Efficient and Intelligent Network Infrastructure Protection Strategies for Complex Attacks, IDS Evasions, Insertions and Distributed Denial of Service

Emmanuel Hooper
Information Security Group University of London Royal Holloway,
Egham, Surrey, TW20 OEX, UK. EHSC, Camarillo, California, USA.
ehooper@aya.yale.edu, E.Hooper@rhul.ac.uk

Abstract

Complex network and internetwork attacks evade the detection of intrusion detection systems including insertions, evasions and distributed denial of service attacks. The presence of these complex attacks along with false positives in intrusion detection systems has resulted in inefficient detection and response to such packets in current network infrastructure systems. In this paper we analyse complex network and internetwork attacks and provide effective intelligent countermeasures ad strategies for containing their adverse impact on network and internetwork infrastructures..

1. Introduction

The major problems in network infrastructures are increasing complex attacks, carefully constructed to evade the detection of intrusion detection systems. These complex attacks include internetwork, network and host IDS insertions, evasions and distributed denial of service attacks. Furthermore, anomalies in TCP control segments, and increasing volumes of protocol anomalies have exacerbated these problems in various network and application infrastructures. An intrusion detection system (IDS) is designed to examine network (network-based IDS) and host (host-based IDS) traffic in order to identify attacks [18]. Standard implementations of intrusion detection and analysis involve manual administrative intervention [1, 4]. However, due to the complex attacks and false positives in IDSs [15], such approaches cannot handle the increasing astute attacks on network infrastructures [13, 22, 24]. Moreover, pattern-matching algorithms [16, 17] generate both false positives and false negatives [5, 16, 19]. Evasions occur when the IDS does not recognise an attack in the endsystem. This results in false negatives, i.e., the IDS assumes that an attack has not occurred when there is in fact an attack on the target system. Insertions occur when the IDS assumes that it has detected an attack due to insertions of false packets in the data stream of the packet. This results in false positives [24], implying that the IDS assumes that an attack has occurred when actually there was no attack [4, 20]. One of the increasing attacks designed to disable both IDSs and firewalls are Distributed Denial of Service (DDOS) attack [21], which due to the current vulnerabilities in IDS and firewall software [23], can equally cause significant adverse effects on the network [11]. Furthermore, other problems include the increase in the volume of various protocols including TCP, ICMP, UDP, and their anomalies in their control segments in various infrastructures, the response to these various attacks have become a challenging task in the detection and response to complex attacks and intrusions.

2. Analysis of complex attacks in network infrastructures

In this section, we analyse the complex attacks and countermeasures including SYN DOS Mitigation, protocol and control anomalies, TCP control segment anomalies, and DDOS Attacks.

2.1. DOS mitigation

Denial of Service (DOS) attacks interrupts network services by flooding a system or host with spurious traffic. One approach to mitigate DOS is via client puzzles, using a cryptographic countermeasure against depletion attacks [12]. The main components of the client puzzle involve the server sending a series of computational puzzles to the client, and subsequent responses from the client to determine if the server is under attack. However, the puzzle time parameters and buffer sizes are limited by properties of hash functions and protocol settings in the theorem and heuristic analysis. Thus the approach is limited by cryptographic attacks.

2.2. DDOS attacks

Distributed Denial of Service (DDOS) is more complex and involves simultaneous attacks from multiple sources directed to various destination targets [21]. The mitigation of Distributed Denial of Service (DDOS) attacks present more challenges than Denial of Service (DOS). DDOS involves attacks from multiple sources to the same destination host or multiple servers. Due to the increase in the variety of astute attacks, DDOS can consist of various protocols, thresholds, attacks volumes and multiple types of attacks at the network periphery – the boundary between the external routers and the DMZ hosting the firewalls. This includes evasions and insertion attacks. The following are samples of DDOS Attacks

TCP Control segment anomaly:

TCP Control segment anomalies are abnormal control segments in TCP packets. See Table 1. Too many attacks from multiple sources are sent to various destination targets.

