How to Spot Security Theater*

Roger G. Johnston, Ph.D., CPP
Vulnerability Assessment Team
Argonne National Laboratory
http://www.ne.anl.gov/capabilities/vat

Bruce Schneier coined the term "Security Theater" to describe the situation where phony security measures provide a feeling of improved security, but in reality provide little or no actual security.[1,2] Another name for Security Theater is "Ceremonial Security".

As a vulnerability assessor, I frequently find Security Theater across a wide range of different physical security devices, systems, and programs, as well as in domestic and international nuclear safeguards. It's important to realize, however, that Security Theater is not automatically a bad thing. It can present the appearance (false though it may be) of a hardened target to potential adversaries, thus potentially discouraging an attack (at least for a while). Security Theater can reassure the public while more effective measures are under development, and help encourage employees and the public to take security seriously.

In international treaty monitoring and verification, Security Theater can help foster an environment of transparency, trust, confidence-building, and international cooperation. Security Theater can provide great photo opportunities for national leaders trying to promote disarmament regimes that may face intense political opposition. It can also serve as a first step in creating new regimes (because Security Theater is always easier than real security). During treaty negotiations, Security Theater can serve as an easy-to-negotiate stand-in for more rigorous security and safeguards procedures to be developed and negotiated in the future. Perhaps most importantly, Security Theater can provide an excuse to get inspectors inside nuclear facilities where their informal observations and interactions with host facility personnel can be of great value to disarmament, nonproliferation, and safeguards efforts.

The real problem occurs when Security Theater is not recognized as such, or when it stands in the way of good security or is actually preferred over real security (because it is easier).

* Reprinted with permission from the Editor's Comments of the Journal of Physical Security, JPS **4**(2), i-viii (2010), http://jps.anl.gov

The best way to spot Security Theater is to critically analyze the security it purports to offer. This, however, takes a lot of work. An easier way is to look for the attributes commonly found with Security Theater. The following is my list. If a third or more of these attributes reasonably apply to a given security device, system, measure, or program, it is likely to be Security Theater. The more the attributes apply, and the more of them that apply, the more likely you are looking at Security Theater, not real Security.

(For more information, see reference [3].)

The Security Theater Attributes Model:

The following are the typical attributes of products, technologies, measures, programs, and procedures that are Security Theater. They are listed in no particular order.

1. There is great urgency to get something out in the field, or at least its acceptance negotiated.

2. The promoters and developers of the technology or procedure earnestly—even desperately—want it to solve the security or verification problems. (Strong proponents of nuclear disarmament and nonproliferation efforts often intensely wish, quite admirably, to make the world safe from nuclear hazards. This can sometimes lead to wishful thinking.[4,5])

3. There is considerable enthusiasm for, great pride in, and strong emotion behind the proposed (or fielded) technology or procedure.

4. The technology or procedure is a pet technology of the promoters and developers, not necessarily the technology or procedure that was chosen from among many candidates as a result of a careful, holistic study of the specific security/safeguards/verification problem of interest.

5. The security/safeguards/verification technology or procedure is viewed with great confidence, arrogance, and/or is represented as “impossible defeat” or nearly so. (Effective security is very difficult to achieve. Generally, if promoters and developers of a given security or safeguards approach or hardware have carefully considered the real-world security issues, they will not be in such a boosterism mode. Fear is, in fact, a good indicator of a realistic mindset when it comes to security.)

6. There is a great deal of bureaucratic or political inertia behind the technology or procedure.

7. Substantial time, funding, and political capital has already been spent developing, promoting, or analyzing the technology or procedure.

8. The people or organization promoting the technology or procedure have a conflict of interest, or at least are unable to objectively evaluate it.

9. No vulnerability assessors, people with a “hacking” mentality, devil’s advocates, outsiders, or creative question-askers have closely examined the technology or procedure (perhaps because they weren’t allowed to).

10. Anybody questioning the efficacy of the technology or procedure is ignored, attacked, ostracized, or retaliated against.

11. The people developing or promoting the technology or procedure have no real-world security experience.

12. The people developing or promoting the technology or procedure are mostly engineers. (No insult to engineers intended here. In our experience, the mindset and practices that makes one good at engineering aren’t the optimal mindset for good security. Engineers tend to work in solution space, not problem space. They tend to view Nature and stochastic failures as the adversary, not maliciously evil people who attack intelligently and surreptitiously. Engineers strive to design devices, hardware, and software that are user friendly, easy to service, and full of optional features—which tends to make attacks easier.)

