Toward Visualised Network Intrusion Detection

J-P. van Riel and B. Irwin

Security and Networks Research Group (SNRG)
Department of Computer Science
Rhodes University, Grahamstown, South Africa
Tel: 046 6038291, Fax: 046 63619155
g02v2468@campus.ru.ac.za, b.irwin@ru.ac.za

Abstract—To deal with the large volume of network data, contemporary solutions seek to automate the process of detecting intrusive activity. However, intrusion detection systems can produce an overwhelming number of alerts, and many false alarms can obscure serious intrusion attempts. To overcome these difficulties, this paper suggests combining dedicated sensor network monitoring with visualisation. With the aim of evaluating intrusion detection systems, we introduce the idea of using graphical representations to superimpose alert information over raw network traffic.

Index Terms—Network monitoring, security, intrusion detection, visualisation.

I. Introduction

Network security monitoring becomes cumbersome when dealing with a large number of log entries and intrusion alerts. Furthermore, actual intrusive activity can be obscured by numerous false alarms. Section II motivates our research agenda, outlining the current issues with network monitoring and intrusion detection. The section also promotes dedicated sensor networks and visualisation as a promising tactic for managing the issues. Section III then discusses the ambitions and evaluative approaches that will be taken on. Section IV follows with a brief discussion of related work, and the current project progress. In closing, section V will then conclude the contribution this research is expected to achieve.

II. Motivation

Automated security measures such as firewalls, network intrusion detection systems (NIDS), and patch management systems are commonly deployed to monitor networks. In uncovering suspicious network activity, the objective of these systems is to reduce the effort expended by network administrators, security professionals, and the like. In practice there are some fundamental issues that need to be addressed, such as the common criticism that NIDS tend to produce an overwhelming number of alerts and false alarms. As argued by Axelsson, to be effective, intrusion detection systems need to be extremely accurate [1]. For large data sets, even low false alarm rates will produce a tedious number of false alarms. An added concern is that NIDS can be agitated by crafted attacks that intentionally overwhelm the system with alerts [2]. Furthermore, signature-based NIDS are poorly suited to detecting novel forms of attack, as they require the malicious activity to be characterised before it is detectable.

One approach to dealing with these difficulties is to "remove the haystack from the needles". Dedicated sensor networks, such as network telescopes or honey-pot networks (honeynets), are designated regions of unassigned IP address space. Network telescopes passively monitor traffic without responding, whereas honeynets attempt to illicit further information by responding to incoming traffic. Except for the necessary monitoring systems, no legitimate services or clients reside in such networks, and hence, all the observed traffic can be treated with suspicion. This reduces the amount of traffic observed and diminishes the concern of false alarms, since observed traffic is either the result of a network error of some sort, or intrusive activity.

A second approach is to visualise network events. As is the case for speech, text is understood in a serial manner. Contrary to this, visual cognition is highly parallel and preattentive [3]. Therefore, the human is visual system is adept pattern recognition, and, unlike signature based intrusion detection, facilitates the observation of unexpected patterns (as claimed in [4] [5] [6]).

III. Objectives and Methodology

With detecting and analysing intrusive network activity as the primary criterion, three things will be assessed: first, the suitability of various graphical techniques for visualising network traffic and intrusion alerts; second, the effectiveness of NIDS at detecting probing activity; and third, the scope of observation afforded by dedicated sensor network monitoring methodologies. To measure the potential of the proposed approaches, usability studies will also be conducted.

The central idea is to visualise intrusion alerts superimposed over raw network traffic. This entails finding suitable graphical techniques to represent the traffic and intrusion alert data. As a design consideration, the intended application is to assess the functioning of a NIDS, and its ability to detect various forms of network probing. In specific, the port-scan detection module of Snort will be investigated [7]. A further idea is to filter out the traffic implicated by alerts.

This work was undertaken in the Distributed Multimedia Centre of Excellence at Rhodes University, with financial support from Telkom SA, Business Connexion, Comverse, Verso Technologies, Tellabs and StorTech THRIP, and the National Research Foundation.

When applied to network data from dedicated sensor networks, this will simplify the process of discovering false negatives, as only unidentified incidents will remain.

Another objective is to perform comparative tests and analysis on data from a network segmented into three regions: a network telescope, a honeynet, and a production network. It is anticipated that network telescope traffic will only observe probing activity, such as network scans. Active honeynet monitoring should be able to illicit further information to characterise exploit attacks. In addition to this, production traffic will provide a reference to assess how the scope of observation is limited when employing these dedicated sensor networks.

