Table of Contents

BioStar 2, HTTP, HTTPS

BioStar 2 and Web Security

Web security is crucial in the modern world because 70% of all hacking is done through the web. Since the web holds the characteristic of easy access, it is also prone to be exposed to vulnerabilities. Hence, attacks through websites are not something that can be prevented by the administrator with careful consideration of tight security.

This article explains the differences of the two security protocols (HTTP and HTTPS) that are being by used by BioStar 2, which is a web-based security platform, and explains the reason why HTTPS should be used.

HTTP

HTTP is an acronym for Hypertext Transfer Protocol. It is used to send and receive HTML (Hypertext Markup Language) documents. It is a protocol that sends data between the web client (user) and web server (service provider) through a web browser. It normally uses the TCP/UDP method and port 80.

HTTP does not maintain its own connection status so data exchange is done through ‘REQUEST’ and ‘RESPONSE’. If this step does not exist, the web server cannot know what page the web browser is requesting, and the web browser cannot know what page the web server is transmitting.

HTTP executes ‘REQUEST’ and ‘RESPONSE’ with unencrypted text so it is faster than HTTPS, but if someone intercepts the data and reads them, they can see the content of the page that the client is observing.

HTTPS

HTTPS is an acronym for Hypertext Transfer Protocol over Secure Socket Layer and is a form of HTTP with enhanced security. When HTTPS is used, all ‘Request’ and ‘Response’ data is encrypted before data is sent to the network. This encrypted layer is composed of SSL (Secure Socket Layer) or TLS (Transport Layer Security). HTTPS may be slower than HTTP because it encrypts the communicated data but provides superior security.

+ SSL and TLS
SSL was developed by Netscape. It was used widely and the name changed to TLS when it was chosen as the international standard by IETF (Internet Engineering Task Force), which is the international organization for standardization. However, the name SSL is still used widely today.

SSL Certificate

SSL certificate is necessary to utilize HTTPS. This is an electronic document that assures client and server communication by a third party (certification authority). When the client connects to the server, the server transmits SSL certificate information to the client and the client communicates after verifying that this certificate is credible.

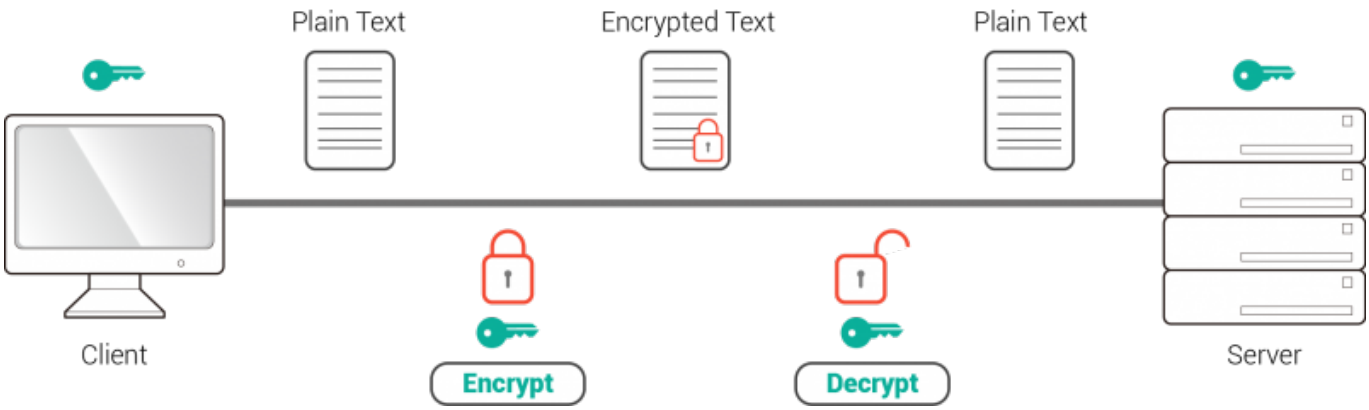
Hence there are no concerns of having private information such as login ID, password and etc. that are input on the web browser to be sniffed if SSL certificate is used. There are also benefits of identifying fraudulent sites and preventing data manipulations.

