Actors and strategies in server vulnerability to POODLE attacks

Delft University of Technology
WM0824TU Economics of Cybersecurity - Assignment Block 3 (Draft)

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

Monday October 1st 2018

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

1 Security issue

The security issue explained is that of vulnerable servers as a consequence of SSL certification, in particular the SSL 3.0 version (SSLv3). Basically, an insecure server is vulnerable to POODLE attacks. In such an attack, an adversary exploits the vulnerability in the SSLv3 certification during the handshake protocol between client and server. He then acts as man-in-the-middle and is able to look into and interfere with the data traffic that uses the insecure channel.

As revealed in the previous report (available on the Github repository), many servers remain vulnerable, even though the SSLv3 has long been replaced by more recent TLS versions (Holmes, 2015). From the analysis in the previous assignment, it was found that most servers in the dataset were either vulnerable for about a week, or for at least the whole period of 35 weeks. The latter means that after the data collection period, these servers were still vulnerable. With regards to security performance, this means that most server owners undertook action/had a response time of within a week, but just as many server owners do not undertake action at all.

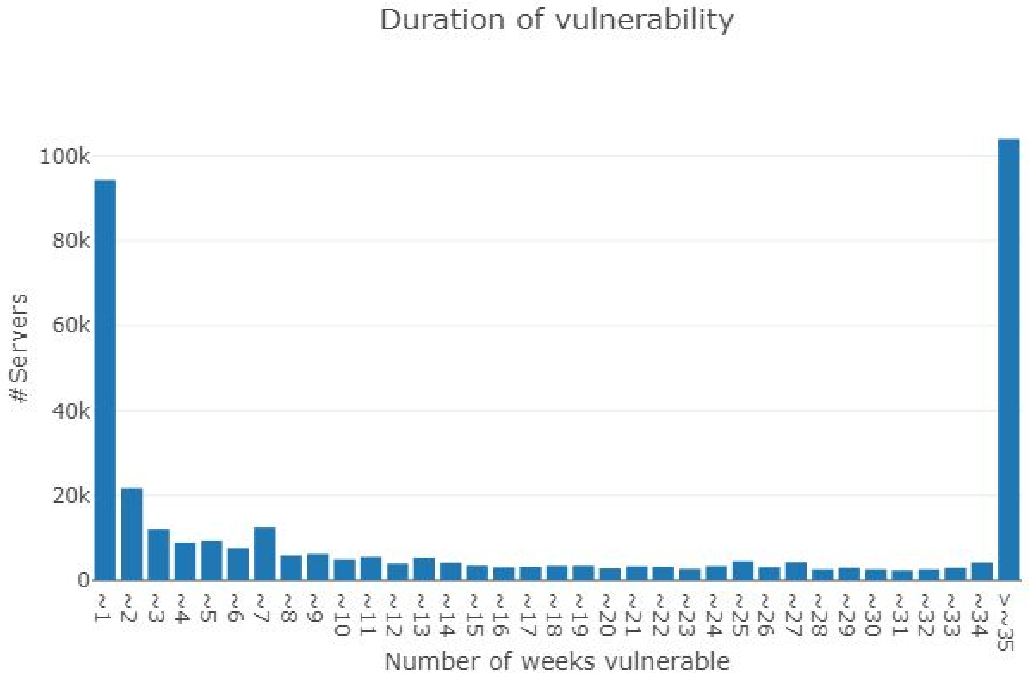

Figure 1: Duration of vulnerability of servers.

2 Actors

2.1 Problem owner

The problem owner for this security issue is the organization responsible for the server, i.e. the server owner. To be clear, the actor perceived as the problem owner can be any of the owners of the vulnerable servers discussed in the dataset. As the owner of the server, we assume the goal of the problem owner is to have secure servers. A fault tree analysis is used to understand which event leads to insecure servers. This is used as a starting point to identify possible strategies by the server owner. Figure 2 shows the developed fault tree. Here, the undesired event is the server being vulnerable to POODLE attacks, i.e. being insecure. There are two ways a server can become insecure: either insecure protocols are used (e.g. SSLv3), or insecure server software is used. Considering the use of insecure protocols, three component failures lead to this: either server configuration is outdated, a new vulnerability is discovered, or fallback to insecure protocols is possible. Similarly, the use of an insecure server software can occur because of insecure acquired server software or outdated server software.

