ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Keyed Oddity Detection System of Key-Recovery Attacks on Kids

Dr.Prasada Rao Mandala, M.Tech, Ph.D
Professor,
Dept of CSE,
Avanthi's St.Theressa institute of Engineering and Technology, Garividi, Vizianagaram,
Andhra Pradesh, India.

Yernagula Dhana Lakshmi
M.Tech,
Dept of CSE,
Avanthi's St.Theressa institute of Engineering and Technology, Garividi, Vizianagaram,
Andhra Pradesh, India.

ABSTRACT:
Most anomaly detection systems rely on machine learning algorithms to derive a model of normality that is later used to detect suspicious events. Some works conducted over the last years have pointed out that such algorithms are generally susceptible to deception, notably in the form of attacks carefully constructed to evade detection. Various learning schemes have been proposed to overcome this weakness. One such system is Keyed IDS (KIDS), introduced at DIMVA "10. KIDS" core idea is akin to the functioning of some cryptographic primitives, namely to introduce a secret element (the key) into the scheme so that some operations are infeasible without knowing it. In KIDS the learned model and the computation of the anomaly score are both key-dependent, a fact which presumably prevents an attacker from creating evasion attacks. In this work we show that recovering the key is extremely simple provided that the attacker can interact with KIDS and get feedback about probing requests. We present realistic attacks for two different adversarial settings and show that recovering the key requires only a small amount of queries, which indicates that KIDS does not meet the claimed security properties. We finally revisit KIDS' central idea and provide heuristic arguments about its suitability and limitations.

INDEX TERMS:
Adversarial classification, anomaly detection, intrusion detection systems, secure machine learning

1. INTRODUCTION:

In recent years use of internet has been increased tremendously.

Most of people used internet to transmit their data and used cloud to save it. There is possibility that the data may get hacked and get misused. For better protection from such unauthorized users various Anomaly intrusion detection schemes are introduced in recent year. Security problem mainly divided into two groups one is malicious and other is non malicious activity. A malicious attack is an attempt to forcefully abuse or take advantage of someone's computer, whether through computer viruses, social engineering, phishing, or other types of social engineering. This can be done with the intent of stealing personal information (such as in social engineering) or to reduce the functionality of a target computer. Malicious Code mostly Hide in Email, Web Content, Legitimate Sites, File Downloads. For example Trojan, Horse, Viruses, Worms, Phishing, Baiting, Spam. Non-malicious attacks occur due to poor security policies and controls that allow vulnerabilities and errors to take place. An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. NIDS is a network security system focusing on the attacks that come from the inside of the network (authorized users). Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. So attacker always try to avoid detection. In terms of network security the evasion attack means bypass a flaw in a security

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

system that allows an attacker to circumvent security mechanisms to get system or network access in order to deliver an exploit, attack, or other form of malware without detection. Evasions are typically used to counter network-based intrusion detection and prevention systems but can also be used to bypass firewalls. A further target of evasions can be to crash a network security device, rendering it in-effective to subsequent targeted attacks. Few detection schemes are introduced in last decade to protect from such evasion attacks. KIDS (Keyed Intrusion Detection System) one of the scheme to avoid evasion attacks. KIDS first time introduced by Mrdovic and Drazenovic at DIMVA'10.Most current network attacks happen at the application layer, analysis of packet payload is necessary for their detection. Unfortunately malicious packets may be crafted to normal payload, and so avoid detection if the anomaly detection method is known. Model of normal payload is key dependent. Key is different for each implementation of the method and is kept secret. Therefore model of normal payload is secret although detection method is public.

This prevents attacks. Payload is partitioned into words. Words are defined by delimiters. Set of delimiters plays a role of a key. This paper is organized as follows. General background of adversarial machine learning in Section 2. Section 3 illustrates the KIDS scheme. Section 4 explains the existing method and Section 5 includes the proposed method . The final section provides a conclusion for our proposed approach.

2. LITERATURE SURVEY:

2.1 PROBLEM STATEMENT:

Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems:

We present the traffic analysis problem and expose the most important protocols, attacks and design issues. Afterwards, we propose directions for further research. As we are mostly interested in efficient and practical Internet based protocols, most of the emphasis is placed on mix based constructions. The presentation is informal in that no complex definitions and proofs are presented, the aim being more to give a thorough introduction than to present deep new insights.

OLAR: On-Demand Lightweight Anonymous Routing in MANETs:

To protect secure MANET communications, several anonymous routing schemes have been proposed to date. However, most previous approaches sacrifice networking performance due to heavy cryptographic operations. In this paper, we devise an On-demand Lightweight Anonymous Routing (OLAR) scheme, applying the secret sharing scheme based on the properties of polynomial interpolation. OLAR is an identity-free routing scheme, which provides source and destination anonymity, end-to-end communication relation anonymity, as well as route anonymity. In addition, the proposed anonymous routing scheme highly decreases the overhead of data transmission, while making packets more untraceable compared to the previous solutions. The performance of OLAR is demonstrated by experiments and comparison.

