DOI:10.30546/gdu.2.2024

İNFORMASİYA TƏHLÜKƏSİZLİYİNDƏ OSI MODELİ

Quliyev Anar Rəsul oğlu
Gəncə Dövlət Universiteti
anar.quliyev.1972@mail.ru

Xülasə. Bu məqalə informasiya təhlükəsizliyində OSI modelinin nəzərdən keçirilməsinə həsr edilmişdir. Bu modeldən istifadə etməklə müxtəlif şəbəkə cihazları bir-biri ilə əlaqə saxlaya bilir. Model, sistemlər arasında qarşılıqlı əlaqənin müxtəlif səviyyələrini müəyyən edir. Belə qarşılıqlı əlaqə zamanı hər bir səviyyə müəyyən funksiyaları yerinə yetirir. Məqalədə OSI modelinin nümunəsindən istifadə edərək informasiya təhlükəsizliyinə baxılır.

Açar sözlər: informasiya, informasiya təhlükəsizliyi, internet, OSİ modeli.

Ключевые слова: информация, информационная безопасность, Интернет, модель OSİ.

Keywords: information, information security, internet, OSI model.

Hər gün internetə daxil olub oradan müəyyən məlumatlar alırıq. Eyni zamanda İnternetdən istifadə edən bütün insanlar böyük miqdarda məlumat yaradırlar. Bir çox şirkətlər öz işlərini qurmaq üçün bu məlumatı toplayır və təhlil edirlər. Hər hansı digər məlumat kimi, bu məlumat da ondan öz məqsədləri üçün istifadə etmək istəyən təcavüzkarlardan qorunmalıdır. Əksər hallarda, onlar istifadəçilər haqqında şəxsi məlumatlara ehtiyac duyurlar, məsələn: bank kartı nömrələri, şəxsi profil parolları, təsdiq kodları və s. İnformasiya təhlükəsizliyi bu cür məlumatların qorunmasına cavabdehdir.

Əvvəlcə "İnformasiya Təhlükəsizliyi" terminina aydınlıq gətirək.

İnformasiya təhlükəsizliyi məlumatın icazəsiz girişinin, hər hansı təhrif və ya dəyişdirilməsinin, yenidən yazılmasının və ya məhv edilməsinin qarşısının alınması məqsədi daşıyr. Bu termin təkcə İT sənayesinə deyil, fiziki məlumatlara da aiddir.

Açıq sistemlərin qarşılıqlı əlaqə modeli (OSI) Beynəlxalq Standartlaşdırma Təşkilatı (İSO) tərəfindən yaradılmış konseptual modeldir və müxtəlif kommunikasiya sistemlərinin standart protokollardan istifadə edərək əlaqə saxlamasına imkan verir . OSI Modeli kommunikasiya sistemini yeddi mücərrəd təbəqəyə bölmək konsepsiyasına əsaslanır. OSI Modelinin hər bir təbəqəsi müəyyən bir işi yerinə yetirir və özündən yuxarı və aşağıda olan 7 təbəqə ilə əlaqə qurur.

Gəlin bu sistemi sıfır səviyyəsindən nəzərdən keçirməyə başlayaq. OSI modelinin özü bu səviyyəni vurğulamır, lakin informasiya təhlükəsizliyi haqqında danışarkən onu qeyd etmək lazımdır.

Dizayn səviyyəsi. İnformasiya təhlükəsizliyi ilə bağlı ən əsas və əsas anlayışlar nəzəri model şəklində təqdim edilir. Məsələn, server avadanlığının quraşdırılması planını tərtib edərkən: elektronikanın harada və necə yerləşdirilməsi, yanğından mühafizə vasitələrinin düzgün yerləşdirilməsi və s.Hal-hazırda, məlumatların sistemli surətinin çıxarılması sistemi dizayn edilməmişdirsə, o zaman məlumatların tam bərpası üçün sadəcə heç bir imkan yoxdur. Belə problemlərin qarşısını almaq üçün bu vəzifəni ayrıca bir şəxs- Təhlükəsizlik Memarı həyata keçirir.

1. Fiziki səviyyə. Bu səviyyədə məlumatın fiziki mühafizəsi işlənir. Bütün bunlar informasiyanın fiziki qorunmasıdır.

2.Kanal səviyyəsi - bu mərhələdə verilənlər bloklarından (bundan sonra çərçivələr) istifadə etməklə lokal şəbəkədə məlumatların ötürülməsi üsulları müəyyən edilir. Bu çərçivələr şəbəkə miqyası səviyyəsi ilə kəsişmir, çünki onlar yalnız lokal şəbəkə sahəsində işləyirlər.

