Security Theater in Future Arms Control Regimes

Roger G. Johnston, Ph.D., CPP
Jon S. Warner, Ph.D.

Vulnerability Assessment Team
Argonne National Laboratory

630-252-6168 rogerj@anl.gov
http://www.ne.anl.gov/capabilities/vat

Argonne National Laboratory

3 sq miles, ~3000 employees, $630+ million annual budget
R&D and technical assistance for government & industry

Vulnerability Assessment Team (VAT)

A multi-disciplinary team of physicists, engineers, hackers, & social scientists.

The VAT has done detailed vulnerability assessments on hundreds of different security devices, systems, & programs.

The greatest of faults, I should say, is to be conscious of none.
-- Thomas Carlyle (1795-1881)

Sponsors
- DHS
- DoD
- DOS
- IAEA
- Euratom
- DOE/NNSA
- private companies
- intelligence agencies
- public interest organizations

Definition

"Security Theater" (or "Ceremonial Security"): measures, procedures, or technologies that give the superficial appearance of providing security without actually countering malicious adversaries to any significant degree.

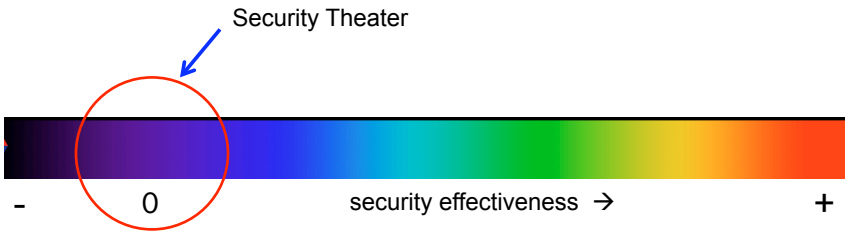
It's Not Always Bad

- Can present the appearance (false though it may be) of a hardened target, thus potentially discouraging attacks (at least for a while).
- Can reassure the public while more effective measures are under development.
- Can help encourage people to take security seriously.
- Can help foster transparency, trust, confidence-building, and international cooperation in international nuclear safeguards.

It's Not Always Bad

- Can provide great photo ops & PR.
- Can serve as a first step in creating new verification regimes.
- During treaty negotiations, can serve as an easy-to-negotiate stand-in for more rigorous future measures.
- Can provide an excuse to get inspectors inside nuclear facilities.

Security is a Continuum



The Problem

When Security Theater:

- gets confused with Real Security
- comes to be viewed as Real Security
- is preferred over Real Security (because it's always easier)

How to Spot Security Theater

Conduct a comprehensive vulnerability assessment

(though this is expensive & time-consuming)

Model Attributes of Security Theater

Predictor

Remedies

Model Attributes of Security Theater

The 25 Common Attributes
of Security Theater

(based on Vulnerability Assessment experience)

Model Attributes of Security Theater

	Attribute	Seals	Inform. Barriers	2-Person Rule
1	Great urgency	0	3	0
2	Earnest—even desperately—desire solve the security/verification problems	2	3	2
3	Considerable enthusiasm for, great pride in, and strong emotion behind	2	2	1
4	Pet technology	2	3	0
5	Confidence, arrogance, "impossible to defeat" attitudes	2	1	2
6	Inertia	3	3	1
7	Substantial time, funding, and political capital has already been spent	3	1	1
8	Conflict of interest/non-objective	2	1	0
9	No VAers, hackers, or devil's advocates	1	3	1
10	Ignore or attack questioners	2	1	0
11	No real-world security experience	2	3	0
12	Mostly engineers	2	2	1
13	A vulnerability assessment only at the end (when it is too late)	2	3	2
14	Band-aid, piling on of non-relevant technology	2	1	0
15	Relying on complexity, high-tech, the latest tech "fad", and/or multiple layers	2	3	1
16	Focus is on software/firmware attacks, not physical attacks	0	2	0
17	Tamper detection is mechanical tamper switch or PSA adhesive label seal	1	2	0
18	No well-defined adversary	2	2	1
19	Little involvement of end users in the development	2	3	1
20	Non-technical people don't understand the technology; bad terminology	3	2	0
21	Control or formalism gets confused with security	2	1	2
22	Domestic and international nuclear safeguards get confused	3	2	2
23	Feel good aura	2	2	1
24	Poor or no use protocols	3	3	3
25	A very difficult security or safeguards problem	3	3	2
	Total out of a possible score of 75	50	55	24

Model Attributes of Security Theater

	Attribute	Poly-graphs	RFIDs for Security	Back-ground Checks
1	Great urgency	1	3	0
2	Earnest—even desperately—desire solve the security/verification problems	3	3	2
3	Considerable enthusiasm for, great pride in, and strong emotion behind	2	2	1
4	Pet technology	2	3	1
5	Confidence, arrogance, "impossible to defeat" attitudes	2	2	1
6	Inertia	3	3	2
7	Substantial time, funding, and political capital has already been spent	1	1	1
8	Conflict of interest/non-objective	0	1	0
9	No VAers, hackers, or devil's advocates	2	3	2
10	Ignore or attack questioners	3	2	1
11	No real-world security experience	1	3	0
12	Mostly engineers	0	2	0
13	A vulnerability assessment only at the end (when it is too late)	3	3	2
14	Band-aid, piling on of non-relevant technology	1	2	0
15	Relying on complexity, high-tech, the latest tech "fad", and/or multiple layers	0	3	1
16	Focus is on software/firmware attacks, not physical attacks	0	0	0
17	Tamper detection is mechanical tamper switch or PSA adhesive label seal	0	1	0
18	No well-defined adversary	2	3	1
19	Little involvement of end users in the development	2	3	1
20	Non-technical people don't understand the technology; bad terminology	2	2	0
21	Control or formalism gets confused with security	3	2	3
22	Domestic and international nuclear safeguards get confused	0	3	0
23	Feel good aura	2	2	1
24	Poor or no use protocols	3	3	2
25	A very difficult security or safeguards problem	3	3	3
	Total out of a possible score of 75	41	58	24

Model Attributes of Security Theater

Security Application	Experience Suggests Sec Theater?	Attributes Score (out of 75)
2-Person Rule	no	24
Background Checks	no	24
Polygraphs	yes	41
Seals	yes	50
Information Barrier	yes	55
RFIDs for Security	yes	58

Problems with the Attribute Model

- Subjective
- Not validated
- Circular logic
- No clear threshold
- Attributes may not be orthogonal
- Weights may not all be equal
- Some attributes may be missing

Countermeasures to Security Theater

WHAT TO DO?

1. Our “Attributes Model”, or something similar, might be useful for raising a red flag, and for suggesting fixes.
2. Perform legitimate (not “rubber stamp”) vulnerability assessments early, often, and iteratively—not only after it is too late to make changes.
3. Focus on the purpose for the technology or procedure, and on what the adversary wants to accomplish and his mindset.
4. Don’t let enthusiasm for solving the security problems steamroll over the realities of the task.

Countermeasures to Security Theater

5. The organization and people developing or promoting a given technology or procedure should not be the ones to decide whether to implement it.

6. Talk (early!) to the people who will use the technology or procedure in the field.

7. Keep in mind that Security Theater—being easier, cheaper, and less painful than Real Security—is going to be more attractive.

Countermeasures to Security Theater

8. Use countermeasures to groupthink & cognitive dissonance

- Involve skeptical and creative people early on
- Seek dissent, criticism, & diversity of opinion
- Appoint a devil's advocate if necessary
- Hold egos in check
- Stay flexible