2.2 PROBLEM SOL:

Reusing the evidence-based model, in this paper, we propose a novel statistical traffic pattern discovery system (STARS). STARS aims to derive the source/destination probability distribution. To achieve its goals, STARS includes two major steps, First is Construct point-to-point traffic matrices using the time-slicing technique, and then derive the end-to-end traffic matrix with a set of traffic filtering rules and the second is Apply a heuristic approach to identify the actual source and destination nodes, and then correlate the source nodes with their corresponding destinations. The best of our knowledge, STARS is the first statistical traffic analysis approach that considers the salient characteristics of MANETs: the broadcasting, ad hoc, and mobile nature and most of the previous approaches are partial attacks in the sense that they

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

either only try to identify the source nodes or to find out the corresponding destination nodes for given particular source nodes. STARS is a complete attacking system that first identifies all source and destination nodes and then determines their relationship.

3. KIDS-A KEYED INTRUSION DETECTION SYSTEM:

Mrdovic and Drazenovic [2] proposed Keyed Intrusion Detection System in which secret key plays important role. Network anomaly detector inspects packet payloads. The proposed method has 3 important steps for implementation of the key. 1)Training Mode In training mode payload divided into words. Words are nothing but the sequence of byte located between delimiters. From this any special two byte assign to secret set S. This set S again classified into normal words, frequency count. 2)Detection Mode In detection mode anomaly score get counted according to word frequency count. 3)Key Selection The Key got selected after its score and checking its detection quality. Repeating all three steps generates new key each time.

1) Training Mode:

In training mode payload divided into words. Words are nothing but the sequence of byte located between delimiters. From this any special two byte assign to secret set S. This set S again classified into normal words, frequency count.

2) Detection Mode:

In detection mode anomaly score get counted according to word frequency count.

3) Key Selection:

The Key got selected after its score and checking its detection quality. Repeating all three steps generates new key each time.

4. EXISTING SYSTEM:

Machine learning algorithms is detection systems rely in existing system. Some works have pointed out that such algorithms are generally susceptible to deception. Recent work has accurately pointed out that security problems differ from other application domains of machine learning in, at least, one fundamental feature: the presence of an adversary who can strategically play against the algorithm to accomplish his goals. A few detection schemes proposed over the last few years have attempted to incorporate defenses against evasion attacks. One such system is keyed intrusion detection system (KIDS), introduced by Mrdovic and Drazenovic at DIMVA'10. KIDS is an application-layer network anomaly detection system that extracts a number of features ("words")from each payload. Dalvi et al. explored the problem of computing optimal strategies to modify an attack so that it evades detection by a Na€ıve Bayes classifier.

DISADVANTAGES OF EXISTING SYSTEM:

- The main problem of this strategy is that it can influence negatively the overall detection performance, particularly increasing the false positive rate.
- When assessing the security of systems such as KIDS, one major problem comes from the absence of widely accepted adversarial models giving a precise description of the attacker's goals and his capabilities.
- Notably in the form of attacks carefully constructed to evade detection. PROPOSED SYSTEM One such system is Keyed IDS (KIDS) some cryptographic primitives, namely to introduce a secret element (the key) into the scheme so that some operations are infeasible without knowing it. In KIDS the learned model and the computation of the anomaly score are both key- dependent.

5. PROPOSED SYSTEM:

We argue that any keyed anomaly detection system (or, more generally, any keyed classifier) must

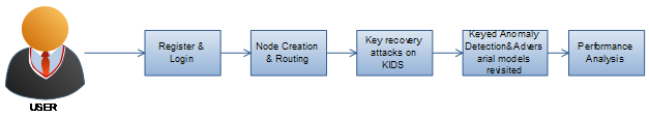
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

preserve one fundamental property: The impossibility for an attacker to recover the key under any reasonable adversarial model. We deliberately choose not to analyze how difficult is for an attacker to evade detection if the classifier is keyed. We believe that this is a related, but different problem. ϖ We pose the key-recovery problem as one of adversarial learning. By adapting the adversarial setting proposed by Lowd and Meek in a related problem (reverse engineering of a classifier), we introduce the notion of gray- and black-box key-recovery attacks. We present two instantiations of such attacks for KIDS, one for each model. Our attacks take the form of query strategies that make the classifier leak some information about the key. Both are very efficient and show that KIDS does not meet the fundamental security property discussed above. Furthermore, we have implemented and experimentally confirmed the correctness of our attacks.

ADVANTAGE OF PROPOSED SYSTEM:

- Prevents an attacker from creating evasion attacks.
- The attacker is to avoid detection

5.1 SYSTEM ARCHITECTURE:



Module Description:

- **Node Creation & Routing**

In this module, a wireless network is created. All the nodes are randomly deployed in the network area. Our network is a mobile network, nodes are assigned with mobility (movement).Source and destination nodes are defined.

Data transferred from source node to destination node. Since we are working in mobile network, nodes mobility is set ie., node move from one position to another.