Table 1. A summary of TCP control segment anomaly

No.	Control Flag	Attack description
1	TCP	Control Segment Anomaly
2	ICMP	ECHO Anomaly
3	TCP	Data Segment Volume Too High
4	UDP	Packet Volume Too High
5	ICMP	Packet Volume Too High
6	IP	Fragment Volume Too High
7	TCP	RST Volume Too High
8	Non-TCP-UDP-ICMP	Volume Too High
9	TCP SYN or FIN	Volume Too High
10	ICMP	Echo Request or Reply Volume Too High

3. Intelligent strategic countermeasures for complex infrastructure attacks

The countermeasures to these complex attacks include the following. We present new intelligent strategies as new extensions to the novel Network Quarantine Channels (NQC) model presented in [9, 8]. These include access controls, limitation of packet rates, threshold limits, and statistical analysis of short-term (abnormal conditions) and long-term (normal conditions) in networks. Furthermore, we present intelligent strategies for containing complex DDOS attacks. These enhancements of the intelligent responses include policies, alert filters, packet filters and attack patterns analysis in the NQC database and feedbacks to the IDS and the firewalls. The feedback from the NQC to the IDS filters out false positives from the IDS using IDS alert filters and policies, and identifies the status of complex attacks on the IDS alert monitor. Then the feedback from the IDS to the firewalls denies complex attacks access to the infrastructures, using firewall packet filters and policies.

3.1. Complex attacks and network quarantine channels

In this section, we present an overview of the new model for handling complex attacks and false positives. This involves divergence of the packets to Network quarantine channels (NQC) for analysis of their identity and status. The packets of these complex attacks are analysed in real-time responses from NQC zones. These responses utilize results of the pattern analysis in the NQC database to analyse subsequent packet contents. The patterns are analysed using classification for similar attacks and clustering for unknown categories of attack patterns. Multiple protocols are examined in different zones and a feedback is sent to the IDS to remove false positives of alerts using the alert filters. Actual attacks are denied access to the destinations in the infrastructures using IDS policies and packet filters in the firewalls. This NQC approach improves on honeypots. Honeypots are vulnerable to attacks from hackers. [2]. NQCs intelligent responses include policies, alert filter, packet filters and attack patterns analysis in the NQC database and feedbacks to the IDS and the firewalls. The patterns are analysed using classification for similar attacks and clustering for unknown categories of attack patterns [10, 14]. Multiple protocols are examined in different zones and a feedback is sent to the IDS to reduce remove false positives of alerts using the alert filters. Actual attacks are denied access to the destinations in the infrastructures using IDS policies and packet filters in the firewalls. This NQC approach improves on honeypots. Honeypots consist of a set of software for interaction with intruders [2]. The two main approaches used in high interaction honeypots are detailed logging [7] and virtual machines [6]. However, these are vulnerable to attacks from hackers.

3.2. Access controls

Multiple access controls on perimeter interfaces and segment nodes are applied towards the mitigation of DDOS [11]. The Access Control Lists (ACLs) are implemented to restrict access to nodes. The connection sessions are logged to generate audit trails for correlation with DDOS, insertion, evasion and subterfuge attacks.

3.3. Packet rates: Packets per second

1. **Long-term distribution profile**: percentage above packets per second, typically in 1 day. This is the
long-term distribution of normal network traffic volume over several weeks.

2. **Short-term distribution profile**: percentage above packets per second. This is the short-term distribution of abnormal network traffic in a few hours or minutes, indicating complex attacks such as abnormal TCP and DDOS attacks.

3.4. Threshold values and attack instance intervals

1. Threshold value: attack instances per interval. This is the time in seconds indicating duration between attacks.

2. **Threshold interval**: time in seconds indicating threshold limit at which the packet is considered as an attack. This is used to detect attacks, usually 5-10 seconds, based on the long-term distribution intervals for normal traffic.

3. **Interfaces IP range**: minimum to maximum packet rates IP range indicating the subnet in which attack occurred.

