



Nuclear Engineering Division



Never miss important updates of this file: download the original pdf at <http://www.ne.anl.gov/capabilities/vat/seals/maxims.html>

Security Maxims

by:

Roger G. Johnston, Ph.D., CPP

rjohnst@anl.gov, 630-252-6168

Argonne Vulnerability Assessment Team

Nuclear Engineering Division

Argonne National Laboratory

Web site: <http://www.ne.anl.gov/capabilities/vat/>

September 2011

Disclaimer

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor UChicago Argonne, LLC, nor any of their employees or officers, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of document authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof, Argonne National Laboratory, or UChicago Argonne, LLC.

Security Maxims

Roger Johnston
Vulnerability Assessment Team
Argonne National Laboratory

<http://www.ne.anl.gov/capabilities/vat>

*The truth will set you free, but first it will piss you off.
Mal Pancoast*

While these security maxims are not theorems or absolute truth, they are in our experience essentially valid 80-90% of the time in physical security and nuclear safeguards. They probably also have considerable applicability to cyber security.

Security Maxims by Roger G. Johnston | Last Updated: September 5, 2011

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: We think this is 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 or fault tree kind of problem, whereas the bad guys typically attack deliberately and intelligently, not randomly. For a discussion about using security methods to improve safety, 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.

Security Maxims by Roger G. Johnston | Last Updated: September 5, 2011

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

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

Comment: This quote is from Tom Baker as Doctor 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.

Comment: From security guru Bruce Schneier.

What a Deal Maxim: The introduction of high-tech security products into your security program will: (1) probably not improve your security, (2) almost certainly increase your overall security costs (though perhaps it will decrease inventory, shipping, or other business costs), and (3) probably increase security labor costs (with the sometimes exception of CCTV).

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

You Must Be High Maxim: Any security product that is labeled “high security” isn't.

That's Extra Maxim: Any given security product is unlikely to have significant security built in, and will thus be relatively easy to defeat.

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.

He Just Seems So Knowledgeable Maxim: Most organizations get the majority of their physical security advice from salespeople (who somehow seem to recommend their own products).

Tamper-Proof Maxim: Any claim by a salesperson about the performance of a physical security product (including the claim of absolute security) will be believed by default by the customer, while warnings about vulnerabilities or limitations by vulnerability assessors or others with first-hand experience will be met with incredulity.

Comment: This wishful thinking maxim is named in honor of the end user who told us that he knew his seals could not be spoofed because the manufacturer calls them “tamper-proof”.

Contrived Dualism/Dualism Maxim: The promoters of any security product meant to deal with any sufficiently challenging security problem will invoke a logical fallacy (called “Contrived Dualism”) where only 2 alternatives are presented and we are pressured into making a choice, even though there are actually other possibilities.

Comment: For example: “We found a convicted felon, gave him a crowbar, and he couldn't make the lock open after whaling on it for 10

Security Maxims by Roger G. Johnston | Last Updated: September 5, 2011

minutes. Therefore, the lock is secure.” Another example, “Nobody in the company that manufactures this product can figure out how to defeat it, and I bet you, Mr./Ms. Potential Customer [never having seen this product before in your life] can’t think up a viable attack on the spot. Therefore, this product is secure.”

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.

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

Comment: From security guru Bruce Schneier. 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”.

Could’ve, Would’ve, Should’ve Maxim: Security Managers will dismiss a serious vulnerability as of no consequence if there exists a simple countermeasure—even if they haven’t bothered to actually implement that countermeasure.

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 by Roger G. Johnston | Last Updated: September 5, 2011

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 (e.g., cryptography) 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. Ironically—and somewhat counter-intuitively—security is usually more effective when it is transparent. This allows for more discussion, analysis, outside review, criticism, and accountability.

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. Also, see Schryver's Law below.

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 are 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.

Security Maxims by Roger G. Johnston | Last Updated: September 5, 2011

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, and/or maximize your organization's ability to bounce back (resiliency).

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, GPS, and many so-called nuclear Material Control and Accountability (MC&A) programs

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.

