Indices of Power in Optimal IDS Default Configuration: Theory and Example

Quanyan Zhu* and Tamer Başar

Coordinated Science Laboratory
Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign

Conference on Decision and Game Theory for Security

Nov. 14, 2011
Outline

• Static and Dynamic IDS Configuration
  – Introduction and motivation
• Default IDS Configuration
  – Attacker and Detector Model
  – Detection Efficiency
• Cooperative Game Model
  – Indices of Power
  – Multi-Linear Extension
• Conclusions and Future Work
Configurations of Intrusion Detection Systems

- **IDS** is an important defense against a variety of attacks that can compromise the security.
  - **Signature-based detection**: base upon the knowledge of attack signatures, e.g. Snort and Bro.
  - **Anomaly-based detection**: raise alerts whenever an abnormal behavior is detected.

- **IDS configuration and control are not trivial**
  - Thousands of rules in 51 categories or libraries.
  - Different levels of detection capabilities available in Snort IDS:
    - (1) Minimum; (2) Medium; (3) Maximum.
  - A tradeoff between **security** enforcement levels and the system performance
Configurations

• IDS configuration balances security and performance.

• $\mathcal{L} = \{l_1, l_2, \ldots, l_N\}$ is the set of finite number of libraries.

• $\mathcal{L}^* = \sigma(\{l_1, l_2, \ldots, l_N\})$ is the set of all possible configurations $F_i, i = 1, 2, \ldots, 2^N$.

• Default configuration: Finding an offline optimal initial IDS configuration.

• Dynamic configuration: Finding an online optimal dynamic IDS configuration policy.
AN ENGINEER DESIGNS A SNAIL....
System Model (I)

• IDS Model
  – Cost $c_i$ is associated with each library $l_i$.
  – Cost $C_{Fi}$ is associated with each configuration $F_i$.
  – An IDS chooses an optimal configuration $F_i$.

• Attacker Model
  – An attacker has different types of attack $a_1, a_2, \ldots, a_M$.
  – Each attack $a_i$ causes a damage $d_i$.
  – An attacker chooses a sequence of attacks, e.g. from attack
trees, $S_i = \{a_1, a_2, a_3, a_4, a_5\}$.

$$a_1 \rightarrow a_2 \rightarrow a_3 \rightarrow a_4 \rightarrow a_5$$
System Model (II)

- Each library $l_i$ can only effectively detect certain attacks.
- We define $P_{li}$ as its scope of detection of $l_i$.

- The sequence $S_i$ is undetectable by the configuration $\{l_1, l_2, l_3\}$.
- Detection effectiveness of a library $l_j$ against attack sequence $S_i$

\[
\eta_{ij} := \frac{v(S_i \cap P_j)}{v(S_i)}
\]
Effectiveness vs. Efficiency

• **Effectiveness** of a configuration $F$ for attack sequence $S_i$.

\[ \eta_i := \frac{\sum_{l_k \in F} v(S_i \cap P_k)}{v(S_i)} . \]

The portion of the attack sequence that can be detected by the configuration.

• **Efficiency** of a configuration $F$ for attack Sequence $S_i$.

\[ \zeta_i := \sum_{l_k \in F} \frac{v(S_i \cap P_k)}{v(T)} . \]

The portion of the coverage of IDS configuration that protects against attack $S_i$. 
Trade-off between Effectiveness and Efficiency

- The efficiency and effectiveness metrics obey the following relation for every sequence of attack $S_i$.

$$\frac{1}{\eta_i} + \frac{1}{\zeta_i} \leq 1.$$
Dynamic Configuration Modeled as a Competitive Markov Decision Process

- The defender chooses a configuration policy that minimizes the long-term cost.
- The attacker chooses a sequence of attacks that maximizes the long-term cost.
- A stationary saddle-point security equilibrium is found for IDS configurations.
- Online Q-learning mechanism is used to learn the adversarial environment.

[Zhu and Başar, CDC 2009]
Default Configuration Using Cooperative Game Theory

• We call a configuration $F$ of an IDS $\omega$-effective for attack sequence $S_i$ if $\eta_i \geq \omega$.

• We can view each possible configuration as a coalition of different libraries.
  – Configuration $\leftrightarrow$ Coalition
  – $\omega$-effective $\leftrightarrow$ Winning
  – Library $\leftrightarrow$ Player

• Each library can be associated with an index of power, signifying its contribution to the detection of intrusion.
  – Shapley Value (SV)
  – Banzhaf-Coleman (B-C) Index
N-Person Cooperative Game Model

- $\mathcal{L} = \{l_1, l_2, \ldots, l_N\}$ is the set of the players.

- A configuration $F$, a subset of $\mathcal{L}$, is a coalition.

- $f: \mathcal{L}^* \to \{0, 1\}$ is a characteristic function of the (simple) game.
  - 1: a configuration $F$ achieves $\omega$-effectiveness.
  - 0: a configuration $F$ fails to achieve $\omega$-effectiveness.

