Preliminary report / Prethodno priopćenje
Manuscript received: 2015-09-10
Revised: 2016-05-27
Accepted: 2016-05-31
Pages: 25 - 32

Analysis of TLS implementation on public Web sites in the Republic of Croatia

Dražen Pranić
Tele2, Zagreb, Croatia
drazen.pranic@tele2.hr

Zlatan Morić
IN2data
Data Science Company Ltd., Zagreb, Croatia
zlatan.moric@in2data.eu

Zdravko Kunić
IN2data
Data Science Company Ltd., Zagreb, Croatia
zdravko.kunić@in2data.eu

Abstract: Practical cryptography represents one of the most important aspects of information security. One of the most important elements of cryptography is Secure Sockets Layer (SSL) protocol, which is the most widely deployed security protocol, used today. Unfortunately SSL protocol is constantly exposed to various threats and vulnerabilities. Heartbleed, POODLE, FREAK are the most notorious SSL bugs in recent period. Many studies have shown that in the SSL implementation of SSL there are many challenges. The focus of this paper is placed on how the leading Croatian companies in the private and public sectors cope with these challenges. From this research it is evident that private companies have better SSL implementation although there are some challenges for both sectors for managing SSL configurations.

Keywords: SSL, TLS, configuration, Heartbleed, Republic of Croatia

INTRODUCTION

Practical cryptography represents one of the most important aspects of information security. The fundamental role of cryptography is protecting confidentiality and integrity of information. However, we are witnessing that protection of data privacy and confidentiality represent huge challenge for each country, company and individual. There are numerous examples of unauthorized access into government, private companies' information systems.[1] Details of massive global communications surveillance, provided by Edward Snowden, also show that almost whole world is affected [6].

One of the most important elements of cryptography is Secure Sockets Layer (SSL) protocol, which is the most widely deployed security protocol used today. This protocol provides an encrypted communication over the Internet or an internal network – typically between a web server and a browser; or a mail server and a mail client. When the SSL protocol was standardized by the IETF, it was renamed to Transport Layer Security (TLS). Many use the TLS and SSL names interchangeably, since SSL protocol is superseded by TLS. This approach will be taken in this paper.

»*SSL use X.509 certificates and hence asymmetric cryptography to authenticate the counterpart with whom they are communicating, and to negotiate a symmetric session key.*« [5] Therefore the implementation of SSL should be focused on protocol configuration and management of X.509 certificates. Many successful SSL attacks[2] show that this task can be quite challenging. According to Forrester Research *»Predictions 2015: Data Security and Privacy Are Competitive Differentiators«* managing the keys and certificates behind SSL is becoming increasingly difficult and critical in both IT security and business terms. The Ponemon Institute's 2015 *»Cost of Failed Trust Report*« estimates that, over the last two years, the number of keys and certificates deployed from web servers to cloud services has grown over 34 percent, to almost 24,000 per enterprise—not counting those used beyond the firewall.

Besides that in last two years quite many high SSL protocol vulnerabilities occurred which affected large part of Internet infrastructure.

In this paper the implementation of SSL protocol on public Web sites in Republic of Croatia will be investigated. In analysis are included the largest companies based on total income and important government institutions like parliament, ministries, president office.

SSL VULNERABILITIES

Information systems vulnerability according to ENISA[3] is defined as *»the existence of a weakness, design, or implementation error that can lead to an unexpected, undesir-*

[1] Target, Home Depot, JP Morgan Chase, Adobe, EBay, Ashley Madison, Sony cases are examples of huge data breaches were millions of customer data leaked due to hacker's attacks.

[2] The theft of data on 4.5M healthcare patients in 2014 started with the exploit of Heartbleed to steal an SL/TLS key and certificate that encrypted sensitive data. (https://www.trustedsec.com/august-2014/chs-hacked-heartbleed-exclusive-trustedsec/)

[3] The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cyber security in Europe.

able event compromising the security of the computer system, network, application, or protocol involved.« [2]

Applying that principle to the SSL protocol, vulnerability can occur due to poor SSL configuration, certificate management or software weakness. In Table 1 are listed some of the more infamous vulnerabilities, their associated attack vector and remediation steps in recent period.