Security Maxims by Roger G. Johnston | Last Updated: September 5, 2011

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 (which you probably will). But if you focus only on the threats, you're likely to be 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.

Pink Teaming Maxim: Most so-called "vulnerability assessments" are actually threat assessments, or some other exercise (like auditing) not well designed to uncover security vulnerabilities.

Comment: This is much more the case in physical security than in cyber security.

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

Often, the evidence offered that no security vulnerabilities exist is that the security manager who expresses this view can't personally imagine how to defeat the security.

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. A common variant of the hopeless maxim is "sure, we could implement that inexpensive countermeasure so that the average person on the street couldn't defeat our security with a bobby pin, but then the bad guys would just come up with another, more sophisticated attack".

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."

Security Maxims by Roger G. Johnston | Last Updated: September 5, 2011

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: From Derek Tabor. 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: From Derek Tabor. 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.

Security Maxims by Roger G. Johnston | Last Updated: September 5, 2011

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. From Craig Tucker.

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. From Craig Tucker.

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.

Comment: From Craig Tucker.

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.

Security Maxims by Roger G. Johnston | Last Updated: September 5, 2011

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*.

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.

30% Maxim: In any large organization, at least 30% of the security rules, policies, and procedures are pointless, absurd, ineffective, or actually undermine security (by either creating cynicism about security, or by driving behaviors that were not anticipated).

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 overconfidence, 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.

Aw Ditz Maxim: Mindlessly auditing if bureaucratic security rules are being followed will usually get confused with a meaningful security review.

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.

Comment: Perceptual blindness is a huge problem for security officers.

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.

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

Comment: Named for scholar and diplomat Kishore Mahubani. He meant to apply this general principle to politics, diplomacy, and public

Security Maxims by Roger G. Johnston | Last Updated: September 5, 2011

policy, but it is also applicable to security.

Hats & Sunglasses Off in the Bank Maxim: Security rules that only the good guys follow are probably Security Theater.

Merton's Maxim: The bad guys don't obey our security policies.

Comment: This maxim is courtesy of Kevin Sweere. It is named after Thomas Merton (1915-1968), a theological writer and philosopher.

Sweere's Maxim (Merton's Corollary): It's worse than that. The bad guys will analyze our security policies and regulations to find exploitable vulnerabilities, including those not envisioned by the good guys.

Wall Street Maxim: Every good idea is eventually a bad idea.

Dumbestic Safeguards Maxim: Domestic Nuclear Safeguards will inevitably get confused with International Nuclear Safeguards (treaty monitoring), including by people and organizations claiming to fully appreciate that the two applications are very different.

Comment: Domestic Nuclear Safeguards is a typical security application, just for very important assets. With International Nuclear Safeguards, in contrast, the bad guys own the assets and facilities of interest, and they fully understand the surveillance, monitoring, and safeguards equipment being used (and may even build, control, and/or install it). It is especially common to overlook or ignore the fact that the adversary in International Nuclear Safeguards is a country, with national- to world-class resources available to defeat the safeguards.

Red Herring Maxim: At some point in any challenging security application, somebody (or nearly everybody) will propose or deploy more or less pointless encryption, hashes, or data authentication along with the often incorrect and almost always irrelevant statement that "the cipher [or hash or authentication algorithm] cannot be broken".

Comment: Product anti-counterfeiting tags and International Nuclear Safeguards are two security applications highly susceptible to this fuzzy thinking.

With anti-counterfeiting tags, it is no harder for the product counterfeiters to make copies of encrypted data than it is to make copies of unencrypted data. They don't have to understand the encryption scheme or the encrypted data to copy it, so that the degree of difficulty in breaking the encryption (usually overstated) is irrelevant. Indeed, if there was a technology that could prevent cloning of encrypted data (or hashes or digital authentication), then that same technology could be used to prevent cloning of the unencrypted original data, in which case the encryption has no significant role to play. (Sometimes one might wish to send secure information to counterfeit hunters in the field, but the security features and encryption typically employed on cell phones or computers is good enough.)

