On the Tradeoff between Privacy and Utility in Collaborative Intrusion Detection Networks-A Game Theoretical Approach

Richeng Jin
Advisor: Prof. Huaiyu Dai
Dept. of ECE, NC State Univ.
Collaborative Intrusion Detection System (CIDS)

- CIDSs consist of several individual IDSs that monitor different parts of a network and exchange data to jointly identify attacks.

- Three main types:
  - Centralized: high detection accuracy, not scalable, SPoF
  - Decentralized: information lost in each level of hierarchy
  - Distributed: scalable, more freedom
Requirements for CIDS

• **Accuracy**
  • Minimize both false positive rate and false negative rate.

• **Minimal overhead**
  • Overhead arises in terms of computation and communication effort.

• **Scalability**
  • Networks of arbitrary large size can be protected by adding detecting resource.
Requirements for CIDS

• Resilience
  • Prevent Single Point of Failures and provide fast restoration mechanisms.

• Privacy
  • Sensitive information should be protected in collaboration.

• Interoperability
  • Interoperate with instances of the same system deployed in other networks.
Motivation

• When a network is under attack, the traffic patterns monitored by different IDSs located at different positions are often correlated, and so are the corresponding intrusion alerts.

• Gathering more traffic information/intrusion alerts will improve the detection performance.

• Sharing traffic information/intrusion alerts may lead to privacy leakage.

• How to balance the detection performance and the privacy requirement? Is it possible to improve both simultaneously?
• A simple example
  • Assume that the network in NCSU centennial campus is under attack, and the IDSs in the network could cooperate for better intrusion detection.
  
  • These IDSs may belong to different organizations. For example, some of them are deployed by NCSU while some others belong to its partners (e.g., ABB).
  
  • On one hand, both parties want to improve the overall detection performance since they are using the same network. On the other hand, sharing traffic information/intrusion alerts may lead to privacy leakage.
E.g., if the IDSs detect the attacks by monitoring the traffic volume, then for IDSs from different organizations, they are not willing to share their traffic information directly with others due to privacy concerns.

- How could these IDSs determine their collaboration strategies, i.e., how much information about the traffic volume should one IDS share with another one?
Objectives

• Given
  • Multiple IDSs monitoring different parts of the same network but belong to different organizations.
  • Different organizations may have different detection and privacy requirements.

• Goals
  • Design a collaboration scheme which gives the best collaboration strategies of all the IDSs.
  • Analyze how detection requirements and privacy constraints would affect the best strategies.
Challenges

1. Intuitively, gathering more traffic information/intrusion alerts would improve the detection performance, but how much the detection rate would increase knowing these extra information?
An information theoretical view

- An IDS accepts and analyzes an input data stream and produces alerts that indicate intrusions.
- The input data stream has two possible status: intrusive (X=1) and normal (X=0).
- The IDS has two possible output: Alert (Y=1), No alert (Y=0)
- Measure the detecting capability: *Intrusion Detection Capability*

$$C_{ID} = \frac{I(X; Y)}{H(X)} = \frac{H(X) - H(X|Y)}{H(X)}$$

- Mutual information measures the reduction of uncertainty of the input by knowing the IDS output.
• The intrusion alerts are exchanged in the collaboration process.
• Knowing others’ detection result would help reduce the uncertainty of the input.
• The resulting intrusion detection capability can be calculated
  \[
  \bar{C}_{ID} = \frac{H(X) - H(X|Y_1, Y_2)}{H(X)}
  \]
2. We need to explore possible methods to protect privacy, and also develop new metrics that can quantify how much privacy is preserved under different collaboration strategies.

• An original alert with type FTP_Glob_Expansion is:
  {SrcIP=10.20.1.1, SrcPort=1042, DestIP=10.10.1.1, DestPort=21, StartTime: 11-10-2004, 15:45:10, EndTime =11-10-2004 15:45:10 }

• Assume DestIP is sensitive, then we may sanitize DestIP to be DestIP=10.10.1.0/24 (network address)

• The privacy been protected could be measured by the entropy introduced by the sanitization.
• The privacy can be measured by the entropy introduced by sending correct information with probability $P$. 

\[\text{Decision}\]

\[
\begin{align*}
\text{IDS1} & : 
\begin{array}{c}
\text{X1} \\
1 & \text{1-FN}_1 \\
0 & \text{FN}_1 \\
0 & \text{1-FP}_1 \\
1 & \\
0 & \\
0 & \\
\end{array}
\begin{array}{c}
\text{Y1} \\
1 \\
0 \\
1 \\
0 \\
0 \\
0 \\
\end{array}
\end{align*}
\]

\[
\begin{align*}
\text{IDS2} & : 
\begin{array}{c}
\text{X2} \\
1 & \text{1-FN}_2 \\
0 & \text{FN}_2 \\
0 & \text{1-FP}_2 \\
1 & \\
0 & \\
0 & \\
\end{array}
\begin{array}{c}
\text{Y2} \\
1 \\
0 \\
1 \\
0 \\
0 \\
0 \\
\end{array}
\end{align*}
\]

\[
\begin{align*}
\text{Y2} & : 
\begin{array}{c}
\text{P} \\
1 \\
0 \\
1 \\
0 \\
0 \\
\end{array}
\begin{array}{c}
\text{Y3} \\
1 \\
0 \\
\end{array}
\end{align*}
\]
Challenges

3. All the IDSs are motivated to cooperate honestly since they are sharing the same network. Nonetheless, it is possible that some of the IDSs are compromised and thus send false information to mislead the others. Also, there may be some selfish IDSs who are not willing to cooperate.

- After receiving the traffic information/intrusion alerts, the IDS could compare the similarity between these information and drop the dissimilar ones.
- IDSs could maintain behavior profiles for other IDSs for abnormal behavior detection.
Success Criteria

• Satisfy the privacy requirements while still allowing effective collaboration.

• Present a tradeoff curve which facilitates the determination of the operation point according to application-specific requirements.

• Achieve the same goals as above in the presence of security attacks (e.g., compromised IDSs).
Thanks!

Questions?