AI-DRIVEN APPROACH FOR ACCESS CONTROL LIST MANAGEMENT

AUTHORS: SHAHATA NADER, HIROKAZU HASEGAWA, HIROKI TAKAKURA
EMAILS: nader@nii.ac.jp, hasegawa@nii.ac.jp, takakura@nii.ac.jp

NATIONAL INSTITUTE OF INFORMATICS
CENTRE FOR STRATEGIC CYBER RESILIENCE RESEARCH AND DEVELOPMENT
TOKYO - JAPAN
Name: Nader Shahata

Career title: Project Researcher at National Institute of Informatics (NII).

Research Interests: Internet Security, Artificial Intelligence and Cloud Computing
Outline

• Introduction
• Background
• Objectives and Goals
• Proposed Idea
• Architecture Overflow
• Architecture Proposal
• Conclusion
Introduction

• Securing our activities online has become a crucial component of our daily life
• Access Control models are essential components in the field of information security
• When our systems are infected, malicious activities removal can be challenging
Background

• ACL systems have some weaknesses
  - Managing an ACL system can be very challenging.
  - ACL maintenance calls for constant work and modification.
  - The ACL needs to be manually updated if the environment changes.

• The network analyst needs to maintain a high number of access control entries which could affect the performance of the network.
  - Managing alerts from an Intrusion Detection System (IDS) can be a challenging task for a network analyst.
  - The volume of these alerts can overwhelm analysts, which may cause inaccurate response taking.
Objective and Goals

• To propose an architecture that can help in increasing the organization’s network security.

• To find an alternative way in dealing with updating ACL rather than depending on the current manual approach.

• To apply AI for generating countermeasures based on ACL rules.

• Helping network analysts when receiving alerts coming from anomaly detection methods (IDS).
Proposed Idea
AI Access Control Advantages

- Detecting New Threats
- Battling Bots
- Breach Risk Prediction
AI Methods

• There are several AI methods such as: Machine learning, natural language processing and deep learning.

• Machine learning will be our preference among them.

• Machine learning models can learn and adapt to new patterns and anomalies without the need for manual rule updates

• It can help in system’s continuous improvement
Architecture Overflow

- Network Traffic
- Firewall Access Logs
- IDS
- Access Rules
- ACL Alerts
- User Activity
- Resource Access Logs
- Existing ACL
- Un/Supervised Detection
- Access Policies
- Anomaly Detected Alerts
- Detected Risk

Data Collection

- Collected Data
- Suspicious behavior
- Access Optimization
- Analyzing Suitable Network

Anomaly Detection

ACL Management

- Access Optimization
- Analyzing Suitable Network

Analysis

Countermeasures

Secure Network

Network Access Logs
Architecture Proposal

Old Alerts: Alerts before ACL applying
New Alerts: Alerts after ACL applying

IDS

Data Processing

Countermeasure

New Alerts

Analyst

Network

Traffic

Network Settings

ACL and Firewalls for Countermeasure

ACL Management Training

Integration

Existing ACL

Network Equipment Deployer

Analyst

Architecture Proposal

Analysis Results
How ACL will be Analyzed

• **Source**: (user, IP address) asking for access.
• **Permission**: What actions will be taken (allowing or denying)
• **Resource**: Which resource (e.g. server) the user applies to.
• **Conditions**: Any conditions that must be met for the rule to be applied.

Checking for Consistency

Identifying Incompatible Rules
Assumptions

✓ The data will be available.
✓ The AI-ACL based model has to be continuously trained.
✓ A precise definition of anomalies is necessary
✓ Access control policies must be predefined and available.
✓ Constant learning and adaptation.
Challenges

• The threat landscape is also continually changing, with new attack vectors appearing frequently.
• False positives and false negatives are possible.
• The Use of VPN
Conclusion

• Managing ACLs for analyzing suspicious traffic and for generating relevant countermeasures.
• Creating wise access control decisions by adopting an AI-based ACL.
• Predicting possible risks that may occur before an incident may happen.
• Helping Network Analysts in identifying alerts efficiently.
Reference List

THANK YOU