SECURITY THEATER IN FUTURE ARMS CONTROL REGIMES

Roger G. Johnston and Jon S. Warner
Vulnerability Assessment Team
Nuclear Engineering Division
Argonne National Laboratory
9700 S. Cass Ave, Building 206, Argonne, IL 60439-4840

ABSTRACT

"Security Theater" (also known as "Ceremonial Security") involves procedures, policies, and technologies that give the superficial appearance of providing security without actually countering malicious adversaries to any significant degree. As vulnerability assessors, we 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. Security Theater is not automatically a bad thing; it can have its uses. The real problem occurs when Security Theater is not recognized as such, or when it stands in the way of good security or is preferred over real security. In this paper, we present a vulnerability assessor's view of where future arms control verification regimes are likely to be plagued by Security Theater, based partially on our understanding of current security vulnerabilities and our experience with Security Theater. We also offer suggestions for spotting Security Theater, and for preventing it. Future nuclear safeguards measures that are particularly at risk for becoming merely Security Theater include tamper-indicating seals and information barriers.

INTRODUCTION

Security guru 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] Another name for Security Theater is "Ceremonial Security". As an example, much of the activities undertaken by airport screeners have been characterized by some as little more than Security Theater.[2]

As vulnerability assessors[3], we 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 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. In this paper, we discuss why we believe Security Theater is going to be a problem in future arms control and nonproliferation regimes—and, indeed, already is to some extent. We offer suggestions for how to detect Security Theater by looking for its characteristic attributes, and propose ways to avoid Security Theater (when it is prudent to do so).

HOW TO TELL SECURITY THEATER FROM THE REAL THING

Of course, labeling security measures as Security Theater is ultimately a value judgment and can be controversial. Moreover, no technology or procedure intended for security is likely to be 100% useless, anymore than it is capable of providing absolute security. Security is a continuum, not binary, with "Security Theater" occupying one end of the spectrum (but not a single point). Nevertheless, we believe there are effective ways to detect when something is primarily Security Theater.

The best way to determine if a given security technology or procedure is primarily Security Theater is to conduct a comprehensive vulnerability assessment to determine how easily the technology or procedure can be defeated or spoofed by the adversary of interest (or even by the average resourceful person on the street). All security technologies and procedures can be defeated or spoofed many different ways[4-6]; the interesting question is how difficult, expensive, time-consuming, and risky is the attack, and what practical countermeasures can be deployed by the good guys.

The problem with a comprehensive vulnerability assessment, however, is that it takes significant time and money; requires creative and knowledgeable assessors who really want to find problems and propose possible countermeasures; and needs organizations, security managers, and verification planners, and perhaps even scientists/engineers, bureaucrats, and diplomats to be willing to hear about the security problems. (As vulnerability assessors, we know that getting security vulnerabilities to be acknowledged can be very challenging.)

In our experience, technologies and procedures that eventually prove to be very easy to attack or spoof—to the point of being Security Theater—almost always exhibit certain attributes. In fact, we can use these attributes to predict fairly reliably how easy it will be for us as vulnerability assessors to demonstrate multiple successful and easy attacks, even before beginning the vulnerability assessment. The attributes that we commonly find in technologies and procedures that are mostly Security Theater are listed below. Naturally, not all Security Theater will exhibit every one of these attributes, and some of the attributes may well apply to security technologies and procedures that are nevertheless highly effective.

The Security Theater Attributes Model: The following are the typical attributes of technologies 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.[7,8])

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 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 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, 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. They 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, 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 procedure.

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 isn't always better.[4])

16. Any consideration of security issues focuses mostly on software or firmware attacks, not on physical security.

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.[3-7])

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

19. 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 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, 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 both arrogance and ignorance. This is the basis of what we call the "Be Afraid, Be Very Afraid Maxim"[3]: 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.

SECURITY SEALS

We believe the use of tamper-indicating seals is often an example of Security Theater. Unlike locks, seals aren't meant to delay or discourage unauthorized entry, but rather record that it took place.[5] (The tamper-evident enclosures used to contain nuclear safeguards cameras or other monitoring equipment is another form for seals.)

