Viewpoint Paper

Changing Security Paradigms*

Roger G. Johnston
Vulnerability Assessment Team, Nuclear Engineering Division
Argonne National Laboratory

Any field is molded and constrained by its paradigms. A "paradigm" can be defined as:
(1) a pattern, example, or model;
(2) a mode of thought or practice;
or
(3) an overall concept or strategy accepted by most people in a given field.

The field of security relies on a number of paradigms, both stated and unstated. Many of these are in the process of changing—or at least should change—in order to adapt to a rapidly changing world and to improve security effectiveness.

This paper offers a brief, bulleted list of some security paradigms that I believe (perhaps currently more out of wishful thinking than empirical evidence) are in the process of changing. The new paradigms I identify here will, I believe, ultimately win out in the end over the old paradigms because they will result in better security. In my view, these emerging changes are worth monitoring and even carefully researching.

Security Paradigm 1 (The Nature of Security)

Old Paradigm:
• Security is binary: an asset is either secure or it is not.
• Check Box mentality.
• There is a minimum level of adequate security and we know what it is.
• There's a right way to do security, and there shouldn't be a lot of questioning.

New Paradigm:
• Security is a continuum, not black & white.
• Nobody knows how much security is "enough".
• Everything is a tradeoff.
• Security should be controversial and open for debate, as should any challenging, complex and important responsibility.

* Editor's Note: This paper was not peer-reviewed. This work was performed under the auspices of the United States Department of Energy (DOE) under contract DE-AC02-06CH11357. The views expressed here are those of the author and should not necessarily be ascribed to Argonne National Laboratory or DOE.

Security Paradigm 2 (Vulnerabilities)

Old Paradigm:
• Find all the vulnerabilities and eliminate them.
• Vulnerabilities are bad news.

New Paradigm:
• There are too many vulnerabilities to find them all, much less eliminate them all.
• Try to find those that are easiest to exploit, most likely to be exploited, and/or easiest to fix.
• We must still manage the vulnerabilities we haven't eliminated, or know nothing about.
• Finding a vulnerability is good news, not bad news, because having found one, we can potentially do something about it. If we're ignorant of it, however, we probably can't fix it.

Security Paradigm 3 (Vulnerability Assessments)

Old Paradigm:
• Vulnerability Assessments (VAs) are done once every 1-5 years.
• Do it right once, and you can phone in future VAs.

New Paradigm:
• A VA is a dynamic, ongoing process that happens every day.
• Vulnerabilities (and our recognition of them) change rapidly with new technologies, different security personnel and adversaries, changing priorities, and improved understanding.

Security Paradigm 4 (Changing Vulnerabilities)

Old Paradigm:
• Vulnerabilities are relatively static.

New Paradigm:
• Vulnerabilities (or our understanding of them) change rapidly over time with new personnel, missions, adversaries, technologies, and insights.
• Fix one vulnerability, and you'll likely introduce multiple new ones or change the old ones.

Security Paradigm 5 (The Purpose of a Vulnerability Assessment)

Old Paradigm:
• A VA is a test you "pass", or a "certification" you receive.

New Paradigm:
• A VA is for the purpose of improving security.
• "Passing" or "Failing" has little meaning.

Security Paradigm 6 (Minor Vulnerabilities)

Old Paradigm:
• Focus on the serious vulnerabilities (easiest to exploit, most likely to be exploited, worst consequence).
• Ignore minor ones.

New Paradigm:
• If the minor vulnerabilities are easy to fix or mitigate, do so because we might be wrong about them being minor, or there might be related serious vulnerabilities that we've overlooked.

Security Paradigm 7 (Audits)

Old Paradigm:
• We insure good security through security surveys and audits: reviewing the security policies, checking on how well security personnel know and follow the rules, and auditing compliance with regulations, guidelines, and policies.
• Focus on the existing security measures, plans, policies, and strategies, and on the currently deployed hardware and software.

New Paradigm:
• We improve security through VAs: finding vulnerabilities and suggesting countermeasures.
• We avoid being overly focused on Plans & Compliance.
• We don't let the good guys and the current security posture define the security problem. The bad guys get to do this.

Security Paradigm 8 (Threats vs. Vulnerabilities)

Old Paradigm:

• Threats (who might attack, when, where, and with what resources and probabilities) are more important to understand than Vulnerabilities (weaknesses in security).