3.5. Statistical analysis

The analysis of normal and abnormal distribution packet rates and threshold values are used to identify the type of attack, packet rate, interface connections and sessions of various types that exhibit abnormal short-term characteristics which deviate from the normal long-term distribution. This is combined with the logs from the access controls such as firewalls, IDS and routers to aggregate and correlate the event anomaly sequences for validation of such attacks. The attacks in insertion, evasion are also contained by the analysis of the packet streams and parameters through packet capture and analysis at intermediary nodes prior to the arrival at the end-systems of the IDS to pre-empt evasion and insertion attacks.

4. Mitigation of Distributed Denial of Service Attacks

In this section we present intelligent strategies for mitigation of DDOS attacks on the perimeter of the network. First, due to the volume of attacks and internal alerts, those internal policies are established to reduce alerts from the IDS sensors, which arise from frequent suspicious attacks. Secondly, a periodic analysis identifies real attacks and intrusions for mitigation of DDOS attacks. DDOS attacks are typically from spoofed source addresses that are sometimes generated at random. Thus mitigation requires several procedures and plans carefully prepared ahead of time.

5. Method

The experiments were conducted as follows. The method involves the diversion of suspect DDOS network attacks to the quarantined channel zones. This is followed by sending responses to the suspicious packets, which appear as valid return packets to the potential attacker. This results in further packets from the attacker, which if they persist, are directed to subsequent zones for additional responses.

5.1. Filtering on Neighbouring Routers

Significant DDOS attacks traverse external routers, thus a critical element of containment is to identify the routers, several hops up from the network, which handles the most packets. However, this requires cooperation from several sources, including those from packets on an upstream router, i.e., neighbouring routers, perimeter gateways and connected Internet Service Provider (ISP) routers.

5.2. Designing of specific access filters to deny external

This involves the denial of external IP addresses using access filters. The logs of the applied rules on the interface that sends traffic to the target include details on the source interface IP and Medium Access Control (MAC) address. The data is used to determine the IP address of the router forwarding the malicious traffic. The process is repeated on the next router to locate the origin of several attackers. Subsequently, proper filters are designed to block the attackers.

5.3. Packet Rate Limiting

An effective method is to apply a limit on the packet rate using the “rate limit” option against the DDOS traffic type. Rate limits restricts the volume of bandwidth for various complex attack types at specific intervals. When the threshold is exceeded, the limited packet is dropped. This is useful when a specific packet is used in the attack. The limitation in this method is to distinguish normal from abnormal traffic. This is accomplished in several approaches as follows.

5.4. Filtering DDOS and Complex Attacks to Null interface

This involves directing the traffic to a NULL interfaces, by forwarding malicious traffic to a non-existent interface known as “Null0”, similar to /dev/null on Unix hosts. Since this is not a valid interface, traffic routed to Null0 is essentially dropped. Moreover, this technique minimizes the impact on the performance of the network and is used to divert DDOS and other complex attacks during to mitigate impact of the DDOS attack.

5.5. Applying Threshold Values to DDOS and Complex Attacks

This involves the use of IDS Threshold values and intervals – short-term and long-term, for DDOS attacks and alerts. The specific DDOS attacks are analysed with an algorithm, which maintains a profile for long-term normal conditions and short-term anomaly volumes of traffic. When the short-term packet rates – packets per second is exceeded in a given interval, then the packets are rejected. This is typically in the ranges of 1 packet/second for less than 1 to 10. The thresholds value (number of attack instances) and interval, such as 5 seconds intervals, are defined to mitigate DDOS attacks. This learning algorithm takes into account, source and destination IPs, and interfaces for pattern recognition of normal acceptable traffic, and abnormal packets.

5.6. Application of Heuristic Algorithmic Tools for Mitigation of DDOS and Complex Attacks

Various heuristics tools with pattern analysis and adaptive techniques for analysing DDOS attacks are used to distinguish between normal traffic and suspicious anomaly traffic. The volume, patterns of normal and misuse large volumes of traffic are filtered and analysed for priorities and access permissions. These are implemented on the perimeter to analyse ingress and egress packets at boundary routers and gateways between the external and DMZ networks.

