Security performance of Internet Hosting Providers for the POODLE vulnerability

Delft University of Technology
WM0824TU Economics of Cybersecurity - Assignment Block 4

Group 16:
Marco Boom: 4393031
Maartje Flipsen: 4206444
Andrew Jiang: 4942795
Bryan van Wijk: 4363329

Monday October 15th 2018

Attachments: https://github.com/bryanvanwijk/TUD_WM0824

1 Security issue

A server can become vulnerable as a consequence of outdated SSL certification, in particular this is the case for the SSL 3.0 version, commonly referred to as SSLv3. In this assignment, the security issue discussed is that of insecure servers due to SSLv3 certification that are therefore vulnerable to POODLE attacks. In a POODLE attack, the handshake protocol between client and server is compromised, as adversaries can exploit the vulnerabilities of SSLv3 at that point. Once the adversary is in, he can act as a man-in-the-middle. This allows him to look into and interfere with the data that is transferred over the insecure connection between client and server.

The data set explored in this assignment and previous assignments shows that many servers still use SSLv3. The data set is used to explore data on Internet Hosting Providers (IHP), which are parties that provide services and web servers to customers, i.e. individuals or organizations that own websites. IHPs are bound to legislation and regulations set by regulators. This can either be a governmental organisation, or a private organisation that shares best-practices and such.

The data set allows to analyze what percentage of servers is vulnerable per Autonomous System Number (ASN). We assume that each IHP runs one ASN, to say something about the number of vulnerable servers per IHS. It is also assumed that any entry in the last week of the data set is still vulnerable. These assumptions allow us to count the distinct IP addresses from the last week of the dataset and to group this by their corresponding ASN. The IP addresses count is then normalized by querying WHOIS databases for all the IP ranges belonging to a given ASN. Following, these ranges are aggregated to return the number of IPs per ASN. Figure 1 shows the resulting percentages of vulnerable IP addresses per ASN in a descending order. For readability purposes, 776 ASNs that has a vulnerable percentage of lower than 5% were filtered out of the figure, making for a total of 791 ASNs.

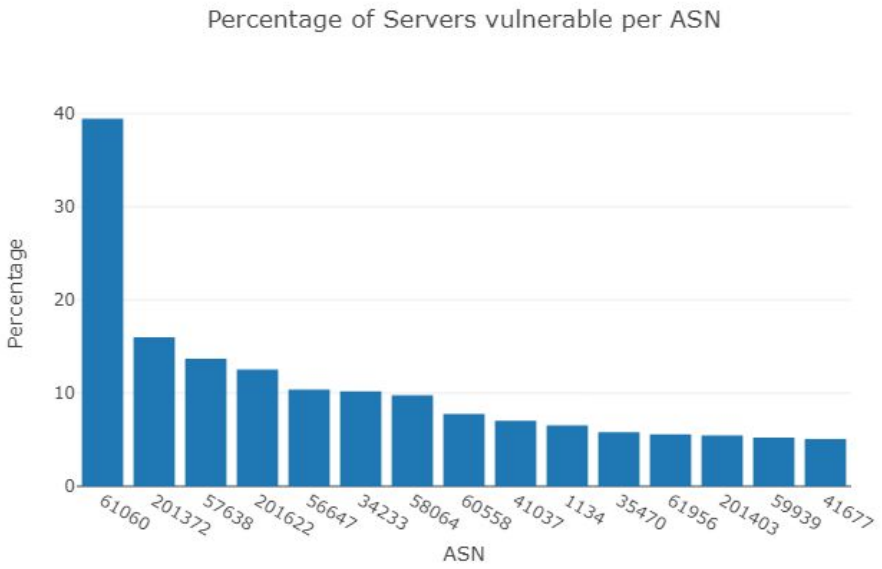

Figure 1: Percentage of servers vulnerable per ASN, for ASNs with vulnerability percentages >5%.

2 Actors

Actors involved in the security issue follow different strategies to mitigate its impact. Three important actors for the security issue are the Internet Hosting provider, the regulators and the customers. In the next three sections, for each actor, one specific countermeasure and its effects for the other actors are analyzed.