- Properties of $f$
  - $f(\mathcal{L}) = 1$, $f$(Empty Set)=0.
  - Superadditivity
  - $f(\{l_i\}) = 0$, for all $l_i$. 
Indices of Power

• Shapley value of library $l_i$

$$\phi_i = \sum_{R \subset \mathcal{L}} \frac{(r - 1)!(N - r)!}{N!} \left[ f(R) - f(R - \{l_i\}) \right]$$

Use the properties of $f$ and let $R'$ be the set of winning coalitions:

$$\phi_i = \sum_{R' \subset \mathcal{L}} \frac{(r - 1)!(N - r)!}{N!}$$

• Banzhaf-Coleman index of library $l_i$

$$\beta_i = \frac{\theta_i}{\sum_{j=1}^{N} \theta_j}$$

Number of swing: $\theta_i$ is the number of coalitions (configurations) that wins ($\omega$-effective) when $l_i$ is included but loses when is not.
Example

• Let $\omega = 3/5$.

• The Shapley values are $\phi_1 = 1/3$, $\phi_2 = 1/6$, $\phi_3 = 1/6$.

• B-C Indices are $\beta_1 = 3/5$, $\beta_2 = 1/5$, $\beta_3 = 1/5$. The swings are
  – $\{(l_1, l_2), (l_1, l_3), (l_1, l_2, l_3)\}$ for $l_1$
  – $\{(l_1, l_2)\}$ for $l_2$
  – $\{(l_1, l_3)\}$ for $l_3$

• $l_1$ is the most important, and $l_2$ and $l_3$ are equally important
Multi-Linear Extension (MLE)

• Extension to deal with multiple cooperative games w. r. t. different attack sequences on an attack graph.

• Each attack sequence $S_j$ is associated with a MLE $h_j$.

• MLE extension of cooperative game with characteristic function $f_j$ is a function

$$h_j(x_1, x_2, \cdots, x_N) = \sum_{R \subseteq \mathcal{L}} \left\{ \prod_{l_i \in R} x_i \prod_{l_i \in \mathcal{L} - R} (1 - x_i) \right\} f_j(R).$$

• Connections with SV and B-C Index:

$$\phi_{ij} = \left. \int_0^1 \frac{\partial h_j(x_1, x_2, \cdots, x_N)}{\partial x_i} \right|_{x_1 = t, x_2 = t, \cdots, x_N = t} \, dt,$$

$$\beta_{ij} = \left. \frac{\partial h_j(x_1, x_2, \cdots, x_N)}{\partial x_i} \right|_{x_1 = \frac{1}{2}, x_2 = \frac{1}{2}, \cdots, x_N = \frac{1}{2}},$$

[Owen 1972, Owen 1988]
Aggregated MLE

- To aggregate the effect of a library detecting a set of sequences of attacks, we can adopt an aggregated MLE

\[ \bar{h} = \sum_{S_j \in \mathcal{M}} p_j h_j \]

- \( p_j \) indicates the frequency of occurrences of the attack sequence \( S_j \).

- Aggregated power indices can be obtained from \( \bar{h} \).

- MLE can be used as a basis for
  - approximation under a large number of rules.
  - asymmetry of permutations: not all arrangements are equally probable.
Optimal Default Configuration

• The indices of power \textit{rank} the importance of each library from high to low.

• The indices can be used to make a decision on which libraries to load when the system is subject to cost constraint $C_0$.

\[
\begin{align*}
\max_{z} & \quad \sum_{l_i \in L} z_i \phi_i \\
\text{s.t.} & \quad \sum_{l_i \in L} z_i c_i \leq C_0 \\
& \quad z_i \in \{0, 1\}, \forall l_i \in L
\end{align*}
\]

• Optimal default configuration is served as an initial condition for dynamic online configuration.
Conclusions

• We have adopted a cooperative game approach to study the influence of each library when forming a configuration to detect intrusions according to some known attack graphs.

• The game-theoretic framework provides metrics on efficiency and effectiveness of detection, which connects the IDS performance with the behavior of the attacker.

• Multi-linear extension offers a technique to generalize the two indices of power, i.e., Shapley value and B-C index, and provides an approach for a large-scale number of libraries.
A Broader Picture

- **Management Layer**
- **Supervisory Layer**
- **Network Layer**
- **Communication Layer**
- **Control Layer**
- **Physical Layer**

- **Libraries** are enriched by the patching and investment decisions from the above.
- Dynamic and Static IDS Configurations
- IDS configuration policies affect the physical layer system performances
Future Work

• The IDS configuration problem enables a cross-layer investigation of the security issues existing on multiple layers of the cyber-physical human systems.

• The optimal default configuration needs to be integrated with dynamic online policies.

• The idea of configuration has also been applied to understand the effectiveness of teaching in classrooms.
