Metrics on server vulnerability to POODLE attacks

Github link: https://github.com/bvanwijk/TUD_WM0824

1 Introduction

A generic definition of cybersecurity is “the absence of threats to acquired values” (Wolfers as cited in Baldwin (1997). With relation to SSL or TLS certification, the term security applies to a secure connection between a client and a server, by the encryption of the channel to provide privacy and reliability transmitted (PCI Security Standards Council LLC, 2016). One speaks of a vulnerability when this connection is not secure. When this vulnerability is exploited, like in the case of data theft, one speaks of a threat. Among the values at stake in this case are confidentiality, message integrity, and endpoint authentication (Kaur, & Kaur, 2017).

The dataset explored in this report, explains the security issue of vulnerable servers as a consequence of SSL certification, in particular the SSL 3.0 version (SSLv3). In 2018, there are still numerous public servers that have SSLv3 enabled as a viable means of encrypted communication between itself and the client, even though the SSL version is known to be vulnerable to POODLE attacks. POODLE stands for Padding Oracle On Downgraded Legacy Encryption. SSLv3 has two encryptions that both have known security issues, namely using the RC4 stream cipher (which have known biases), and block ciphers in CBC mod, which can be exploited with the POODLE attack. Though SSLv3 is used less often since the introduction of the TLS protocols, some legacy products may be dependent on SSL 3.0 and are unable to be upgraded. In such a case, TLS clients can downgrade the protocol to avoid interoperability bugs on the server-side. This downgrade can also be triggered by adversaries, when interfering with a handshake attempt between client and server (Möller, Duong, & Kotowicz (2014)). The adversary then becomes a ‘man-in-the-middle’, able to intercept data from the client and the server. This compromises the security of the client, thus harming its values like privacy, confidentiality, integrity and authenticity. If the attack is successful, the client and the server start communicating over a weakly-encrypted connection, which can be decrypted by the adversary. In this way the adversary can steal sensitive data from a data owner. The data theft could harm the data owner in cases like identity theft.

With the security values of the client compromised, the ones responsible for the servers (henceforth referred to as security decisionmakers (SDMs)), should be incentivized to improve their security measures. For example, they should update the servers to use TLS versions 1.2 or higher (PCI Security Standards Council LLC, 2016). However, such security measures are accompanied by costs, and server managers may not be willing to pay for these costs, based on their current information on the vulnerability and the threat. To justify the security improvement necessary to eliminate possible POODLE exploits, metrics that can aid in the decision-making of the SDM are presented and proposed. Metrics are often seen as a subjective approximation rather than an objective attribute, but in the domain of cybersecurity, metrics are used to assess how well an entity is secured against external threats, or how effective security measures are (Black, Scarfone, & Souppaya, 2009), and should remain as objective as possible.

The following section discusses the dataset which was accessed, cleaned, and prepared to derive the metrics, which are in turn defined in section 3. The resulting metrics and visualizations of these metrics are presented in the same section and reflected upon in section 4. Finally, conclusions are presented in section 5.

2 Data

The dataset consists of a large number entries of connections to vulnerable servers. The servers are all located in the Netherlands and are tested on average once a week. The total dataset consists of 28,357,106 records which makes it difficult to query the data in a reasonable amount of time. An Amazon Redshift SQL server was set up to move the workload to the cloud, with the data set imported as one large table. Jupyter notebook in conjunction with Python was used to connect to the Redshift cluster and to plot the results from the queries, which may be found in the aforementioned Github repository. The data contained some rows with extra garbage columns which were removed before the data was added to the SQL server. The initial dataset can be found at:
https://surfdrive.surf.nl/files/index.php/s/3l3byoxrUJM8mKd.

3 Metrics

Metrics have criteria. A good metric is objective, quantitative, obtainable, repeatable and time-dependent (Abbadi, 2008). Based on these prerequisites, this section discusses metrics on SSL certification and the metrics chosen for the specific dataset. Later in section 4, the criteria will be used to reflect upon the chosen metrics.