IV. Related Work And Progress

Stephen Lau's "Spinning Cube of Potential Doom" visualises TCP connection attempts in a 3-D scatter-plot of points [8]. The three respective axes represent the source IP address, destination IP address and destination port. The use of points in his visualisation concept offers promising scalability in comparison to line-based visualisations because line-based visualisations tend to suffer from confusing line-crossover and excessive occlusion [9]. Although effective at saliently conveying network scanning activity, Lau's implementation lacks several key features found in other network visualisations, such as filtering controls, a variable replay rate [5], an adjustable time-frame for displaying events [6], transparent fading of aged events [4], and the ability to visually scale down into sub-ranges of the data. These valuable features, as well as other enhancements, have been implemented in our pilot project called InetVis (Internet Visualisation). InetVis has been employed in network telescope traffic analysis, and has uncovered intrusive activity missed by the Snort NIDS [7] [9] [10].

Visualisations for viewing NIDS alerts have recently been developed. 'Visual Firewall' is comprised of several subcomponent visualisations that separately view different facets of the data. It focuses on conveying relations between the source addresses, destination ports, IDS alarms, and firewall functioning [11]. Instead, our research proposes finding suitable graphical techniques for superimposing IDS alerts over raw traffic to produce one integrated view. 'SnortView' visualises NIDS alerts in conjunction with system logs, but has scalability limitations [12]. 'IDS RainStorm' is capable of viewing local network address space larger than tow class B's, and hence, is more scalable, but it only represents IDS alerts [13].

V. Conclusion

Combing dedicated sensor network monitoring and visualization will help alleviate problems with scalability and false alarms. By visualising and superimposing intrusion alerts over raw traffic, the functioning of automated security measures can be assessed and provide improved insights.

References

[1] S. Axelsson, "The Base-Rate Fallacy and the Difficulty of Intrusion Detection", *ACM Transactions on Information and System Security*, Vol. 3 No. 3, ACM Press, New York, 2000, pp.186-205.

[2] W. Yurick, "Controlling Intrusion Detection Systems by Generating False Positives: Squealing Snort Proof-of-Concept", in *Proc. of the 27th Annual IEEE Conference on Local Computer Networks*, IEEE Computer Society, Washington, DC, USA, 2002, pp. 134-135.

[3] C Wickens, D. Sandry, and M Vidulich, "Compatibility and resource competition between modalities of input, central processing, and output", in *Human Factors*, Vol. 25, No. 2, 1983, pp. 227-247.

[4] R. Ball, G.A. Fink, and C. North, "Home-centric visualization of network traffic for security administration", in *Proc. of the 2004 ACM Workshop on visualization and Data Mining for Computer Security*, ACM Press, New York, 2004, pp. 55-64.

[5] M. Fisk, S.A. Smith, P.M. Weber, S. Kothapally, and T.P. Caudell, (2005, May, 25th) "Immersive Network Monitoring", in *proc. PAM2003 – Passive and Active Measurement 2003* [Online], NLANR, 2003. Available: http://public.lanl.gov/mfisk/papers/pam03.pdf

[6] X. Yin, W. Yurcik, M. Treaster, Y. Li, and K. Lakkaraju. "VisFlowConnect: netflow visualizations of link relationships for security situational awareness". *Proceedings of the 2004 ACM Workshop on visualization and Data Mining for Computer Security*, ACM Press, New York. 2004. p. 35-44, 2004.

[7] Snort network intrusion prevention and detection system (2006, April, 17th), *Snort Users Manual 2.4.0RC1* [Online], Sourcefire, Inc. Available: http://www.snort.org

[8] S. Lau, "The Spinning Cube of Potential Doom", *Communications of the ACM Archive*, Volume 47, Issue 6, ACM Press, New York. 2004, pp. 25-26.

[9] J-P. van Riel, B. Irwin, "A Visual Tool for Network Telescope Traffic Analysis", in *Proceedings of the 4th International Conference on Computer Graphics, Virtual Reality, Visualisation and Interaction in Africa*, ACM Press, New York. 2006. pp. 85-89.

[10] J-P. van Riel, B. Irwin, "Identifying and Investigating Intrusive Scanning Patterns by Visualizing Network Telescope Traffic in a 3-D Scatter-plot", (Accepted for publication) in the *6th Annual Information Security South Africa (ISSA) Conference,* to be published. Available: http://www.infosecsa.co.za

[11] C.P. Lee, J. Trost, N. Gibbs, R. Beyah and J.A. Copeland, "Visual Firewall: Real-time Network Security Monitor", in *proc. of the 2005 IEEE Workshop on Visualization for Computer Security*, IEEE Computer Society, Los Alamitos, CA, USA. 2005, pp. 129-136.

[12] H. Koike and K. Ohno, "SnortView: Visualization System of Snort Logs", *Proc. of the 2004 ACM Workshop on visualization and Data Mining for Computer Security*, ACM Press, New York, 2004, pp. 143-147.

[13] K. Abdulla, C. Lee, G. Conti, J.A. Copeland and J. Stasko, "IDS RainStorm: Visualising IDS Alarms", in *Proc. of the 2005 IEEE Workshop on Visualization for Computer Security*, IEEE Computer Society, Los Alamitos, CA, USA. 2005, pp. 1-10.

J-P van Riel (B.Sc. Honours, Computer Science) is currently in his first year of a masters degree. His interests include computer graphics, networks, and information security.