5.7. Datasets

The datasets were obtained from alerts on suspicious network traffic from various source hosts, generated by the IDS detection mechanism and logged in the IDS Database. The logs consisted of both complex attack types and suspicious traffic, some of which turned out to be false positives. The logs consist of approximately 45 Gigabytes of data over a period of 40 days from a commercial network environment.

5.8. Network environment

The network environment consists of NQCs isolated by subnets and PIX Firewalls [3] from the internal network. The subnets of the NQCs have different IP addresses than those of the internal network. Furthermore, Network Address Translation (NAT) is used to hide the internal IP addresses from the suspect host and the firewalls prevent access to the NQCs. The IDS (Intrushield IDS)[18] in the DMZ examines the attacks at the perimeter and these are analyzed in the IDS console, along with potential internal violations at IDS (4001) and stored in the IDS Database.

6. Results

The results for the reduction of false positives in various alert categories and increase in the detection accuracy of complex attacks are described below in Table 2. The columns depicting the results on false positives for the alerts and the NQC-IDS detection accuracies are defined as follows:

Alerts: Number of alerts generated by the IDS detection mechanism for both benign (normal) connections and false positives.

Actual attacks: Actual number of attacks identified by the NQC, Attacks, and sent to IDS alert monitor.

IDS % False positives: Percentage of false positives identified by the IDS, FP(IDS) without NQCs.

NQC IDS % False positives: Percentage of false positives identified by IDS using the NQC, FP(NQC), given by

$$\mathrm{FP(NQC)} = (\mathrm{Alerts} - \mathrm{Attacks}) \times 100\ \mathrm{Alerts}$$

Reduction in % False positives: Reduction in false positives using NQC, R(FP), given by

$$\mathrm{R(FP)} = (\mathrm{FP(IDS)} - \mathrm{FP(NQC)}) \times 100\ \mathrm{FP(IDS)}$$

NQC IDS % Detection Accuracy: Percentage of false positives identified by IDS using the NQC, FP(NQC), given by

$$\text{Accuracy(NQC)} = 100 - \text{FP(NQC)}$$

Totals: Totals (sum) for “Alerts” and “Actual attack” columns.

Averages: Averages (mean values) for “IDS False positives”, “NQC IDS False positives”, “Reduction in False positives” and “Detection Accuracy NQC IDS” columns. The results for this category of complex traffic are shown in Table 2. The average percentage of false positives for this alert category identified by IDS using the NQC is 0.35%. The average percentage reduction in false positives using NQC is 99.49%. Improved detection accuracy of IDS using NQC for this category is 96.65%.

Table 2. Results: Reduction of false positives - Complex attacks and DDOS Parameters and signatures

Attack descriptions	# Alerts	# Actual attacks	NQC IDS % False Positives	IDS % False Positives	Reduction % False Positives	NQC IDS % Detection Accuracy
TCP Control Segment Anomaly	2302	2294	0.35%	99.10%	99.65%	99.65%
ICMP ECHO Anomaly	4234	4202	0.76%	92.50%	99.18%	99.24%
TCP Data Segment Volume Too High	2100	2094	0.29%	95.20%	99.70%	99.71%
UDP Packet Volume Too High	2125	2112	0.61%	97.50%	99.37%	99.39%
ICMP Packet Volume Too High	5234	5228	0.11%	97.20%	99.88%	99.89%
IP Fragment Volume Too High	5521	5510	0.22%	92.40%	99.78%	99.80%
TCP RST Volume Too High	6529	6502	0.41%	93.20%	99.56%	99.59%
Non-TCP UDP ICMP Volume Too High	1240	1220	1.61%	94.50%	98.29%	98.39%
TCP SYN or FIN Volume Too High	8526	8512	0.16%	90.20%	99.82%	99.84%
ICMP Echo or Reply Volume Too High	7532	7512	0.27%	91.50%	99.71%	99.73%
Total and Averages	45343	45186	0.35%	99.10%	99.65%	99.65%