3.1 Metrics in utopia and in practice

For a security decision maker (SDM) in the field of SSL, an ideal metric could be the incident rate. An incident rate informs him on the probability of a POODLE attack when using SSLv3. As well, the SDM as the firm with an outdated server, will be interested in potential losses. As the server configuration puts its current clients in jeopardy of having their supposedly secure information stolen, these clients may switch to another service that are utilizing servers that take proper security measures. Also in consideration are the losses of new clients that will notice the use of outdated security measures (possibly due to a prompt in their modern web browsers or operating system).

In practice however, the metrics on losses are very difficult to capture. Therefore, it is not expected for these metrics to be encountered or derived from the dataset. Best practices on this subject are relatively difficult to find, since the solution to the issue is quite straightforward, since it would simply involve disabling SSLv3. However, there are more generic metrics for information security, as suggested by Cipher (n.d.). Among them are metrics like number of systems with known vulnerabilities and number of SSL certificates configured incorrectly. Both of these metrics apply to our entire dataset.

3.3 Chosen metrics

Taking the above into account, the following 3 preliminary definitions for the metrics were chosen and designed from the dataset:

1. The number of servers that are no longer vulnerable.
2. The duration of vulnerability of the server.
3. Percentage of vulnerable servers per country.

4 Preliminary results

This section discusses the preliminary results on the metrics that can help explain the security issue of vulnerable servers. Each of the three first sections discuss a metric, whereas in section 4.4. the metrics will be reflected upon.

4.1 Number of servers no longer vulnerable

At the start of the data collection on January 1st 2018, 171.280 vulnerable servers were detected. As is shown in Figure 1, the amount of vulnerable servers declined since the beginning of this year. On the latest date in the dataset, August 27th 2018, 145.159 servers were labeled as vulnerable. This results in a total decline of 26.121 servers. This is a drop of merely 15% over the course of almost 9 months.

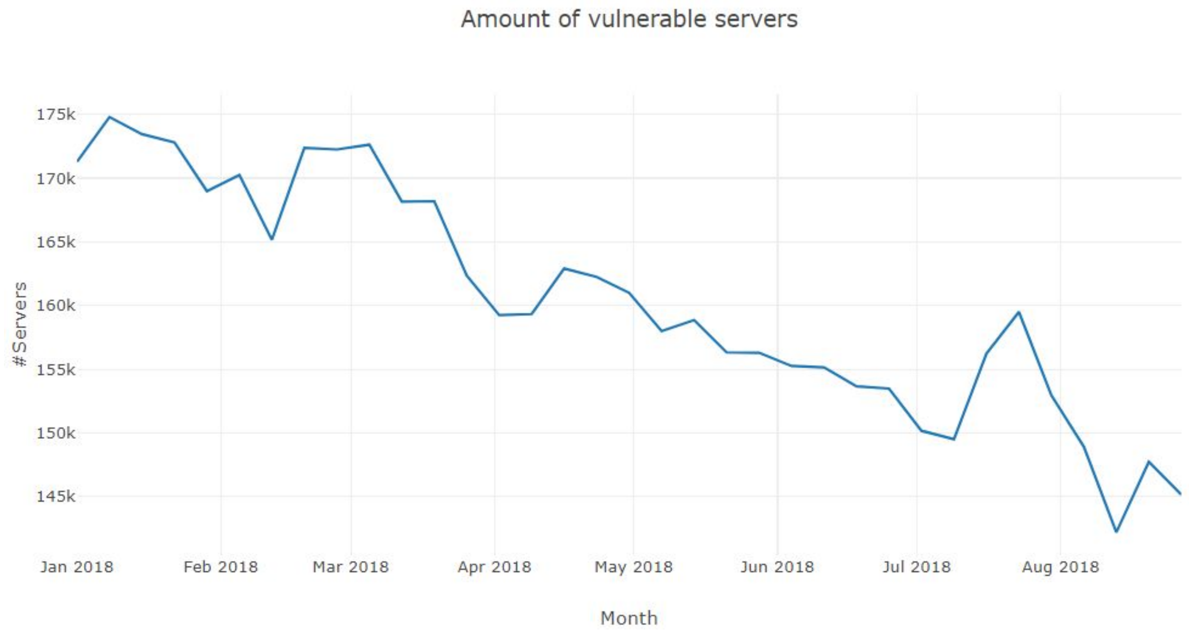

Figure 1: Amount of vulnerable servers detected.