- **Key- Recovery Attacks on Kids:**

When assessing the security of systems such as KIDS, one major problem comes from the absence of widely accepted adversarial models giving a precise description of the attacker's goals and his capabilities one such model for secure machine learning and discussed various general attack categories. Our work does not fit well within because our main goal is not to attack the learning algorithm itself, but to recover one piece of secret information that, subsequently, may be essential to successfully launch an evasion attack.

- **Keyed Anomaly Detection and Adversarial Models:**

Revisited closely related to the points discussed above is the need to establish clearly defined and motivated adversarial models for secure machine learning algorithms. The assumptions made about the attacker's capabilities are critical to properly analyze the security of any scheme, but some of them may well be unrealistic for many applications. One debatable issue is whether the attacker can really get feedback from the system for instances he chooses. This bears some analogies with Chosen-Plaintext Attacks (CPA) in cryptography. This assumption has been made by many works in secure ma-chine learning, including ours.

- **Performance Analysis and Result Comparison:**

For performance evaluation we use the following graph

– Packet delivery ratio
– Throughput
– Delay

6. CONCLUSION:

We addressed the problem of securely transmitting provenance for sensor networks, and proposed a light-weight provenance encoding and decoding scheme based on Bloom filters.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The scheme ensures confidentiality, integrity and freshness of provenance. We extended the scheme to incorporate data-provenance binding, and to include packet sequence information that supports detection of packet loss attacks. Experimental and analytical evaluation results show that the proposed scheme is effective, light-weight and scalable. In future work, we plan to implement a real system prototype of our secure provenance scheme, and to improve the accuracy of packet loss detection, especially in the case of multiple consecutive malicious sensor nodes.

REFERENCES:

[1] H. Lim, Y. Moon, and E. Bertino, "Provenance-Based Trustworthiness Assessment in Sensor Networks," Proc. Seventh Int'l Workshop Data Management for Sensor Networks, pp. 2-7, 2010.

[2] I. Foster, J. Vockler, M. Wilde, and Y. Zhao, "Chimera: A Virtual Data System for Representing, Querying, and Automating Data Derivation," Proc. Conf. Scientific and Statistical Database Management, pp. 37-46, 2002.

[3] K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, "Provenance-Aware Storage systems," Proc. USENIX Ann. Technical Conf., pp. 4-4, 2006.

[4] Y. Simmhan, B. Plale, and D. Gannon, "A Survey of Data Provenance in E-Science," ACMSIGMOD Record, vol. 34, pp. 31-36, 2005.

[5] R. Hasan, R. Sion, and M. Winslett, "The Case of the Fake Picasso: Preventing History Forgery with Secure Provenance," Proc. Seventh Conf. File and Storage Technologies (FAST), pp. 1-14, 2009.

[6] S. Madden, J. Franklin, J. Hellerstein, and W. Hong, "TAG: A Tiny Aggregation Service for Ad-Hoc Sensor Networks," ACM SIGOPS Operating Systems Rev., vol. 36, no. SI, pp. 131-146, Dec. 2002.

[7] K. Dasgupta, K. Kalpakis, and P. Namjoshi, "An Efficient Clustering Based Heuristic for Data Gathering and Aggregation in Sensor Networks," Proc. Wireless Comm. and Networking Conf., pp. 1948-1953, 2003.

[8] S. Sultana, E. Bertino, and M. Shehab, "A Provenance Based Mechanism to Identify Malicious Packet Dropping Adversaries in Sensor Networks," Proc. Int'l Conf. Distributed Computing Systems (ICDCS) Workshops, pp. 332-338, 2011.

[9] L. Fan, P. Cao, J. Almeida, and A.Z. Broder, "Summary Cache: A Scalable Wide-Area Web Cache Sharing Protocol," IEEE/ACM Trans. Networking, vol. 8, no. 3, pp. 281-293, June 2000.

[10] A. Kirsch andM. Mitzenmacher, "Distance-Sensitive BloomFilters," Proc.Workshop Algorithm Eng. and Experiments, pp. 41-50, 2006.

[11] C. Rothenberg, C.Macapuna, M.Magalhaes, F. Verdi, and A. Wiesmaier, "In-Packet Bloom Filters: Design and Networking Applications," Computer Networks, vol. 55, no. 6, pp. 1364-1378, 2011.

[12] M. Garofalakis, J. Hellerstein, and P. Maniatis, "Proof Sketches: Verifiable In-Netwok Aggregation," Proc. IEEE 23rd Int'l Conf. Data Eng. (ICDE), pp. 84-89, 2007.

Author's Details:

Dr.Prasada Rao Mandala, M.Tech, Ph.D
Professor, Dept of CSE, Avanthi's St.Theressa institute of Engineering and Technology, Garividi, Vizianagaram, Andhra Pradesh, India.

Yernagula Dhana Lakshmi
M.Tech, Dept of CSE, Avanthi's St.Theressa institute of Engineering and Technology, Garividi, Vizianagaram, Andhra Pradesh, India.