Poodle SSL

Group 16 - Draft Assignment Block 2

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

Introduction

For this assignment, we are looking into the dataset on SSL certificates, and the security issues that arises with SSL 3.0 version. In 2018, there are still numerous public servers that are negotiating to SSL 3.0 as a means of encrypted communication between itself and the client. This SSL version is vulnerable to POODLE attacks. POODLE stands for Padding Oracle On Downgraded Legacy Encryption. SSL 3.0 has two encryptions that both have known security issues, namely using the RC4 stream cipher (which have known biases) and block ciphers in CBC mode. The latter can be exploited with the POODLE attack. Though SSL 3.0 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 attackers, when interfering with a handshake attempt between client and server (Möller, Duong, & Kotowicz (2014)).

Steps

The dataset itself is ambiguous whether it informs us about poodle incidents, or just general SSL/TLS use. Without a better understanding/description of the data provided, one cannot exclude the possibility that the data is providing certain metrics. For example, the field ‘ssl_poodle’ contains Y for all rows. Assuming this Y stands for yes, one can continue to think that this means the POODLE attack applies to this server. If that is the case, then the dataset reports on incidents, rather than general data collection on various server certificates. Therefore, one of the first steps is to gather more information about the data descriptions. Secondly, we will continue to inspect the dataset and determine what type of data we’re dealing with and what information can be fetched from the data. Once there is a clear picture on the fields of interest, we will determine which metrics are possible to derive from the set. Following, these fields will be tracked over time.

Metrics

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 an SSL version 3.0, i.e. the threat. If the SDM is a web browser developer, an additional ideal metric could be the losses of users, because they no longer want to use the vulnerable SSL 3.0. protocol. Similar, if the SDM is the firm with an outdated server, potential losses are of interest. As the server configuration puts its current customers in jeopardy of having their

supposedly secure information stolen, these customers may switch to another server. Also in consideration are the losses of new customers that will notice the use of outdated security measures (possibly due to a prompt in their modern web browsers).

In practice, the metrics on losses are very difficult to capture. Therefore, we do not expect to encounter or derive these metrics in the dataset. The incident rate however, can be derived from the dataset when we assume that the data consists of incidents. Yet, this is a vary raw assumption and can be falsified easily with a better data description. Easier identifiable metrics are vulnerability metrics, like the use of the SSL 3.0 as the handshake protocol. Similar, the use of the RC4 cipher suite is a vulnerability metric.

Taking the above into account, we chose the following preliminary definitions for the metrics we can design from the dataset:

- If the handshake field of a record contains SSLv3, the record is labeled vulnerable.
- If the cipher_suite field of a record contains RC4, the record is labeled vulnerable.
- If the cipher_suite field of a record contains SSLv3 after the same host used a higher TLS version before, the corresponding IP address can be labeled suspicious.
- Else, the record is labeled not vulnerable.

Preliminary results

In order to get a better understanding of how many servers switched from SSLv3 to a newer, more secure handshake protocol, the data set was filtered such that IPs which occur more only once are removed. The results then show that at the last collection instance of every unique IP address and port pair in the data set (Since one IP address may have multiple servers running on different ports with different configurations), 3459 out of 371541 servers are still using SSLv3 to perform a handshake. Compared to very first collection instance of every unique IP address in the data set, 3471 out of 371541 servers were using SSLv3 to perform a handshake. This means that only 12 servers have switched to a newer protocol.

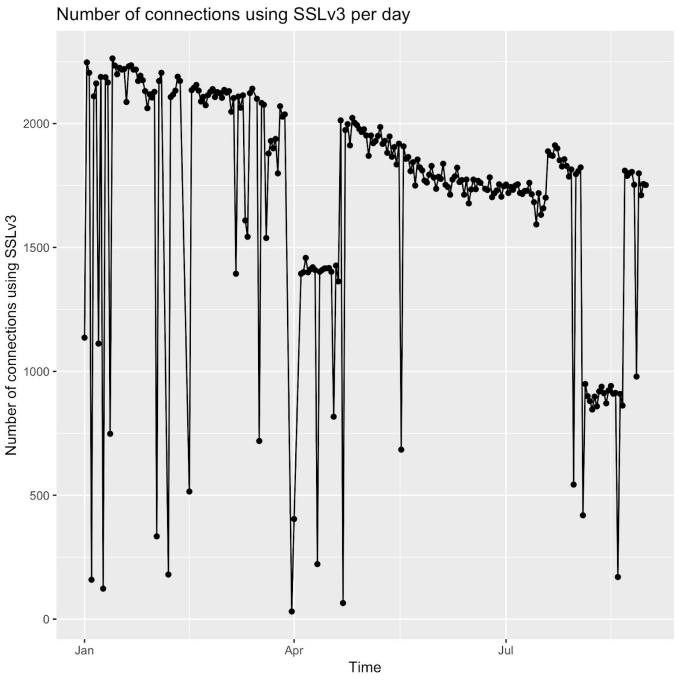
A point of interest was also whether any organization had downgraded in security by switching from a newer, more secure handshake protocol to SSLv3, and from the data set, it seems that 13 servers did indeed do so; however, upon closer examination, these servers appear to have the entire certificate changed when they had switched from TLS down to SSLv3, which could be an indication that the IP was simply relinquished by its original owner and assigned to another entity. Further investigation is required on how frequent IP reassignment occurs, and how that affects the trends and metrics set out in this report.

