SSL/TLS SERTIFIKATLARI

Qurbonmurodov Diyorbek Ulug'bek o'g'li
Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti talabasi

Annotatsiya: Ushbu maqolada SSL/TLS protokollari va ularning xususiyatlari, ishlatilish holatlari haqida qisqacha to'xtalib o'tildi.

Kalit so'zlar: SSL/TLS, PKI, simmetrik kalit, assimmetrik kalit.

Hozirgi kunda internet tarmog'idan foydalanuvchilar SSL/TLS protokollari va sertifikatlari haqidagi tushunchalarga ko'p duch keladi. Keling shu haqida qisqacha nazariy ma'lumot berib o'tamiz.

SSL nima?

SSL - bu veb-sayt va foydalanuvchining veb-brauzeri o'rtasida yuborilgan ma'lumotlarni himoya qiluvchi xavfsizlik texnologiyasi.

Onlayn tranzaktsiyalar paytida xakerlar kredit karta raqamlari kabi nozik ma'lumotlarni o'g'irlashining oldini olish uchun mo'ljallangan , SSL ma'lumotlarni faqat mo'ljallangan oluvchi o'qiy olishiga ishonch hosil qilish uchun shifrlaydi. Bu jarayon kiberjinoyatchilarning ma'lumotni ushlashi va o'g'irlashini qiyinlashtiradi.

TLS nima?

TLS SSL bilan bir xil ishni bajaradi. Biroq, bu yangi texnologiya bo'lgani uchun u odatda kuchliroq shifrlashni, yaxshilangan xavfsizlikni va yaxshi ishlashni ta'minlaydi.

Sizning veb-saytingiz foydalanuvchilarga xavfsizligini ko'rsatish va ularning tranzaktsiyalari va tafsilotlari xavfsiz ekanligiga ishonch hosil qilish uchun SSL yoki TLS sertifikatini talab qiladi.

SSL/TLS sertifikati raqamli obyekt bo'lib, tizimlarga identifikatsiyani tekshirish va keyinchalik Secure Sockets Layer/Transport Layer Security (SSL/TLS) protokoli yordamida boshqa tizim bilan shifrlangan tarmoq ulanishini o'rnatish imkonini beradi. Sertifikatlar ochiq kalitlar infratuzilmasi (PKI) deb nomlanuvchi kriptografik tizimda qo'llaniladi. PKI bir tomonga boshqa tomonning identifikatorini sertifikatlar yordamida aniqlash imkoniyatini beradi (agar ikkala tomon ham sertifikat organi deb nomlanuvchi uchinchi shaxsga ishonsa). Shu tarzda, SSL/TLS sertifikatlari tarmoq ulanishlarini himoya qilish va Internetdagi veb-saytlar identifikatorini, shuningdek, shaxsiy tarmoqlardagi resurslarni aniqlash uchun raqamli identifikatsiya vazifasini bajaradi.

SSL/TLS sertifikatlari veb-sayt foydalanuvchilari orasida ishonchni mustahkamlaydi. Kompaniyalar SSL/TLS bilan himoyalangan veb-saytlarni yaratish uchun veb-serverlarga SSL/TLS sertifikatlarini o'rnatadilar.

SSL/TLS sertifikatlari identifikatorlarni autentifikatsiya qiladi va SSL/TLS orqali shifrlangan ulanishlarni faollashtiradi :

- Mijoz kirish sahifasi kabi himoyalangan manbaga kirishni so'raydi.

- Server o'zining SSL sertifikatini, shu jumladan ochiq kalitni yuborish orqali javob beradi.
- Mijoz sertifikatning haqiqiy va ishonchli ekanligini tekshiradi. Bu serverning haqiqiyligini ta'minlaydi.
- Mijoz simmetrik seans kalitini yaratadi va uni serverning ochiq kaliti bilan shifrlaydi. Bu seans kalitini serverga xavfsiz tarzda uzatadi. Server seans kalitini shaxsiy kaliti bilan parolini hal qiladi. Ikkala tomon ham barcha uzatilgan ma'lumotlarni shifrlash va shifrini ochish uchun simmetrik seans kalitidan foydalanadi.

SSL/TLS da ishlatiladigan shifrlash kalitlarining ikki turi mavjud:

Asimmetrik kalitlar - umumiy va shaxsiy kalit juftligi serverni aniqlash va shifrlangan seansni boshlash uchun ishlatiladi. Shaxsiy kalit faqat serverga ma'lum, ochiq kalit esa sertifikat orqali baham ko'riladi.

Simmetrik seans kalitlari - har bir ulanish uchun bir martalik kalitlar yaratiladi va uzatilgan ma'lumotlarni shifrlash/shifrini ochish uchun ishlatiladi. Simmetrik kalitlar assimetrik shifrlash yordamida xavfsiz almashinadi.

SSL/TLS bir nechta simmetrik shifrlarni va assimetrik ochiq kalit algoritmlarini qo'llab-quvvatlaydi. Masalan, 128 bitli kalitlarga ega AES umumiy simmetrik shifrdir, RSA va ECC esa odatda assimetrik algoritmlardan foydalanadi.

Xulosa

Shunday qilib SSL/TLS foydalanuvchilar o’rtasida xavfsiz ma’lumot almashinuvini ta’minlab beradi. Bunda simmetrik va assimmetrik kriptografik shifrlash algoritmlaridan foydalanadi.

Foydalanilgan adabiyotlar:

https://www.websitepulse.com/blog/ssl-vs-tls-difference-and-best-protection
https://www.ssl.com/article/what-is-ssl-tls-an-in-depth-guide/
https://aws.amazon.com/ru/what-is/ssl-certificate/