New Paradigm:
• Typically vulnerabilities trump threats: If you get the vulnerabilities right, you are probably ok if you get the threats wrong (which is easy to do because you are mostly speculating). But knowing the threats without understanding the vulnerabilities isn't very helpful.

Security Paradigm 9 (Threat Assessments vs. Vulnerability Assessments)

Old Paradigm:
• A Threat Assessment is a Vulnerability Assessment.

New Paradigm:
• Threat Assessments and Vulnerability Assessments are two different activities, both of which contribute to overall Risk Management (along with understanding assets, consequences if those assets are attacked, etc.).

Security Paradigm 10 (Features & Vulnerabilities)

Old Paradigm:
• Vulnerabilities exist independent of attacks.
• Facility features, structures, entry points, and missing security measures are vulnerabilities.

New Paradigm:
• Potential attacks are the vulnerabilities.
• Facility features, structures, entry points, and missing security measures are relevant only to the extent that they can play a role in an attack.
• A facility feature is not a vulnerability independent of the various attack scenarios that can utilize it.

Security Paradigm 11 (Formalism, Rigor, & Perspective for Vulnerability Assessments)

Old Paradigm:
• VAs should be formal, rigorous, objective, consistent, and reproducible.
• They should be from the perspective of the existing security deployment.

New Paradigm:
• VAs must be creative, subjective, intuitive, and done from the perspective of the bad guys.
• Formalistic (checklist) methods can still be used as a starting point, but we need to watch out for sham rigor, the fallacy of precision, and the fact that most vulnerabilities are critically dependent on local details and personnel.

Security Paradigm 12 (Vulnerability Assessment Personnel)

Old Paradigm:
• Only security experts trained in the formalism can participate in a Vulnerability Assessment.

New Paradigm:
• Clever, creative, hands-on, hacker and loophole finders familiar with the facility or organization should also be involved, even if not security professionals.

Security Paradigm 13 (Vulnerability Assessment Follow-up)

Old Paradigm:
• Vulnerability Assessors are finished once vulnerabilities or non-compliances are identified.

New Paradigm:
• (The same) Vulnerability Assessors are brought back after countermeasures are deployed to see if they are effective, and to determine what new vulnerabilities have been introduced as a result.

Security Paradigm 14 (Compliance)

Old Paradigm:
• Compliance gets us good security.

New Paradigm:
• Compliance—though it may be necessary and can be of value—often causes distractions, gets in the way of good security, or can even be wholly incompatible with it.
• Common sense and true security must trump security rules.
• If a given security rule truly makes sense for a given situation, enforce it. If, however, it is stupid or there is a better way, get rid of it, change it, or authorize an exception.

Note: Examples of Compliance Harming Security
- *All the paperwork, bureaucracy, data recording, & preparation for audits causes distractions and wastes resources.*
- *Creates wrong mindset: Security = Busy Work; Mindless rule-following; the Brass are responsible for security strategies & tactics, not me.*
- *An over-emphasis on fences (4.5 – 15 sec delay), entry points, and force-on-force attacks that leads to bad security.*
- *Background checks & polygraphs are the only recognized countermeasures to the Insider Threat.*
- *Security clearances require self-reporting of professional social or mental health counseling, thus discouraging such counseling.*
- *The rules require overly predictable guard patrols & shift changes.*
- *Little room for flexibility, individual initiative, hunches, resourcefulness, observational skills, or people skills among security personnel.*

Security Paradigm 15 (Confidence)

Old Paradigm:
• If we're in good compliance, we can feel fairly confident about our security.
• Security is almost guaranteed if everybody will do his/her job.

New Paradigm:
• Even if we're in compliance, we need to feel scared. Confidence is always over confidence.
• Security is difficult, and may not be fully possible.

Security Paradigm 16 (Special Cases)

Old Paradigm:
• Security Managers, Auditors, & Vulnerability Assessors frown on exemptions and special cases.

New Paradigm:
• Security Managers, Auditors, & Vulnerability Assessors encourage exemptions and special cases (and the independent, local reasoning they entail) when this improves acceptance, productivity, and security.

Security Paradigm 17 (Training Security Personnel)

Old Paradigm:

• Training for security personnel is mostly about making them understand security rules, policies, and procedures.
• Performance for security personnel is measured by how well they adhere to security rules, policies, and procedures

New Paradigm:
• Training for security personnel emphasizes "What if?" exercises (mental and field practice).
• Performance for security personnel is measured by how effectively and resourcefully they deal with day-to-day real-world security issues, and with "What if?" exercises.