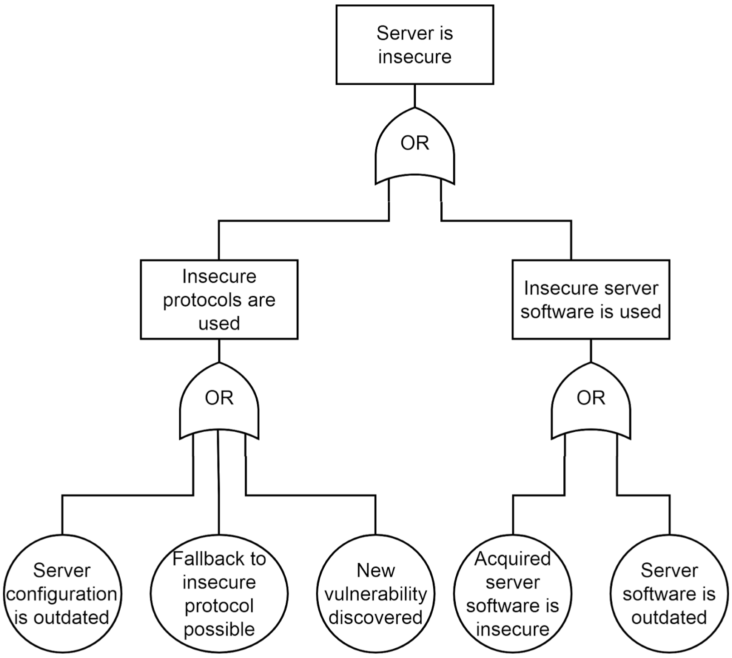
Server is insecure
OR
Insecure protocols are used
Insecure server software is used
OR
OR
Server configuration is outdated
Fallback to insecure protocol possible
New vulnerability discovered
Acquired server software is insecure
Server software is outdated

Figure 2: Fault tree analysis for insecure servers.

2.2 Problem owner strategies

We assume that the goal of the problem owner is to have secure servers. Figure 2 informs us on the components relevant to the event of a server being insecure. Strategies to prevent these component failures can thus lead to the achievement of the goal of the problem owner. These strategies consist of the deployment of means by the problem owner. The problem owner has several means to its disposal, all to achieve its goal of secure servers. The means-end diagram in Figure 3 displays the possible means of the server owner that help achieve its goal. To avoid possible influential factors, these means go a bit broader than means aimed solely at preventing secure server software to avoid vulnerability to POODLE attacks. Thus, the top rectangle in the diagram states the main goal of the problem owner. Each rectangle underneath states a mean that contributes to the achievement of the main goal. Therefore, each arrow answer the question ‘how can the goal be achieved?’. The advantage of this approach is that means are very specific and other than technical means are also considered.

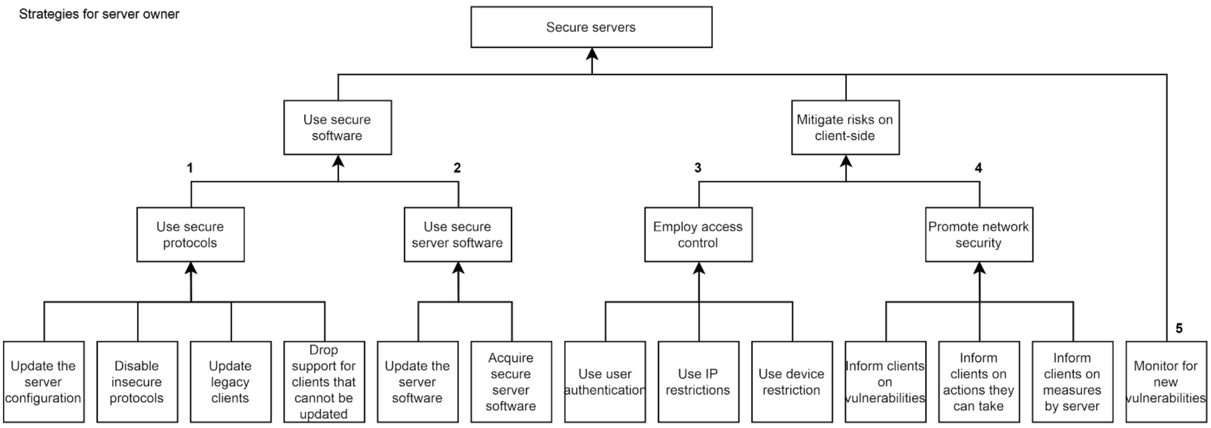
Strategies for server owner
Secure servers
Use secure software
Mitigate risks on client-side
1
2
3
4
5
Use secure protocols
Use secure server software
Employ access control
Promote network security
Update the server configuration
Disable insecure protocols
Update legacy clients
Drop support for clients that cannot be updated
Update the server software
Acquire secure server software
Use user authentication
Use IP restrictions
Use device restriction
Inform clients on vulnerabilities
Inform clients on actions they can take
Inform clients on measures by server
Monitor for new vulnerabilities

