ISSN: 2349-5197
Impact Factor: 2.715

INTERNATIONALJOURNALOFRESEARCH SCIENCE& MANAGEMENT

SURVEY ON METHODS FOR EVASION ATTACK DETECTION

Mrs. Ashvinee N. Kharat ∗[1], Prof. Mr. (Dr.). B. D. Phulpagar[2]
∗[1]Student, Department of Computer Engineering, P.E.S Modern College of Engineering, Pune, India.
[2]Assistant Professor, Department of Computer Engineering, P.E.S Modern College of Engineering, Pune, India.

DOI: 10.5281/zenodo.831440
Keywords: Network Security, evasion attack, counter measures.

Abstract
Network security has become more necessary to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern and the history of security sanctions a better understanding of the emergence of security technology. Network attacks had become a curse to technology, where attacker destroy or gain illegal access to system recourses and restrict the legitimate users from accessing the information. In this paper, we are going study different type of network security attack and learn counter measures for that attack. We are also going to study different techniques to detect such attacks.

Introduction
The world is becoming more interconnected with the advent of the Internet and incipient networking technology. There is a large amount of personal, commercial, military, and government information on networking infrastructures ecumenical. Network security is becoming of great consequentiality because of intellectual property that can be easily acquired through the internet. Based on this research, the future of network security is forecasted. Incipient trends that are emerging will withal be considered to understand.

Network security:
System and network technology is a key technology for a vast variety of applications. Security is crucial to networks and applications. Although, network security is a critical requirement in emerging networks, there is a significant lack of There exists a "communication gap" between the developers of security technology and developers of networks. Network design is a well-developed process that is predicated on the Open Systems Interface (OSI) model. The OSI model has several advantages when designing networks. It offers modularity, flexibility, ease of use, and standardization of protocols. The protocols of different layers can be facilely coalesced to engender stacks which allow modular development. The implementation of individual layers can be changed later without making other adjustments, allowing flexibility in development.

When considering network security, it must be accentuated that the whole network is secure. Network security does not only concern the security in the computers at each end of the communication chain. When transmitting data, the communication channel should not be vulnerably susceptible to assail. A possible hacker could target the communication channel, obtain the data, and decrypt it and reinsert an erroneous message.
Securing the network is just as paramount as securing the computers and encrypting the message. When developing a secure network, the following need to be considered [1]:
a. **Access** – authorized users are provided the expedient to communicate to and from a particular network
b. **Confidentiality** – Information in the network remains private
c. **Authentication** – Ensure the users of the network are who they say they are
d. **Integrity** – Ensure the message has not been modified in transit
e. **Non-repudiation** – Ensure the user does not refute that he used the network

NETWORK ATTACKS
A. Denial of service Attack:
A Denial-of-Accommodation attack (DoS) occurs when an assailant continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages, and/or other commands. These cause legitimate users to does not be able to get on the network and may even

cause the network to crash. These attacks rely on the abuse of protocols such as the Extensible Authentication Protocol (EAP). The DoS attack in itself does little to expose organizational data to a malicious attacker, since the interruption of the network obviates the flow of data and authentically indirectly for fends data by obviating it from being transmitted. The usual reason for performing a DoS attack is to observe the recovery of the wireless network, during which all of the initial handshake codes are re-transmitted by all devices, providing an opportunity for the malicious attacker to record these codes and use sundry "cracking" implements to analyze security impotencies and exploit them to gain unauthorized access to the system.

