



Institutional Sign In

All



[ADVANCED SEARCH](#)

Conferences > 2024 International Conference... ?

Detection of Zero-Day Attacks on IoT

Publisher: IEEE [Cite This](#) [PDF](#)

Shay Reardon ; Murtadha D. Hssayeni ; Imadeldin Mahgoub **All Authors** ...



170
Full
Text Views

Alerts

[Manage Content Alerts](#)
[Add to Citation Alerts](#)

Abstract



Download
PDF

Document Sections

- I. Introduction
- II. Methodology
- III. Results and Discussions
- IV. Conclusion

Abstract:

Zero-day attacks are cybersecurity attacks that seek to exploit an unknown vulnerability in Internet of Things (IoT). This makes zero-day attacks inherently difficult to ... [View more](#)

Metadata

Abstract:

Zero-day attacks are cybersecurity attacks that seek to exploit an unknown vulnerability in Internet of Things (IoT). This makes zero-day attacks inherently difficult to detect and costly to network administrators. Current methods of detection utilize machine learning methodologies for intrusion detection. However, these methods suffer from low performance in specific zero-day attacks. This study proposes novel features built upon network flow and raw packet data aiming to detect zero-day attacks. Our testing approach utilizes fix traditional machine learning algorithms (Decision Tree (DT), Support Vector Machine (SVM), K-Nearest Neighbor (KNN), Logistic Regression (LR), Gaussian Naive Bayes (NB), and Random Forest (RF)) with split-at-scenario cross-validation. We find that our engineered features achieve consistent high detection rates with three models (DT, SVM, and RF), whereas these models fail to detect at least one of the attacks when using raw features. Our results display potential for utilizing the proposed flow-based complex features to detect unknown network attacks with Internet of Battle Things (IoBT) applications.

Published in: 2024 International Conference on Smart Applications, Communications and Networking (SmartNets)

Date of Conference: 28-30 May 2024

DOI: 10.1109/SmartNets61466.2024.10577735

Date Added to IEEE Xplore: 05 July 2024

Publisher: IEEE



► ISBN Information:

Conference Location: Harrisonburg, VA, USA

▼ ISSN Information:

☰ Contents

I. Introduction

Zero-day attacks are cybersecurity attacks that seek to exploit a vulnerability that is unknown to network administrators. This vulnerability is known as a zero-day vulnerability. While the vulnerability remains unknown, the developers cannot patch it, and anti-virus software cannot detect attacks exploiting it. But, by the time developers find the vulnerability or attack, the damage to the company or consumer has already been done. Zero-day cost an average of 1.2 million USD per attack [1], [2] and can last an average of 312 days [3]. It is estimated that every 17 days one of these attacks is discovered [4]. Also, there is a 15 % increase in these attacks. To monitor for these costly attacks, Intrusion Detection Systems (IDS) are required to detect zero-day attacks and vulnerabilities.

Authors



Figures



References



Keywords



Metrics



More Like This

Construction of a Meteorological Data Support Vector Machine Drought Prediction Model Based on Machine Learning Algorithms
2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON)
Published: 2024

Wi-Fi Network Intrusion Detection: Enhanced with Feature Extraction and Machine Learning Algorithms
2024 8th International Artificial Intelligence and Data Processing Symposium (IDAP)
Published: 2024

Show More

IEEE Personal Account

CHANGE
USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS
VIEW PURCHASED
DOCUMENTS

Profile Information

COMMUNICATIONS
PREFERENCES
PROFESSION AND
EDUCATION
TECHNICAL INTERESTS

Need Help?


US & CANADA: +1 800
678 4333

WORLDWIDE: +1 732
981 0060

CONTACT & SUPPORT

Follow

f  **in** 

About [IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [IEEE Ethics Reporting](#)  | [Sitemap](#) | [IEEE Privacy Policy](#)

A public charity, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2024 IEEE - All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies.

IEEE Account

- » [Change Username/Password](#)
- » [Update Address](#)

Purchase Details

- » [Payment Options](#)
- » [Order History](#)
- » [View Purchased Documents](#)

Profile Information

- » [Communications Preferences](#)
- » [Profession and Education](#)

» [Technical Interests](#)

Need Help?

» **US & Canada:** +1 800 678 4333

» **Worldwide:** +1 732 981 0060

» [Contact & Support](#)

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2024 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.