SSL Cryptography

There are several concepts that should be grasped to understand SSL. SSL uses two encryption methods: symmetric-key encryption and asymmetric-key. The password which is used by these two encryptions is called the key. The encrypted result changes based on this key and therefore it is not possible to decrypt if the key is unknown.

Symmetric-Key Encryption (Symmetric Key)

The symmetric key uses the same key to encrypt and decrypt. For example, if encryption was done through the key 1245, the key necessary for decryption would be 1245.



The size of symmetric keys are generally 128 or 256 bits and it is more difficult to crack passwords with larger keys. For example, the 128 bit key can have 2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456 different combinations of passwords and it would take thousands of years in order to crack a 128 bit key with brute-force attack.

Encryption Algorithms

- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)
- 3DES
- IDEA (International Data Encryption Algorithm)
- Blowfish
- Twofish
- Serpent
- CAST5
- RC4

Advantages

- Since one key is used, messages and files can be encrypted and decrypted alone by the key holder.
- This method is 100~1000 times faster than the public key encryption which uses two keys.
- Less resources are used because only one key is encrypted.

Disadvantages

- There needs to be a secure channel which will allow sending and receiving of the symmetric key.
- Since the sender and receiver uses the same key, the message received from a specific user cannot be verified. There is no method to check if the received message matches the original message if another user who has the same symmetric key changes the message in the middle. Hence, the user is vulnerable to hacks if the symmetric key is exposed.
- If there are many connecting users, a key distribution problem will occur and will consume

corresponding system resources.

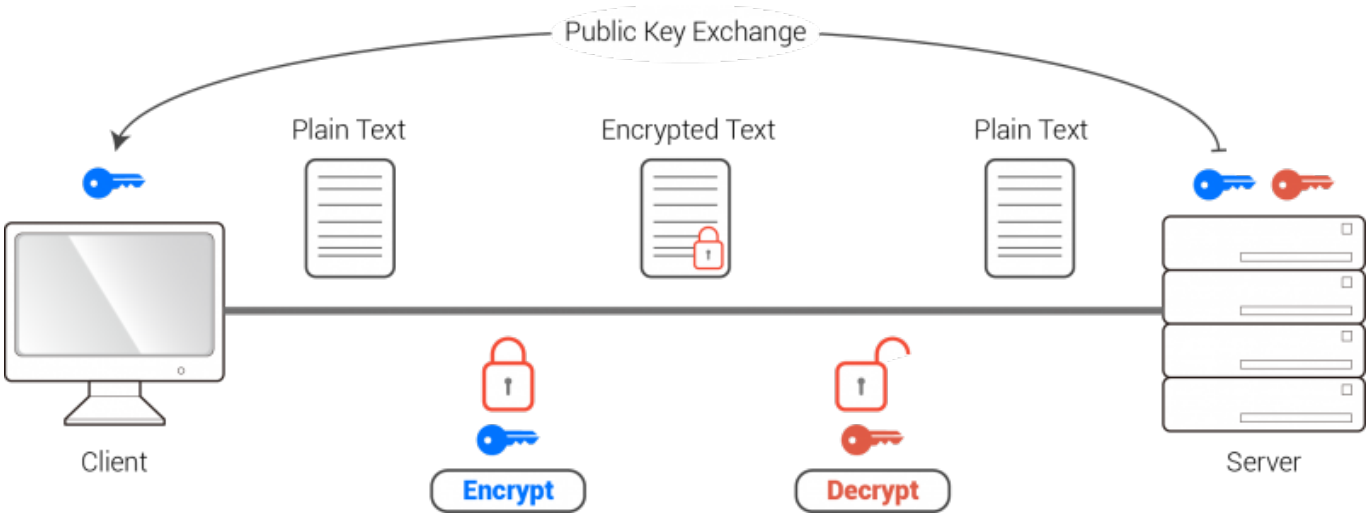
+ Brute-force Attack
This is an attack method that calculates every possible combination to crack a specific password. Most encryption methods are theoretically not safe from brute-force attacks. Encrypted information can be decrypted if enough time is available.

