SSL protokolunun təhlükəsizliyinin hazırki vəziyyəti

Fərhad Rəhimli[1], İradə Rəhimova[2]

[1]*Azərbaycan Respublikası Rabitə və Yüksək Texnologiyalar Nazirliyi yanında*
Elektron Təhlükəsizlik Mərkəzi
[2]*Azərbaycan Dövlət Texniki Universiteti*
[1]farhad@cert.az, [2]ika1402@mail.ru

***Xülasə*— Kriptoqrafiya informasiya təhlükəsizliyinin ən mühüm vasitələrindən biridir. Lakin son illərdə kriptoqrafik sistemlərdə aşkar olunan çox sayda kritik boşluqlar təhlükəsiz kommunikasiyaların təhlükəsizliyini həqiqətən kölgə altına salır. 1990-cı illərdə yaradılmış SSL (Secured Socket Layer) və onu əvəz edən TLS (Transport Layer Security) kriptoqrafik protokolları bu gün İnternet şəbəkəsində təhlükəsiz ötürməni təmin edən ən əhəmiyyətli texnologiyalardandır. Bu məqalədə həmin protokollara qarşı məlum hücumlar və aşkar olunmuş boşluqlar təhlil edilir, SSL protokolunun etibarlılığı qiymətləndirilir.**

Açar sözlər*— *SSL, OpenSSL, RSA, Poodle, Freak, MITM, kriptoqrafik protokol, şifrələmə, deşifrələmə, CVE.

I. GİRİŞ

SSL-in zəif nöqtələrini və hücum vektorlarını başa düşmək üçün onun ümumi iş prinsipini qeyd edək (SSL-in işləmə prisipi haqqında ətraflı məlumat istinadlarda mövcuddur).

Veb bələdçi (kliyent) SSL-dən istifadə edən bir veb resursu (server) açmağa cəhd etdiyi zaman onlar arasında SSL təsdiqləmə (SSL Handshake) adlı proses əmələ gəlir. Bu prosesdə üç açar istifadə olunur: gizli açar, açıq açar və sessiyanın açarları. Məlumdur ki, assimetrik kriptoqrafiyanın şifrələmə və deşifrələmə prosesləri böyük hesablama resursları tələb edir. Buna görə də SSL-də açıq və gizli açarlar yalnız SSL-i təsdiqləmə vaxtı simmetrik sessiya açarını yaratmaq üçün istifadə olunur. SSL əlaqəsi təsdiqləndikdən sonra bütün məlumatlar simmetrik sessiya açarı ilə şifrələnir.

1. Kliyent server ilə əlaqə yaradır. Kliyent serverdən özünü təsdiqləməsini tələb edir.
2. Server kliyentə öz SSL sertifikatının və açıq açarlarının nüsxələrini (surətlərini) göndərir.
3. Kliyent sertifikatın etibarlılığını, istismar vaxtını, həqiqiliyini və veb istinadın ünvanını yoxlayır. Kliyent sertifikatı tanıdığı halda, serverin açıq açarından istifadə edərək simmetrik sessiya açarını yaradır, şifrələyir və serverə göndərir.
4. Server təhlükəsiz sessiya yaratmaq üçün gizli açardan istifadə edərək simmetrik sessiya açarını deşifrələyir və həmin sessiya açarı ilə təsdiq bayrağını (acknowledgement) şifrələyərək kliyentə göndərir.
5. Server və kliyent bütün məlumat mübadiləsini sessiya açarı ilə həyata keçirir.

Ümumiyyətlə, SSL-də aşağıdakı alqoritmlər istifadə olunur:

- Açarların mübadiləsi və onların həqiqiliyinin təsdiqlənməsi üçün − ECDH, SRP, PSK, RSA, Diffie-Hellman;
- Autentifikasiya üçün − DSA, ECDSA, RSA;
- Simmetrik şifrələmə üçün − Triple DES, AES, Camellia, İDEA, DES, RC2, RC4;
- Heş funksiyalar üçün −MD2, MD4, MD5, SHA1.

