Journal of Air Transport Management xxx (2015) 1–8

Contents lists available at ScienceDirect

Journal of Air Transport Management

journal homepage: www.elsevier.com/locate/jairtraman

Assessing the effectiveness of layered security for protecting the aviation system against adaptive adversaries☆

Brian A. Jackson [a, *], Tom LaTourrette [b]

[a] RAND Corporation, 1200 South Hayes Street, Arlington, VA 22202, USA
[b] RAND Corporation, 1776 Main Street, Santa Monica, CA 90401, USA

ARTICLE INFO

Article history:
Available online xxx

Keywords:
Security evaluation
Adversary adaptation
Homeland security
Critical infrastructure protection
Counterterrorism

ABSTRACT

The idea of layering of protective measures is integral to aviation security doctrine. It is intuitive that one layer could compensate for limitations of another, and that multiple layers will create sequential obstacles to successful attack. Though this certainly can be the case, layers in a multi-layer security system will not always combine as straightforwardly as intuition would suggest, making the evaluation of a layered security effort difficult. Insights from other fields – including the analysis of safety systems – have identified effects that can cause layers to undermine one another. Other mechanisms can produce mutual reinforcement where layers provide greater protection together than the sum of their individual effects. When behavior of adaptive attackers is considered, how the effects of multiple layers combine to influence the net performance of the security system overall becomes more complex. The paper explores both of these classes of effects and their implications for both security evaluation and decisionmaking.

The idea of layered security, or defense in depth, is a central tenet – perhaps the defining concept – in framing the approach to modern aviation security. Indeed, in the way the U.S. Transportation Security Administration (TSA) describes what it does to the public and to the policy makers overseeing its performance, layered security is front and center. Fig. 1, below, is TSA's visual depiction of the concept for broad audiences, the value of the approach described as follows:

> "Each one of these layers alone is capable of stopping a terrorist attack. In combination their security value is multiplied, creating a much stronger, formidable system. A terrorist who has to overcome multiple security layers in order to carry out an attack is more likely to be pre-empted, deterred, or to fail during the attempt." (US TSA, 2014).

This approach is consistent with general security doctrine that teaches that defense in depth is important when protecting targets that might be attacked by an enemy. Though this belief comes in part from concern about the ability of attackers to breach individual layers, it also comes from an appreciation of the limits of most security measures (e.g., US DOT, 2003; Schneier, 2003; Garcia, 2000; Anderson, 2008; Frazier et al., 2009; US TSA, 2014). Combining multiple imperfect measures is a central strategy to hedge against individual measures' limitations. In both the safety and security fields, this has been evocatively described as the "Swiss Cheese" model – where even if each layer of protection is viewed as a slice of cheese peppered with holes, a stack of slices will be unlikely to have a path through all the slices from top to bottom.

But while a simple and compelling analogy that drives home the concept of layered security, the Swiss cheese model doesn't actually demonstrate how to think through the most key security questions for a planner. For example, given an existing stack of slices, how should we compare the costs and benefits of adding another? And in security planning, unlike in the cheese stacking metaphor, security measures function differently from each other and therefore may combine in ways that can be quite different than the simple analogy might suggest. When the choices available to attackers to respond to new security measures are considered as well, the problem can become even more complex. As a result, the planner or analyst considering a layered security strategy must do more than simply count up paths through the

☆ Analyses by RAND or its researchers do not necessarily reflect the opinions of RAND or of its research clients and sponsors. Comments on the paper's content should be directed to the authors at the contact addresses above.

* Corresponding author.
E-mail addresses: bjackson@rand.org (B.A. Jackson), toml@rand.org (T. LaTourrette).