Asymmetric-Key Encryption (Public Key and Private Key)

Symmetric-key encryption is useless when the key is leaked since it uses a single key. To prevent this issue, the public key encryption was conceived.

The public key method uses two keys (public key and private key). If a file is encrypted through key A, it can be decrypted with key B and if it is encrypted with key B it can be decrypted with key A. These keys work as pairs. Therefore, since A-B key are pairs, it cannot be decrypted with key C.

Public key is distributed with encryption and the private key is the key held by the distributor of the public key. In a server and client example, the private key is held by the server and the encrypted public key is provided to the client. The client encrypts the data with the public key provided by the server and transmits the data. The server decrypts the encrypted data with the private key. Even if the public key is exposed during this process, a malicious hacker would not know the private key so the data cannot be decrypted.



In addition to encrypting and securing data, the public key method can also be used to verify the identity of the person distributing the data. This method includes the server encrypting its own data through the private key and decrypting the data through the public key. In this case, the encrypted data can be decrypted by anyone who has a public key but encrypting is only possible by the server. If decryption is possible through the public key, it means that the key is a pair with the private key of the server. This encryption through the private key is called digital certification and decryption by the

client is called signature verification. Therefore, the purpose of this method is not to protect data but to guarantee the identity of the person providing the data.

Encryption Algorithms

- RSA (Rivest-Shamir-Adleman cryptosystem)
- DSA (Digital Signature Algorithm)

Advantages

- A secure channel, which is necessary for a symmetric-key encryption, is not necessary since the public key is used.
- Users are safe from external attacks because encryption and decryption is done through two different keys.