Table 1: *SSL/TLS Vulnerabilities.*

Name	Date Identified	Attack Vector	Remediation
Heartbleed	4/2014	Exploits vulnerability in OpenSSL that allows attacker on the open Internet to read memory and compromise keys.	Patch vulnerable servers. Generate new key pair. Install new certificate. Revoke old certificate.
POODLE	9/2014	Known flaw in SSL v3.0 that allows exploitation of way it ignores padding bytes when running in cipher block chaining (CBC) mode.	Disable SSLv3.0 on both servers and clients, starting with servers that have highest impact. Upgrade to TLS v1.2, which is not vulnerable.
FREAK	3/2015	A vulnerable browser connects to a susceptible web server that accepts »export-grade« encryption.	Server: Test and configure disable support for TLS export cipher suites as well as other cipher suites that are known to be insecure and enable forward secrecy. Client (Browser): Update, patch, maintain secure configuration.
DROWN	3/2016	An attacker can potentially use this flaw in SSL 2.0 to decrypt RSA-encrypted cipher text from a connection using a newer SSL/ TLS protocol version, allowing them to decrypt such connections.	Disable SSLv2.0 on server. Use latest TLS v1.2 protocol.

HEARTBLEED

According to many sources, the Heartbleed bug was one of the biggest security threats the Internet has ever seen. The bug has affected many popular websites and services and was disclosed in April 2014 in the OpenSSL cryptography library, which is a widely used implementation of the SSL protocol. It results from improper input validation in the implementation of the SSL heartbeat extension, thus the bug's name derives from *»heartbeat«.* When it is exploited it leads to the leak of memory contents from the server to the client and from the client to the server.

At the time of disclosure, some 17% (around half a million) of the Internet's secure web servers certified by trusted authorities were believed to be vulnerable to the attack, allowing theft of the servers' private keys and users' session cookies and passwords. Since vulnerability in heartbeat extension is present from February 2012 many security professionals advised end users to change password for affected Web services because sensitive account information (such as passwords and credit card numbers) were exposed for two years period. The list of affected Internet giants was impressive: Google, Facebook, Twitter, Instagram, Yahoo, etc [4].

POODLE

In late September 2014, a team at Google discovered a serious vulnerability in SSL 3.0 that can be exploited to steal certain confidential information, such as cookies. This vulnerability, was known as »POODLE« (which stands for Padding Oracle On Downgraded Legacy Encryption).

To work with legacy servers, many TLS clients implement a downgrade dance: in a first handshake attempt, offer the highest protocol version supported by the client; if this handshake fails, retry (possibly repeatedly) with earlier protocol versions. Unlike proper protocol version negotiation (if the client offers TLS 1.2, the server may respond with, say TLS 1.0), this downgrade can also be triggered by network glitches, or by active attackers.

So if an attacker that controls the network between the client and the server interferes with any attempted handshake offering TLS 1.0 or later, such clients will readily confine themselves to SSL 3.0. Therefore any website that supports SSL 3.0 is vulnerable to POODLE and only solution to mitigate this vulnerability is disable it.

But a new variant of the original POODLE attack was announced on December 8, 2014. This attack exploits implementation flaws of CBC encryption mode in the TLS 1.0 - 1.2 protocols. Even though TLS specifications require servers to check the padding, some implementations fail to validate it properly, which makes some servers vulnerable to POODLE even if they disable SSL 3.0.

FREAK

At March 3, 2015, researchers announced a new SSL/TLS vulnerability called the FREAK attack (which stands for Factoring Attack on RSA-EXPORT Keys). Basically, some sites'

implementations of secure sockets layer technology, or SSL, contain both strong encryption algorithms and weak encryption algorithms. Connections are supposed to use the strong algorithms, but it allows an attacker to intercept HTTPS connections between vulnerable clients and servers and force them to use weakened encryption, which the attacker can break to steal or manipulate sensitive data.
Compare to other vulnerabilities this security flaw was designed in deliberately. »*Back in the early 1990s when SSL was first invented at Netscape Corporation, the United States maintained a rigorous regime of export controls for encryption systems. In order to distribute crypto outside of the U.S., companies were required to deliberately* »weaken« the strength of encryption keys. For RSA encryption, this implied a maximum allowed key length of 512 bits.« [1].