Another point of interest was regarding the number of insecure certificates that servers were using by the subject country, where the subject country is the country of origin of the organization running the server. 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 an 100% accurate indicator of the organization’s location; it is however, data that is still quite insightful. Grouping the servers that are still using SSLv3 at the end of the data collection process, the following results were determined:

subject_country	count
	1027
--	5
AU	1
BE	1
CA	1
CN	8
DE	2
GB	2
LU	1
NL	52
PH	2
RU	1
SE	28
TW	2274
UK	2
US	52

Which demonstrates that most vulnerable servers seems to be in relation to Taiwan, followed by unknown countries. The vulnerable servers from all other known countries pales in comparison. This prompts further investigation into the specific circumstances surrounding Taiwan that would explain this phenomenon.

Another way to get a better understanding of the data is to look at the number of connections using SSLv3 per day and per week, this is shown in figure 1 This is not directly a good security metric because the same servers are not tested every day. Less connections using SSLv3 does not indicate there are less server vulnerable it could also indicate there are less vulnerable servers tested. Figure 2 presents the relative number of connections using SSLV3, but again this does not give a very reliable security metric.



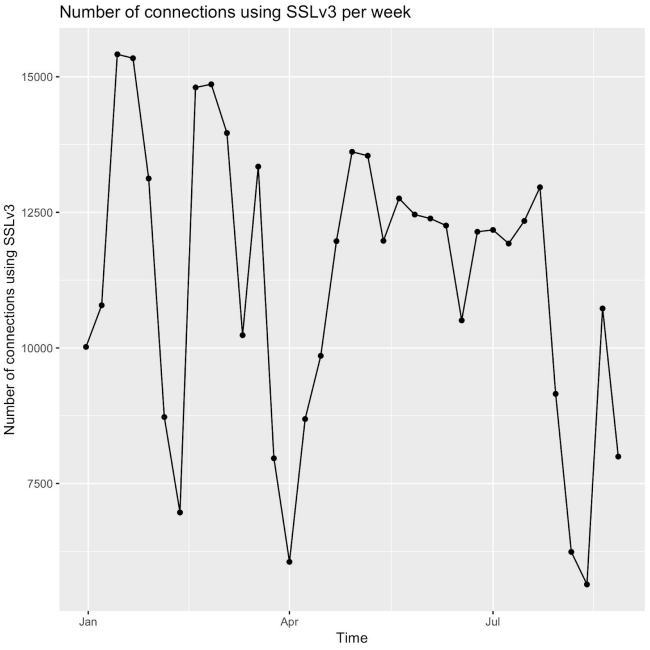
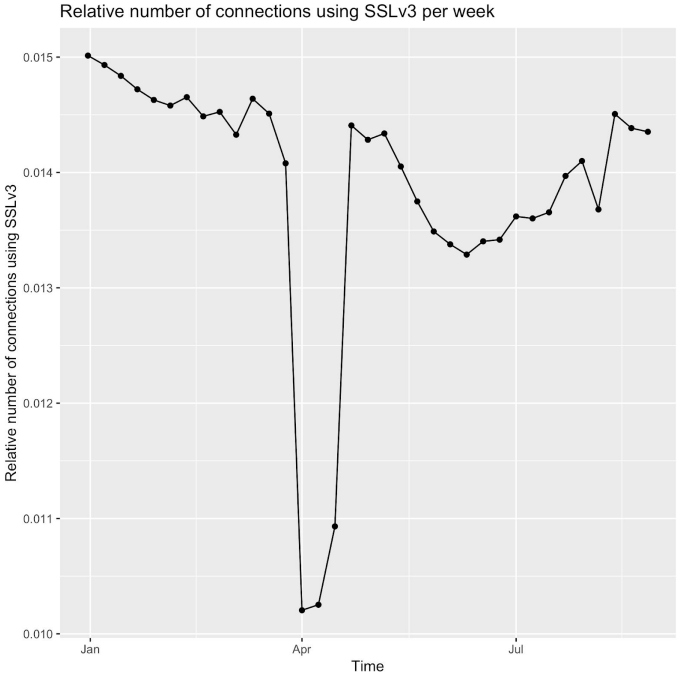


Figure 1 Number of connection using SSLv3 per day and week



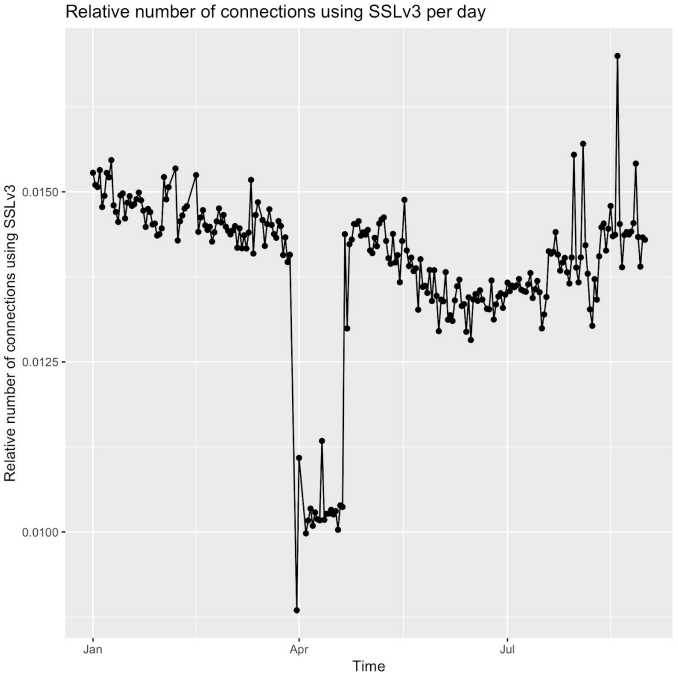


Figure 2 Relative number of connection using SSLv3 per day and week

References

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