DOI:10.30546/gdu.2.2024

Yükü paylamaq üçün kanal və şəbəkə təbəqələrinin ayrılması lazımdır. Nəticədə, keçid səviyyəsinin protokolları yalnız yerli çatdırılma və ünvanlamaya diqqət yetirə bilər. Məlumat bağlantısı səviyyəsini 2 alt səviyyəyə bölmək olar:

1. məntiqi keçid nəzarəti (LLC) səviyyəsi.
2. media giriş səviyyəsi (MAC),

MAC təbəqəsinin əsas vəzifəsi mühitin özünə daxil olmaq prosedurudur.

Bu kanal təbəqəsi ümumiyyətlə niyə lazımdır?

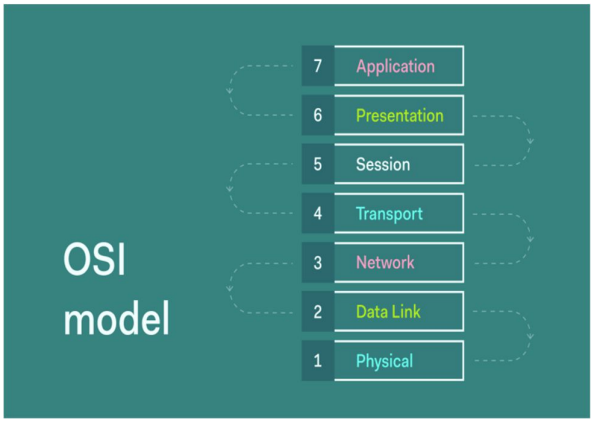
Bütün qurğular eyni anda ətraf mühitdən istifadə etməyə çalışdıqda, çərçivələrin üst-üstə düşməsində uyğunsuzluq (toqquşma) baş verir, nəticədə bu cihazlar sinxronizasiya edə bilmir. Link lay protokolları isə bu cür halları aşkar edir və ətraf mühiti toqquşmaların azaldılması və ya tamamilə qarşısının alınması üçün mexanizmlərlə təmin edir. Bundan əlavə, bu səviyyədə diqqət etməli olduğunuz əsas vəzifə rollar sisteminə uyğun işləyən ətraf mühitə çıxış sistemidir. Hər bir istifadəçiyə müəyyən icazələr və məhdudiyyətlər daxil olan xüsusi bir rol verilir.

3. Şəbəkə səviyyəsi – bu mərhələdə bir-birindən uzaqda olan serverlər arasında verilənlərin ötürülməsi yolunu müəyyən etmək üçün şəbəkə səviyyəsinin protokolları lazımdır.

Nəzərdən keçirilən OSI modelinin şəbəkə səviyyəsində təhlükəsiz virtual kanallar formalaşdırarkən şəffaflıq və qorunma keyfiyyəti arasında optimal balans əldə edilir. Şəbəkə qatında təhlükəsizlik tədbirlərinin yerləşdirilməsi onları proqramlar üçün görünməz edir, çünki şəbəkə səviyyəsi ilə tətbiq arasında nəqliyyat səviyyəsi protokolu həyata keçirilir. İstifadəçilər üçün təhlükəsizlik prosedurları İnternet protokolunun özü kimi şəffafdır. Şəbəkə səviyyəsində trafikin qorunması və açarların idarə edilməsi funksiyalarını kifayət qədər tam şəkildə həyata keçirmək mümkündür, çünki mesaj paketləri məhz şəbəkə səviyyəsində yönləndirilir.

Şəbəkə qatını qorumaq üçün mübadilə iştirakçılarının autentifikasiyası, tunel trafiki və IP paketlərinin şifrələnməsi üçün istifadə olunan IPSec (Internet Protocol Security) protokol yığını istifadə olunur. IPSec protokolunun əsas məqsədi IP şəbəkələri üzərindən təhlükəsiz məlumat ötürülməsini təmin etməkdir. IPSec arxitekturası IPv4 protokolu ilə uyğun olduğundan (İnternet protokolunun 4-cü versiyası, bunun sayəsində bütün müasir İnternet işləyir), əlaqənin hər iki ucunda onun dəstəyini təmin etmək kifayətdir; aralıq şəbəkə qovşaqları IPSec haqqında ümumiyyətlə heç nə "bilməyə" bilər. IPSec həm bu gün İnternetdə istifadə olunan hazırkı IPv4 versiyasından, həm də tədricən İnternetə təqdim olunan IPv6-nın yeni versiyasından trafiki qoruya bilər.2

4. Nəqliyyat səviyyəsi tətbiq məlumatı ilə qarşılaşan birinci təbəqədir və onu ötürməyə hazırlamaq proseduruna başlayırsa, əgər şəbəkə səviyyəsi verilənlərin hansı yolla göndəriləcəyini müəyyən edirsə, o zaman nəqliyyat səviyyəsi onu hazırlayır və göndərir.