7. Discussion

The divergence of Complex Web attacks to the NQC hosts for mitigation and analysis detect complex attacks and reduce false positives. This involves directing the traffic sent to the victim host to another host in the NQC. This acts a decoy for the destination hosts, so that the packets are logged for analysis. This host includes IDS sensors with specific DDOS thresholds to isolate and filter normal traffic for access based on source and destination IP addresses and traffic distribution profile for normal and anomaly traffic patterns. In addition, hosts with specific packet filters and log filters based on source and destination IP addresses are used to analyse inbound traffic between the perimeter and the DMZ. Furthermore the load is distributed between various servers and load balancers to isolate legitimate and suspicious traffic. The reduction in false positives for complex alerts and attacks by 99.49% is very important, since this enabled the NQC-IDS to distinguish between false positives and actual attacks. This also reduced the number of alerts generated by the IDS for alerts on complex attacks. The average 0.35% of false positives means that the normal operating conditions using the NQC-based ID generated minimal false positives. This reduction also implies that the detection accuracy of the IDS for complex attacks using NQC improved by 96.65%. This provides an effective detection and response strategy for complex attacks that attempt to evade the IDS.

8. Conclusion

Finally, the Network security strategies for complex network traffic re-routes packets, adaptively responds to packets and sends feedbacks to the IDS. These are used to mitigate and filter out false positives from the alert view and indicate the status of real attacks. The correlation of filtered logs from firewalls, IDSs and external routers identify complex attacks. These approaches provide effective intelligent countermeasures for containment of complex attacks and false positives in various application, network and database infrastructures. This involves effective strategies and design of network security, network architectures and interfaces, network performance and management, internetworking and quality of service.

9. References

[1] E. Amoroso. “A policy model for denial of service.” In Proceedings of the Computer Security Foundations Workshop III, pages 110–997, IEEE Computer Society Press, Franconia, NH, USA, June 1990.

[2] E. Balas and C. Viecco. “Towards a third generation data capture architecture for honeynets.” In Proceedings of the 2005 IEEE Workshop on Information Assurance and Security, pages 110–997, IEEE Computer Society Press, United States Military Academy, West Point, NY, USA, June 15–17 2005.

[3] Cisco Systems Inc. Cisco PIX firewall 525 and Software, version 6.0, San Jose, CA, USA, 2005.

[4] F. Cuppens. “Managing alerts in multi-intrusion detection environment.” In Proceedings 17th Annual Computer Security Applications Conference, pages 22–31, New Orleans, 2001.

[5] H. Debar and A. Wespi. “Aggregation and correlation of intrusion-detection alerts. In Recent Advances in Intrusion Detection (RAID2001), volume 2212 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2001, pages 85–103.

[6] T. Holz and F. Raynal. “Detecting honeypots and other suspicious environments.” In Proceedings of the Sixth IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, USA, IEEE Computer Society Press, June 15–17 2005.

[7] Honeypot Project. “Know your enemy:genii honeynets.” 2005. http://www.honeynet.org/papers/gen2/index.html.

[8] E. Hooper. “Experimental validation and analysis of an intelligent detection and response strategy to false positives and network attacks. ” In Proceedings of IEEE Intelligence and Security Informatics Conference (ISI 2006), volume 3975 of Lecture Notes in Computer Science, Spinger-Verlag Publishers. San Diego, CA, USA, May 23–24 2006, pages 711–714.

[9] E. Hooper. “An intelligent detection and response strategy to false positives and network attacks.” In Proceedings of the Fourth IEEE International Workshop on Information Assurance (IWIA 2006), IEEE Computer Society Press, University of London, Royal Holloway, United Kingdom, April 13–14 2006, pages 12–31.