Security Paradigm 18 (Security Awareness Training for Employees)

Old Paradigm:
• Security Awareness Training for general employees is for the purpose of threatening and intimidating them into compliance with the rules.

New Paradigm:
• Security Awareness Training seeks to motivate and educate general employees about security, and seeks their help.
• The emphasis is on what's in it for them, the organization, and the country.

Note: Effective Security Awareness Training
+ *We train dogs. We educate, remind, encourage, motivate people.*
+ *It should promote, sell, & motivate good security by employees, contractors, and vendors.*
+ *Use examples. Show people how to do things, don't tell them what not to do.*
+ *Avoid the negative terms: Don't! Never! No!*
+ *What's in it for me?*
+ *Make connections to personal security: home computer security, burglary, identity theft, etc.*
+ *Refer to news stories about security breaches in other organizations and the consequences.*
+ *Have metrics for effectiveness of the training (and the security)*
+ *No dumb trivia questions on the quiz, e.g., "Who is head of Department S-47?"*
+ *Use people-oriented instructors, not bureaucrats, technocrats, burnouts, zombies, or dead wood.*
+ *Be entertaining, vivid, & positive, NOT threatening, boring, patronizing, or full of organizational charts, talking head videos with camera-challenged executives, references to federal CFRs, or self-serving fluff about HR, the security organization, senior managers, or the training department.*
+ *Comedy, Violence (verbal, physical, or implied), & Sexiness are memorable.*
+ *Less is more. Stick with the most important security issues.*
+ *Security Awareness posters should offer useful security tips & solutions, not*

platitudes, mindlessness, insults, & threats. They should be designed so that they are not the target of ridicule, scorn or vandalism.

Security Paradigm 19 (People)

Old Paradigm:
• Process and Technology (in that order) are our main tools for providing security.

New Paradigm:
• People and Process (in that order) are our main tools (though Technology can help).

Security Paradigm 20 (Who Provides Security)

Old Paradigm:
• Trained security personnel provide security.
• Regular employees, contractors, & visitors are the enemies of good security.

New Paradigm:
• (The Insider Threat not withstanding) regular employees, contractors, visitors, and neighbors provide security, with help from trained security professionals.

Security Paradigm 21 (Security Experts)

Old Paradigm:
• Security managers and security consultants are the main experts on Security.

New Paradigm:
• Frontline security personnel and regular employees are the main experts on local Security.

Security Paradigm 22 (Hazing as a Metric)

Old Paradigm:
• Security is painful and must inconvenience and hassle employees, contractors, visitors, & customers if it is to be effective.
• Hassling is a metric for security effectiveness.

New Paradigm:

• Security must not interfere with productivity any more than necessary.
• Once Security becomes the enemy of productivity and employees, all is lost and the bad guys have partially won.
• Employee acceptance is one metric for effective Security.

Security Paradigm 23 (Insider Threat Mitigation)

Old Paradigm:
• Ignore or under-estimate the Insider Threat.
• Deploy minimal (or no) countermeasures.
• Don't consider employee disgruntlement as an important Insider Threat issue, or something that can be mitigated.

New Paradigm:
• Use proactive countermeasures for the Insider Threat, including mitigation of employee disgruntlement.
• Recognize that domestic violence is often brought into the workplace.

Security Paradigm 24 (Due Diligence)

Old Paradigm:
• Due Diligence is doing the absolute minimum we can get away with, or what keeps us out of trouble with juries, or what similar facilities do, or what the rules, regulations, and guidelines specify, or what higher-ups and auditors make us do.

New Paradigm:
• Due Diligence is providing the best security we can.

Security Paradigm 25 (High Technology as a Silver Bullet)

Old Paradigm:
• Technology will solve some or all of my security problems.
• High tech = high security.

New Paradigm:
• Technology solves nothing (though it can be a useful tool).
• High-tech security devices, systems, and programs are often the easiest to defeat (with low-tech methods).

Security Paradigm 26 (The Past as a Guide to the Future)

Old Paradigm:
• Past security incidents (at my facility or others that are similar) are the best guide to future ones.

New Paradigm:
• Past security incidents may be a good place to start thinking about security, but they are not enough. Future catastrophic security incidents (especially terrorist attacks) often haven't occurred previously, plus each facility and security application is unique.

