Reliability Engineering and System Safety 149 (2016) 137–147

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Defending a single object against an attacker trying to detect a subset of false targets

R. Peng [a,*], Q.Q. Zhai [b], G. Levitin [c,d]

[a] Donlinks School of Economics and Management, University of Science & Technology Beijing, Beijing, China
[b] School of Reliability and Systems Engineering, Beihang University, Beijing, China
[c] The Israel Electric Corporation Ltd., Israel
[d] Collaborative Autonomic Computing Laboratory, School of Computer Science, University of Electronic Science and Technology of China, Chengdu, China

ARTICLE INFO

Article history:
Received 19 May 2014
Received in revised form
23 December 2015
Accepted 1 January 2016
Available online 13 January 2016

Keywords:
Reliability
Vulnerability
Defense
Attack
False targets
Contest success function

ABSTRACT

Deployment of false targets can be a very important and effective measure for enhancing the survivability of an object subjected to intentional attacks. Existing papers have assumed that false targets are either perfect or can be detected with a constant probability. In practice, the attacker may allocate part of its budget into intelligence actions trying to detect a subset of false targets. Analogously, the defender can allocate part of its budget into disinformation actions to prevent the false targets from being detected. In this paper, the detection probability of each false target is assumed to be a function of the intelligence and disinformation efforts allocated on the false target. The optimal resource distribution between target identification/disinformation and attack/protection efforts is studied as solutions of a non-cooperative two period min–max game between the two competitors for the case of constrained defense and attack resources.

© 2016 Elsevier Ltd. All rights reserved.

1. Introduction

Safeguarding against intentional external impacts becomes increasingly important in system survivability and defense theory [1,2]. When survivability of systems exposed to intentional attacks is concerned, such measures as protection and deployment of false targets become essential elements of the defense strategy. The defender must make a decision about distribution of the system's defense resources among different defensive measures.

The protection of systems against intentional attacks has been studied in many papers, such as [3–5]; see also [6] for related works and [7] for a comprehensive review. The protection is a technical or organizational measure which is aimed to reduce the vulnerability of protected system elements. The vulnerability of each element is its destruction probability when it is attacked. It can be determined by an attacker–defender contest success function [8]. The contest between the defender and the attacker is usually modeled as a two-period game [9–11]. The defender moves first distributing its defense resource among different elements to minimize the expected damage to the system under the assumption that the attacker will use the most harmful strategy to attack. When the attacker moves, it has full knowledge about the defender's resource allocation and it can optimally allocate its attacking resource so that the expected damage to the system is maximal. In these papers the optimal resource allocation problem is formulated as a min–max problem: the defender chooses its free choice variables to minimize the system vulnerability corresponding to the most harmful attacker's action.

Besides protecting system elements, deploying false targets is another measure to defend systems against intentional attacks. The aim of deploying false targets is to mislead the attacker so that the genuine system elements will be attacked with smaller probability or less attack effort. A false target is sometimes called a decoy and is termed as honey pot within computer security. It may be a wooden fake tank designed to mislead the crew of a fighter plane in a war. Blanks [12] provides historical examples for the use of decoys in WWII and the 1990–1991 Operation Desert Storm, and writes that the U.S. Army (at one point prior to 1994) invested $7.5 M into fielding multispectral tactical decoys.

The efficiency of false targets in defense strategy has been studied in [13], which assumes that there is a single genuine target to protect and false targets can be deployed to distract the attacker. Levitin and Hausken [14] studied the optimal resource allocation between constructing redundant genuine elements, protecting these elements and deploying false targets. Hausken and Levitin [15] studied the optimal resource allocation in protecting system elements and deploying false targets in series systems. It is assumed in these papers that the attacker cannot

* Corresponding author. Tel.: +86 13051540519.
E-mail address: pengrui1988@ustb.edu.cn (R. Peng).

http://dx.doi.org/10.1016/j.ress.2016.01.002
0951-8320/© 2016 Elsevier Ltd. All rights reserved.