DROWN

In March 2016 group of researches published a scientific article about new SSL attack called DROWN.[4] This paper has attracted a lot of attention since according to researchers almost one third of all Web sites are vulnerable to this attack.
Acronym DROWN stands for »Decrypting RSA with Obsolete and Weakened eNcryption«. DROWN is a classic example of a »cross protocol attack«. This type of attack makes use of flaws in one protocol implementation (SSL 2.0) to attack the security of connections made under a different protocol (TLS). More concretely, DROWN is based on the fact that both SSL 2.0 and TLS support RSA encryption. TLS properly defends against certain well-known attacks on this encryption while SSL 2.0 export suites emphatically do not.

ANALYSIS OF SSL IMPLEMENTATION IN CROATIA

Analysis of SSL protocol implementation in Croatia was conducted against public Web sites of the largest companies based on total income and important government institutions like parliament, ministries, president office, etc. In this analysis all relevant companies from financial sector (banks, insurance, pension funds, etc.) due to importance of this sector for each society are also included. Information about top companies in Croatia based on total income is provided by Financial agency (FINA)[3].
The analysis of the SSL protocol implementation is focused on presence of most important vulnerabilities (Heartbleed, POODLE, FREAK) and configuration errors (usage of obsolete SSL protocols, not supported latest TLS protocol, usage of weak encryption algorithms). The results of those SSL checks form a single grade which is used to compare quality of SSL implementation between different Web sites. Analysis is performed with several publicly available tools/Web sites:

- Qualys SSL Labs,
- SymantecCryptoReport,
- DigiCert SSL Certificate Checker.

[4] Full article can be found on https://drownattack.com/drown-attack-paper.pdf.

Outcome of each Web site analysis with those tools are thoroughly checked and entered into spreadsheet in appendix 1.[5]

PRIVATE VS. PUBLIC SECTOR

The analysis includes 87 subjects which have SSL enabled on their public Web sites. It is worth to mention that many Web sites that should be in the scope of this analysis don't have SSL enabled and therefore are not included in analysis.

In Table 2 is shown SSL grade distribution base on property. From this table it is evident that private companies have better SSL implementation on public Web sites:

- 34% of private companies have grade A and only 4% grade F,
- 29% of state companies have grade A and 13% grade F.

Those results are not surprise. Actually there are two main reasons of why private sector has better SSL implementation:

a. Private sector is generally more concerned about information security. In these days is quite common to have position of security manager in company. System of decision-making and responsibility is generally better implemented in the private sector.
b. Lots of services in finance sector in Croatia are offered online: Internet banking, insurance policies, etc. Those services are sensitive and business critical. Therefore SSL implementation in finance sector should be better than in other sectors. This is clearly visible in Table 3.

Table 2: *SSL grade distribution based on type of property.*

Grade	**A**		**B**		**C**		**D**		**E**		**F**		Total	Total
Property	#	%	#	%	#	%	#	%	#	%	#	%	#	%
Mixed	1	11%	1	11%		0%	6	67%		0%	1	11%	9	100%
Private	16	34%	4	9%	7	15%	10	21%	8	17%	2	4%	47	100%
State	9	29%	3	10%		0%	10	32%	5	16%	4	13%	31	100%
Grand Total	**26**	**30%**	**8**	**9%**	**7**	**8%**	**26**	**30%**	**13**	**15%**	**7**	**8%**	**87**	**100%**

Table 3: *SSL grade distribution in finance sector.*

Grade	**A**		**B**		**C**		**D**		**E**		**F**		Total	Total
Sector	#	%	#	%	#	%	#	%	#	%	#	%	#	%
Finance	13	35%	3	8%	3	8%	10	27%	6	16%	2	5%	37	100%
Grand Total	**13**	**35%**	**3**	**8%**	**3**	**8%**	**10**	**27%**	**6**	**16%**	**2**	**5%**	**37**	**100%**

[5] Full analysis is available on https://drive.google.com/file/d/0B2nxuG8Alz6oRHRtY1BLemRkUGc/view?usp=sharing.

