General Sum Markov Games for Strategic Detection of Advanced Persistent Threats using Moving Target Defense in Cloud Networks

Sailik Sengupta • Subbarao Kambhampati
Ankur Chowdhary • Dijiang Huang

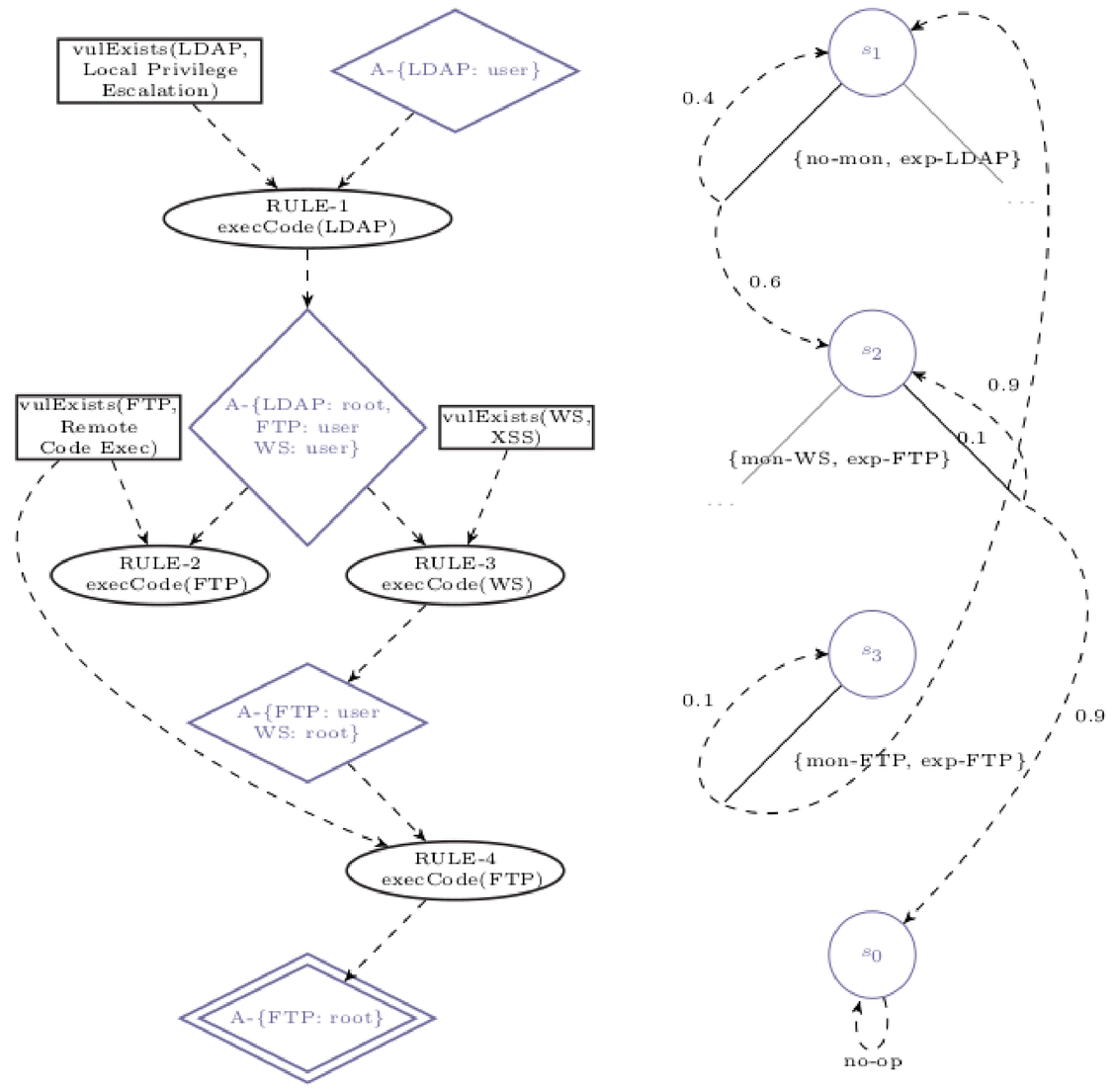
Arizona State University

GameSec 2019

Placing all detection systems in the cloud results in reduced Quality of Service (QoS). Any static placement of detection systems can be easily evaded by an adversary.