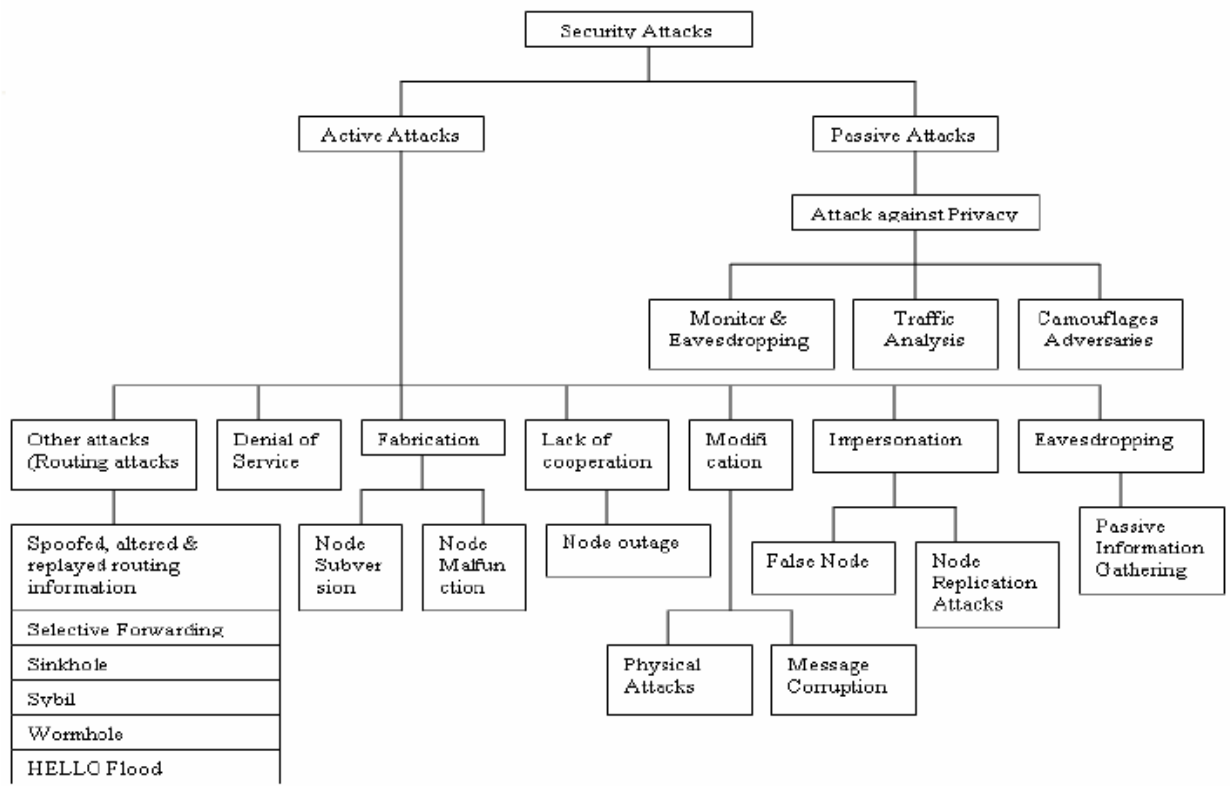

Figure 1: General Classification of Security Attacks

B. Jamming Attack:

Since RF (radio frequency) is essentially an open medium, jamming can be an immensely colossal quandary for wireless networks. Jamming is one of many exploits used compromise the wireless environment. It works by gainsaying accommodation to sanctioned users as legitimate traffic is jammed by the inundating frequencies of illegitimate traffic. A knowledgeable attacker with the right tools can easily jam the 2.4 GHz frequency in a way that drops the signal to a caliber where the wireless network cans no longer function.

C. Man in The Middle Attack:

The man-in-the-middle attack in cryptography and computer security is a form of active eavesdropping in which the assailer makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straight forward in many circumstances.

D. Interception Attack:

The wireless network used a username and password to allow access to the local network, the attacker can use a Wireless Sniffer for an attack. An attacker can sniff and capture legitimate traffic. Many of the tools that

accomplish this are based on capturing the first part of connection session, where the data would typically include the username and password. With this, the intruder can then be disguised as that user by using this captured information. Wireless sniffing requires the attacker to be within the range of the wireless traffic.

E. RAP Attack:

RAP (Rogue Access Points) have become an astronomically immense issue in wireless security. A Rogue Access Point is one connected to a network without authorization from an administrator. With low end access points steadily decrementing in price and incrementing in availability, RAPs have become much more common. Additionally, many of these access points contain features that make them proximately invisible when coupled with legitimate networks, doing a fine job to conceal their presence. Rogues Access Points are often created by employees looking for additional liberation in the work environment. Many employees simply bring in their access points from home and plug them right into their work stations and the company LAN without consent from administrators. These types of RAPs are potentially hazardous as many people who engender them are not cognizant of the security issues associated with a wireless network.

F. MAC Spoofing Attack:

MAC spoofing attacks are attacks launched by clients on a Layer 2 network. Assailers spoof their MAC address to perform a man-in-the-middle (MiTM) attack. In one common attack, the attacker pretends to be the default gateway and sends out a gratuitous Address Resolution Protocol (ARP) to the network so that users send their traffic through the attacker rather than the default gateway. The attacker then forwards user traffic to the real default gateway. An assailant on an expeditious enough host can capture and forward packets so that victims do not notice any change in their network access. Many implements available for download from the Internet, such as Ettercap, can accomplish such a task, and obviating such attacks is quite problematic.

