AN ATTACKER-DEFENDER MODEL FOR CYBER SECURITY

Mehmet Ertem, Department of Industrial Engineering, University of Wisconsin-Madison, 1550 Engineering Drive, Room 3237, Madison, WI 53706, USA

Vicki M. Bier, Department of Industrial Engineering, University of Wisconsin-Madison, 1550 Engineering Drive, Room 3270A, Madison, WI 53706, USA

Abstract

We propose a general defender-attacker model for security of computer networks, using attack graphs to represent the possible attacker strategies and defender options. The defender's objective is to maximize the security of the network under a limited budget. In the literature, most network-interdiction models allow the attacker only one attempt (assuming that the attacker is captured and disabled after a single failure); other models allow multiple attempts, but assume that any subsequent attempt begins at the point in the network where the previous attempt failed. These models are not appropriate for computer security, where the attacker could be operating from the safety of a foreign country, and the cost of starting over with a completely different attack strategy may be quite low.

To represent the ability of the attacker to launch multiple attempts, we represent the attacker's success or failure on any one arc of the attack graph probabilistically, and formulate the resulting security problem as a multiple-stage stochastic network-interdiction problem. In the resulting game, a non-myopic defender anticipates both the attacker's strategy choices, and their probability of success or failure, and chooses a single defensive strategy (i.e., a set of arcs in the attack graph to protect) by which to defend against multiple attempted attacks. The attacker then launches an optimal attack against the system, assuming knowledge of which arcs have been protected. If the attacker fails at the first attempt, a second-stage optimal attack strategy is chosen, based on a revised attack graph showing which arcs have already been successfully traversed (now assumed to have success probabilities of 1), and which arc led to failure of the first-stage attack (now assumed to have a success probability of 0). We solve the resulting stochastic-optimization problem using two-stage stochastic optimization with recourse and explore the attacker's non-myopic attack strategies.