxim: The more important the security application, the less careful and critical thought and research has gone into it.

Comment: Research-based practice is rare in important security applications. For example, while the security of candy and soda vending machines has been carefully analyzed and researched, the security of nuclear materials has not. Perhaps this is because when we have a very important security application, committees, bureaucrats, power grabbers, business managers, and linear/plodding/unimaginative thinkers take over.

That's Entertainment Maxim: Ceremonial Security (a.k.a. "Security Theater") will usually be confused with Real Security; even when it is not, it will be favored over Real Security.

Comment: Thus, after September 11, airport screeners confiscated passengers' fingernail clippers, apparently under the theory that a hijacker might threaten the pilot with a bad manicure. At the same time, there was no significant screening of the cargo and luggage loaded onto passenger airplanes.

Ass Sets Maxim: Most security programs focus on protecting the wrong assets.

Comment: Often the focus is excessively on physical assets, not more important intangible assets such as intellectual property, trade secrets, good will, an organization's reputation, customer and vendor privacy, etc.

Vulnerabilities Trump Threats Maxim: If you know the vulnerabilities (weaknesses), you've got a shot at understanding the threats (the probability that the weaknesses will be exploited, how, and by whom). Plus you might even be ok if you get the threats all wrong. But if you focus only on the threats, you're probably in trouble.

Comment: It's hard to predict the threats accurately, but threats (real or imagined) are great for scaring an organization into action. It's not so hard to find the vulnerabilities if you really want to, but it is usually difficult to get anybody to do anything about them.

Mermaid Maxim: The most common excuse for not fixing security vulnerabilities is that they simply can't exist.

Onion Maxim: The second most common excuse for not fixing security vulnerabilities is that "we have many layers of security", i.e., we rely on "Security in Depth".

Comment: Security in Depth has its uses, but it should not be the knee jerk response to difficult security challenges, nor an excuse to stop thinking and improving security, as it often is.

Hopeless Maxim: The third most common excuse for not fixing security vulnerabilities is that "all security devices, systems, and programs can be defeated".

Comment: This maxim is typically expressed by the same person who initially invoked the Mermaid Maxim, when he/she is forced to acknowledge that the vulnerabilities actually exist because they've been demonstrated in his/her face.

Takes One to Know One: The fourth most common excuse for not fixing security vulnerabilities is that "our adversaries are too stupid and/or unresourceful to figure that out."

Comment: Never underestimate your adversaries, or the extent to which people will go to defeat security.

Depth, What Depth? Maxim: For any given security program, the amount of critical, skeptical, and intelligent thinking that has been undertaken is inversely proportional to how strongly the strategy of "Security in Depth" (layered security) is embraced.

Redundancy/Orthogonality Maxim: When different security measures are thought of as redundant or "backups", they typically are not.

Comment: Redundancy is often mistakenly assumed because the disparate functions of the two security measures aren't carefully thought through.

Tabor's Maxim #1 (Narcissism Maxim): Security is an illusionary ideal created by people who have an overvalued sense of their own self worth.

Comment: This maxim is cynical even by our depressing standards—though that doesn't make it wrong.

Tabor's Maxim #2 (Cost Maxim): Security is practically achieved by making the cost of obtaining or damaging an asset higher than the value of the asset itself.

Comment: Note that "cost" isn't necessarily measured in terms of dollars.

Buffett's Maxim: You should only use security hardware, software, and strategies you understand.

Comment: This is analogous to Warren Buffett's advice on how to invest, but it applies equally well to security. While it's little more than common sense, this advice is routinely ignored by security managers.

Just Walk It Off Maxim: Most organizations will become so focused on prevention (which is very difficult at best), that they fail to adequately plan for mitigating attacks, and for recovering when attacks occur.

Thursday Maxim: Organizations and security managers will tend to automatically invoke irrational or fanciful reasons for claiming that they are immune to any postulated or demonstrated attack.

Comments: So named because if the attack or vulnerability was demonstrated on a Tuesday, it won't be viewed as applicable on Thursday. Our favorite example of this maxim is when we made a video showing how to use GPS spoofing to hijack a truck that uses GPS tracking. In that video, the GPS antenna was shown attached to the side of the truck so that it could be easily seen on the video. After viewing the video, one security manager said it was all very interesting, but not relevant for their operations because their trucks had the antenna on the roof.

Galileo's Maxim: The more important the assets being guarded, or the more vulnerable the security program, the less willing its security managers will be to hear about vulnerabilities.

Comment: The name of this maxim comes from the 1633 Inquisition where Church officials refused to look into Galileo's telescope out of fear of what they might see.

Michener's Maxim: We are never prepared for what we expect.

Comment: From a quote by author James Michener (1907-1997). As an example, consider Hurricane Katrina.