ATTACK DETECTION METHOD

A. Multimodal biometric systems against spoofing attacks:

Multimodal biometric systems have been originally proposed to improve the personal identity recognition performance, through the combination of information coming from different biometric traits, which can surmount the constraints and the impuissance's intrinsically in every individual trait. A multimodal biometric system is made up of two or more sensors, each one based on a different biometric trait. The information emanating from the sensors can be integrated at different calibers: sensor, feature, matching score, and decision [30]

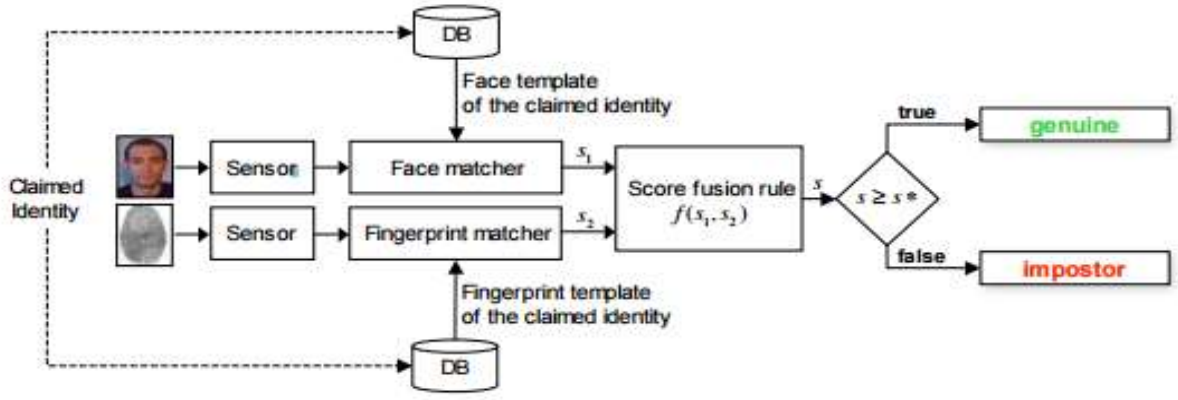

Figure 2: A bimodal biometric system made up of a fingerprint and a face sensor, whose matching scores are combined through a fusion rule

Such a multimodal system operates as follows (see also Fig. 2). At the design phase, authorized users (clients) are enrolled: their biometric traits are stored in a database, together with the corresponding identities. During

operation, each user submits the requested biometric traits to the sensors, and claims the identity of a client. Then, each matcher compares the submitted trait with the corresponding template of the claimed identity, and provides a real-valued matching score (denoted here as s1 and s2, respectively for the fingerprint and the face matcher): the higher the score, the higher the similarity. Finally, the matching scores are combined through a fusion rule which outputs a new real-valued score f(s1, s2): the claimed identity is accepted and the person is classified as a genuine user, if f(s1, s2) ≥ s ∗ ; otherwise, it is classified as an impostor. The term s ∗ is an acceptance threshold that must be set during design according to application requirements in terms of false acceptance (FAR) and false rejection (FRR) rates.

B. multimodal biometric fusion methods against spoof attacks

In this work we consider only the verification task (i.e. the utilizer has claimed an identity and the system needs to decide if the user is genuine or impostor). Let M be the number of biometric systems to be fused. Fig. 2 illustrates the general multimodal architecture when M ¼ 2. The biometric information is fused at the matching score level. This means that each biometric system i ¼ 1; ... ; M individually performs a matching between the enrolled sample and the test sample, and computes a similarity score si between the two samples. We consider that for each biometric system i, there exists an expert that, given a test sample, can provide a score qi that measures the quality of the biometric sample. The set X ¼ fs1; ... ; sM; q1; ... ; qMg forms the input for the fusion scheme that process these inputs and produces a single scalar output z such that higher values of z indicate that the user is genuine (or impostor). A threshold operation is applied to the output z for final classification between impostor or genuine. The security of each biometric system i is modeled by the parameter ci, which represents how arduous it is to spoof the biometric system i. It should be noted that it is very hard (if not impossible) to measure the security of a biometric system [10]. In this work, we manually set the parameter ci predicated on general erudition about the security of each biometric. A qualitative assessment of the security for some biometrics can be found in [1].