2.1 Problem owner: Internet Hosting Provider (IHP)

An IHP can update the configurations of the servers themselves enforcing their customers to use a newer SSL version. The incentive to use this countermeasure would be the prevented loss for when the communication with one of their servers is intercepted.

If the IHP deploys this strategy, this would not likely carry any costs for the regulators. The regulators will have benefit with this countermeasure, because it is a countermeasure that is easily checked and regulated. It will thereby prevent all attacks using the SSL vulnerability in an optimal way.

There is also a downside to this countermeasure, as the customers could experience costs due to this strategy. They could experience interoperability issues and their end-users are possibly unable to connect to the servers when they don't support a newer SSL version. Another cost the customers will experience are the server updating costs where they most likely will be charged for. On the other side the customers will also experience benefits. From the customer's point of view, their risk is now transferred to the IHP. So, they benefit from the secure servers.

2.2 Regulators

Regulators can impose fines and regulations and enforce these to push the industry to mitigate the security issue in question.

If the regulators would deploy this strategy, this would result in increased costs for companies/organizations, and as such, more overhead in the cost of doing business, which might be detrimental to the economy. However, this would force adoption of more secure standards, thus reduce the risk of fraud and security incidents across the board, thereby benefiting the society as a whole.

Given the existence of a two-sided market relationship here, it is very difficult for the market to grow, and for dominant players to take actions in the interest of security due to the low risk of market displacement, as mentioned in the video lectures. Therefore, governments have an incentive to further grow and advance this market, and can do so by deploying the security measure as outlined.

2.3 Customers (server owners)

Customers can update their server configuration to use only secure protocols. This would imply that the IHP enables the configuration by customers and it is agreed upon that customers are responsible for the configuration.

The deployment of this strategy by customers incurs several costs. First, for the customers themselves, costs are related to the wages paid for the activity of updating the configuration. Second, it's possible that some end-users do not support newer protocols and therefore they will be unable to continue visiting the customers' website. Due to this, the customer would suffer some loss of income.

While there are costs for the customer associated with this strategy, it's benefit is that the risk of incidents drops. Therefore, there is a lower probability on leaking data. Depending on the business scale the customer operates on, the prevented losses are more significant. For example, a customer that operates a popular webshop, could be more likely to benefit from a lower probability of leaked data than a webshop that has very little traffic.

3 Factors influencing the metric

The metric displayed in Figure 1 shows the performance differences between the different ASNs or IHPs as we assumed an ASN to be equal to an IHP. Thus, the metric is an indicator for the IHP security performance.

Some IHPs might have a higher percentage of servers vulnerable for the poodle attack than others. Factors influencing the differences among IHP security performance are investigated in the next sections.

3.1 Factors explaining the variance in the metric

The variance in security performance among IHPs can be caused by several drivers. Firstly, the access policy on how customers of IHPs can access their servers might differ, making it for the customers harder or impossible to remotely access some configuration options. This could mean that they are simply unable to update the servers themselves and have to rely on the IHP to update the servers. Secondly, IHPs could be missing the capabilities to update the server configuration because knowledge is lacking. Or there is simply not enough capacity, i.e. not enough skilled employees, to update the servers. Thirdly, business culture can play an important role. Due to differences in business culture IHPs can have different levels of risk tolerance. Thereby, some IHPs may simply accept the risk of using an insecure protocol, therefore scoring poorer on security performance. Fourth, even when the IHPs have security policies in place to only use the more secure SSL protocols, the quality between the security policies might differ. To ensure this rule is followed, you need to constantly monitor the SSL version used and take action when a lower SSL version is used on regular basis. Lastly, some IHPs might be more popular by customers with lower security demands which means there is less incentive to provide more secure servers with up to date protocols. Conversely, customers who demand more security could choose to merely use IHPs that have better security performance, or at least more controls in place.

To summarize, there are multiple facets influencing the variance in security performance of IHPs. Their respective impact is difficult to quantify, as not only the concepts are difficult to define quantitatively, but also data collection is a challenge. A possibility to still capture some of these factors is to look at the country that the ASN/IHP owner is located in. This is explored in the further sections.

