



Nuclear Engineering Division



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

# Devil's Dictionary of Security Terms

by:

Roger G. Johnston, Ph.D., CPP

 [rjohnst@anl.gov](mailto: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/>

February 2013

## 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.

# Devil's Dictionary of Security Terms

February 2013  
Roger Johnston  
Vulnerability Assessment Team  
Argonne National Laboratory

**Chief Security Officer (CSO):** The manager we marginalize, under-fund, and then blame for security incidents.

**contract guard force:** We can blame somebody else for the incompetence of the guards.

**proprietary guard force:** Our guards view their job as some kind of entitlement.

**Post 9/11:** The time period when we could all stop thinking profoundly about security.

**We stand behind our product:** That's the only safe place to stand.

**impossible to defeat:** Trivial to defeat.

**high security product:** Not a high security product.

**high technology:** (1) The owner's manual is badly written. (2) An excuse to stop thinking about security.

**the next generation:** Our components are so old, we can't buy them anymore.

**Our product has undergone extensive testing:** It hasn't.

**X is a recognized security expert:** Incredibly, X has somehow managed to stay employed in security for a number of years.

**proactive security:** We send around a lot of memos.

**convergence:** People from the IT and Security Departments now have even more issues to squabble over.

**We want to follow a middle path between due diligence and paranoia:** We don't want to hear about any #&!@!# vulnerabilities.

**We will take these recommendations under advisement:** We won't.

**security awareness training:** Presentations that convince employees who once vaguely thought that security might be a good idea that they were sadly mistaken.

**counter-intelligence program:** Our security awareness training is so awful, it insults everyone's intelligence.

**counter-intelligence officer:** Someone who doesn't want to hear about your security concerns because they will only make his job more difficult.

**insider threat:** We can't handle the external threats, so we'll threaten our co-workers as a distraction.

**security plan:** Looking busy.

**security official:** Someone who won't let security get in the way of doing his job.

**nuclear inspection:** Looking busy.

**nuclear material control and accountability (MC&A):** An inventory system for nuclear material that is so devoid of security features and so utterly susceptible to spoofing that nobody can reasonably draw any meaningful conclusions about theft or diversion.

**security metrics:** (1) The creative use of numbers to justify more funding. (2) Made up numbers to make it look like we are doing something.

**ROI (Return on Investment):** The creative use of numbers to justify more funding.

**RFID:** An itty, bitty magical device that solves all security problems.

**polygraph (“lie detector”):** A device invented by William Marston in the 1920’s with about as much grounding in reality as his other major invention (Wonder Woman).

**encryption/data authentication/digital signatures:** (1) Magical techniques for engendering irrational confidence in the security or veracity of data being exchanged between two devices or systems, each designed, constructed, programmed, owned, operated, controlled, and maintained by personnel who are utterly untrustworthy. (2) An imaginary silver bullet for dealing with any challenging security problem.

**quantum cryptography:** Maybe quantum mechanics can make up for our utter lack of security.

**All security devices, systems, and programs can be defeated:** But not ours.

**due diligence:** Doing the minimum we can get away with and still avoid major jury awards.

**best practice:** Those guys don’t know what the hell they are doing either, but at least they seem confident.

**industry standard:** Badly done.

**industry leader:** More at fault for lousy security than almost anybody else.

**security standard:** A committee of special interests tries to legitimize bad practice and sloppy terminology through formal means.

**secret password:** Any password that the user forgets because nobody can remember 16 gibberish characters.

**public key:** We can’t keep the key secret so it’s pretty much floating around among the general public.

**private key:** I humorously made up a key that is a string of obscenities and must now keep it secret to avoid getting in trouble.

**key control (encryption):** Some cockamamie scheme or other for getting keys to only the authorized personnel.

**key control (physical security):** All the high-security keys are stored in 1 cabinet which can be easily picked open.

**keyless entry:** If you poke the door with a credit card or paper clip, it will open.

**keyed alike:** We screwed up and made every lock open with 1 key.

**keyed different(ly):** Somehow, none of our keys opens any of our locks.

**TSA approved lock:** The TSA certifies that this luggage lock offers no security whatsoever.

**hinges:** Hardware on a door that allows the door to swing open. Typically located on the same side of the door as the lock or seal.

**hasp:** The flimsy, poorly designed, and badly corroded hardware through which a lock or seal is passed.

**tamper-proof seal:** We and/or our customers don't really understand tamper detection.

**tamper-resistant seal:** We and/or our customers don't really understand tamper detection.

**high security seal:** We and/or our customers don't really understand tamper detection.

**This is a security seal and this is an indicative seal:** We and/or our customers don't really understand tamper detection.

**unique seal serial number:** It's unlikely a seal in this order has the same serial number.

**ISO 17712 Seal Standard:** People (who seem confused about what a tamper-indicating seal is) define simple-minded, arbitrary, and irrelevant "testing" standards for them.