Accountability 1 Maxim: Organizations that talk a lot about holding people accountable for security are talking about mindless retaliation, not a sophisticated approach to motivating good security practices by trying to understand human and organizational psychology, and the realities of the workplace.

Accountability 2 Maxim: Organizations that talk a lot about holding people accountable for security will never have good security.

Comment: Because if all you can do is threaten people, rather than developing and motivating good security practices, you will not get good results in the long term.

Blind-Sided Maxim: Organizations will usually be totally unprepared for the security implications of new technology, and the first impulse will be to try to mindlessly ban it.

Comment: Thus increasing the cynicism regular (non-security) employees have towards security.

Better to be Lucky than Good Maxim: Most of the time when security appears to be working, it's because no adversary is currently prepared to attack.

Success Maxim: Most security programs “succeed” (in the sense of their being no apparent major security incidents) not on their merits but for one of these reasons: (1) the attack was surreptitious and has not yet been detected, (2) the attack was covered up by insiders afraid of retaliation and is not yet widely known, (3) the bad guys are currently inept but that will change, or (4) there are currently no bad guys interested in exploiting the vulnerabilities, either because other targets are more tempting or because bad guys are actually fairly rare.

Rigormortis Maxim: The greater the amount of rigor claimed or implied for a given security analysis, vulnerability assessment, risk management exercise, or security design, the less careful, clever, critical, imaginative, and realistic thought has gone into it.

Catastrophic Maxim: Most organizations mistakenly think about and prepare for rare, catastrophic attacks (if they do so at all) in the same way as for minor security incidents.

I am Spartacus Maxim: Most vulnerability or risk assessments will let the good guys (and the existing security infrastructure, hardware, and strategies) define the problem, in contrast to real-world security applications where the bad guys get to.

Methodist Maxim: While vulnerabilities determine the methods of attack, most vulnerability or risk assessments will act as if the reverse were true.

Rig the Rig Maxim: Any supposedly “realistic” test of security is rigged.

Tucker's Maxim #1 (Early Bird & Worm Maxim): An adversary is most vulnerable to detection and disruption just prior to an attack.

Comment: So seize the initiative in the adversary's planning stages.

Tucker's Maxim #2 (Toss the Dice Maxim): When the bullets start flying, it's a crapshoot and nobody can be sure how it'll turn out.

Comment: So don't let it get to that point.

Tucker's Maxim #3 (Failure = Success Maxim): If you're not failing when you're training or testing your security, you're not learning anything.

Gunslingers' Maxim: Any government security program will mistakenly focus more on dealing with force-on-force attacks than on attacks involving insider threats and more subtle, surreptitious attacks.

D(OU)BT Maxim: If you think Design Basis Threat (DBT) is something to test your security against, then you don't understand DBT and you don't understand your security application.

Comment: If done properly—which it often is not—DBT is for purposes of allocating security resources based on probabilistic analyses, not judging security effectiveness. Moreover, if the threat probabilities in the DBT analysis are all essentially 1, the analysis is deeply flawed.

It's Too Quiet Maxim: "Bad guys attack, and good guys react" is not a viable security strategy.

Comment: It is necessary to be both proactive in defense, and to preemptively undermine the bad guys in offense.

Nietzsche's Maxim: It's not winning if the good guys have to adopt the unenlightened, illegal, or morally reprehensible tactics of the bad guys.

Comment: "Whoever fights monsters should see to it that in the process he does not become a monster." Friedrich Nietzsche (1844-1900), *Beyond Good and Evil*. There are important lessons here for homeland security.

Patton's Maxim: When everybody is thinking alike about security, then nobody is thinking.

Comment: Adapted from a broader maxim by General George S. Patton (1885-1945).

Kafka's Maxim: The people who write security rules and regulations don't understand (1) what they are doing, or (2) how their policies drive actual security behaviors and misbehaviors.

By the Book Maxim: Full compliance with security rules and regulations is not compatible with optimal security.

Comment: Because security rules & regulations are typically dumb and unrealistic (at least partially). Moreover, they often lead to over-confidence, waste time and resources, create unhelpful distractions, engender cynicism about security, and encourage employees to find workarounds to get their job done—thus making security an "us vs. them" game.

Cyborg Maxim: Organizations and managers who automatically think "cyber" or

“computer” when somebody says “security”, don’t have good security (including good cyber or computer security).

Caffeine Maxim: On a day-to-day basis, security is mostly about paying attention.

Any Donuts Left? Maxim: But paying attention is very difficult.

Wolfe’s Maxim: If you don’t find it often, you often don’t find it.

He Who’s Name Must Never Be Spoken Maxim: Security programs and professionals who don’t talk a lot about “the adversary” or the “bad guys” aren’t prepared for them and don’t have good security.

Mahbubani’s Maxim: Organizations and security managers who cannot envision security failures, will not be able to avoid them.