13. Vulnerabilities are only considered, and vulnerability assessors only involved, after the development of the technology or procedure has been nearly completed. (At this point, it is usually too difficult to make necessary changes to improve the security for economic, political, timeliness, inertia, or psychological reasons).

14. The technology or procedure involves new technology piled on existing technology or procedures in hopes of getting better security, but without actually addressing the Achilles heel of the old technology or procedures.

15. The technology or procedure relies primarily on complexity, advanced technology, the latest technological “fad”, and/or multiple layers. (High technology does not equal high security, and layered security—so called “security in depth”—isn’t always better.[6,7])

16. Any consideration of security issues focuses mostly on software or firmware attacks, not on physical security, and only on high-tech attacks (even though low-tech attacks are usually sufficient, even against high-tech devices or systems [6].)

17. The main tamper detection mechanism—if there even is one—is a mechanical tamper switch or an adhesive label seal. (This is approximately the same, in our experience, as having no tamper detection at all.[8])

18. The technology or procedure is not directed against a specific, well-defined adversary with well-defined resources and goals.

19. Front line security personnel and the end users of the technology or procedure have never been consulted and/or the technology or procedure is being forced on them from above. (These are the people who understand the real-world implementation issues, and are the ones who will have to make the technology or procedure actually work).

20. The technology or procedure is not well understood by the non-technical people proposing or promoting it (or by the people in the field who are to use it), and/or the terminology being used is misleading, confusing, sloppy, or ambiguous.

21. Particularly with security procedures: control or formalism gets confused with security.

22. Domestic and international nuclear safeguards get confused. (These two security applications are remarkably dissimilar.[9,10])

23. The technology or procedure in question makes people feel good. (In general, real security doesn't make people feel better, it makes them feel worse. This is because it is almost always more expensive, time-consuming, and painful than Security Theater. When security or safeguards are thoroughly thought-through, the difficulty of the task and knowledge of the unmitigated vulnerabilities will cause alarm. Fear is a good vaccine against arrogance, complacency, and ignorance. This is the basis of what we call the "Be Afraid, Be Very Afraid Maxim"[11]: If you're not running scared, you have bad security or a bad security product.)

24. The use protocols for the technology or procedures are non-existent, vague, or ill-conceived.

25. The security application is exceeding difficult, and total security may not even be possible.

26. The terminology is vague, confusing, misleading, or full of wishful thinking, e.g., "high security", "tamper-proof", "pick proof", "undefeatable", "impossible to defeat", "due diligence", "barrier", "certified", "fully tested", "reliable", "real-time", "zero error rate", "unique", "industry leader", "industry standard", "best practice", etc.

References

1. B Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* (Springer, 2003).

2. NPR, “Are Post-Sept. 11 Airport Screens Just 'Security Theater'?”, http://www.npr.org/templates/story/story.php?storyId=112725333.

3. RG Johnston and JS Warner, “Security Theater in Future Arms Control Regimes”, *Proceedings of the 51st INMM Meeting*, Baltimore, MD, July 11-15, 2010.

4. RG Johnston, "Tamper Detection for Safeguards and Treaty Monitoring: Fantasies, Realities, and Potentials", *Nonproliferation Review* **8**, 102-115 (Spring 2001).

5. C Tavris and E Aronson, *Mistakes Were Made (But Not by Me): Why We Justify Foolish Beliefs, Bad Decisions, and Hurtful Acts* (Mariner, 2008).

6. RG Johnston and JS Warner, “The Dr. Who Conundrum: Why Placing Too Much Faith in Technology Leads to Failure”, *Security Management* **49**, 112-121 (2005).

7. RG Johnston, “Lessons for Layering”, *Security Management* **54**, 64-69, (2010).

8. RG Johnston and RG Johnston, “Handbook of Security Blunders”, *Proceedings of the 51st Annual INMM Meeting, Baltimore*, MD, July 11-15, 2010.

9. RG Johnston and M Bremer Maerli, “International vs. Domestic Nuclear Safeguards: The Need for Clarity in the Debate Over Effectiveness”, *Disarmament Diplomacy*, issue 69, pp 1-6, February-March 2003, http://www.acronym.org.uk/dd/dd69/69op01.htm.

10. M Bremer Maerli and RG Johnston, “Safeguarding This and Verifying That: Fuzzy Concepts, Confusing Terminology, and Their Detrimental Effects on Nuclear Husbandry”, *Nonproliferation Review* **9**, 54-82 (2002), http://cns.miis.edu/npr/pdfs/91maerli.pdf.

11. Argonne National Laboratory, Vulnerability Assessment Team, http://www.ne.anl.gov/capabilities/vat and especially http://www.ne.anl.gov/capabilities/vat/seals/maxims.html.