Figure 3: strategies of the server owner (problem owner).

To start, the server owner can take preventive measures to achieve secure servers. The server owner can use secure software and mitigate risks on the client side.

The first strategy available to the problem owner to prevent insecure servers, is to use secure protocols. This is also the most relevant strategy for the security issue of POODLE vulnerabilities. To use secure protocols, the server owner should either update the server configuration, or prevent fallbacks (a.k.a. downgrades) to insecure protocols. The first can be achieved by simply updating the server configuration. The latter can be achieved only when the server owner disables insecure protocols, like SSLv3. However, additional means like updating legacy clients and dropping support for clients that cannot be updated also contribute to secure protocols.

The second strategy relates to the use of secure server software. As shown in Figure 2, either the acquirance of insecure server software can result in insecure server software, or the server software that has become outdated. These two component failures can be prevented by the problem owner by simply updating the server software of acquiring secure software for the server.

The third and fourth preventive strategies are focused on the mitigation of risks on the client side by the server owner. To mitigate, the server owner can employ access control (strategy 3) by using user authentication, or by restricting certain IP addresses or devices. Similarly, the server owner can promote security in the network of his server and clients (strategy 4), by informing the clients on measures taken by the server owner, on vulnerabilities and on measures the client can take.

Finally, the server owner has a detective strategy, by choosing to monitor new vulnerabilities (strategy 5).

2.3 Other actors

As mentioned before, in the security issue of vulnerable servers, clients and adversaries are involved. Clients can either be individuals or organizations, the same applies to adversaries. However, because the goals and means of the individuals and organizations are expected to overlap significantly, they are taken as one actor.
Besides clients and adversaries, the actor network surrounding the security issue involves security providers and regulators. Security providers are companies that design and sell the server software. Regulators consists of governments or internationally acclaimed NGOs that develop standards for voluntary compliance groups.

2.4 Other actors' strategies

The regulators can play a large role in legislation, litigation and standardization. With regards to the server vulnerability, regulators can design and implement regulations that stimulate security measures by the problem owner, like the disablement of protocol fallback. For regulators, the strategy has shifted to have more applicable laws and regulations in various areas regarding data protection and security (See the NIS Directive and GDPR in Europe). This reduces the risk of losses for consumers and corporations when an incident occurs, albeit at an increased cost to organizations, which need to implement measures to be compliant with these laws/regulations.

Clients cannot make the servers secure, but they can undertake risk aversion measures like avoiding a handshake with an insecure protocol. As well, they can ask for support from the server owner, and they can (like in the case of the Google Chrome privacy settings) do naming and shaming, causing the server owner clients.

For clients, security awareness has risen due to data breaches where personal information was compromised (e.g., Equifax), and as such, the strategy for clients has been to demand higher levels of security and better practices from service providers, or to be more risk averse. This also reduces the risk of losses when an incident occurs.