What makes no sense is putting encrypted data on a product, with or without it including encrypted data about an attached unique anti-counterfeiting tag; the bad guys can easily clone the encrypted data without having to understand it. When there is a unique anti-counterfeiting tag on a product, only the degree of difficulty of cloning it is relevant, not the encryption scheme. The use of unique, one-of-a-kind tags (i.e., complexity tags) does not alter the relative unimportance of the encryption as an anti-counterfeiting measure.

Sometimes people promoting encryption for product anti-counterfeiting vaguely have in mind an overly complicated (and usually incomplete/flawed) form of a virtual numeric token ("call-back strategy"). ([See RG Johnston, "An Anti-Counterfeiting Strategy Using Numeric Tokens", International Journal of Pharmaceutical Medicine **19**, 163-171 (2005).]

Encryption is also often thought of as a silver bullet for International Nuclear Safeguards, partially for reasons given in the Dumbestic Safeguards Maxim. The fact is that encryption or data authentication is of little security value if the adversary can easily break into the equipment holding the secret key without detection (as is usually the case), if there is a serious insider threat that puts the secret encryption key at risk (which is pretty much always the case), and/or if the surveillance or monitoring equipment containing the secret key is designed, controlled, inspected, maintained, stored, observed, or operated by the adversary (as is typically the case in International Nuclear Safeguards).

It's Standard Maxim: As a general rule of thumb, about two-thirds of security "standards" or "certifications" (though not "guidelines") make security worse.

Security Maxims by Roger G. Johnston | Last Updated: September 5, 2011

Alice Springs Maxim: Organizations will be loathe to factor in local, on-the-ground details in deciding what security resources to assign to a given location or asset. One-size-fits-all will be greatly preferred because it requires less thinking.

Comment: This maxim is named after the standard reassurance given to worried tourists in Australia that “there aren’t a lot of shark attacks in Alice Springs”.

Follow the Money Maxim: Security attention and resources will usually be doled out in proportion to the absolute dollar value of the assets being protected, not (as it should be) in proportion to the risk.

Laws

The following are general “laws” that also apply to security:

Fudd’s Law: If you push on something hard enough, it will fall over.

First Law of Revision: Information necessitating a change of design will be conveyed to the designers after—and only after—the plans are complete.

Hellrung’s Law: If you wait long enough, it will go away.

Grelb’s Law: But if it was bad, it will come back.

Brien’s First Law: At some time in the life cycle of virtually every organization, its ability to succeed in spite of itself runs out.

Bucy’s Law: Nothing is ever accomplished by a reasonable person.

Stewart’s Law: It is easier to get forgiveness than permission.

Horngren’s Law: The Real World is a special case.

Glazer’s Law: If it says “one size fits all”, then it doesn’t fit anybody.

Gold’s Law: If the shoe fits, it’s ugly.

Firestone’s Law: Chicken Little only has to be right once.

Shaw’s Law: Build a system that even a fool can use, and only a fool will want to use it.

Byrne’s Law: In any electrical circuit, appliances and wiring will burn out to protect the fuses.

Security Maxims by Roger G. Johnston | Last Updated: September 5, 2011

Ginsberg's Laws from the beat poet Allen Ginsberg (1926-1997):

The First Law of Thermodynamics: "You can't win."

The Second Law of Thermodynamics: "You can't break even."

The Third Law of Thermodynamics: "You can't quit."

Putt's Law: Technology is dominated by two types of people: those who understand what they do not manage, and those who manage what they do not understand.

Clarke's First Law: When a distinguished but elderly scientist states that something is possible, he is almost certainly right. When he states that something is impossible, he is very probably wrong.

Hawkin's Law: Progress does not consist of replacing a theory that is wrong with one that is right. It consists of replacing a theory that is wrong with one that is more subtly wrong.

Schryver's Law: Sufficiently advanced incompetence is indistinguishable from malice.

Kernighan's Law: Debugging is twice as hard as writing the software in the first place. Therefore, if you write the software as cleverly as possible, you are (by definition) not smart enough to debug it.