Review of Automated Intrusion Detection System Journals

Narshion Ngao
SCT-C004-3717-2017 Msc. Computer Systems - 2018
Jomo Kenyatta University of Agriculture & Technology
Course: ICS 3210 - Information Systems Security and Audit

***Abstract*— This is a review of journals in the area of using Artificial Intelligence for Intrusion Detection and Prevention Systems. The journals have discussed the milestones that have been achieved in the area of network security particularly intrusion detection. They has also highlighted several Machine Learning algorithms that can be applied in this area to improve the IDS systems. Four articles have been reviewed titled as follows: -**

1) **Automatic Detection and Correction of Vulnerabilities using Machine Learning by Robin Tommy and others.**
2) **Machine Learning Classification Model For Network Based Intrusion Detection System by Sanjay Kumar and others**
3) **Preventing Attacks and Detecting Intruder for Secured Wireless Sensor Networks by Gauri Kalnoor and Jayashree Agarkhed**
4) **Web Application Security: Threats, Countermeasures, and Pitfalls by Hsiu-Chuan Huang and others.**

The following text describes a brief overview of what these articles have reviewed in this field.

I. Automatic Detection and Correction of Vulnerabilities using Machine Learning

A. Authors

(Robin Tommy, Gullapudi Sundeep and Hima Jose, 2017).

B. Overview

This paper reviews machine learning approaches for prevention, detection and correction of vulnerabilities. It focuses on web applications particularly those published over the internet. The main concern here is that many web applications have undetected vulnerabilities and allow for threats to maximize an attack. A discussion of software testing has been provided in the introduction. Between the two main types of testing, white box and black box, the latter is considered a better approach to use when designing an intrusion detection algorith as it mimicks an attack. Black box testing is also called penetration testing. Various methods of securing web applications have been highlighted including firewalls, Bug Terminating Bots and IDS systems. The components of an IDS system have also been discussed in broader terms and then in more detail during the discussion on implementation of an IDS algorithm. The following key areas formed the main text of this paper.

- Components of a Machine Learning IDS System
- Implementation
- Case Study

C. Components of a Machine Learning IDS System

1) Scanners: In web application security, scanners refer to the web crawlers that automatically browse web pages to find vulnerabilities based on tests done on them. They collect the data needed to train the model and are also used to improve the model using re-scan feature. The main types of threats on the web are SQL injections and cross site scripting.

2) Fortifier: After the scanner is read the traffic, a fortifier is used to correct the vulnerabilities that have been detected. It suggests to the user to fix the vulnerability by providing a secure code that can be used in the stead of the weaker one.

3) Centralized Server: This component maintains the details of all the existing vulnerabilities and current patches. It uses Support Vector Ma-

chine algorithms to improvise performance of its web scans.

4) Firewall: Helps protect the web application from known malicious web users and denial of service attacks.

D. Implementation

This section describes how a machine learning algorithm can be implemented for intrusion detection and prevention in a web application use case. A Bug Terminating Bot (BTB) is an example of such algorithms. The paper has reviewed how it was implemented.

E. Case Study

Finally the paper discusses a test case in which the BTB was used, its performance results and graph showing how effective the application was in detecting vulnerabilities.

II. Machine Learning Classification Model For Network Based Intrusion Detection System

A. Authors

(Sanjay Kumar, Ari Viinikaineny and Timo Hamalainenz, 2016)

B. Overview

This papers focuses on Machine Learning models for Network Intrusion Detection Systems particularly around the android mobile system. A survey at Alcatel-Lucent indicated that 71 percent of smart phones do not have an antivirus and a mobile antivirus can detect only 50 % of threats. It is evident that providing an extra layer of security at the network level can help protect many mobile subscribers. This research work evaluated the effectiveness of machine learning techniques in network-based intrusion detection systems. It also underpins the main objectives of such an implementation as being: -

- to increase the detection rate
- to reduce false positives
- to detect unknown threats.

The research started with an enumeration of all mobile threats, then went on to review several Network based Intrusion Detection Systems and then settled on an implementation model.

C. Network based Intrusion Detection Systems

This is an IDS that monitors traffic for any suspicious, anomalous or unauthorised activity which could result to a cyber attack. They are based on two categories: 1, Misuse Detections - which are signature based and 2, Anomaly Detection which are behaviour based. A review of datasets used in network intrusion detection was discussed including mobile based datasets which enumerate specific mobile threats.

D. Machine Learning Classification Model

The paper dived deep into the implementation of a classification model for network intrusion detection. First we highlight the steps for building a machine learning classifier are: -

1) Traffic Generation
2) Preprocessing
3) Building Machine learning classification model
4) Evaluation of Machine learning classifiers

1) Traffic Generation: This is a sensor for getting both benign and malicious data that will be fed into the model.