Nomenclature

A, a	costs of attacker's and defender's impact effort unit
B, b	costs of attacker's and defender's intelligence effort unit
m	attacker–defender impact contest intensity
f	attacker–defender intelligence contest intensity
g	defender's impact superiority parameter
h	defender's intelligence superiority parameter
H	number of deployed false targets
J	number of false targets the attacker tries to detect
k	number of detected false targets
w	target detection probability (function of x, X, H, J, h and f)
X	attacker's impact-intelligence resource distribution parameter
x	defender's protection-disinformation resource distribution parameter
p_k	the probability that k false targets are detected
Q_k	number of attacked targets in the case that k false targets are detected
R, r	total attacker's and defender's resources
S, s	attacker's and defender's per-target intelligence and disinformation efforts
T, t	attacker's and defender's per-target impact and protection efforts
V	overall GO destruction probability
$v_k(Q_k)$	conditional GO destruction probability given k FTs are detected and Q_k targets are attacked
$V(H, x, X, J)$	overall GO destruction probability given the attacker chooses the most harmful $(Q_0,\ldots,Q_{min(J,H)})$
$V(H, x)$	overall GO destruction probability given the attacker chooses the most harmful (J,X) and $(Q_0,\ldots,Q_{min(J,H)})$

distinguish the genuine object from false targets, that is, it has no preference in attacking the genuine object and a false target. In practice the false targets are usually imperfect, i.e. they are possible to be detected by the attacker. Levitin [16,17] distinguished false targets with genuine objects by the probability of being attacked in the case of imperfect attacker's knowledge about the system, where the probability of being attacked for false targets is determined by some imaginary damage. Peng et al. [18,19] studied system defense strategies with imperfect false targets, which assumed that the detection probability of each false target is constant. This assumption does not address the case when the attacker can allocate part of its budget into intelligence actions trying to detect a subset of false targets. Analogously, the defender can allocate part of its budget into disinformation actions in order to deploy the false targets and prevent them from being detected. In [20,21] it is assumed that if the attacker's intelligence actions succeed, the attacker can identify and attack the defended object and ignore all false targets. However, in many cases the intelligence actions can result in identifying a part of false targets (for example, when the attacker can detect only specific features of the false targets), and the attacker has a set of unidentified targets when it launches the attack.

This paper considers defending a single genuine object including the strategy of deploying false targets that can be detected by the attacker individually and independently. The detection probability of each false target is assumed to be a function of the intelligence and disinformation efforts allocated on it. Both the attacker's and the defender's resources are fixed and both of them have full knowledge about efforts of each other. The contest between the defender and the attacker is modeled as a two-period game where the defender moves in the first period, and the attacker moves in the second period. As pointed out in [22], the most conservative strategy is "particularly appropriate in the design of robust military systems". In this paper we study the defender's strategy which minimizes the object destruction probability assuming that the attacker always chooses the most harmful strategy no matter what the defender's strategy is.

Section 2 presents the model, including the model assumptions and its formulation. Section 3 studies the most harmful attack strategy when the defense strategy is given. In Section 4, the optimal defense strategy and attack strategy are studied. The main results of this paper are summarized in Section 5.

2. The model

2.1. Assumptions

1. The defender uses identical false targets and allocates the disinformation efforts evenly among them.
2. The attacker allocates the intelligence efforts evenly among the targets it tries to detect.
3. The attacker allocates the attack effort evenly among all the attacked targets.
4. The attacker can successfully identify some targets as false targets (by detecting some features that characterize the FTs), but cannot confidently identify any target as the genuine object (the fact that specific FT features are not detected can mean either that the detection failed or that the target is the genuine object).

2.2. Model formulation

The defender deploys one genuine object and H false targets. The total attacker's resource is R. The attacker can allocate part of its resource RX $(0 \le X \le 1)$ into intelligence effort aimed at detecting J $(0 \le J \le H+1)$ false targets among the $H+1$ targets. The cost of the intelligence effort unit is B. The intelligence effort allocated on each target is $S=RX/(BJ)$. Once the attacker has detected a certain number k $(0 \le k \le \min(H,J))$ of false targets, it chooses Q_k targets among the $H-k+1$ undetected targets to attack such that Q_k maximizes the destruction probability of the genuine object. The cost of the attack effort unit is A. The attack effort allocated on each attacked target is $T=R(1-X)/(Q_kA)$.

The defender's total resource is r. It distributes part of its resource rx $(0 \le x \le 1)$ into disinformation actions, which includes deploying H false targets and preventing the false targets from being detected by the attacker, and distributes its remaining resource $r(1-x)$ into protecting the genuine object. The cost of the protection effort unit is a. The cost of the disinformation effort unit is b. The effort for protecting the defended object is $t=r(1-x)/a$, whereas the disinformation effort allocated on each false target is $s=rx/(bH)$. We should note that a and b determine the effectiveness of resources (e.g. dollars) in protection and disinformation actions (it is the same for A and B for the attacker). Their determination varies from case to case. An example for determining b is as follows. Suppose we are to deploy fake tanks into a battle. If the attacker (e.g. an unmanned aerial vehicle. UAV) discriminates the targets by vision, then b can be the ratio between the money spent

Download English Version:

https://daneshyari.com/en/article/807671

Download Persian Version:

https://daneshyari.com/article/807671

Daneshyari.com