3.2 Impact of ASN owner country

Investigating impact of the country where the IHP is based, requires the collection of extra data, next to the dataset of vulnerable servers in the Netherlands. In the following calculations the ASN lookup tool from Ultratools (2018) is used to retrieve the countries of the ASN owners. As mentioned before we assume an ASN to be equal to an IHP. Based on this data the impact of an IHP owner being located in another country than the Netherlands is investigated.

For simplicity we split IHPs in two groups, the first group being the IHP for which the percentage of vulnerable servers in their network is above the median percentage of vulnerable servers. The second group are the IHPs for which this percentage is below the median value. The definition of a vulnerable server is in this case a server using SSLv3 as calculated in the introduction. A Dutch IHP is defined as companies which are registered in the Netherlands according to the ASN registration. Table 1 shows the amount of IHPs located in the Netherlands, grouped by registered nationality and by amount of servers above or under the median value. It becomes apparent that approximately 70% of Dutch IHPs located in the Netherlands are more vulnerable than median, opposing, about 18% of non-Dutch IHPs. However, to truly say something about the impact of ASN owner country, more thorough statistical analysis is required.

Table 1: Data for server vulnerability of Dutch/non-Dutch IHPs located in the Netherlands.

IHPs located in the Netherlands		**ASN owner country**		**Total**
		Dutch	**non-Dutch**	
Percentage of vulnerable servers	>0.19%	346	52	**398**
	<0.19%	162	228	**390**
	Total	**508**	**280**	**788**

The impact of owner country on IHP security performance can be analyzed by measuring the odds ratio. This ratio is the probability of being more vulnerable than median (having a relatively high percentage of vulnerable servers) divided by being less vulnerable than median (having a relatively low percentage of vulnerable servers). The data from table 1 is used as input for the following equations:

(1) For IHP registered by a Dutch company: $\frac{P(>0.19\%)}{P(<0.19\%)} = \frac{346/508}{162/508} = 2.136$

(2) For IHP registered by a non-Dutch company: $\frac{P(>0.19\%)}{P(<0.19\%)} = \frac{52/280}{228/280} = 0.228$

(3) Estimated odds ratio: $OR = \frac{odds\ Dutch\ IHP}{odds\ non{-}Dutch\ IHP} = \frac{2.136}{0.228} = 9.37$

The last equation return the odds ratio that a Dutch IHP located in the Netherlands has a relatively high percentage of vulnerable servers. This odds ratio is 9.37. Thus, the odd that a Dutch IHP has a relative high percentage of vulnerable servers, is (9.37 - 1 = 8.37 =) 837% higher than a non-Dutch IHP.

This indicates a high association between the relative number of vulnerable servers and whether the IHP is a Dutch or non-Dutch company. A possible explanation could be that ASNs owned by a non-Dutch company are larger companies with larger budgets and interests. A IHP hosting millions of servers world wide with many important clients who will require the IHP to provide a secure environment or otherwise go to another IHP. Local Dutch IHPs with only the local grocery stores as customers are likely less demanding in security requirements and are not able to investigate in updating their servers regularly.

4 Conclusion

The security performance in server vulnerability by Internet Hosting Providers (IHPs) can vary. Several factors can explain this variance, e.g. access controls, capabilities and culture.

As these factors are difficult to quantify, and data collection proves to be a challenge, the impact of IHP owner country is investigated as a proxy. Here it is assumed that an IHP is equal to an ASN. The ASN owner country is the country that the ASN is officially registered to. To determine the impact of owner country on security performance, IHPs are counted for two categories: percentage of vulnerable servers above and below the median value of 0.19% (derived from the data set) and Dutch or non-Dutch origin countries. When the percentage of vulnerable servers supersedes 0.19%, the IHP is said to have a relative high percentage of vulnerable servers. Using the odds ratio to measure association, it was found that the odds that a Dutch IHP located in the Netherlands has a relative high percentage of vulnerable servers is 837% higher than a non-Dutch IHP located in the Netherlands.

5 References

Ultratools. (2018). ASN lookup tool August 2018 Overview. Retrieved October 13, 2018, from https://www.ultratools.com/tools/asnInfo