2) Preprocessing: Labeling of datasets and generation of classifiers. Including defining evaluation techniques.

3) Building Machine learning classification model: These were built using decision trees and rule based algorithms.Machine Learning algorithms that were used in this research are J48, Random Forest, RIDOR, JRIP and PART.

4) Evaluation of Machine learning classifiers: Several experiments were performed on different datasets in order to evaluate the performance of the model based on Machine Learning classifiers. Eight Datasets were created according to different criteria and conditions. Validation methods used were cross validation and percentage split.

Several experiments were conducted and the paper has put in place the results of the experiment. In its conclusion, the final outcome of this research is that the model developed in this research was able to detect known and unknown threats. Although, mNIDS produced high accuracy, but it can be further improved when it will be used with in conjunction with the traditional intrusion detection systems.

III. Preventing Attacks and Detecting Intruder for Secured Wireless Sensor Networks

A. Authors

(Gauri Kalnoor and Jayashree Agarkhed, 2016)

B. Overview

This paper talks about wireless sensor networks, their use cases and implementations. A new type of Intrusion Detection System is proposed called hybrid IDS. Hybrid IDS is a type of IDS that considers the advantages of both misuse-based (and signature-based) and anomaly based detection IDS.

C. Intrusion Detection Approaches

Various approaches for intrusion detection have been discussed. In summary, there are distributed approaches which are based on multi-agent IDS frameworks for wireless sensor networks. The other major category is the hybrid IDS systems that are based on probability on trust, isolation and detection.

D. Intrusion Detection and Prevention Algorith

Two algorithms are demonstrated using pseudo codes and a discussion on implementation. One based on distributed and the other based on hierarchy.

E. Results

Analysis and metrics on performance of the models have been described. The following methods were used: -

- Detection Rate (DR) of an Intruder attack
- False Positive Rate (FPR)
- The False Alarm Rate
- Accuracy Rate
- Forward transmission ratio FT

In conclusion, WSN is an emerging technology and is applied in various applications like object tracking, military applications and smart homes. Since, WSN are vulnerable to several attacks as they are deployed in an open and unprotected environment. Security is an important feature for the deployment of Wireless Sensor Networks.

IV. Web Application Security: Threats, Countermeasures, and Pitfalls

A. Authors

(Hsiu-Chuan Huang, Zhi-Kai Zhang, Hao-Wen Cheng, and Shiuhpyng Winston Shieh, 2017)

B. Overview

According to the most recent security reports, more than 229,000 attacks against websites occur each day, and more than 76 percent of websites contain unpatched vulnerabilities. This paper therefore focuses on identifying threats of these attacks, counter measures that can be applied and challenges encountered so far!

C. Threats

The most common threats in web applications are: -

1) SQL Injections
2) Cross-site scripting

1) SQL Injections: These are attacks on web pages that take advantage of poorly written database queries. They exploit the application by using smart codes to induce their malicious code through the database.

2) Cross-site scripting: These happen when web pages outputting information are not properly escaped. The attacker is able to introduce client side code like javascript that can run on a users computer once the page is opened.

D. SQL INJECTION AND XSS COUNTERMEASURES

The below counter measures were discussed in this paper: -

1) Secure implementation: Making sure that all code that reads or writes databases is safely escaped using tools like ”mysql real escape” and code that outputs to browsers is escaped.

2) Penetration testing: Conducting rigorous white-box testing to identify all vulnerabilities and effectively implementing the right measures to remove the vulnerabilities.

3) Defense mechanism deployment: Implementing web application firewalls that are able to scan all inbound traffic and can detect attacks.

V. CONCLUSIONS

The field of artificial intelligence is gaining momentum especially in this new era of advanced computing. various fields such as Information Systems Security are now taking advantage of this field to optimize security in systems and provide more secure networks.

REFERENCES

[1] Robin Tommy, Gullapudi Sundeep and Hima Jose, 2017. Automatic Detection and Correction of Vulnerabilities using Machine Learning.

[2] Sanjay Kumar, Ari Viinikaineny and Timo Hamalainenz, 2016. Machine Learning Classification Model For Network Based Intrusion Detection System

[3] Gauri Kalnoor and Jayashree Agarkhed, 2016. Preventing Attacks and Detecting Intruder for Secured Wireless Sensor Networks.

[4] Hsiu-Chuan Huang, Zhi-Kai Zhang, Hao-Wen Cheng, and Shiuhpyng Winston Shieh, 2017. Web Application Security: Threats, Countermeasures, and Pitfalls