C. Thwarting Signature Learning by Training Maliciously

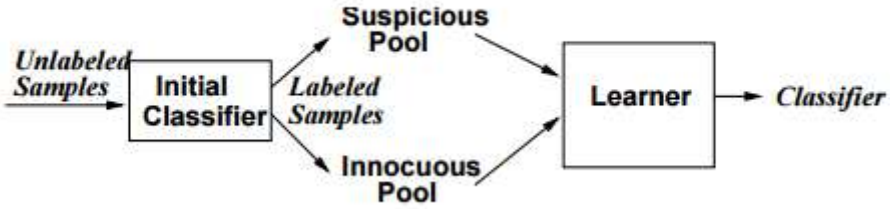

Figure 3: Schematic Lerner Approach

We define the classifier generation quandary as a cognition quandary in an adversarial environment. – We describe attacks on learning classifier engenderers that involve meticulous placement of features in the target-class training data, the innocuous training data, or both, all toward coercing the generation of a classifier that will exhibit many erroneous positives and/or erroneous negatives. – We analyze and simulate these assailments to demonstrate their efficacy in the polymorphic worm signature generation context. We withal implement them, to demonstrate their practicality. We conclude that the quandary of a delusive adversary must be taken into account in the design of classifier generation systems to be utilized in adversarial settings. Possible solutions include designing learning algorithms that are robust to malignantly engendered training data, training utilizing malevolent data samples not engendered by a maleficent source, and performing deeper analysis of the malevolent training data to determine the semantic consequentiality of the features being included in a classifier, rather than treating samples as opaque "bags of bits."

D. Inferring Internet Denial-of-Service Activity

As noted in the precedent section, assailers commonly spoof the source IP address field to conceal the location of the assailing host. The key observation abaft our technique is that for direct denial-of-accommodation attacks, most programs cull source addresses at arbitrary for each packet sent. These programs include all of the most

popular distributed assailing implements: (Shaft, TFN, TFN2k, trinoo, all variants of Stacheldraht, mstream and Trinity).

Attack Classification

After amassing an astronomically immense trace of backscatter packets, the first task is post-processing the trace. For this we group accumulations of cognate packets into clusters representing attacks. The cull of a categorical aggregation methodology presents consequential challenges.

1. Flow-based classification

For the purport of this study, we define a flow as a series of consecutive packets sharing the same target IP address and IP protocol. We explored several approaches for defining flow lifetimes and settled on a fine-tuned timeout approach: the first packet visually perceived for a target engenders an incipient flow and any adscititious packets from that target are counted as belonging to that flow if the packets are received within five minutes of the most recent packet in this flow. The cull of parameters here can influence the final results, since a more conservative timeout will incline to suggest fewer, longer attacks, while a shorter timeout will suggest a sizably voluminous number of short attacks. We culled five minutes as a human-sensible balance that is not unduly affected by punctuated attacks or transitory outages.

2. Event-based classification

Because the cull of flow parameters can impact the estimated duration of an assailment, the flow-predicated method may obscure fascinating time-domain characteristics. In particular, attacks can be highly variable – with periodic bursts of activity – causing the flow-predicated method to prodigiously underestimate the short-term impact of an assailment and aggrandize the long-term impact. We utilize an event-predicated relegation method keyed entirely on the victim's IP address over fine-tuned time-windows for examining time-domain qualities, such as the number of simultaneous attacks or the distribution of assailment rates, for these analyses we divide our trace into one minute periods and record each attack event during this period.

E. Stastical Spam Filters

In this paper, we investigate good word attacks, in which a spammer integrates extra words or phrases to a spam message that are typically associated with legitimate email. Of the many spam filters in existence, we restrict our attention to the naive Bayes filter, the most popular spam filter, and the maximum entropy filter, one of the most popular text-classification filters. For these filters, a spammer simply needs to identify a list of words considered "strongly legitimate" by the filter to mount an effective good word attack. We develop and test good word attacks for two scenarios. In passive attacks, the attacker constructs a word list without any feedback from the spam filter. Attacks of this type amount to educated guesses regarding which words are "good" and which are "bad." In active attacks, the attacker is allowed to send test messages to the filter to determine whether or not they are labeled as spam. While active attacks can yield much better word lists, they may not always be possible since they require the assailant to have user-level access to the spam filter.