We have studied many hundreds of different seals and many different seal use programs[3-7], and have come to the conclusion that seal and tamper-detection programs deployed by many security programs (nuclear and non-nuclear) are largely Security Theater. The seals typically possess serious design flaws and can be easily spoofed. The seal use protocols (exactly how the seals are used) are inadequate, and the seal installers and inspectors almost always lack the specific training and hands-on experience they need to reliably detect tampering. This is very unfortunate because tamper detection is a critical element of any successful nuclear safeguards program (domestic or international) and well as many non-nuclear security programs.

Certainly all of these problems could be fixed (for example, better seals are possible[5,6]), but this would require significant time, commitment, and resources to implement, as well as a willingness to admit to the problem.

In thinking about seals and a typical nuclear seal-use program, we believe that the following attributes from the above list for Security Theater often apply: 2-14, 18, 21 & 24. That's 64% of the 25 total attributes. Attributes 1, 15, 17, 19, 20, & 25 are also somewhat common (another 24%). Identifying which attributes apply in general or to a given security/safeguards program is obviously open for debate. The point here is that our above Attribute Model for warning about the risk of Security Theater does indeed seem to suggest there is a problem with seals, which is consistent with our experience.

INFORMATION BARRIERS

An information barrier is a system for making classified measurements on nuclear material or warheads, but providing the results in an unclassified form that can nevertheless convince inspectors of the authenticity of what was measured. Information barriers may play a major role in future dismantlement and nonproliferation regimes.[11,12]

There are 3 main security challenges to overcome:

1. The Information Barrier must work reliably.

2. The Information Barrier must not release classified information.

3. The Information Barrier must produce results believable to inspectors even (as is likely) if it must be is constructed, controlled, and operated by the nation being inspected.

Problems #1 and #2 are not trivial, but are no doubt solvable. In our view, problem #3 may not be solvable, but is at least a much more difficult challenge than the first two.

Much of the past and current work on information barriers, however, concerns mostly problems #1 and #2. The work and analysis for #3 has focused primarily on software/firmware integrity and authentication, data encryption/authentication, looking for a "hidden switch", or creating the equivalent of a safe or secure "trusted" container.[11-14] The first four issues are not, in our view as vulnerability assessors, the most likely attack vectors. We believe the emphasis on safes or trusted containers demonstrates a fundamental misunderstanding of the problem, and may represent an all too familiar confusing of domestic and international nuclear safeguards.[9,10]

We believe previous, current, and future work on information barriers has or is likely to have the following attributes: 1-9, 11, 13, 16, 19, 20, 22, 23, & 25, which is 68% of the total attributes. Attributes 10, 15, 17, 18 & 24 may also be a problem (20% of the attributes). Based on this result, our skepticism about being able to solve problem #3, and our knowledge of many kinds of attacks on electronics and safeguards systems, we think Information Barriers have a high probability (if they are ever fielded) of being little more than Security Theater unless great care is taken.

TWO-PERSON RULE

For comparison, we can consider the two-person rule. This is a requirement that more than one person be involved in any crucial activity. For nuclear applications, the two-person (or multi-person) rule specifies that more than one person needs to be present near certain categories of nuclear material, or when hazardous operations are to be undertaken.

Most people would support the idea that a two-person rule is probably a prudent security practice. There nevertheless are problems with it. Most organizations (including the United States Department of Energy) don't define the rule very specifically, and it often gets implemented in an inconsistent manner. Moreover, the two-person rule has been largely unstudied (except for applications involving intercontinental ballistic missile silos.)

Applying our Security Theater Attributes test, we believe that the following attributes are typically relevant for most nuclear two-person rules: 2, 5, 6, 9, 21, & 24 (24%), with 13, 18, 19, 23, & 25 (20% of the attributes) sometimes being a problem. These are much lower scores than for seals or information barriers, suggesting the two-person rule (despite its deficiencies) is less likely to be Security Theater.