Interesting to see in figure 1, is the fact that the metric experiences a rise over the summer months, followed by a significant drop. Without further investigation of the servers where this was the case, one can merely speculate to the cause of this sudden rise and drop. For example, the influence of news items on the matter could have caused more awareness and therefore more action taken by the security decision makers. Similarly, a change in regulations could have been reason to update to a more secure TLS version.

4.2 Duration of vulnerability of the server

All servers are checked for the presence of the vulnerability at least once in a week. When a server does not appear in the dataset for at least 7 days, it implies that the server is not vulnerable anymore. The duration of vulnerability was measured by picking the week a server appears for the first time and the week the server ceases to appear on the list again, and counting the difference between these weeks. A count of how long the servers are vulnerable for in weeks may be found below in Figure 2.

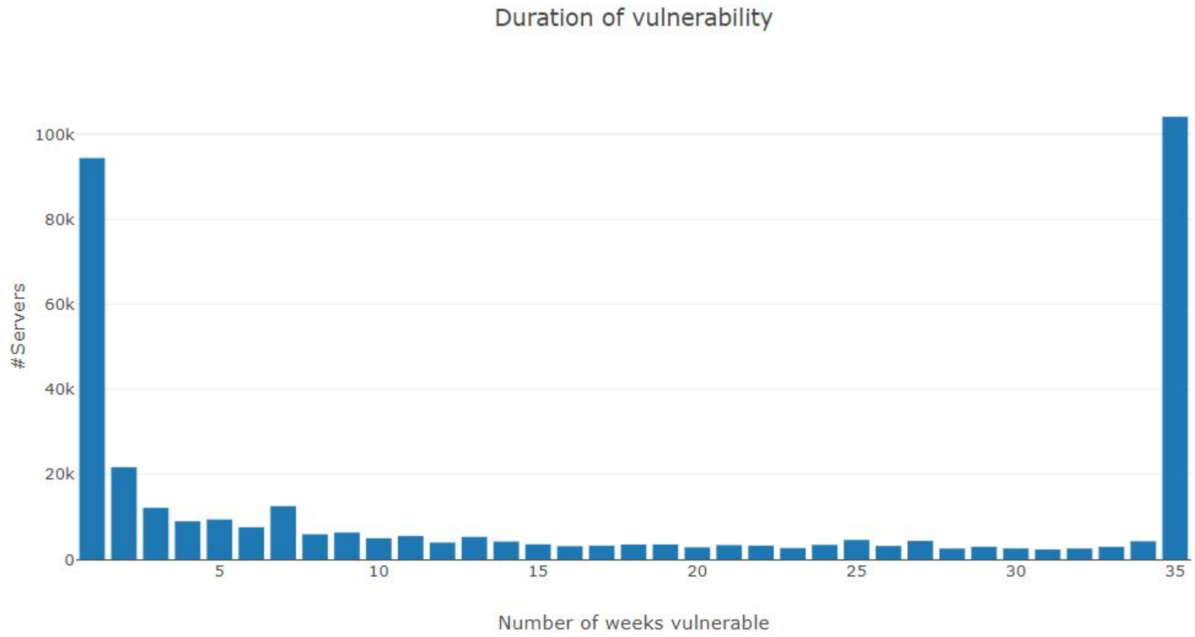

Figure 2: Duration of vulnerability per week.

During the research period, most servers were vulnerable for at least the whole period of 35 weeks. This leads to a speculation that most servers are still vulnerable. On the other hand, there were almost just as much servers vulnerable for about 1 week. A possible cause of the latter could have arisen due to the set of servers in the dataset changing every week, which is likely due to the internet never being constant, and servers bring brought up and taken down all the time. This means that vulnerable servers that were briefly put up and then taken down are also part of the data set, skewing the number of servers that were vulnerable for one week or less.

