

Peter the Great St.Petersburg Polytechnic University
Institute of Computer Science & Technologys

Department of Computer Systems & Software Engineering

Laboratory №5 Report

Discipline: Information Security

Theme: A free online service Qualys SSL Labs – SSL Server Test

Made by student of group. 13541/3

_____ D.V. Kruminsh
(signature)

Lecturer

_____ N.V. Bogach
(signature)

Saint-Petersburg
2017

Contents

1	A free online service Qualys SSL Labs – SSL Server Test	2
1.1	Task	2
1.1.1	Study	2
1.1.2	Exercises	2
2	Work Progress	3
2.1	Study	3
2.1.1	Learn how to deploy SSL/TLS correctly	3
2.1.2	Learn SSL security issues – POODLE, HeartBleed	3
2.2	Exercises	4
2.2.1	Choose one domain from a list of Recent Best and one from Recent Worst at SSL Server Test – study reports and explain their summary . .	4
2.2.2	Analyse a SSL-based domain	5
3	Conclusion	7

A free online service Qualys SSL Labs – SSL Server Test

SSL Server Test performs a deep analysis of the configuration of any SSL web server on the public Internet.

1.1 Task

1.1.1 Study

1. Learn how to deploy SSL/TLS correctly;
2. Learn SSL security issues – POODLE, HeartBleed.

1.1.2 Exercises

1. Choose one domain from a list of Recent Best and one from Recent Worst at SSL Server Test – study reports and explain their summary;
2. Analyse a SSL-based domain:
 - Explain Summary;
 - Explain the abbreviations in Configuration;
 - Comment on Protocol Details;
 - Conclude about SSL status.

Work Progress

2.1 Study

2.1.1 Learn how to deploy SSL/TLS correctly

1. Private Key and Certificate

- Use 2048-Bit Private Keys
- Protect Private Keys
 - Generate private keys on a trusted computer;
 - Password-protect keys from the start to prevent compromise;
 - After compromise, revoke old certificates and generate new keys;
 - Renew certificates yearly.
- Make sure you cover enough of the domain names you use;
- Obtain Certificates from a Reliable CA;
- Use Strong Certificate Signature Algorithms.

2. Configuration

- Use Complete Certificate Chains(two or more certificates);
- Use Secure Protocols(SSL v2, SSL v3, TLS v1.0, TLS v1.1, and TLS v1.2);
- Use Secure Cipher Suites(to ascertain that you are communicating directly with the desired party (and not through someone else who will eavesdrop));
- Use Forward Secrecy(protocol feature that enables secure conversations that are not dependent on the server's private key);
- Use Strong Key Exchange;
- Use up-to-date software.

2.1.2 Learn SSL security issues – POODLE, HeartBleed

POODLE(Padding Oracle On Downgraded Legacy Encryption) is a vulnerability in SSLv3. The attacker sends data to the server on the SSL3 protocol from the changed target, which allows him to decrypt 1 byte for 256 requests. This is due to the fact that SSLV3 does not take into account the MAC address.

HeartBleed is a security bug in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol. It allows unauthorized reading of memory on a server that may contain a variety of private data at this time.

2.2 Exercises

2.2.1 Choose one domain from a list of Recent Best and one from Recent Worst at SSL Server Test – study reports and explain their summary

Let's check site of my university - **www.spbstu.ru**.

First of all, there are several problems with certificate:

- not trusted and self signed;
- weak encryption algorithm - SHA-1.