VULNERABILITIES/CONFIGURATION ISSUES IN SSL IMPLEMENTATION

As is mentioned before in this paper this analysis is focused on presence of important vulnerabilities and configuration errors in SSL protocol implementation. Our analysis will try to identify which part of the SSL implementation are challenging for companies in Croatia. Which security flaws, vulnerabilities are fixed and where are still present failures in SSL implementation.

Analyzed Croatian Web sites are most vulnerable to POODLE security flaw:

- 26 Web sites are vulnerable to POODLE attack,
- 11 Web sites are vulnerable to FREAK attack,
- 9 Web sites vulnerable to DROWN attack,
- 0 Web sites are vulnerable to Heartbleed attack.

POODLE is still a huge challenge for many Web sites, not just in Croatia, due to the need to support SSL 3.0 protocol. In normal operation, SSL 3.0 shouldn't needed by the vast majority of sites. Although it's likely that there's a long tail of clients that don't support anything better.

Besides completely disabling old SSL protocols there are other options for mitigating POODLE bug. One of them is enabling TLS_FALLBACK_SCSV feature. Therefore in this analysis there are Web sites that are not vulnerable to POODLE but support old SSL protocols.

Situation with configuration errors/flaws in SSL implementation at analyzed Croatian Web sites is much worse compare with resilience to most famous SSL bugs:

- 65 Web sites are using weak encryption algorithms (for example RC4 cipher),
- 59 Web sites are supporting old SSL protocols (SSL 3.0 and/or SSL 2.0);
- 44 Web sites are not supporting latest SSL protocol (TLS 1.2).

In configuration errors/flaws of SSL implementation both private and public sector are on the same level. This is clearly seen from Table 4 where usage of weak encryption algorithms is analyzed.

Table 4: *Usage of weak encryption algorithms.*

	Weak encryption algorithms					
	No		**Yes**			
Sector	#	%	#	%	**Total #**	**Total %**
Mixed	1	11%	8	89%	9	100%
Private	13	28%	34	72%	47	100%
State	8	26%	23	74%	31	100%
Grand Total	22	25%	65	75%	87	100%

Obviously companies were more focused to mitigate risks related with »famous« security flaws like Heartbleed, POODLE, FREAK. This conclusion is particularly true for Heartbleed attack whereas main remediation activity was patching of vulnerable Web site and all analyzed companies deployed needed security patch.

Actually the challenge is to maintain secure SSL configuration since many Web sites are not aligned with good practice. Many organization have complex IT systems with lots of internal and external Web sites and it can be challenging to maintain secure SSL configurations in all of them. In order to improve Web sites SSL configuration security here are two most important recommendations:

- disable usage of SSL 3.0 and SSL 2.0,
- disable usage of weak ciphers (DES, RC4), prefer modern ciphers (AES), modes (GCM), and protocols (TLS 1.2).

CONCLUSION

Security of SSL implementation is one of top priority for each company. This task represent huge challenge due to serious threats, vulnerabilities in technology itself and complex SSL implementations. Nowadays SSL certificates are present almost on every device towards which is necessary to encrypt communication. Despite high-profile scandals over systemic weaknesses, including Heartbleed, POODLE and FREAK, the greatest threat to the security of SSL/TLS implementation appears to be the lax controls most organizations exert over securing SSL configuration and certificates/keys. Results of this research clearly show that top companies/public administration in Republic of Croatia are aligned with this world trend. Top security flaws are mainly mitigated while in SSL configurations exist serious security errors.

In order to have secure SSL implementation it is necessary to follow well known best practice which cover various aspects of SSL security. One of the best framework which includes detail SSL security controls is »Top 20 security controls« from SANS institute. By following framework like this SSL security will be significantly improved.

REFERENCES

[1] (2015-05-03) http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html
[2] (2016-05-30) https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary
[3] (2015-07-10) http://www.fina.hr/Default.aspx?art=11553
[4] (2014-04-10) http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/
[5] (2016-05-30) http://searchsecurity.techtarget.com/definition/Secure-Sockets-Layer-SSL
[6] (2013-11-01) http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1