Security Paradigm 27 (Prevention vs. Mitigation, Recovery, and Resiliency)

Old Paradigm:
• Focus on Prevention
• Reactive security
• We prepare to fight the last war
• Scapegoating, fingerpointing, & over reaction after a serious security incident
• Panic-mode chasing after snake oil "solutions" and fads.

New Paradigm:
• Focus on Prevention, Mitigation, Recover, & Resilience
• Proactive security
• We prepare to fight the next war
• Learn from security incidents, with increased commitment after a serious incident, not retribution
• Do intelligent analysis and R&D for long-term solutions

Security Paradigm 28 (Layered Security)

Old Paradigm:
• Layered Security ("Security is Depth") is a mindlessly applied approach when security managers and organizations wish to avoid thinking carefully, critically, and creatively about security.
• "We have layered security" is the automatic knee-jerk response when any new vulnerabilities are discovered or there are security concerns or questions.

New Paradigm:
• Layered Security is implemented only after a careful analysis of the purpose of each layer, and how the various layers interact and support or interfere with each other.
* Having multiple layers is never used as an excuse to stop thinking, or avoid improving any one layer or the overall effectiveness of security.

Security Paradigm 29 (Perceptual Blindness)

Old Paradigm:
• The fact that people (including security guards, and seal & safeguards inspectors) are remarkably poor observers (and don't fully realize it) is not factored into security strategies.
• The power of misdirection, distraction, and sleight-of-hand is not appreciated.

New Paradigm:
• The lessons from 50 years of experiments by cognitive psychologists are taken to heart and the fact that people are lousy observers and aren't fully aware of it will be factored into any security plan.
• Countermeasures to perceptual blindness are developed and deployed, including the effective use of technology to overcome human perceptual and cognitive weaknesses.
• Awareness training about misdirection, distraction, and sleight-of-hand is common for security guards, inspectors, and other security professionals.

Security Paradigm 30 (Security Theater)

Old Paradigm:
• Security Theater (fake security for show) is often preferred over real security because it is easier and takes less thought.

New Paradigm:
• Security Theater is easy to spot using effective vulnerability assessments and/or by its characteristic attributes. (See, for example, RG Johnston and JS Warner, "Security Theater in Future Arms Control Regimes", Proceedings of the 51st INMM Meeting, Baltimore, MD, July 11-15, 2010.)

Security Paradigm 31 (Cognitive Dissonance)

Old Paradigm:
• Cognitive Dissonance—the mental tension between what we want to be true (we have good security) and what is likely to be true (there are problems)—is a major impediment to good security and security improvements.

New Paradigm:
• The signs of cognitive dissonance are recognized and the dangers are neutralized. These dangers include *self-justification* (self-serving rationalization and excuse making),

paralysis or *stagnation* (failure to confront serious problems or make necessary changes), *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).

Security Paradigm 32 (Security Culture & Climate)

Old Paradigm:
• The importance of having a healthy Security Culture is given lip service, but the concept is ill-defined and under-analyzed.

New Paradigm:
• Security Culture & Climate and their effects on security effectiveness are carefully considered, thoroughly analyzed, and fully appreciated.

Security Paradigm 33 (Security Standards)

Old Paradigm:
• Security Standards often institutionalize misleading terminology and sloppy practice.
• They tend not to be researched based, and frequently over simplify complex issues, and discourage careful, critical, and creative thinking about security issues.
• Security Standards are often manufacturer-dominated and used as weapons to exclude competitors and discourage alternate approaches (rather than encouraging compatibility and mutual cooperation).
• The "certifications" that get institutionalized are often meaningless.
• The standards can make security products and practices worse, and can be very difficult to modify or improve once in place.
• The claimed consensus is often illusionary.

New Paradigm:
• Security Standards avoid the problems of inflexibility, one-size-fits-all thinking, over simplification, and domination by special interests.
• Security efficacy, product quality, careful thinking, understanding, compatibility, and mutual cooperation are all enhanced by the Security Standard, not degraded.
• Sound terminology and best practices are encouraged.

Note: In my view, the recently instituted ISO Standard 17712 for mechanical seals (http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41017) is a good, bad example of a severely flawed security standard that may even be dangerous.

Security Paradigm 34 (Control)

Old Paradigm:
• Control is Security.

New Paradigm:
• Control should not get confused with Security, and should be avoided to the extent practical.
• Privacy rights and civil liberties must be protected in any security program.
• We don't win against terrorists by becoming like them, or violating our fundamental principles and values.