**seal inspection:** Looking busy.

**electronic seal:** A type of tampering-indicating seal that frees up the seal inspector from having to worry about whether the seal was smashed open, if there is a large hole in the container, or if the door was ever closed.

**cargo security:** Busy work that keeps the insurance company happy.

**real-time monitoring/intrusion alarm:** Our guard force ignores the evidence of nefarious activity immediately, rather than at a later time.

**tamper-evident packaging:** A strategy for reducing jury awards when tampering inevitably happens.

**product tampering:** Well these things happen.

**product counterfeiting:** Our main concern is the safety of our customers. (Of course, the millions of dollars in lost sales are irrelevant.)

**product anti-counterfeiting tag:** Something a manufacturer or product counterfeiter places on a product to make the customer think it is authentic.

**hologram:** A pretty, color-changing silvery sticker that hypnotizes the customer or shop clerk into thinking the product is authentic.

**color shifting:** Our printing processes are so poor, you never know what color(s) you will end up with.

**unique identifier:** A technique or technology so lame, nobody else bothers with it.

**biometric verification vs. identification:** You tell us who you are first, before we calculate who you are.

**surveillance camera:** A video system with such poor resolution, you couldn't recognize your own mother.

**CCTV (closed circuit television):** A video system designated as "closed circuit" to distinguish it from broadcast TV, which the guys in the guard station are really watching.

**security integrator:** A vendor who can wire together a bunch of security hardware in a manner that doesn't trip the circuit breakers.

**dual technology:** Incorporating a second technology to distract the end user from the inadequacies of the first technology, and from questioning the overall efficacy of the security product.

**passive infrared detector (PIR):** A security device that doesn't do much.

**motion detector:** A device to detect if employees are inappropriately playing Frisbee or tossing around a nerf basketball when they should be working.

**risk management:** We collect all our wishful thinking, denial, and ignorance about security in one place, ideally accompanied by impressive looking matrices and lots of rankings/probabilities we made up.

**Design Basis Threat:** Maybe if we string together 3 nouns without adjectives so that it sounds like gibberish, a blatantly obvious concept will seem profound.

**threat matrix:** Maybe if we put the superficially obvious in a table, along with random rankings and numbers, it will look profound.

**loss event probability:** The odds of theft, made up by guys so far removed from reality that they call it a "loss event".

**vulnerability assessment:** (1) A rubber stamp approval of our previous choice of security products, vendors, or strategies. (2) We found some guys who, for sufficient money, reported that no parts are missing. (3) A threat assessment where we are confused about the difference between threats and vulnerabilities.

**We use the X method for threat/vulnerability assessment:** We'll pretty much go to any lengths to avoid thinking profoundly & creatively about security.

**vulnerability assessors:** Wise-guy troublemakers who appreciate the value of nothing, especially hard work.

**red team:** The wise guys flagged for retaliation.

**resilience:** We're flexible as to whom we will name as the scapegoat(s) after the next serious security incident.

**chain of custody:** A piece of paper, never to be examined, on which arbitrary individuals illegibly scribble their initials or signature for the purpose of making it look like we have some kind of security procedure in place.

**countermeasure:** A half-baked, token attempt to deal with the gaping holes in our security.

**secret:** Our security procedures are such a joke, we have to keep them hidden out of sheer embarrassment.

**civil liberties:** We will be polite while we take liberties with your Constitutional rights.

**security in depth (layered security):** We're desperately hoping that multiple layers of lousy security will somehow magically add up to good security.

**compliance-based security:** We cleverly switch our responsibility towards compliance, rather than security (which is hard).

**satisfy the auditors:** We've pretty much given up trying to provide good security.

**spam:** Emails generated by anybody but you.

**zero-day attack:** The time origin for the start of a malware attack, designated as "zero-day" because we haven't actually thought about security prior to this time.

**intrusion:** Access by unauthorized personnel that we unfortunately managed to detect despite our best efforts to stay blissfully ignorant.

**end user:** (1) The sucker or poor sap who buys/uses our security products. (2) The place or person where common sense, accountability, and any concept of security cease.

**security culture:** Something we automatically say is critical for good security, but haven't bothered to think about or analyze.

**tailgating/piggybacking:** A frowned upon practice unless you are late for work.

**embedded system:** (1) A product that incorporates computers or microprocessors that are buried as deep as possible inside the product in hopes that the end user won't discover the software bugs, security flaws, design blunders, and general incompetence. (2) A product that employs a computer or microprocessor dedicated to a specific task because the developer is not clever enough to write multi-tasking code. (3) A product that contains a computer with way too much computing power for the relevant application—thus increasing marginal cost and opening up all kinds of unnecessary security vulnerabilities—because the developer is too lazy to develop an interface to the end user on a simple microprocessor.