http://dx.doi.org/10.1016/j.jairtraman.2015.06.009
0969-6997/

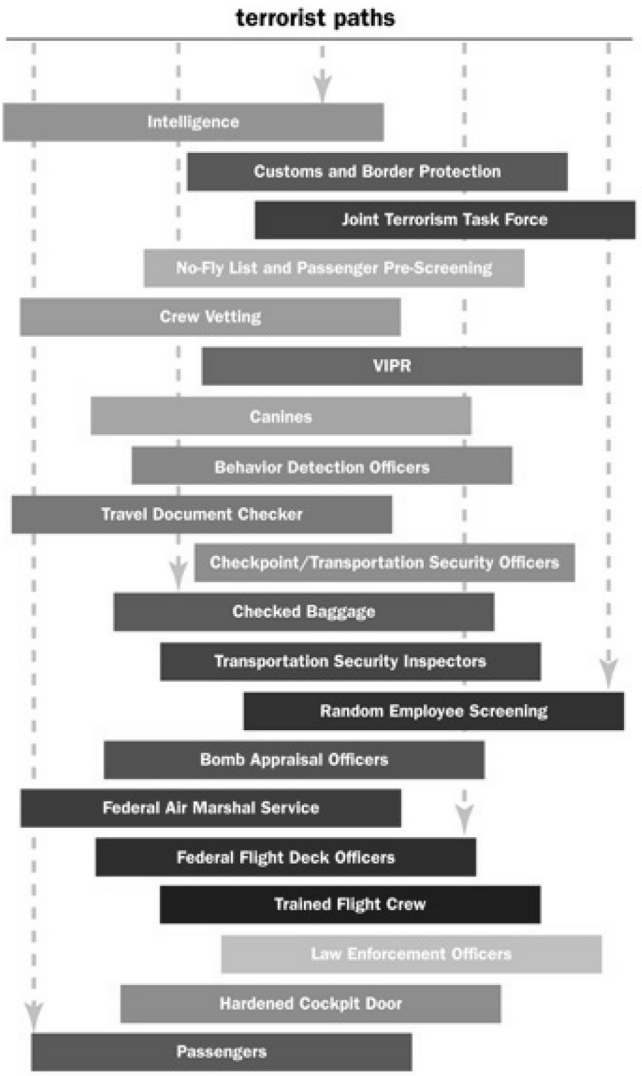

Fig. 1. TSA layered security figure (US TSA, 2014). Notes: VIPR, Visible Intermodal Prevention and response [teams].

holes in each layer or weigh how many holes a new layer might fill.

The focus of the paper is essentially to unpack the simple picture of layered security that Fig. 1 implies—layers stacking up on one another to provide more and more effective security effectiveness. To do so, we do two things: First, we look at how the different functions of security measures and ways those functions interact can make assessing the security value of a layered security system quite difficult. Second, we turn to the issue of how adversary behavior affects outcomes—since in security, the attacker always "gets a vote" on outcomes. We then conclude with a discussion of the main takeaways from this discussion, which frame both the need – and the analytical requirements – for a fundamental revisiting of future aviation security strategy.

1. Individual components of layered security efforts

To successfully stage an attack, an attacker has to find and fix target, gain access to it with the resources necessary to produce the outcomes desired, and have the opportunity to initiate and complete the operation effectively. Security measures and processes affect the ability of attackers to take the steps required to stage an attack and do so in very different ways – e.g., in Fig. 1, the layer labeled "Intelligence" represents something very different than the one representing the Federal Air Marshals Service. The first step for understanding the construction and evaluation of a layered security strategy therefore must be producing a reasonable way of defining the differences between different security measures.

For thinking about different types of security that go into layered strategies and whose effects therefore need to be assessed together, we use the categories in Table 1, which are based on the function that the measures provide and the stage of the attack they affect[1]:

Since we are most concerned with the aviation security context, we set aside the first category since it is only relevant for a subset of targets in the aviation system. We also do not address response and recovery measures simply to limit the scope of the paper. Looking at Fig. 1, it is easy to see examples that fall into different categories. Intelligence efforts are detection activities, as are canines that seek to sniff out the presence of explosives devices. Reinforced cockpit doors are simple hardening measures, acting as barriers that must be overcome by an attacker to gain access. Air marshals or armed flight deck officers allow interdiction of an attack in progress. It is also possible for individual security measures to play multiple roles in a security strategy. For example, a guard force patrolling the perimeter of a facility would both act as detectors and as pre-attack interdiction if the attackers are crossing that perimeter, though when those same guards are deployed dynamically to respond to an attack-in-progress elsewhere they will provide post-initiation interdiction capability.

2. Assessing the combined performance of security layers

Though defining a taxonomy of different ingredients for a layered security effort requires specifying the different effects of measures in isolation – providing a probability to detect, some reduction in consequences, etc. – the true analytic challenge for system thinking is evaluating the performance of layers together. While such analysis is needed to capture the comparatively simple interactions among layers alluded to above (i.e., detection and response measures being interdependent), there are a number of other analytic complexities in working through the combination of multiple layers that must be accounted for.

In considering layered protection around a target, one of most straightforward and intuitive parts of understanding performance is a simple question of coverage. There are a variety of paths through which a single target could be attacked. Taking as an example an airport bombing, the bomb could be brought into the airport through the main entrance or via a service entrance elsewhere. There are also many ways to attack the same target with different distributions of potential consequences. Though we introduced this paper by questioning the simple analogy of security measures as pieces of Swiss cheese and attempting to make sure that "all the holes didn't line up," that basic concept is a starting point for combining the performance of different security layers.

A specific layer of security could affect one, several, or all

[1] Our framework is slightly more complex – but compatible with – the broadly used categorization of security measures as detecting, delaying, or responding to attempted penetration (e.g., Garcia, 2000).

Please cite this article in press as: Jackson, B.A., LaTourrette, T., Assessing the effectiveness of layered security for protecting the aviation system against adaptive adversaries, Journal of Air Transport Management (2015), http://dx.doi.org/10.1016/j.jairtraman.2015.06.009