4.3 Percentage of vulnerable servers per country

For this metric, vulnerable servers were defined as servers that continued to be present in the data set during the last week that data was being collected. To deal with the matter of exposure that can affect the relation between the amount of servers in a country and the country the server resides in, the data is first normalized. This is done by accounting for the number of servers in the country. https://www.shodan.io is used to get the number of hosts per country. It is important to note that this measure is not definitive, as the subject country is an optional field within a certificate, and is not a 100% accurate indicator of the organization's location; it is however, data that is still quite insightful.

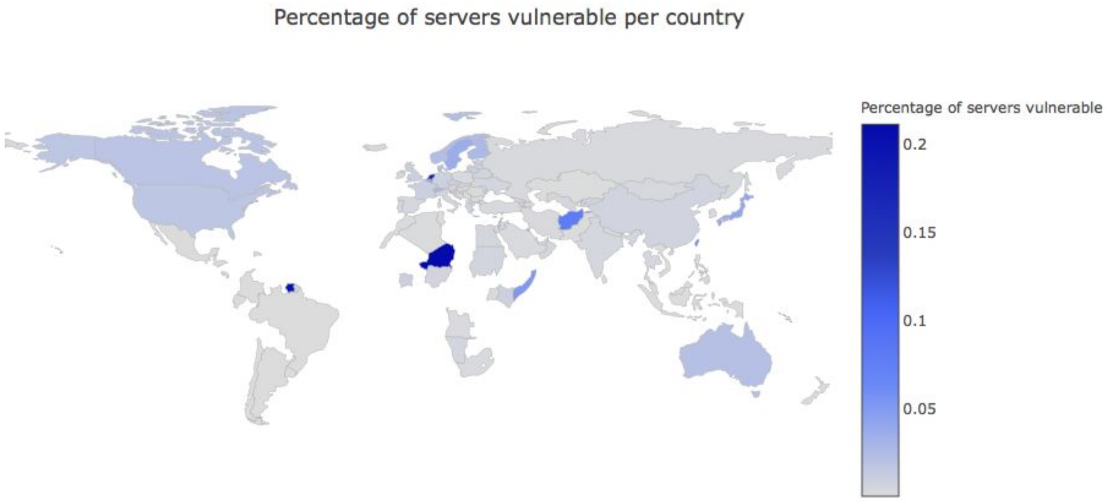
Percentage of servers vulnerable per country
Percentage of servers vulnerable
0.2
0.15
0.1
0.05

Figure 3: Percentage of vulnerable servers per country.

Figure 3 show the result of this metric on a world map with all countries in the dataset. An interactive map is available at https://bit.ly/2PXjP9y.

The country with the most vulnerable servers is Bouvet Island, followed by Niger, Suriname, Cook Island, and the Netherlands. However, results show that Bouvet island has a vulnerable server percentage of 4.5%, which is an order of magnitude larger than the ~0.2% of the other countries in the top 5 list. Bouvet Island is also an uninhabited island (Central Intelligence Agency, n.d.), leading to the belief that this data is a clear outlier, and should be ignored, as already done on the map in Figure 3. Bouvet Island aside, this metric leads to a hypothesis that hosts from smaller, less developed regions have greater trouble in securing their servers against vulnerabilities. It is worth noting that the Netherlands is the only highly developed region in the top five, and that is likely because the data set was primarily made up of IPs from the Netherlands, and as such, the results are skewed due to that. However, since the total number of hosts per country may not be the same as all the hosts scanned to generate the dataset, these results can only serve to gain helpful insights and hypotheses, and further investigation must be taken prior to making conclusions from these results.

4.4 Reflection on the metrics

Like stated in section 3, metrics have criteria. The criteria are objectivity, obtainability, repeatability, time-dependency and being a quantitative rather than qualitative attribute (Abbadi, 2008). Thus, the metrics created before can be scored on the criteria. In Table 1, a green highlight refers to a good score of the metric on the criterium. From this table one can see that the metrics scored quite well in general on the criteria.

Table 1: Metrics' score on criteria.