Bu alqoritmlərdən birində mövcud olan hər hansı bir boşluq və ya onların düzgün olmayan tətbiqi SSL-in bütün təhlükəsizliyinə ciddi təsir edə bilər.

II. MÖVCUD BOŞLUQLAR VƏ ONLARIN TƏSİR DAİRƏSİ

POODLE (Padding Oracle On Downgraded Legacy Encryption) və ya CVE-2014-3566. CBC-rejim (şifrə-mətn bloklarının qoşulma rejimi) − əks əlaqə mexanizmi ilə işləyən simmetrik bloklama şifrələməsinin rejimlərindən biridir. Belə ki, şifrələmə zamanı açıq mətn bloku bloklama alqoritmindən keçir və əvvəlki bloka əsasən dəyişilir. Sadə dildə desək, blokun ölçüsü 8 baytdırsa, onda açıq mətnə 1-8 bayt mətn əlavə olunur ki, həmin bloka sıxışdırıla bilsin. Həmçinin, cari addımda *N* bayt əlavə olunursa, bu baytların sonuncusunun dəyəri *N*-1-ə bərabər olacaq. Bu halda deşifrələmə mümkün olacaq.

Misal üçün bizim şifrə 3DES-CBS rejimində deşifrə olunur. Onda axırıncı baytın dəyərləri yoxlanılır. Onlar mütləq 0-7 bayta bərabər olmalıdır. Bu isə bizə digər blokların son baytları barədə məlumat verə bilər. Bu baytların dəyişdirilməsinin MAC (Message Authentication Code) tərəfindən yoxlanılmaması − bədniyyətliyə kifayət qədər məlumatı deşifrə etməyə imkanı verir.

Hücumu həyata keçirtmək üçün klassik MITM (Man in the middle) sxemi yetərlidir. Saxta WiFi şəbəkəsi yaradaraq, bədniyyətli şəxs istifadəçinin açmaq istədiyi "https" saytı üçün veb bələdçi tərəfindən hazırlanmış cookie faylları JavaScript vasitəsi ilə əldə edə bilər. Deməli, bədniyyətli cookie-nin son baytının 0-7 kimi bütün dəyərlərini sadalayaraq serverə göndərir və onun reaksiyasına görə düzgün baytı müəyyən edə bilir. Bir baytı tapdıqdan sonra bədniyyətli eyni addımları təkrarlıyır. 256 sorğu ərzində 1 bayt məlumat deşifrə etmək mümkün olur.

SSL 3.0 versiyasında tapılan bu boşluq bütün SSLv3 versiyalarına şamil olunur. Bu boşluq protokolun strukturu ilə bağlıdır və heç bir proqram təminatının tətbiqi vasitəsi ilə bağlanıla bilməz. Belə kritik nasazlıqlardan sonra SSL protokulunun istifadəsi, ümumiyyətlə, tövsiyə olunmur.

POODLE boşluğu aşkar olduqdan dərhal sonra dünya üzrə SSLv3 istifadəsi 90%-dən 60%-dək qədər azalıb (2014), cari ildə (2015) isə bu göstərici 45%-dək enib. Eletkron Təhlükəsizlik Mərkəzinin araşdırmaları nəticəsində məlum olmuşdur ki, ölkədə mövcud olan internet resurslarının 18%-ində POODLE boşluğu var.

