Argonne NATIONAL LABORATORY

... for a brighter future

U.S. Department of Energy

UChicago ▸ Argonne LLC

A U.S. Department of Energy laboratory managed by UChicago Argonne, LLC

Physical Security Maxims

Roger G. Johnston, Ph.D., CPP

Vulnerability Assessment Team

Argonne National Laboratory
rogerj@anl.gov 630-252-6168
http://www.ne.anl.gov/capabilities/vat

Security Maxims

The following maxims, based on our experience with physical security, nuclear safeguards, & vulnerability assessments, are not absolute laws or theorems, but they will be essentially correct 80-90% of the time.

Argonne NATIONAL LABORATORY

Security Maxims

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).

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".

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

Security Maxims

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

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.

Schneier's Maxim #1: The more excited people are about a given security technology, the less they understand (1) that technology and (2) their own security problems.

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

Security Maxims

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.

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.

Security Maxims

Yipee 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".

Security Maxims

I Just Work Here Maxim: No salesperson, engineer, or executive of a company that sells 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.

Security Maxims

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.

Security Maxims

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

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

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

Plug into the Formula Maxim: Engineers don't understand security. They think nature is the adversary, not people. They tend to work in solution space, not problem space. They think systems fail stochastically, not through deliberate, intelligent, malicious intent.

Security Maxims

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: Few security devices, systems, or programs will ever be used properly.

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

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.)

Security Maxims

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.

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.

Security Maxims

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.

Security Maxims

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.

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.

Security Maxims

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.

Security Maxims

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.

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 has gone into it.

Security Maxims

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.

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

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

Security Maxims

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 and by whom). Plus you might even be ok if you get the threats all wrong. But if you focus mostly on the threats, you're probably in trouble.

Security Maxims

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".

Hopeless Maxim: The third most common excuse for not fixing security vulnerabilities is that "all security devices, systems, and programs can be defeated". (This is typically expressed by the same person who initially invoked the Mermaid Maxim.)

Security Maxims

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

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