

PETER THE GREAT ST.PETERSBURG POLYTECHNIC UNIVERSITY
DEPARTMENT OF COMPUTER SYSTEMS & SOFTWARE ENGINEERING

Laboratory report №5

Discipline: «Information Security»

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

Made by student:

Volkova M.D.

Group: 13541/2

Lecturer:

Bogach N.V.

Saint-Petersburg
2018 y.

Contents

| | | |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| 1 | Laboratory work №5 | 2 |
| 1.1 | Work purpose | 2 |
| 1.2 | Task | 2 |
| 1.3 | Study | 3 |
| 1.3.1 | Learn how to deploy SSL/TLS correctly | 3 |
| 1.3.2 | Learn SSL security issues POODLE, HeartBleed | 3 |
| 1.4 | Exercises | 4 |
| 1.4.1 | 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 |
| 1.4.2 | Analyse a SSL-based domain | 6 |
| 1.5 | Conclusion | 7 |

Laboratory work №5

1.1 Work purpose

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

1.2 Task

Study

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

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:
 - (a) Explain Summary
 - (b) Explain the abbreviations in Conguration
 - (c) Comment on Protocol Details
 - (d) Conclude about SSL status

1.3 Study

1.3.1 Learn how to deploy SSL/TLS correctly

Private Key and Certificate

- Use 2048-bit private keys
- Protect private key
 - Generate private keys and certificate requests (CSRs) on the trusted computer.
 - To prevent key compromise, use password protection.
 - After compromising, revoke old certificates and generate new keys.
 - Update certificates each year with new private keys.
- Make sure you cover enough of the domain names you use.
- Obtain certificates from trusted certification authorities.
- Use reliable certificate signing algorithms.

Configuration

- Configure the correct certificate chains (one certificate is not enough for one certificate)
- Use secure protocols. For example, TLS v1.0, v1.1 and v1.2
- Use secure encryption algorithms (for example symmetric with keys of at least 128 bits)
- Monitoring the selection of the encryption algorithm.
- Support Forward Secrecy - features a protocol that allows you to exchange data regardless of the private key of the server.
- Disable client security validation capabilities.

Application Design

- Use HSTS (HTTP Strict Transport Security), a mechanism that activates the forced secure connection through the HTTPS protocol.
- Disable the caching for the important content from the content security cutoff point.
- Use protected cookies.

1.3.2 Learn SSL security issues POODLE, HeartBleed

POODLE – 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.

To implement a POODLE attack, you must:

- Have the ability to listen and replace the attacker's traffic
- Have the ability to make requests on behalf of the attacker with known attack text

HeartBleed – s 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.

1.4 Exercises

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

Example one of the best report

As an example of the best report, take a report on one of the <https://github.com> domain servers:

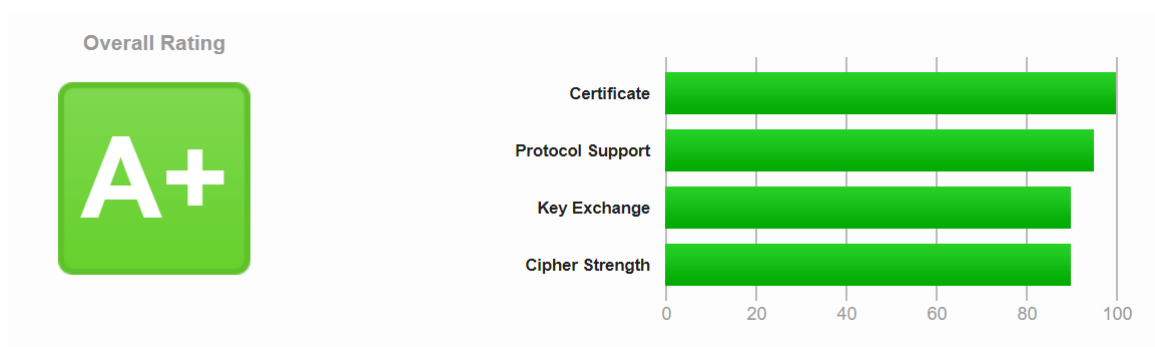


Рис. 1.1: Summary of github.com analyze


| | | |
|-----------------------------------------------------------------------------------|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | Server Key and Certificate #1 | |
| | Subject | github.com Fingerprint SHA256: 25fe3932d9638c8afca19a2987d83e4c1d98db71e41a480398ea226abd8b9316 Pin SHA256: pL1+qb9HTMRZJmuC/bB/ZI9d302BYrrqiVuRyW+DGrU= |
| | Common names | github.com |
| | Alternative names | github.com www.github.com |
| | Serial Number | 0bfdb4090ad7b5e640c30b16c9529a27 |
| | Valid from | Thu, 10 Mar 2016 00:00:00 UTC |
| | Valid until | Thu, 17 May 2018 12:00:00 UTC (expires in 4 months and 10 days) |
| | Key | RSA 2048 bits (e 65537) |
| | Weak key (Debian) | No |
| | Issuer | DigiCert SHA2 Extended Validation Server CA AIA: http://cacerts.digicert.com/DigiCertSHA2ExtendedValidationServerCA.crt |
| | Signature algorithm | SHA256withRSA |
| | Extended Validation | Yes |
| | Certificate Transparency | Yes (certificate) |
| | OCSP Must Staple | No |
| | Revocation information | CRL, OCSP CRL: http://crl3.digicert.com/sha2-ev-server-g1.crl OCSP: http://ocsp.digicert.com |
| | Revocation status | Good (not revoked) |
| | DNS CAA | No (more info) |
| | Trusted | Yes Mozilla Apple Android Java Windows |