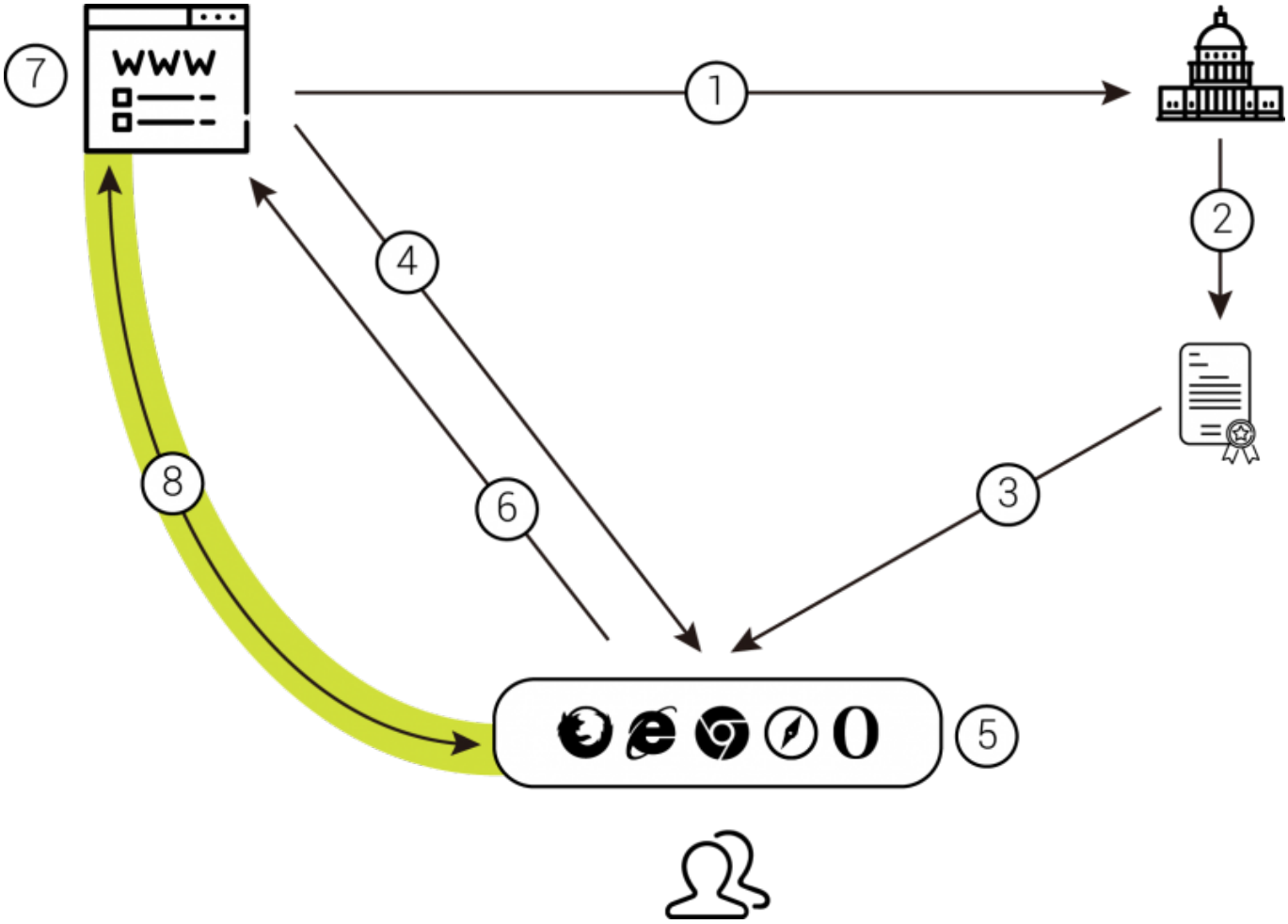
Disadvantages

- Asymmetric Encryption is around 100~1000 times slower than symmetric-key encryption.
- It requires more resources than symmetric-key encryption.

Combining Symmetric-Key and Asymmetric-Key Encryption

Symmetric-key encryption and asymmetric-key encryption both have their special advantages but also have problems of key transport and degraded performance. Consequently, a hybrid cryptosystem was developed to ameliorate these issues.

The communication method using SSL certification and a hybrid cryptosystem is a combination of symmetric encryption and asymmetric encryption.



Process

1. The website submits its own information and website's public key to the certification authority.
2. The certification authority verifies the website information and the website's public key and then encrypts them with the certification authority's private key. This is the SSL certification.
3. The certification authority provides its public key to the web browser.
4. When the user connects to the website with a web browser, the website sends its SSL certification to the web browser. This SSL certificate holds the website's information and the website's public key encrypted with the private key of the certification authority.
5. The web browser decrypts the SSL certification with the certification authority's public key and verifies the information.
6. The pre-shared key is encrypted with the website's public key which is included in the SSL certificate and is sent to the website.
7. The website decrypts the encrypted pre-shared key sent by the web browser with its own private key and obtains the pre-shared key. Hence the pre-shared key created by the web browser has been safely transmitted to the website.
8. The communication between the web browser and the website is executed securely by utilizing the pre-shared key.

* The pre-shared key is a key necessary for symmetric-key encryption and the communication between the web browser and the website is encrypted through symmetric-key encryption.

Conclusion

HTTPS provides robust security by utilizing the SSL certificate. BioStar 2 supports both HTTP and HTTPS and provides certifications to be used in HTTPS communication. This certification is not a certificate signed by an official Certification Authority.

You will be able to use BioStar 2 with enhanced security on HTTPS if you purchase SSL certificate signed by an officially authorized authority.

+ Certificate authority
You can learn more about the types of Certification Authorities at Wikipedia.
https://en.wikipedia.org/wiki/Certificate_authority