[10] L. J. Hubert and F. B. Baker. “An empirical comparison of baseline models for goodness-of-fit in r-diameter hierarchical clustering. ” Classification and Clustering, 1977.

[11] C. Jin, H. Wang, and K. G. Shin. “Hop-count filtering: an effective defense against spoofed DDoS traffic.” In Proceedings of the 10th ACM conference on Computer and communications security, Washington D.C., USA, ACM Press, 2003, pages 30–41.

[12] A. Juels and J. Brainard. “Client puzzles: A cryptographic countermeasure against connection depletion attacks.” In Proceedings of 1999 Network and Distributed Systems Security Symposium NDSS, San Diego, CA, February 1999, Internet Society . pages 151–165.

[13] K. Julisch. “Using Root Cause Analysis to Handle Intrusion Detection Alarms.” PhD thesis, University of Dortmund, 2003.

[14] M. S. Kamel and M. Ismail. “Multidimensional data clustering: Utilizing hybrid search strategies. Pattern Recognition.” January 1989, 22:75–89.

[15] R. P. Lippmann, S. E. Webster, and D. Stetson. “The effect of identifying vulnerabilities and patching software on the utility of network intrusion detection.” Computer Networks: The International Journal of Computer and Telecommunications Networking, 3949 of Lecture Notes in Computer Science, 2002, 307–326.

[16] M. V. Mahoney and P. K. Chan. “An analysis of the 1999 DARPA Lincoln Laboratory evaluation data for network anomaly detection.” In Recent Advances in Intrusion Detection (RAID2003), volume 2820 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2003, pages 220–237.

[17] S. Manganaris, M. Christensen, D. Zerkle, and K. Hermiz. “A data mining analysis of RTID alarms.” Computer Networks: The International Journal of Computer and Telecommunications Networking, 34(4): 2000, 571–577.

[18] Network Associates. NAI Intruvert IDS: 1200, 2600 and 4000 Series, Santa Clara, CA, USA. 2004.

[19] L. Portnoy, E. Eskin, and S. Solfo. “Intrusion detection with unlabelled data using clustering.” In Proceedings of ACM CSS Workshop on Data Mining Applied to Security (DMSA- 2001), 2001, pages 76–105.

[19] T. H. Ptacek and T. N. Newsham. “Insertion, evasion and denial of service: Eluding network intrusion detection. Technical Report, Secure Networks (McAfee) Inc., Santa Clara, CA, USA, January 1998. http://citeseer.ist.psu.edu/ptacek98insertion.html.

[20] P. Reiher. “A taxonomy of DDoS attack and DDoS defense mechanisms.” 34(2): April 2004, 39–53.

[21] R. Shai, S. Jha, and B. P. Miller. “Automatic Generation and Analysis of NIDS Attacks.” Full Technical Report, Computer Sciences Department, University of Wisconsin, Madison, 2004.

[22] T. E. Uribe and S. Cheung. “Automatic analysis of firewall and network intrusion detection system configurations.” In Proceedings of the 2004 ACM workshop on Formal methods in security engineering, Washington, D.C., USA, ACM Press, 2004, pages 66–74.

[23] J. Wang and I. Lee. “Measuring false-positive by automated real-time correlated hacking behavior analysis.” In Information Security 4th International Conference, volume 2200 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2001, pages 512–535.

Authors

Emmanuel Hooper

Dr. Emmanuel Hooper earned a record of 3 PhDs within 5 years. He earned a PhD at the University of London, Royal Holloway, Information Security Group, UK, 2007; a PhD in Computing Sciences from the University of East Anglia, UK, 2006; and PhD in Historical Statistical research from the University of Birmingham, UK, 2005. He holds a BSEE from Portsmouth University, UK, multiple MA degrees from various universities including Yale University, USA, He has 27 years experience in infrastructure security and is an adjunct faculty member at the University of California, Riverside, USA. He is a member of various organizations including IEEE, a researcher and consultant in security for various major US and UK companies and President of EHSC/CISO in Camarillo, California, USA.