Intrusion Detection System: Facts, Challenges and Futures

By Gina Tjhai

13th March 2007

Network Research Group

Overview

- Introduction
- Challenges of current IDS
- Potential solutions
- Alarm Correlation
- Existing methods of Alarm Correlation
- Future IDS developments

Introduction

What is actually Intrusion Detection System (IDS)?

- A component of computer and network infrastructure which is aimed at detecting attacks against computer systems and networks, or information system.

IDS implementation:

- As a hardware installed on the network
- Or as an agent on an existing piece of hardware that is connected to the network.

Introduction

- Component of IDS
  - Information Collection
  - Detection
  - Response
- Parameters of IDS
  - Accuracy
  - Performance
  - Completeness

Introduction

IDS Classification

- Sources
  - Application-based
  - Host-based
  - Network-based
  - Hybrid
- Detection Mechanism
  - Misuse detection
  - Anomaly based
  - Hybrid
- Response
  - Active
  - Passive

Challenges of IDS

- Runtime limitations
- Specification of detection signatures
- Dependency on environment

High rate of false alarms – the limiting factor for the performance of an intrusion detection system

Is fine-tuning effective?

Potential Solutions

- *Data mining*

  The creation of complex database which is used to record data related to specific activities. Through the data generated, a pattern or model will be developed by knowledge seeker based on the accumulated data processed by the algorithm implemented on the front end application.

- *Examples:*
  - Applying the concept of root cause (“the reason for which alerts occur”) (Dain and Cunningham 2001)
  - Sequential pattern mining and episode rules (Lee and Stolfo 2000)

Potential Solutions

- *Machine learning technique*

  Referring to a system capable of the autonomous acquisition and integration of knowledge

- Example:
  - Alert Classification → true positives and false positive (Pietraszek 2004)

Potential Solutions

- *Co-simulation mechanism (based on a biological immune mechanism)* (Qiao and Weixin 2002)
  - Integrating the misuse detection technique with the anomaly detection technique
  - Applying a co-stimulation mechanism

Alarm Correlation

Alert Correlation

"Correlating alarms": combining the fragmented information contained in the alert sequences and interpreting the whole flow of alerts

Functional requirements:

- Modifying alarms
- Suppressing alarms
- Clearing active alarms
- Generating new alarms
- Delaying alarms

Existing methods of Alarm Correlation

- **Correlating alerts based on the prerequisites of intrusion** → providing a high level of representation of the correlated alerts, and thus reveals the structure of series of attacks. (Ning et al. 2001)

- **Correlating alerts based on the similarities between alert features** → grouping alerts into scenario depending on the number of matching attributes from the most general to the most specific cases. (Debar and Wespi 2001)

Existing methods of Alarm Correlation

- **Alarm correlation based on chronicle formalism** → multi-event correlation component using input IDS alerts (Morin and Debar 2003)
- **Probabilistic approach to alert correlation** → providing a mathematical framework for fusing alerts that match closely but not perfectly (Valdes and Skinner 2001)

Future Development of IDS techniques

Why use Artificial Intelligence?

- Flexibility (vs. threshold definition)
- Adaptability (vs. specific rules)
- Pattern Recognition (and detection of new patterns)
- Faster computing (faster than human)
- Learning abilities

AI tools:

- Neural Network
- Fuzzy logic
- Others

Future Development of IDS techniques

Artificial Neural Network

Neural Network → identifying the typical characteristics of system user and statistically identify significant variations from the user's established behaviours.

Type of Neural Network

- Multilayer perceptron
- Self Organising Map
- Radial basis neural networks
- Support Vector Machine
- Other

Future Development of IDS techniques

***Potential implementation of Artificial Intelligence techniques on alert correlation*:**

- Multilayer perceptron and Support Vector Machine
  - Probabilistic output of these methods support the causal relationships of alerts, which is helpful for constructing attack scenarios (Zhu and Ghorbani 2006)
- Fuzzy Cognitive Modelling
  - A causal knowledge based reasoning mechanism with fuzzy cognitive modelling is used to correlate alerts by discovering causal relationships in alert data (Siraj and Vaughn 2005)

Conclusions

- The problem of high false alarm rate has become one of the most critical issues faced by IDS today.
- The future of IDS lies on data correlation
- Alarm correlation mechanism aims at acquiring intrusion detection alerts and relating them together to expose a more condensed view of the security issues.
- Artificial Intelligence plays an important role in improving the performance of IDS technology.

Conclusions

Benefit of Artificial Intelligence:

- Flexibility (vs. threshold definition)
- Adaptability (vs. specific rules)
- Pattern Recognition (and detection of new patterns)
- Faster computing (faster than human)
- Learning abilities

References

- Allen, J., Christie, A. et al (2000), 'State of the Practice of Intrusion Detection Technologies', Technical Report CMU/SEI-99-TR-028, Carnegie Mellon University, available online: http://www.sei.cmu.edu/publications/documents/99.reports/99tr028/99tr028abstract.html, date visited: 22 January 2007
- Lee, W., Stolfo, S.J. (2000), "A Framework for Constructing Features and Models for Intrusion Detection Systems", ACM Transactions on Information and System Security 3(4) pp. 227-261
- Pietraszek, T., Tanner, A. (2005), "Data mining and machine learning - Towards reducing false positives in intrusion detection", Information security technical report [1363-4127] 10(3) pp. 169-183
- Pietraszek, T.: Using Adaptive Alert Classification to Reduce False Positives inIntrusion Detection. In Jonsson, E., Valdes, A., Almgren, M., eds.: RAID '04:Proc. 7th Symposium on Recent Advances in Intrusion Detection. Volume 3224 ofLNCS., Springer-Verlag (2004) 102–124
- Julisch, K. (2001), "Mining Alarm Clusters to Improve Alarm Handling Efficiency", In:ACSAC '01: Proc. 17th Annual Computer Security Applications Conference (AC-SAC), ACM Press pp. 12–21
- Siraj, A., Vaughn, R. (2005), "A Cognitive Model for Alert Correlation in a Distributed Environment" Lecture Notes in Computer Science vol. 3495/2005, pp. 218-230

References

- Qiao, Y., Weixin, X.: A Network IDS with Low False Positive Rate. In Fogel,D.B., El-Sharkawi, M.A., Yao, X., Greenwood, G., Iba, H., Marrow, P., Shackleton,M., eds.: CEC '02: Proc. IEEE Congress on Evolutionary Computation, IEEE Computer Society Press (2002) 1121–1126
- Ning, P., Reeves, D., Cui, Y. (2001) "Correlating Alerts Using Prerequisites of Intrusions" Technical Report TR-2001-13, North Carolina State University
- Debar H. and A. Wespi. (2001) "Aggregation and Correlation of Intrusion-Detection Alerts", In Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection, Davis, CA, USA, pp. 85-103, October 2001
- Valdes, A. and Skinner, K. (2001), "Probabilistic Alert Correlation", In Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection, Davis, CA, USA, October, pp. 54-68
- Morin, B., Debar, H., "Correlation of Intrusion Symptoms: an Application of Chronicles" (2003), Proceedings of the 6th symposium on Recent Advances in Intrusion Detection (RAID 2003), Carnegie Mellon University, Pittsburg, PA,. Springer LNCS 2820, pages 94-112.
- Zhu, B., Ghorbani, A. (2006), "Alert Correlation for Extracting Attack Strategies", International Journal of Network Security 3(2), pp. 244-258


Q & A
Thank You