802.11 Network Intrusion Detection using Genetic Programming

Patrick LaRoche
Faculty of Computer Science
Dalhousie University
Halifax, Nova Scotia
B3H 1W5, Canada
plaroche@cs.dal.ca

A. Nur Zincir-Heywood
Faculty of Computer Science
Dalhousie University
Halifax, Nova Scotia
B3H 1W5, Canada
zincir@cs.dal.ca

ABSTRACT

Genetic Programming (GP) based Intrusion Detection Systems (IDS) use connection state network data during their training phase. These connection states are recorded as a set of features that the GP uses to train and test solutions which allow for the efficient and accurate detection of given attack patterns. However, when applied to a 802.11 network that is faced with attacks specific to the 802.11 protocol, the GP's detection rate reduces dramatically. In this work we discuss what causes this effect, and what can be done to improve the GP's performance on 802.11 networks.

Categories and Subject Descriptors

I.2.6 [**Artificial Intelligence**]: Learning—*Parameter learning*

General Terms

Algorithms, Security

Keywords

Genetic Programming, 802.11, WiFi, Intrusion Detection, Denial of Service

1. INTRODUCTION

Previous work on network intrusion detection systems using genetic programming techniques have been focused on efficiency and detection rates when applied to ethernet network audit data [7]. This work has improved the speed and accuracy of the GP based systems, while providing an end solution that is simple to understand. This transparency allows the solution to be easily decoded and used as rules and signatures for further attack detection. For this reason, we investigate the use of GPs as an intrusion detection system for 802.11 networks.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
GECCO'05, June 25–29, 2005, Washington, DC, USA.
Copyright 2005 ACM 1-59593-097-3/05/0006 ...$5.00.

GP based intrusion detection systems use network audit data in order to train and produce rules that detect network attacks. These network audit trails compose of features based on connection data. Past work has focused on the use of 8 *basic* features [7]. It has been shown that this feature selection has a high detection rate of 95.15% on Denial of Service attacks from the DARPA 98 Intrusion Detection Benchmark [6]. Unfortunately, this selection does not include features that are required to correctly identify low level attacks on the 802.11 MAC protocol. This omission results in a low detection rate when faced with such attacks.

By focusing on a 802.11 network, we must re-evaluate the feature selection of previous work. The selection of features must ensure that new attacks which target the MAC layer protocol of 802.11 networks are detectable. Specifically our work focuses on Denial of Service (DoS) attacks against the 802.11 MAC layer, of which wireless networks are vulnerable [3].

2. 802.11 SPECIFIC DOS ATTACKS

As shown by [1], a vulnerability exists in the MAC layer of the IEEE 802.11 protocol. This vulnerability allows for potential Denial of Service attacks to exploit the 802.11 MAC layer. In [3] Bellardo and Savage identified and demonstrated several 802.11 attacks that exploit these vulnerabilities and the severe effect they can have on network usability. For our work we focus on the Denial of Service attacks, specifically the de-authentication attack. By inserting this attack into an 802.11 network, it has been shown to eliminate the target client's ability to access the network [3].

This type of de-authentication attack is real and is easily performed on a 802.11 network using tools that are readily available. Some tools that are available to date are (that we are aware of) Airjack [5] and void11 [4] . These tools are not only readily available on the Internet but with some basic skill are easily implemented and deployed. It is the reality of these attacks that is the motivation behind training GP based intrusion detection systems for 802.11 networks.

3. FEATURE SELECTION

Previous work done by Song et al [7] has used a limited 8 *basic* features for training and testing of the GP. These features are described as "Basic features of an Individual TCP connection" [7] . Here in lies the problem, the training data is simply consisting of TCP connection data, but not frames associated with lower level protocol functions. The

result is data from MAC frames is never used during the training of the GP's solution, limiting the GP's ability to detect attacks that are only visible by watching these frames.

By omitting MAC layer frames from the training data, a denial of service attack that specifically targets weaknesses in the MAC layer of the 802.11 protocol are not detectable. If we include the 802.11 management frames [2], specifically the sequence number associated with the de-authentication frames [8] the GP will be given the appropriate data to adequately train itself. The current technique of using TCP connection data as the training and testing data for a GP based IDS fails to give the GP this required data to identify MAC protocol specific attacks.

4. DISCUSSION

By exploring the feature set selection for a GP that has been proven to be efficient in training time, effective in detection as well as transparent in its solution [7], we will allow the GP to correctly detect a new family of attacks, specifically 802.11 MAC protocol attacks. This will allow the GP based IDS to be implemented on a 802.11 network while still providing all the benefits achieved in previous work. By the addition of features from each frame on the network, we hope to increase the GPs ability to detect MAC protocol Denial of Service attacks without lengthening the training time. Future work will focus on allowing the GP to train and test in a distributed fashion over a 802.11 network.

5. ACKNOWLEDGMENTS

This research is supported by the NSERC Discovery and the CFI New Opportunities grants. This work is conducted as part of the NIMS project at `http://www.cs.dal.ca/projectx/`.

6. REFERENCES

[1] AusCERT. Denial of Service Vulnerability in IEEE 802.11 Wireless Devices . AusCERT AA-2004.02, Australian Computer Emergency Response Team, http://www.auscert.org.au/render.html?it=4091, 13 May 2004.

[2] IEEE-SA Standards Board. *ANSI/IEEE Std 802.11, 1999 Edition (R2003)*. IEEE, New York, NY, USA, 1999.

[3] J.Bellardo and S.Savage. 802.11 denial-of-service attacks: real vulnerabilities and practical solutions. In *USENIX Security Symposium*, pages 15–28, 2003.

[4] R. Lfoeter. Wireless Lan Security Framework htttp://www.wlsec.net/void11/, 2002.

[5] M. Lynn and R. Baird. Advanced 802.11 attack. *Black hat Briefings*, July 2002.

[6] D. Song, R. Curry, M. I. Heywood, and A. N. Zincir-Heywood. On the efficient mining of network audit data using genetic programming. In *GECCO 2004 Workshop Proceedings*, Seattle, Washington, USA, 26-30 June 2004.

[7] D. Song, M. I. Heywood, and A. N. Zincir-Heywood. A linear genetic programming approach to intrusion detection. In *Genetic and Evolutionary Computation – GECCO-2003*, volume 2724 of *LNCS*, pages 2325–2336, Chicago, 12-16 July 2003. Springer-Verlag.

[8] S. T, L. Y.-X., and H. Owen. Wireless Intrusion Detection and Response: A case study using the classic man-in-the-middle attack. In *IEEE Wireless Communications and Networking Conference*, Atlanta Ga., March 2004.