Security providers have similar goals to the problem owner, since their revenue model is based on the security they can deliver to their security consumer (here the server owner). Security providers deliver the server software, along with updates for it, and thereby influence how secure server software is. The speed with which the security provider responds to vulnerabilities, can also be relevant to the security of the server. For security providers, the strategy has shifted to changing default configurations in products that security consumers use so that by default, they will be more secure (Beck, 2014; Prince, 2014). This reduces risks for the security consumer, since it is less likely for them to make an error in configuration that will cause a security issue in the future if the default configuration is already secure.

Adversaries are actors that would want to enforce strategies that increase the risks for the problem owner. So, their interest are opposite of the other actors at play. The adversaries in the case of vulnerable servers to POODLE could impose strategies that make investing in security by the server owner seem unattractive. For example, adversaries could create a botnet posing as clients with outdated servers, requesting the support for SSLv3 by a server. For the server owner receiving these requests, a large amount of support requests for SSLv3 could make it unattractive to stop supporting SSLv3 by e.g. disabling fallbacks.

For adversaries, the migration of the majority of internet users to modern, up-to-date, and secure browsers means that attacks such as POODLE are much less exploitable, and thus, they must change their attack vector in order to continue to succeed. This could mean exploiting newer vulnerabilities, or some sort of phishing attempt. As such, it has reduced the risk of the POODLE attack specifically, but may have increased the risk of incidents regarding other security vulnerabilities in the future.

3 Return on Security Investment

We calculate the ROSI for the first strategy of the server owner described earlier, which is updating to secure protocols. To use secure protocols, the server owner should either update the server configuration to completely disable insecure protocols, or prevent fallbacks (a.k.a. downgrades) to insecure protocols.

The calculation is made for one company we have chosen from our dataset, which is Sony Entertainment. We assume the same goals and means apply as discussed in the first section. At the end of the data set, they are one of the organizations with the largest number of servers that still remain vulnerable (at 2310 unique server IDs), and as such, analyzing such an organization makes the calculations more interesting.

Before we can calculate the actual ROSI we will first look at the estimated costs and benefits. These values depend on a lot of factors and are hard to estimated correctly. Therefore, we had to make assumptions about the correctness of the used numbers.

3.1 Costs

There are a few costs that would be incurred. For the estimation of costs we will reason following a scenario where Sony Entertainment suffered a breach, after which clients are fully aware of the security issues.

Firstly, losing customers because they only support SSLv3 and not a newer protocol. The percentage of affected users will be assumed to be approximately the market share of Internet Explorer 6, a very popular browser a few years ago, and one that supports nothing higher than SSLv3. The IE6 market share is 0.1%, based on (W3Counter, n.d.). Most of Sony’s servers in the dataset have a common name in the certificate of *.playstation.net, and Sony has approximately 4M visits per month to playstation.net (SimilarWeb, 2018). Based on this statistic, this means that there are 4K monthly users unable to use the services anymore offered by Sony Entertainment, this is 48000 customers on a yearly basis. Referencing Louis (2011), a user is worth on average $4USD/year this is a loss of 48K * $4 = $192K/year. There would likely also be additional customer support costs associated with this endeavour. This could be for training existing customer service agents to know how to address customers calling about this issue, or for creating a new support line specifically for this issue. Based on the prices for call center services from WorldWide Call Center (n.d.), we can make an upper-bound estimate of roughly $30USD/hour, at a rate of 10 hours a day. This yields a cost of $30 * 10 * 365 = $109,500/year.

Secondly, actually disabling SSLv3 on the servers will at least require the man hours to update every server. As an upper-bound, let us estimate the amount of work to be roughly 1 week to upgrade 2310 servers by a 4 man team; this yields 160 hours on the project. At a rate of $50 salary per hour, this leads to a one-time expenditure of 160 * $50 = $8000. Plus the cost of the updated software version and future maintenance, which we estimate to be $100 per server per year for all servers, which translates to another $23100/year.

The total cost for this risk strategy is a fixed $8000 upfront, with a yearly recurring cost of $192000 + $109500 + $23100 = $324,600/year (see Table 1).

Table 1: Estimated costs.

