A Queuing Formulation of Intrusion Detection with Active and Passive Responses

Wei T. Yue, Metin Cakanyildirim, Young U. Ryu

Department of Information Systems and Operations Management
School of Management
The University of Texas at Dallas
Richardson, Texas 75083-0688, USA
Introduction

- Traditional IDS response tends to be passive – “passive response”
- Secondary investigation required because IDS is still imperfect
- Secondary investigation may not occur instantaneously
- These days, IDS can be set up to respond to events automatically – “active response”
Introduction

- Active response – dropping connection, reconfiguring networking devices (firewalls, routers), additional intelligence mining (honeypots)

- We only consider terminating connection
Introduction

- In the intrusion detection process, IDS configuration decision and the alarm investigation decision are related.
- Alarm investigation resource would affect the delays in response in both active and passive response.
- If multiple alarm types involved, which alarm to investigate is an issue.
Research Goals

- Finding the corresponding configuration and investigation decision for the active and passive response approach

- Determine the “switching” policy on intrusion response
Problem Description

- Passive response
  - potential damage cost - resulting from alarmed events not investigated immediately
  - low false alarm costs since alarmed events are not disrupted
Problem Description

- Active response
  - It could prevent attack damage because the events are terminated immediately
  - higher false alarm costs contingent on the performance of the IDS
Problem Description

- Active response: false alarm cost is related to delay
- Passive response: damage cost is related to delay
Problem Description

- Undetected, or non-alarmed intrusive events are assumed to be the same for the two response approach.

- Given the parameter values, the decisions involved with the active and passive response approaches are different.
IDS Quality: ROC curve

- A representation of IDS quality – detection rates ($\Omega(P_F)$) and false alarm rate ($P_F$)

- IDS quality can be determined experimentally – MIT Lincoln Lab (Lippman et al 2000a 200b), Columbia IDS group (Lee and Stolfo, 2000), etc
IDS Quality: ROC curve
A Queuing Model of Intrusion Detection

- Benign and intrusive event arrivals – Independent Poisson process with rate $\lambda_B$ and $\lambda_I$
- $N$ – number of investigator
- $\mu$ - investigation rate
- $E(W(P_F,N)) = \frac{1}{N \mu - P_F \lambda_B - \Omega(P_F) \lambda_I}$
A Queuing Model of Intrusion Detection: Active Response

\[
\text{Traffic inspected by IDS} = \lambda
\]

- Alarm
  - Investigation cost = \( C_s \)
  - Benign
  - Intrusive
- No alarm
  - Benign
  - Intrusive

Waiting/False alarm cost = \( P_f \lambda_b E(P_f, N) C_f \)

No cost incurred

Damage cost = \( (1 - \Omega(P_f)) \lambda_r A \)
A Queuing Model of Intrusion Detection: Passive Response

Traffic inspected by IDS = \( \lambda \)

- Alarm
  - Investigation cost = \( C_i \)
  - Benign
    - No cost incurred
  - Intrusive
    - Waiting/Damage cost = \( \Omega(P_F)\lambda_I E(P_F, N)C_d \)

- No alarm
  - Benign
    - No cost incurred
  - Intrusive
    - Damage cost = \( (1 - \Omega(P_F))\lambda_I A \)
A Queuing Model of Intrusion Detection

Active Response

$$\min_{0 \leq P_F \leq 1, \ N \geq 0} P_F \lambda_B E(W(P_F, N)) C_f + (1 - \Omega(P_F)) \lambda_I A + NC_s$$

Passive Response

$$\min_{0 \leq P_F \leq 1, \ N \geq 0} \Omega(P_F) \lambda_I E(W(P_F, N)) C_d + (1 - \Omega(P_F)) \lambda_I A + NC_s$$

- We rewrite the N in terms of slack service rate S
  - $$S = \mu N - P_F \lambda_B - \Omega(P_F) \lambda_I$$
Linear Piecewise ROC

\[ \frac{1 - b\phi}{1 - b} \]

Probability of Detection \( P_D \)

Probability of False Alarm \( P_F \)
Optimal Configuration and Investigation

\[
\Omega_P(P_F) = \begin{cases} 
\phi P_F & \text{if } P_F \leq b \\
 b\phi + \frac{(1-b\phi)}{(1-b)}(P_F - b) & \text{if } P_F \geq b 
\end{cases}
\]

\[
S^*_A(P_F) = \left( \frac{\mu \lambda_B C_f}{C_s} \right)^{1/2} (P_{A,F})^{1/2}
\]

\[
S^*_P(P_F) = \left( \frac{\mu \lambda_I C_d}{C_s} \right)^{1/2} \left[ \Omega(P_{P,F}) \right]^{1/2}
\]
### Hybrid Response

<table>
<thead>
<tr>
<th>Active $(P_F, P_D)$</th>
<th>Passive $(P_F, P_D)$</th>
<th>$T C_A &gt; T C_P$ Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>$b, b\phi$</td>
<td>$b, b\phi$</td>
<td>$\lambda_B C_f \geq \phi \lambda_I C_d$  <strong>I</strong></td>
</tr>
<tr>
<td>$b, b\phi$</td>
<td>1,1</td>
<td>$(1 - b\phi)\lambda_I A \mu - C_s [\lambda - \lambda_B b - \lambda_I b\phi] \geq \frac{2\sqrt{C_s \mu} [\sqrt{C_d \lambda_I} - \sqrt{C_f \lambda_B b}]}{2\sqrt{C_s \mu} [\sqrt{C_f \lambda_B} - \sqrt{C_d \lambda_I b\phi}]}$  <strong>II</strong></td>
</tr>
<tr>
<td>1,1</td>
<td>$b, b\phi$</td>
<td>$(1 - b\phi)\lambda_I A \mu - C_s [\lambda - \lambda_B b - \lambda_I b\phi] \leq \frac{2\sqrt{C_s \mu} [\sqrt{C_f \lambda_B} - \sqrt{C_d \lambda_I b\phi}]}{2\sqrt{C_s \mu} [\sqrt{C_f \lambda_B} - \sqrt{C_d \lambda_I b\phi}]}$  <strong>III</strong></td>
</tr>
<tr>
<td>1,1</td>
<td>1,1</td>
<td>$\lambda_B C_f \geq \lambda_I C_d$  <strong>IV</strong></td>
</tr>
</tbody>
</table>
Hybrid Response

<table>
<thead>
<tr>
<th>Active $P_F, P_D$</th>
<th>Passive $P_F, P_D$</th>
<th>$\lambda_B C_f \leq \lambda_I C_d$</th>
<th>$\lambda_I C_d \leq \lambda_B C_f \leq \phi \lambda_I C_d$</th>
<th>$\lambda_B C_f \geq \phi \lambda_I C_d$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$b, b\phi$</td>
<td>$b, b\phi$</td>
<td>Active I</td>
<td>Active I</td>
<td>Passive I</td>
</tr>
<tr>
<td>$b, b\phi$</td>
<td>1,1</td>
<td>Passive</td>
<td>Passive II</td>
<td>Passive</td>
</tr>
<tr>
<td>1,1</td>
<td>$b, b\phi$</td>
<td>Passive III</td>
<td>Passive III</td>
<td>Passive</td>
</tr>
<tr>
<td>1,1</td>
<td>1,1</td>
<td>Active IV</td>
<td>Passive IV</td>
<td>Passive IV</td>
</tr>
</tbody>
</table>
Conclusion

- Derive optimal intrusion detection decisions with linear piecewise function
- Extend the study with other types of ROC functions
- Include multiple types of alarm