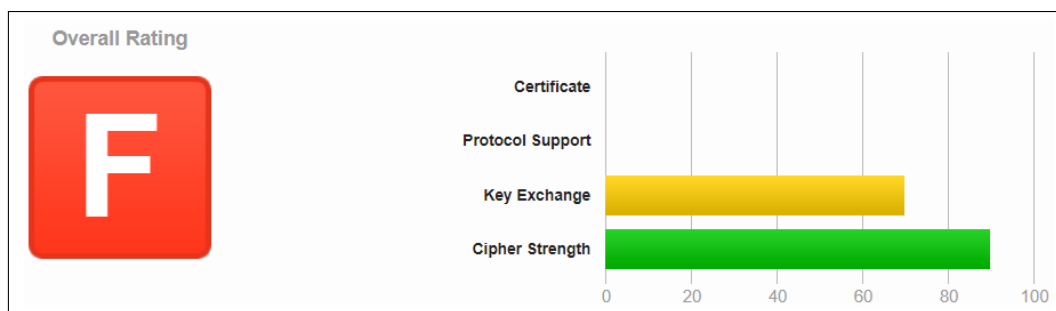


Figure 2.1: Certificate analyze


Certificate #1: RSA 1024 bits (SHA1withRSA)	
 Server Key and Certificate #1	
Subject	Bitrix Fingerprint SHA256: 82e6415d0b13998d2fa67934b527efea9dd7953c7fe6d7ca330b2b80d89d509c Pin SHA256: gX/eGOGsl06gXqTeBXILSgKzuzqu7KKlmmNGgAfR/Ew=
Common names	Bitrix
Alternative names	- INVALID
Serial Number	00d430f95745220dfc
Valid from	Tue, 05 Aug 2014 05:18:28 UTC
Valid until	Fri, 02 Aug 2024 05:18:28 UTC (expires in 6 years and 7 months)
Key	RSA 1024 bits (e 65537) WEAK
Weak key (Debian)	No
Issuer	Bitrix Self-signed
Signature algorithm	SHA1withRSA INSECURE
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	None
DNS CAA	No (more info)
Trusted	No NOT TRUSTED (Why?)

Figure 2.2: Certificate of www.spbstu.ru

Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	Yes INSECURE (more info)
Forward Secrecy	Weak key exchange WEAK
ALPN	No
NPN	Yes http/1.1
Session resumption (caching)	Yes

Figure 2.3: SSL vulnerability

The main reason why the result of the analysis is F, is **OpenSSL Padding Oracle vuln.(CVE-2016-2107)** that provides to do some things. A remote attacker could possibly use this flaw to retrieve plain text from encrypted packets by using a TLS/SSL or DTLS server as a padding oracle.

2.2.2 Analyse a SSL-based domain

In my opinion this domain is pretty good from a security perspective. Server supports:

- current best **TLS 1.2**;
- forward Secrecy with the reference browsers;
- server is safe to POODLE attacks.

Explain the abbreviations in Configuration

- TLS – Transport Layer Security.
- SSL – Secure Sockets Layer.
- RSA is an abbreviation for the names Rivest, Shamir and Adleman.
- RC4 - Rivest cipher 4 or Ron's code 4.
- SHA – Secure Hash Algorithm.
- AES – Advanced Encryption Standard.
- CBC – Cipher Block Chaining.
- 3DES – Triple Data Encryption Standard.
- SNI – Server Name Indication
- NPN – Next Protocol Negotiation.
- HSTS – HTTP Strict Transport Security.

- HPKP – HTTP Public Key Pinning.
- HTTP – HyperText Transfer Protocol

Comment on Protocol Details

- Secure Renegotiation - resume TLS connection.
- BEAST attack - attack by the BEAST utility (Browser Exploit Against SSL / TLS).
- POODLE is a vulnerability that allows you to decrypt the contents of a secure communication channel.
- Heartbleed - an error in OpenSSL, which allows unauthorized reading of memory on the server up to 64 kilobytes per request. An attack can be made an infinite number of times.
- Downgrade attack is an attack in which the user is forced to use less secure protocols that are still supported for compatibility reasons.
- Forward Secrecy is a protocol feature that provides secure data exchange, it does not depend on the server's private key. With encryption algorithms that do not support Forward Secrecy, it is possible to decrypt previously encrypted conversations using the private key of the server.
- Next Protocol Negotiation - the client tells the server what protocols it would like to communicate with and the server can answer the most preferred one that it knows.
- Strict Transport Security - a mechanism that activates the forced secure connection over HTTPS. This security policy allows you to immediately establish a secure connection, instead of using HTTP. The mechanism uses a special HTTP Strict-Transport-Security header to switch a user who has logged over HTTP to an HTTPS server.

Conclude about SSL status

The domain has the rating (F) for the implementation of SSL. It has next disadvantages:

- private key is not strong enough(RSA 1024 not enough to be secure in 2017);
- Vulnerability names OpenSSL Padding Oracle vuln.(CVE-2016-2107);
- Server supports weak Diffie-Hellman (DH) key exchange parameters.

Conclusion

In this laboratory work I studied the capabilities of the SSL Labs service, analyzing the quality of domain security.

Services like **ssllabs.com** are useful to hackers for attacks and system administrators to prevent them.

In this service i analuze domain **www.spbstu.ru**. A report on this domain was viewed, and details were explored. As result my university site is not protected as well.