FREAK və ya CVE-2015-0204. 1990-cı illərdə ABŞ-ın qanunvericiliyinə müvafiq olaraq kriptoqrafik sistemlərin xarici ölkələrə ixracına qadağa və ya məhdudiyyət qoyulub. Bunun səbəbi Milli Təhlükəszilik Agentliyinin (National Security Agency − NSA) o dövr üçün güclü sayılan hesablama vasitələrindən istifadə edərək xarici ölkələrə ixrac olunan kriptoqrafik sistemlərin qırılmasının mümkünlüyüdür. Həmin dövrdə RSA 512 bit uzunluğu olan açarları yalnız MTA-ə (NSA) məxsus superkompüterlər vasitəsi ilə sadayalaraq qırmaq mümkün idi. Belə ki, şirkətlər bu qanuna uyğun olmaq üçün xaricə ixrac edilən bütün RSA açarları və ya digər kriptoqrafik alqoritmləri "zəif" parametrlərə tənzimləyibilər. Buna görə də SSL-in müəllifləri Cipher Suit (Şifrələrin uyğun olması) mexanizmini tətbiq ediblər. SSL-in təsdiqləməsi zamanı Cipher Suit mexanizmi server tərəfindən istifadə edilən kriptoqrafiya metodunun kliyentin istifadə etdiyi kriptoqrafiya metoduna uyğun olub-olmamasını yoxlayaraq müvafiq kriptoloji alqoritmləri seçmək imkanını verir. Susma rejimində bu mexanizm ən güclü kriptoqrafiya metodunu seçməlidir.

20 ildən sonra OpenSSL kitabxanasının dəfələrlə yenilənməsi və susma rejimində "zəif" açarların söndürülmüş vəziyyətdə olmasına baxmayaraq, bədniyyətli həm kliyenti, həm də serveri "zəif" kriptoqrafik parametrlərdən (export cipher suits) istifadə etməyə məcbur edə bilər.

Bu boşluq həm server, həm də kliyent tərəflərinə təsir edir. Ənənəvi olaraq MITM (Man in the Middle) hücum sxemi ilə bu boşluğu istismar edək.

1. Kliyent serverə standart RSA cipher suite baradə sorğu göndərir;
2. Bədniyyətli sorğunu dəyişdirir və serverə RSA-i ixrac etmək sorğusunu göndərir;
3. Server uzun müddətli açarla imzalanmış 512 bit uzunluğu olan RSA açarı ilə cavab verir;
4. Kliyent zəif açarı qəbul edir;
5. Bədniyyətli zəif açarın modulunu vuruqlara ayıraraq gizli (deşifrələmə) açarı əldə edir;
6. Artıq bədniyyətli üçün bütün kommunikasiyalar açıq mətn şəklində göndərilir.

Bəllidir ki, RSA 512 bit uzunluğu olan açarları bu gün bulud texnologiyalarından istifadə edərək 12 saat ərzində yoxlayıb qırmaq mümkündür. FREAK yüz minlərlə populyar veb resurslarda aşkar olunub, Azərbaycanda isə bu rəqəm mövcud olan veb resursların 0.13%-ni təşkil edir.

Çoxfunksionallıq, daşınanlıq və asanlıq kimi xassələrin əvvəlcədən SSL-in təməlinə qoyulmasına baxmayaraq, onun istifadəsi bu gün tamamilə təhlükəli hesab olunur və onu istifadə edən tərəflər qısa vaxt ərzində TLS protokoluna keçməlidir və ya ən azı SSL-in parametrləri ən təhlükəsiz şəkildə tənzimlənməlidir.

Qeyd edək ki, Google gələcəkdə şifrələnmiş trafik mübadiləsinin həcminin artacağını nəzərə alaraq, artıq SPDY adlı öz təhlükəsizlik protokolunu yaradıb, sınaqdan keçirir və yaxın zamanlarda SSL-in yeni alternativlərinin istifadəsini müşahidə edəcəyik.

ƏDƏBİYYAT

[1] https://en.wikipedia.org/wiki/Padding_(cryptography)
[2] https://en.wikipedia.org/wiki/Padding_oracle_attack
[3] https://www.openssl.org/~bodo/ssl-poodle.pdf
[4] https://www.trustworthyinternet.org/ssl-pulse/
[5] https://zmap.io/sslv3/#affected
[6] https://en.wikipedia.org/wiki/FREAK
[7] http://resources.infosecinstitute.com/ssl-attacks/
[8] https://freakattack.com/
[9] https://www.smacktls.com/#freak
[10] http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html
[11] https://eprint.iacr.org/2013/049.pdf
[12] https://en.wikipedia.org/wiki/SPDY