OTHER AT-RISK TECHNOLOGIES AND PROCEDURES

We believe there are other security technologies and procedures for nuclear applications that are at great risk of becoming little more than Security Theater. We believe this based on our experience with vulnerability assessments on a wide variety of physical security devices, systems, and programs[3], but also based on our judgment of how various security technologies and procedures

score in our "Security Theater Attributes Model" discussed above. These at-risk security technologies and procedures include tags, encryption and data authentication, cargo security, video surveillance, real-time monitoring and tracking, optimizing security culture/climate, and mitigation of the Insider Threat. See references 1, 4, & 15-17 for further discussion.

WHAT TO DO?

The countermeasures for avoiding Security Theater are relatively straightforward, and some are not much different from countermeasures for groupthink and cognitive dissonance.[4,8] Perform legitimate (not "rubber stamp") vulnerability assessments early, often, and iteratively—not only after it is too late to make any changes. Focus on what the purpose is for the technology or procedure, and on what the adversary wants to accomplish and his mindset. Involve skeptical and creative people early on in analyzing the technology or procedure. Appoint a devil's advocate if necessary. Don't let the enthusiasm for solving the security problems steamroll over the realities of the task. The organization and people developing or promoting a given technology or procedure should not be the ones to decide whether to implement it. Hold egos and boosterism in check. Talk (early!) to the people who will use the technology or procedure in the field. Always bear in mind that Security Theater—being easier, cheaper, and less painful than real security—is going to be more attractive than real security. Our "Attributes Model", or something similar, might be useful for raising a red flag that Security Theater is likely.

CONCLUSION

"Security Theater"—going through the motions of providing effective security or safeguards—is not always a bad thing. But it should never be confused with real security, nor interfere with it. The best way to check for Security Theater is to conduct a comprehensive and legitimate vulnerability assessment, but this isn't always practical. Being alert for the presence of Security Theater, knowing its characteristic attributes, and applying common sense countermeasures can go a long way towards avoiding it.

ACKNOWLEDGEMENT AND DISCLAIMER

This work was performed under the auspices of the United States Department of Energy (DOE) under contract DE-AC02-06CH11357. The views expressed in this paper are those of the authors and should not necessarily be ascribed to Argonne National Laboratory or DOE.

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. Argonne National Laboratory, "Vulnerability Assessment Team", http://www.ne.anl.gov/capabilities/vat.

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

5. RG Johnston, "Tamper-Indicating Seals", *American Scientist* **94**, 515-523 (2005).

6. JS Warner and RG Johnston, "Chirping Tag and Seal", *Proceedings of the 51st Annual INMM Meeting, Baltimore*, MD, July 11-15, 2010.

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

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

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. Oleg Bukharin, "Appendix 8A. Russian and US technology development in support of nuclear warhead and material transparency initiatives", pp 171-173, in *Transparency in Nuclear Warheads and Materials: The Political and Technical Dimensions* (Oxford University Press, 203), http://books.sipri.org/files/books/SIPRI03Zarimpas/SIPRI03Zarimpas08A.pdf.

12. American Physical Society, *Technical Steps to Support Nuclear Arsenal Downsizing*, http://www.americanphysicssociety.com/policy/reports/popa-reports/upload/nucleardownsizing.PDF.

13. JL Fuller and JK Wolford, "Information Barriers", IAEA-SM-367/17/01, http://www-pub.iaea.org/MTCD/publications/PDF/ss-2001/PDF%20files/Session%2017/Paper%2017-01.pdf.

14. WQ Bowen and A Persbo, "How might states, or the international community, go about implementing the dismantlement of nuclear weapons systems in an accurate way with would engender international confidence?" (2009), www.icnnd.org/research/BowenPersboCountingNW5ii09.doc.

15. 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).

16. RG Johnston, et al., "Nuclear Safeguards and Security: We Can Do Better", *Proceedings of the 10th International Conference on Environmental Remediation and Radioactive Waste Management (ICEM'05)*, Glasgow, Scotland, September 4-8, 2005.

17. EG Bitzer, PY Chen, and RG Johnston, “Security in Organizations: Expanding the Frontiers of Industrial-Organizational Psychology”, *International Review of Industrial and Organizational Psychology* **24**, 131-150 (2009).