Nəqliyyat səviyyəsində adətən iki protokol var: TCP və UDP.

TCP (Transmission Control Protocol) - bu protokolun əsas vəzifəsi tətbiq səviyyəsindən gələn məlumatları seqmentləşdirmək və portlardan istifadə edərək tətbiqləri ünvanlamaqdır. TCP həmçinin təmin edir:

1. Seqmentlərin etibarlı çatdırılması.
2. Qəbul zamanı seqmentlərin sifarişi.
3. Seanslarla işləmək.

DOI:10.30546/gdu.2.2024

4. Ötürmə sürətinə nəzarət.

UDP – (User datagram protocol) – bu protokolun əsas vəzifəsi TCP-yə bənzəyir, lakin əlavə olaraq:

1. Tətbiq səviyyəsindən alınan məlumatları seqmentləşdirir.
2. Portlardan istifadə edərək işləyən proqramları ünvanlayır.

Nəqliyyat qatını qorumaq üçün əsas protokollar: TLS (nəqliyyat qatının təhlükəsizliyi), sələfi SSL kimi (təhlükəsiz yuvalar təbəqəsi) İnternetdəki qovşaqlar arasında təhlükəsiz məlumat ötürülməsini təmin edən kriptoqrafik protokollardır. TLS və SSL istifadəsi:

1. Doğrulama üçün asimmetrik şifrələmə.
2. Məxfilik üçün simmetrik şifrələmə
3. Mesajın bütövlüyünü qorumaq üçün mesajın identifikasiyası kodları.

Bu protokol veb brauzerlər, e-poçt, ani mesajlaşma və İP telefoniya kimi İnternet proqramlarında geniş istifadə olunur.

5. Seans səviyyəsi - bu səviyyə nisbətən nadir hallarda istifadə olunur, bir çox protokollar öz funksionallığını öz nəqliyyat qatlarında həyata keçirir;

Seans səviyyəsinin əsas funksiyası sessiyanı təşkil etmək, yəni iki kompüter sistemi arasında əlaqə zamanı idarəetmənin ötürülməsidir. Seans məlumatların ötürülməsi istiqamətini müəyyən edir (bu, birtərəfli və ya ikitərəfli ola bilər), həmçinin bir sorğunun növbəti sorğunun qəbul edilməsindən əvvəl tamamlanmasını təmin edir.

Seans qatı həmçinin aşağıdakı əlavələrdən bəzilərini dəstəkləyə bilər:

- dialoqun idarə edilməsi.
- markerin idarə edilməsi.
- əməliyyatların idarə edilməsi.

Bəzi protokolların işləməsi üçün istənilən vaxt yalnız bir tərəfin kritik əməliyyatlara cəhd edə bilməsi vacibdir. Hər iki tərəfin eyni vaxtda eyni əməliyyatı yerinə yetirmək cəhdinin qarşısını almaq üçün tokenlərdən istifadəyə əsaslanan xüsusi nəzarət mexanizmi həyata keçirilir. Bu halda, əməliyyatı yerinə yetirmək üçün yalnız hazırda tokeni tutan tərəfə icazə verilir. Tokenin hansı tərəfdə olduğunu və onun iki tərəf arasında necə ötürüldüyünü təyin etmək token idarəetmə adlanır.

Məlumatların ötürülməsi və ötürülən məlumatın etibarlılığını təmin etmək üçün məlumat axınına nəzarət nöqtələri daxil edilir. Bu halda, nasazlıq baş verərsə, seans səviyyəsi əvvəlki yoxlama məntəqəsindən məlumatların yönləndirilməsinə davam edə bilər. Bu nəzarət nöqtələri sinxronizasiya nöqtələri adlanır. Sinxronizasiya nöqtələrinin idarə edilməsi əməliyyatların idarə edilməsi adlanır.

Sessiya qatı vəziyyətində, müəyyən məlumatların ötürülməsi üçün təhlükəsiz rabitə kanalının yaradılmasına diqqət yetirməliyik. Bu vəziyyətdə SSL protokolundan istifadə olunur. SSL (Secure Sockets Layer) protokolu OSI modelinin seans səviyyəsində işləyən və TLS ilə əvəz olunana qədər nəqliyyat qatında müəyyən bir nöqtədə işləyən təhlükəsiz kanal protokolu kimi istifadə olunur. Bu protokoldan istifadə edir