Existing MTD for detection system placement do not consider multi-stage attack modeling and assume attacks and detection always succeed. Partial observability hinders scalability.

Markov Game modeling using Attack Graphs. General-sum game because an attacker does not care about defender's QoS metrics.



Transitions

Use of exploitability score (ES) considers the difficulty of an attack in determining the probability of its success.

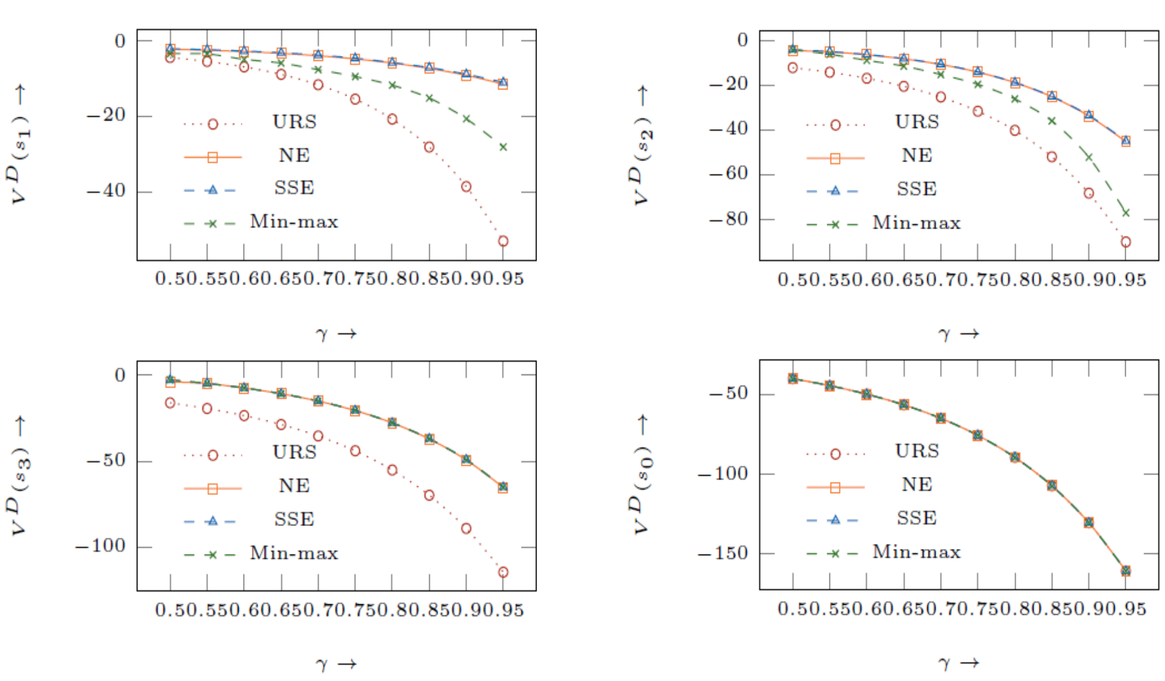
Utilities

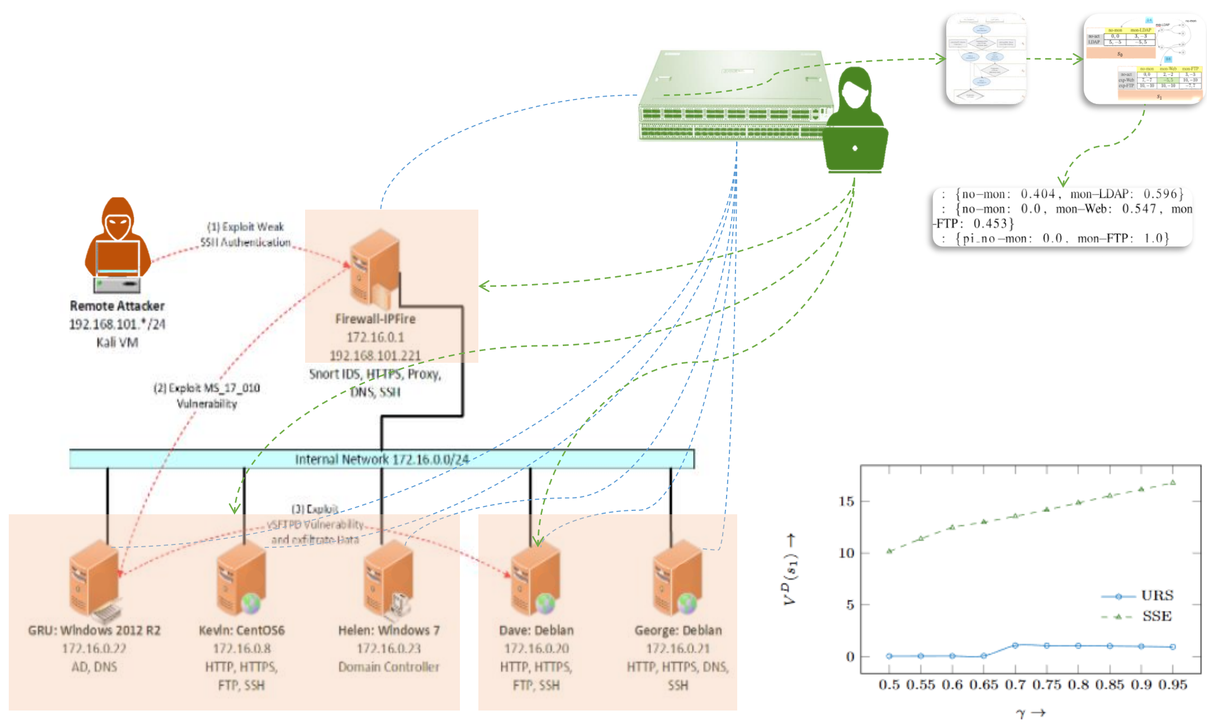
Use of Impact Score (IS) to determine the impact of attacks.
Use of MiniNET simulations to determine the impact of an IDS on QoS metrics.

Threat model assumes attacker has an idea of the defender's placement strategy. Dynamic programming approach to find the Stackelberg Strategy in the Markov Game.

Algorithm 1 Dynamic Programming for finding SSE in Markov Games

procedure GIVEN $(S, M, E, \tau, U^D, U^A, \gamma^D = \gamma^A = \gamma)$,
OUTPUT$(V^i(s), \pi^i(s)\ \forall\ i \in \{A, D\})$
  $V(s) = 0\ \forall\ s$
  loop: $i == k$ break;
  // Update Q-values
