CERIAS

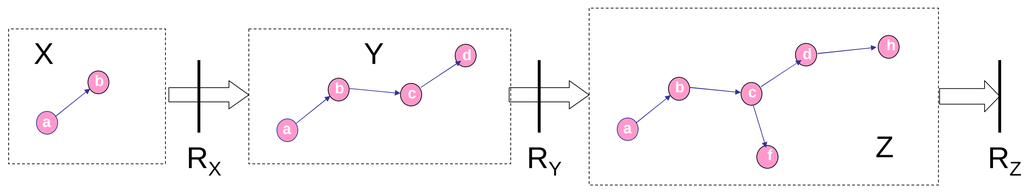
the center for education and research in information assurance and security

The Search for Optimality in Online Intrusion Response for a Distributed E-Commerce System

Yu-Sung Wu, Gaspar Howard, Matthew Glause, Bingrui Foo, Saurabh Bagchi, Eugene Spafford

Dependable Computing Systems Laboratory

Break-down of a multi-stage attack into multiple snapshots



In snapshot X, attacker achieves stages a and b.

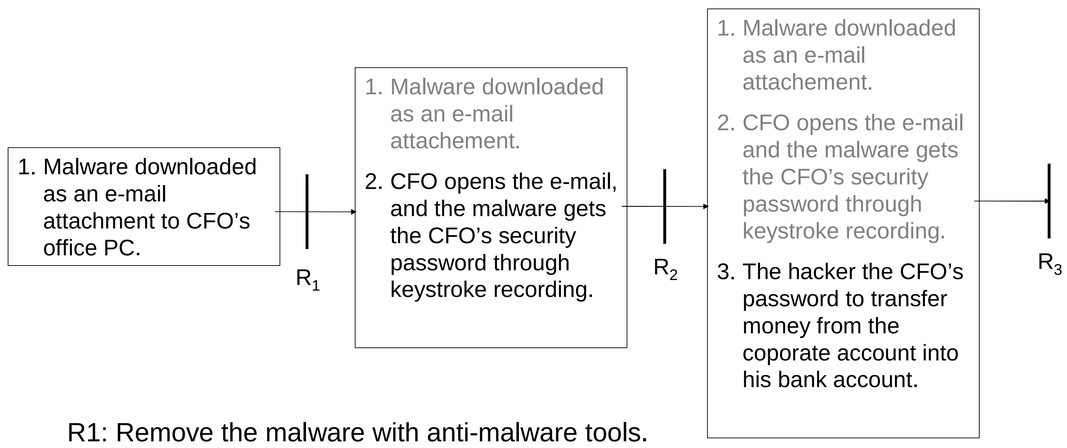
In snapshot Y, attacker achieves a, b, c, and d.

In snapshot Z, ….

A response mechanism decides the response combination (RC_i) following each snapshot.

$$RC_i = f(s_i, H)$$

Q: What will be the best response combination RC_i for each attack stage ?



R1: Remove the malware with anti-malware tools.

R2: Change the CFO's security password.

R3: Freeze the corporate account.

Optimality of a response combination

A system has transaction goals and security goals that it needs to meet through the time of operation.

Ex: providing e-mail service, ensuring the confidentiality of sensitive data, and etc.

Attacks are meant to cause impacts to some of these goals.

Ex: Denial of service on the e-mail service. Stealing the sensitive data.

Assume the impact from an attack to the system can be quantified through a vector IV with each element in the IV corresponding to the impact on each of the transaction/security goals.

– Let the impact vector associated with the k^{th} attack stage n_k be $IV(n_k)$.

The responses can potentially have impact on the system transaction/security goals (side-effects).

– Let $IV(r_k)$ be the impact vector associated with response r_k.