İnformasiya mübadiləsinin təhlükəsizliyini təmin etmək üçün informasiyanın mühafizəsinin kriptoqrafik üsulları. SSL protokolu iki şəbəkə abunəçisi arasında təhlükəsiz kanal yaratmaq, o cümlədən onların qarşılıqlı autentifikasiyası, ötürülən məlumatların məxfiliyini, bütövlüyünü və həqiqiliyini təmin etmək üçün bütün funksiyaları yerinə yetirir. Konfidensiallıq simmetrik seans açarlarından istifadə etməklə ötürülən mesajların şifrələnməsi yolu ilə təmin edilir ki, onlar əlaqə qurarkən tərəflər mübadiləsi aparırlar. Seans açarları da şifrələnmiş formada ötürülür və onlar abunəçi sertifikatlarından çıxarılan açıq açarlar vasitəsilə şifrələnir. Mesajları qorumaq üçün simmetrik açarların istifadəsi simmetrik açara əsaslanan

DOI:10.30546/gdu.2.2024

şifrələmə və deşifrə proseslərinin sürətinin asimmetrik açarlardan istifadə ilə müqayisədə əhəmiyyətli dərəcədə yüksək olması ilə əlaqədardır. Dövriyyədə olan məlumatların həqiqiliyi və bütövlüyü elektron rəqəmsal imzanın formalaşdırılması və yoxlanılması yolu ilə təmin edilir. SSL protokoluna əsasən, virtual şəbəkənin son nöqtələri arasında kripto-təhlükəsiz tunellər yaradılır. Hər bir təhlükəsiz tunelin təşəbbüskarları tunelin son nöqtələrindəki kompüterlərdə işləyən müştəri və serverdir.

OSI modelinin daha iki təbəqəsi də (nümayiş və tətbiq) var, lakin onlar təhlükəyə daha az həssasdırlar, çünki onlar yalnız istifadəçiyə şəbəkə ilə əlaqə saxlamağa imkan verir.

Beləliklə, yekunda demək istərdim ki, bizim dövrümüzdə informasiyanı qorumaq üçün təhlükəsiz informasiya mühitinin yaradılması üçün səriştəli çoxsəviyyəli mühafizə və məhdudiyyətlər sistemi qurmaq lazımdır.

Bu işdə nümunə olaraq OSI modelindən istifadə etməklə informasiya təhlükəsizliyini araşdırdıq. Biz OSI modelinin müxtəlif səviyyələrində məlumat mübadiləsi, toplanması, redaktə edilməsi və yaradılması üçün təhlükəsiz mühitin layihələndirilməsində nümunələri, müxtəlif şəbəkə protokollarının necə işlədiyi və onların şəbəkə strukturuna təsirini təhlil etdik.

Məlumatların mühafizəsi sahəsi sənaye cəmiyyətindən informasiya cəmiyyətinə keçidlə əlaqədar olaraq dövrümüzdə ən perspektivli sahədir. Qlobal rəqəmsallaşmanı həyatımızın bütün sahələrində müşahidə edə bilərik. Ümumdünya şəbəkəsində çoxlu məlumat toplanır və bu məlumatların qorunması indi daha çox tələb olunur.

Ədəbiyyat

1. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. Питер, 2012. – 960 с.
2. Кручинин С.В. Стеки сетевых технологий TCP/IP и OSI/ISO // Вопросы науки [Современные технологии и технический прогресс. Сборник статей по материалам Международной научно-практической конференции 16 апреля 2015 г. Воронеж], 2015, Т.3. с.145-147
3. Кручинин С.В., Лазарев В.В. Программа настройки ПО СТ //Свидетельство о регистрации программы для ЭВМ № 2011618880, 15.11.2011. Москва. Федеральная служба по интеллектуальной собственности, патентам и товарным знакам.
4. http://www.protocols.ru/files/RFC/rfc3286.pdf

МОДЕЛЬ OSI В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Кулиев Анар Расул оглы

Резюме

Данная статья посвящена обзору модели OSI в информационной безопасности. Используя эту модель, различные сетевые устройства могут взаимодействовать друг с другом. Модель определяет различные уровни взаимодействия между системами. При таком взаимодействии каждый уровень выполняет определенные функции. В статье рассматривается информационная безопасность на примере модели OSI.

DOI:10.30546/gdu.2.2024

OSI MODEL IN INFORMATION SECURITY

Guliyev Anar Rasul oglu

Summary

This article is dedicated to reviewing the OSI model in information security. Using this model, different network devices can communicate with each other. The model defines different levels of interaction between systems. During such interaction, each level performs certain functions. The article examines information security using the example of the OSI model.

Rəyçi: dos. G.Verdiyeva
İnformatika və cəbr kafedrasının 31may 2024-cü il tarixli 13 saylı protokolu.
Daxil olma tarixi 05 iyun 2024-cü il