	The number of servers that are no longer vulnerable	**The duration of vulnerability of the server**	**Percentage of vulnerable servers per country**
Objective	Once a server disappears from the dataset, it is assumed to be no longer vulnerable. This assumption is based on the fact that the dataset merely consists of cases of vulnerable servers. The use of the metric therefore does not change under different research questions.	The metric relies on the same assumption that the dataset only contains vulnerable servers. The occurrence of servers in the dataset is counted on a weekly basis. Therefore, it does not rely on interpretation or other information.	Discover the difference between countries for the percentage of vulnerable servers. Unfortunately, due to the lack of country specification on some certificates, as well as the normalization process, it does quite heavily rely on interpretation and other supporting information.
Obtainable	Well obtainable, since one can derive this from the amount of servers that 'disappear' from the dataset	Obtainable. A list of vulnerable servers on a weekly basis is required and some calculations must be performed.	Well obtainable, but dependent on how well the country is specified in the certificates.
Repeatable	The same calculation can be performed on more data, giving different results, but without losing its meaning.	The same calculation can be performed on more data, giving different results, but without losing its meaning.	The same calculation can be performed on more data, giving different results, but without losing its meaning.
Time-dependent	This metric varies over time, so it is time-dependent.	Yes	Yes
Quantitative	Yes	Yes	Yes

5 Conclusion

Using SSLv3 on a server is a known vulnerability to POODLE attacks. In such an attack, adversaries act as men-in-the-middle to intercept data traffic over insecure connections. This intercepted data can then be used for criminal activities, such as identity theft, fraud, or extortion. The solution to the vulnerability issue of servers is to end the use of SSLv3 by updating to TLS versions instead. However, as the dataset explored in this report shows, there are still servers operating with SSLv3, despite the vulnerability being first discovered back in 2014.

To get a better understanding of the vulnerable servers, three metrics were designed. First, the number of vulnerable servers was reviewed over time. Over the course of 35 weeks, 15% of the servers disappeared from the dataset, which indicated that these servers were no longer considered vulnerable at the end of the data set collection phase. Next, the duration of the vulnerability was inspected, with most servers found as vulnerable over the entire period of data collection. Yet, almost the same number of vulnerable cases were detected and solved within one week, leading to the belief that the number of new servers being brought up and taken down over the course of the data collection has a measurable impact on the conclusions being drawn. Finally, the origin countries of the vulnerable servers were inspected, to see which countries have the most vulnerable servers. The countries with the most vulnerable servers were Bouvet Island, Niger, Suriname, Cook Island, and the Netherlands, in that order, with Bouvet Island being an outlier that should be ignored.

To conclude, the metrics designed in this report tell us a little more about the vulnerability of servers to POODLE attacks. Yet, as with all metrics, these metrics have their flaws. Without further investigation of potential causes of the results, the explanations provided cannot be 100% verified, as there are simply more variables that can explain the relations between the metric variables.

6 References

Abbadi, Z. (2006). Security Metrics. What Can We Measure? Retrieved September 21, 2018, from https://www.owasp.org/images/b/b2/Security_Metics-_What_can_we_measure-_Zed_Abbadi.pdf.

Baldwin, D. A. (1997). The Concept of Security. *Review of International Studies*, *23*, 5–26. https://doi.org/10.1007/978-3-642-29299-6

Central Intelligence Agency. (n.d.). The World Factbook. Retrieved September 23, 2018, from https://www.cia.gov/library/publications/the-world-factbook/geos/print_bv.html

Cipher. (n.d.). 10 Cybersecurity Metrics You Should Be Monitoring. Retrieved September 21, 2018, from https://blog.cipher.com/10-cybersecurity-metrics-you-should-be-monitoring

Kaur, P., & Kaur, G. (2017). Review of Role of SSL in Cyber Security. *International Journal of Advanced Research in Computer Science*, *8*(4), 187–190. Retrieved from www.ijarcs.info

Möller, B., Duong, T., & Kotowicz, K. (2014). This POODLE Bites: Exploiting The SSL 3.0 Fallback. *Security Advisory*, 1–6. https://doi.org/10.1145/1629575.1629606

PCI Security Standards Council LLC. (2016). *Migrating from SSL and Early TLS*. *Pci Dss Resources*.