  Update $Q^D(s, m, e)$ and $Q^A(s, m, e)\ \ \forall\ s \in S, m \in M(s), e \in E(s)$
    using U^D, U^A and $V(s)$.
  // Do value and policy computation
  Calculate $V^i(s)$ and $\pi^i(s)$ for $i \in \{A, D\}$ using the values $Q^i(s, m, e)$
  $i \leftarrow i + 1$
  goto *loop*.
end procedure





- For states further away from the goal, don't need to monitor at times to enhance performance QoS.

$\pi_{\text{MG-SSE}}(s_1)$: {no–mon: 0.097, mon–LDAP: 0.903}
$\pi_{\text{MG-SSE}}(s_2)$: {no–mon: 0.0, mon–Web: 0.539, mon–FTP:0.461}
$\pi_{\text{MG-SSE}}(s_3)$: {pi_no–mon: 0.0, mon–FTP: 1.0}

- For states closer to the goal, not monitoring is not an option. Security becomes more important that performance.

Emulation on ThoThlab

- Movement strategy is pre-computed.
- SDN used to switch IDS deployments.

This work is supported in part by Naval Research Lab N00173-15-G017, AFOSR grant FA9550-18-1-0067, the NASA grant NNX17AD06G,ONR grants N00014-16-1-2892, N00014-18-1-2442, N00014-18-12840, NSF-USDGE-1723440, OAC-1642031, SaTC-1528099, 1723440 and NSF-China 61628201and 61571375. The first author is also supported by an IBM Ph.D. Fellowship.