Results and discussion

We have taken results based on accuracy parameter. In this result we have shown that our proposed method achieves better accuracy than existing approaches. Below we have mention the accuracy result into table.

$$\text{Accuracy} = \frac{(TP+FP)}{(TP+FP+TN+FN)}$$

Where, TP = True positive
FP = False positive.
TN = True negative.
FN = False negative

Algorithms	Correct Classification	Wrong Classification
SVM Classifier	105	0
Adaboost Classifier	101	4

Tabel 1: Classification Accuracy

Conclusion

Network security is a paramount field that is increasingly gaining attention as the cyber world expands. The security threats and internet protocol were analyzed to determine the compulsory security technology. The security technology is mostly software predicated, but many prevalent hardware contrivances are utilized. The current development in network security is not very impressive. This paper summarizes the assailments and their relegations in wireless sensor networks and additionally an endeavor has been made to explore the security mechanism widely used to handle those assailments. This survey will hopefully incentivize future researchers to come up with more perspicacious and more robust security mechanisms and make their network safer.

Acknowledgements

I would like to thank our HOD Prof.Dr.(Mrs) S.A.Itkar for her support during my project. Also I would like to thank to my guide Prof.Mr.(Dr.).B. D. Phulpagar for their innovative idea who gave me scope for this project work.

References

[1] B. Biggio, Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Security evaluation of biometric authentication systems under real spoofing attacks," IET Biometrics, vol. 1, no. 1, pp. 11–24, 2012.

[2] R. N. Rodrigues, L. L. Ling, and V. Govindaraju, "Robustness of multimodal biometric fusion methods against spoof attacks," J. Vis. Lang. Comput., vol. 20, no. 3, pp. 169–179, 2009.

[3] J. Newsome, B. Karp, and D. Song, "Paragraph: Thwarting signature learning by training maliciously," in Recent Advances in Intrusion Detection (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2006, pp. 81–105.

[4] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring Internet denial-of-service activity," ACM Trans. Comput. Syst., vol. 24, no. 2, pp. 115–139, 2006.

[5] D. Lowd and C. Meek, "Good word attacks on statistical spam filters," in Proc. 2nd Conf. Email Anti-Spam, Palo Alto, CA, USA, 2005.

[6] B. Nelson et al., "Misleading learners: Co-opting your spam filter," in Machine Learning in Cyber Trust. New York, NY, USA: Springer, 2009, pp. 17–51.

[7] B. Biggio et al., "Security evaluation of support vector machines in adversarial environments," in Support Vector Machines Applications, Y. Ma and G. Guo, Eds. Cham, Switzerland: Springer, 2014, pp. 105–153.

[8] N. Dalvi, P. Domingos, Mausam, S. Sanghai, and D. Verma, "Adversarial classification," in Proc. 10th ACM SIGKDD Int. Conf. Knowl. Disc. Data Min., Seattle, WA, USA, 2004, pp. 99–108.

[9] B. Biggio, G. Fumera, and F. Roli, "Design of robust classifiers for adversarial environments," in Proc. IEEE Int. Conf. Syst. Man Cybern., Anchorage, AK, USA, 2011, pp. 977–982.

[10] L. Huang, A. D. Joseph, B. Nelson, B. Rubinstein, and J. D. Tygar, "Adversarial machine learning," in Proc. 4th ACM Workshop Artif. Intell. Security, Chicago, IL, USA, 2011, pp. 43–57.

[11] B. Biggio, G. Fumera, and F. Roli, "Security evaluation of pattern classifiers under attack," IEEE Trans. Knowl. Data Eng., vol. 26, no. 4, pp. 984–996, Apr. 2014.

[12] M. Brückner, C. Kanzow, and T. Scheffer, "Static prediction games for adversarial learning problems," J. Mach. Learn. Res., vol. 13, pp. 2617–2654, Sep. 2012.

[13] M. Barreno, B. Nelson, R. Sears, A. D. Joseph, and J. D. Tygar, "Can machine learning be secure?" in Proc. ACM Symp. Inf. Comput. Commun. Security (ASIACCS), Taipei, Taiwan, 2006, pp. 16–25.

[14] G. L. Wittel and S. F. Wu, "On attacking statistical spam filters," in Proc. 1st Conf. Email Anti-Spam, Mountain View, CA, USA, 2004.

[15] A. Kolcz and C. H. Teo, "Feature weighting for improved classifier robustness," in Proc. 6th Conf. Email Anti-Spam, Mountain View, CA, USA, 2009.

[16] B. Biggio, G. Fumera, and F. Roli, "Multiple classifier systems for robust classifier design in adversarial environments," Int. J. Mach. Learn. Cybern., vol. 1, no. 1, pp. 27–41, 2010.