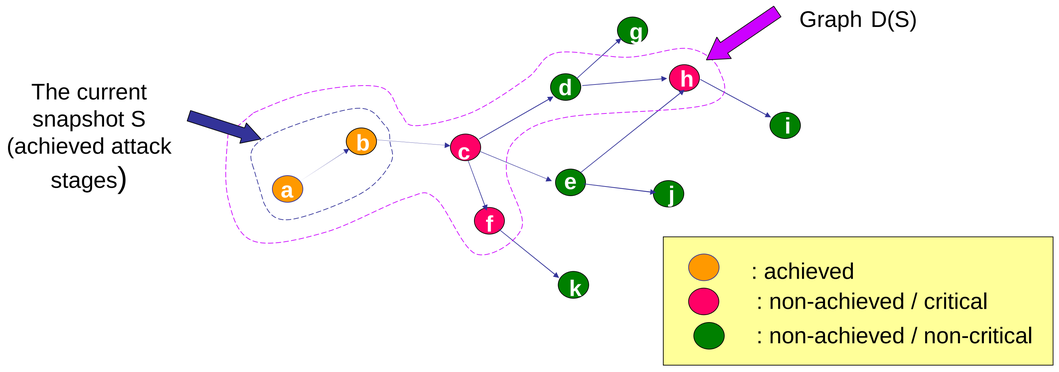
We formally define the cost for a response combination RC_i as:

$$Cost(RC_i) = | Iv(RC_i) | = \left| \sum_{k=1}^{m} Iv(n_k) \Pr ob(n_k) + \sum_{k=1}^{n} Iv(r_k) \right|$$

The optimality of a response combination RC_i is tied with achieving the minimum Cost(RC_i).

The ADEPTS approximation approach

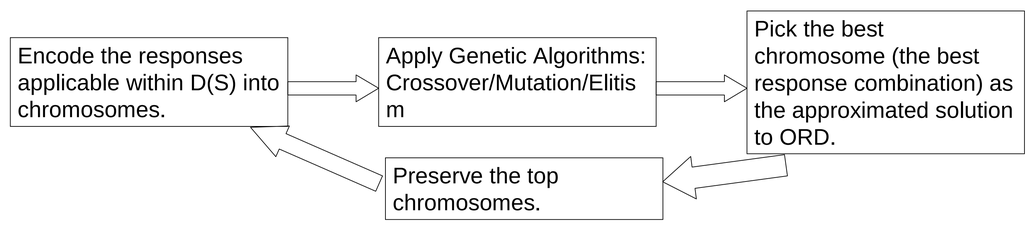
1st step: The Domain Graph



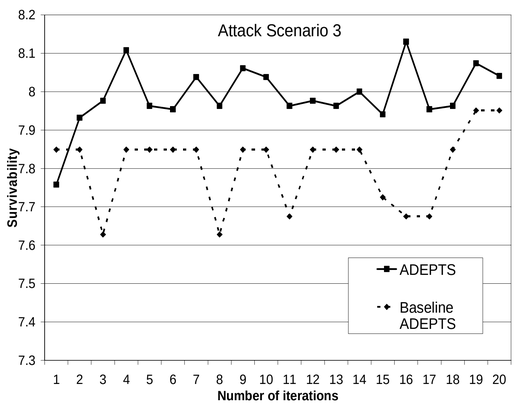
Potentially, there can be zillions of potential "next stages" from an attack snapshot. This poses an issue even with a polynomial time approximation algorithm to the problem of ORD (optimal response decision).

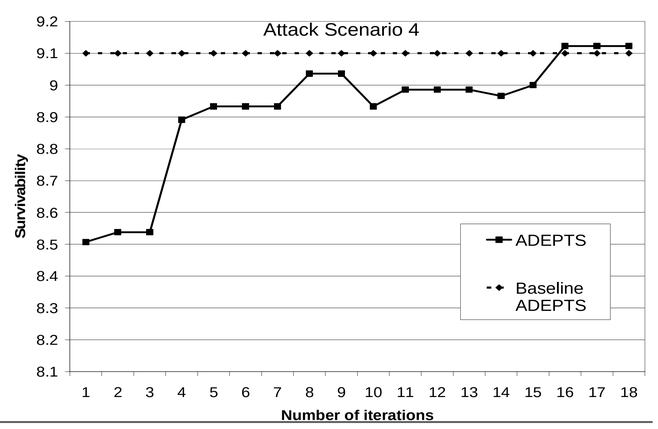
We solve this problem by limiting the search space to a subset of all potential attack stages to the ones which are deemed to be critical (with high enough IV/reaching probability). We call the subset "the domain graph" with respect to a snapshot.

2nd step: approximate ORD with genetic algorithm.



Experiment result





PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center