Рис. 1.2: Server key and certificate of github.com domain

With this certificate there are practically no problems with any of the tests. We can be sure that the data of users of resource <https://github.com> can not be intercepted or replaced by an attacker.

Example one of the worst report

As an example of the best report, take a report on one of the <http://spbstu.ru> domain servers:

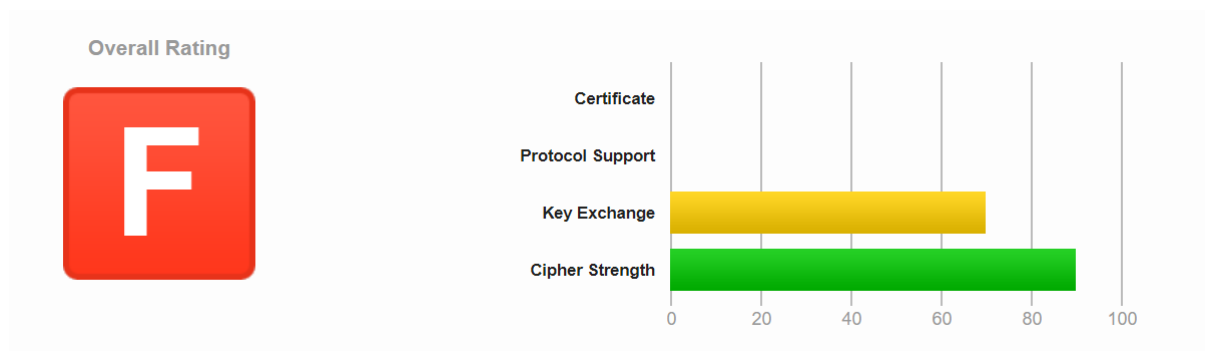


Рис. 1.3: Summary of spbstu.ru analyze


| | |
|------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
|  Server Key and Certificate #1 | |
| Subject | Bitrix Fingerprint SHA256: 82e6415d0b13998d2fa67934b527efea9dd7953c7fe6d7ca3 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 6 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?) Mozilla Apple Android Java Windows |

Рис. 1.4: Server key and certificate of spbstu.ru domain

This certificate has several basic problems:

- Not trusted and self signed.
- Weak encryption algorithm.

Data transmitted over the network can easily be intercepted by an attacker.

1.4.2 Analyse a SSL-based domain

Explain Summary

Server certificate is often the weakest point of an SSL server configuration. A certificate that is not trusted (i.e., is not ultimately signed by a well-known certificate authority) fails to prevent man-in-the-middle (MITM) attacks and renders SSL effectively useless. A certificate that is incorrect in some other way (e.g., a certificate that has expired) erodes trust and, in the long term, jeopardizes the security of the Internet as a whole.

For these reasons, any of the following certificate issues immediately result in a zero score:

- Domain name mismatch.
- Certificate not yet valid.
- Certificate expired.
- Use of a self-signed certificate.
- Use of a certificate that is not trusted (unknown CA or some other validation error).
- Use of a revoked certificate.
- Insecure certificate signature (MD2 or MD5).
- Insecure key.

Explain the abbreviations in Conguration

- TLS – Transport Layer Security.
- SSL – Secure Sockets Layer.
- RSA – 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** – resuming 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.
- **Downgrade attack** is an attack in which the user is forced to use less secure protocols that are still supported for compatibility reasons.
- **TLS compression** – In 2012, CRIME attack showed how TLS compression can be used by attackers to identify details of sensitive data (for example, session cookies).
- **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.

- **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 <http://spbstu.ru> has the rating "F" for the implementation of SSL. It's due to the following reasons:

- Not trusted and self signed.
- 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.

The domain <http://github.com> has the rating "A+" for the implementation of SSL, because it is not subject to known vulnerabilities, trusted, and has a crypto-stable key length.

1.5 Conclusion

In this lab, we studied the «Qualys SSL Server Test» tool designed to test domains for the quality of the SSL/TLS encryption implementation. This resource provides an assessment of the quality of implementation based on many criteria and characteristics and then issues an assessment of the quality of implementation on its own scale of marks. It can be useful to identify unsafe resources on which your data can be stolen.