	Costs	Units
Disabling costs	8,000	$
Customer loss	192,000	$/year
Customer support costs (upper-bound)	109,500	$/year
Software & maintenance costs	23,100	$/year
Total fixed costs	8,000	$
Total recurring costs	324,600	$/year
Total costs for 1 year	332,600	$

3.2 Benefits

Next to the costs for executing the risk strategy, there are the benefits. Benefits can be perceived as prevented losses. Therefore, we are again exploring the costs, yet now in the scenario where a breach has occurred and clients are fully aware of the security issues at Sony Entertainment. Several types of prevented losses can be distinguished: reputation loss and the costs of litigation and fines as a consequence of the breach.

The prevented reputation loss is estimated to be $200000, based on the average costs of cyber incidents found by Romanosky (2016). This is a rough estimate as it will depend on the the media attention and other factors in the future, and will likely decrease over time. As well, because of the size and market share of the company, it is likely for these costs to be much higher. The security investment will also prevent Sony Entertainment to be sued by clients which will at least prevent the costs for lawyers which will be around $26000 per month, or $312000/year. With the new privacy laws in europe the company could also get a fine for not protecting their users privacy enough. This fine could be $32000 for every month the servers are still vulnerable, resulting in $384000/year. The estimated cost reduction for one year will be $200K + $312K + $384K = $896K (see Table 2).

Table 2: Estimated benefits.

	Benefits	Units
Prevented reputation loss	200,000	$
Litigation costs	312,000	$/year
Prevented fines	384,000	$/year
Total fixed benefits	200,000	$
Total recurring benefits	696,000	$/year
Total benefits for 1 year	896,000	$

3.3 ROSI calculation

Based on the calculated cost and benefit, we can calculate the ROSI for the first year as follows:

$$ROSI = \frac{Risk\ Exposure * Risk\ Mitigated\ - cost}{cost} = \frac{896000 * 1.0 - 332600}{332600} = 1.69 = 169\%$$

This means the risk strategy to update insecure servers and prevent fall backs is a cost-effective strategy, since the savings from investment would be equivalent to a 169% payback on the security investment. Given that the risk is also totally and completely mitigated, this is a good result.

4 Conclusion

There are still many servers vulnerable, even though the SSLv3 has long been replaced by more recent TLS versions. The problem owner for this security issue is the organization responsible for the server, i.e. the server owner. From the perspective of the server owner possible strategies are investigated. The most relevant strategy is to prevent fallback to less secure protocols and update the security protocols. Another strategy is a preventive strategy focused on the mitigation of risks on the client side by the server owner. The server owner can employ access control by using user authentication, or by restricting certain IP addresses.

There are different actors involved in this security issue for example the regulators, they can play a large role in legislation, litigation and standardization. Other actors are the clients they cannot make the servers secure, but they can undertake risk aversion measures like avoiding a handshake with an insecure protocol. With the risen security awareness they demand higher levels of security from the server owners. Adversaries are actors that would want to enforce strategies that increase the risks for the problem owner. So, their interest are opposite of the other actors at play.

The ROSI calculation focussed on the strategy to use secure protocols, the server owner should either update the server configuration, or prevent fallbacks to insecure protocols. From the calculated ROSI can be concluded that this strategy is a cost-effective strategy.

5 References

Beck, B. (2014). LibreSSL 2.1.1. Released. Retrieved September 28, 2018, from https://marc.info/?l=openbsd-announce&m=141347213320729&w=2

Holmes, D. (2015). How much is my traffic is still SSLv3? Retrieved September 28, 2018, from https://devcentral.f5.com/articles/how-much-of-my-traffic-is-still-sslv3

Louis, T. (2011). How Much Is A User Valued At? Retrieved September 30, 2018, from https://www.businessinsider.com/how-much-is-a-user-worth-2011-7?international=true&r=US&IR=T

Prince, M. (2014). SSLv3 Support Disabled By Default Due to POODLE Vulnerability. Retrieved September 28, 2018, from https://blog.cloudflare.com/sslv3-support-disabled-by-default-due-to-vulnerability/

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

SimilarWeb. (2018). Playstation.net August 2018 Overview. Retrieved September 30, 2018, from https://www.similarweb.com/website/playstation.net

WorldWide Call Center. (n.d.). Outsourcing Costs | Call Center Pricing. Retrieved September 30, 2018, from https://www.worldwidecallcenters.com/call-center-pricing/