KF7004 – MComp Computing Research Project
MComp Research Proposal

16018262

Sept 22

Contents

1 Research question

Is there enough data within website log files to detect attacks on websites using a formulaic approach

2 Aims

The aim of this research is to build upon work carried out as part of a 2019 Study by Smith P. looking at a formula approach to detecting risks posed by website traffic. The work done by Smith attempted to use website log files to detect suspicious activity on a website. This work will collect more data to prove the accuracy of this approach. As well as expanding the number of data points to detect attacks for example who the network an IP belongs to and the user agents. The study by Smith P. only has a relatively small data set to it is hard to draw any wider conclusions about the accuracy of the technique proposed, therefore one of the primary aims of this study is to collect a wider data set.

3 literature review

In a study by Zhijun et al. in 2020, they state that "Low-rate Denial of service (LDoS) attacks has become one of the biggest threats to the Internet, cloud computing platforms, and big data centers" (Zhijun et al. 2020) showing the need for an effective attack detection tool. Studies by Adi (summary here) however Zhijun et al. notes that "Moreover, the detection judgement and defence decision can be achieved by analysing

unknown patterns and correlations in network traffic, and grasping other relevant intrinsic information in network traffic." (Zhijun et al. 2020) this study aims to do that.

The method proposed in the aims, has not been documented as a approach to detect attacks, therefore there is a lack of literature so the review will focuses on gaps in knowledge and where this work fits within that.

Erwin Adi has done a lot of research into Low-rate Denial of Service (LDoS) attacks. His primary paper looks at CPU depletion as an indicator of attack. In the same paper, Adi himself admits that this maybe a flawed technique for attack detection. Adi et al. 2016

Most previous studies into detecting Low Bandwidth attacks only look at a single data point such as CPU. This research proposes to look across multiple data points to detect attacks. Furthermore Staniford, Hoagland and McAlerney suggest that storing large amounts of network traffic may be impractical Staniford, Hoagland, and McAlerney 2002. However Zhijun et al. states that "A huge amount of network traffic can be collected, stored, organized and classified by big data analysis. Moreover, the detection judgement and defense decision can be achieved by analyzing unknown patterns" Zhijun et al. 2020 Therefore if there is a need for a large amount of data, that may be impractical to store. One solution may be to look at the data already available to analyse and designing a suitable way to analyse that data.

All the research done to date looks at traffic flow in various ways, however it fails to take into account where that traffic is coming from, for example, most cyber attacks emanate from Russia and China, so the research is ignoring a key area that needs to be explored.

3.1 revlantcy

The work is relevant due to the increasing number of websites increasing as nearly all businesses have a website. In the aftermath of remote working and lock downs E-commerce sites increased (CITE NEEDED) the types of attacks the study aims to detect can be hard to identify. Cloudflare notes in August 2022 that

As websites become part of daily life the number of sites online is increasing as such there are more and more potential targets for attackers and more exploits are discovered, as attacks get more complex the is a need for different detection techniques.

4 ethics

4.1 Research Ethics

When thinking about an ethical way of conlecting data one of the key questions is should the website data is collected say the data is being used for this?

4.2 Wider Ethics

References

Adi, Erwin et al. (2016). "Distributed denial-of-service attacks against HTTP/2 services". In: *Cluster Computing* 19.1, pp. 79–86. ISSN: 1573-7543. DOI: 10.1007/s10586-015-0528-7. URL: https://doi.org/10.1007/s10586-015-0528-7.

Staniford, Stuart, James A Hoagland, and Joseph M McAlerney (2002). "Practical automated detection of stealthy portscans". In: *Journal of Computer Security* 10.1-2, pp. 105–136.

Zhijun, Wu et al. (2020). "Low-Rate DoS Attacks, Detection, Defense, and Challenges: A Survey". In: *IEEE Access* 8, pp. 43920–43943. DOI: 10.1109/ACCESS.2020.2976609.