**“AZƏRBAYCAN HAVA YOLLARI”**

**QAPALI SƏHMDAR CƏMİYYƏTİ**

**MİLLİ AVİASİYA AKADEMİYASİ**

**Sərbəst iş №2**

**Fakültə:** “Aerokosmik”

**İxtisas:** “İnformasiya Texnologiyaları”

**Fənn:** “Veb sistemləri və texnologiyaları”

**Mövzu:**  “Məlumatların şifrələnmə metodları”

**Qrup: “**2441a”

**Tələbə: “**Ələkbərov Emil**”**

**Müəllim: “**Heydərzadə Nübar Azad**”**

**BAKI 2024**

Məlumatların şifrələnməsi, onların güvənli bir şəkildə paylanması, saxlanması və göndərilməsi üçün əhəmiyyətli bir prosesdir. İşlənmiş məlumatlar istifadəçilər tərəfindən yalnız məqsədə uyğun şəxslərə açılmalıdır. İşte, məlumatların şifrələnməsində yaygın olaraq istifadə olunan bir neçə metod:

**1. Simmetrik Şifrələmə:** Bu metodda, eyni şifrə açarı (key) məlumatın şifrələnməsi və deşifrə edilməsi üçün istifadə olunur. Məsələn, DES (Data Encryption Standard), AES (Advanced Encryption Standard) və RC4 kimi protokollar simmetrik şifrələmə üsulları təmin edir.

**2. Asimmetrik Şifrələmə:** Bu metodda, iki ayrı şifrə açarı istifadə olunur: açıq açar (public key) və gizli açar (private key). Məlumat açıq açarla şifrələnərək göndərilir və yalnız qarşı tərəfin gizli açarı ilə deşifrə edilə bilər. RSA (Rivest-Shamir-Adleman) və Elliptic Curve Cryptography (ECC) kimi protokollar asimmetrik şifrələmə üsullarına nümunədir.

**3. Hash Funksiyaları:** Hash funksiyaları, məlumatları bir bütün kimi götürüb, onlardan istifadə edilən alqoritmaya əsasən bəlli uzunluqda bir ifadə (hash) yaradır. Bu, məlumatların bəzi qarşılıqlarını verir və buna görə də şifrələnmənin təhlükəsizliyini artırır. MD5, SHA-1 və SHA-256 kimi hash funksiyaları yayğın istifadə olunur.

**4. Salqın (Block Cipher) Şifrələmə:** Bu şifrələmə metodu, məlumatı bəlli böyüklikdə olan bloklara bölməklə və sonra hər bir bloku ayrı-ayrı işləməklə işləyir. DES və AES, salqın şifrələmə üsullarına nümunədir.

**5. Hibrid Şifrələmə:** Hibrid şifrələmə, simmetrik və asimmetrik şifrələmə metodu kombinasiyasıdır. Tipik olaraq, əsas məlumat simmetrik şifrələnir və sonra açıq açarla şifrə açarı şifrələnərək göndərilir. Alıcı, açıq açarı istifadə edərək simmetrik şifrə açarını açar və məlumatı deşifrə edə bilər.

**6. Quantum Şifrələmə:** Quantum şifrələmə, kvant mexanikası prinsiplərindən istifadə edir və şifrələməyə kömək edən qabiliyyətləri təmin edir. Bu metod, məlumatın qeyri-müəyyənlik prinsiplərinə əsaslanan qarışıqlıqla şifrələnməsindən istifadə edir.

Bu, əsas şifrələmə metodlarının bir siyahısıdır. Təhlükəsizlik məqsədi ilə, ən uyğun şifrələmə metodunun seçilməsi məlumatın cürünə və hansı növ təhlükəsizlik təhdidinin mövcud olduğuna görə dəyişə bilər.

Məlumatların şifrələnməsi ümumi və effektiv təhlükəsizlik üsuludur - təşkilatın məlumatlarını qorumaq üçün düzgün seçimdir. Bununla belə, bir neçə fərqli şifrələmə metodu mövcuddur, buna görə necə seçirsiniz?

Kibercinayətlərin artdığı bir dünyada şəbəkə təhlükəsizliyini qorumaq üçün bir çox metodun mövcud olduğunu bilmək təsəllivericidir. Əsl problem internet təhlükəsizliyi üzrə mütəxəssisin öz təşkilatının xüsusi vəziyyətinə ən uyğun olan hansı üsullardan istifadə etməli olduğuna qərar verməkdir.

**Data Şifrələmə nədir?**

Verilənlərin şifrələnməsi məlumatların şifrələnməsi yolu ilə mühafizə üsuludur ki, onlar yalnız düzgün şifrələmə açarına malik olan şəxs tərəfindən deşifrə edilə və ya ona daxil ola bilsinlər. Şəxs və ya qurum şifrələnmiş məlumatlara icazəsiz daxil olduqda, o, şifrələnmiş və ya oxunmaz görünür.

Məlumatların şifrələnməsi verilənlərin oxuna bilən formatdan şifrələnmiş məlumat parçasına çevrilməsi prosesidir. Bu, tranzit zamanı məxfi məlumatları maraqlandıran gözlərin oxumasının qarşısını almaq üçün edilir. Şifrələmə sənədlərə, fayllara, mesajlara və ya şəbəkə üzərindən hər hansı digər ünsiyyət formasına tətbiq oluna bilər.

Məlumatlarımızın bütövlüyünü qorumaq üçün şifrələmə vacib bir vasitədir və onun dəyərini şişirtmək mümkün deyil. İnternetdə gördüyümüz demək olar ki, hər şey, istər veb-saytlar, istərsə də proqramlar kimi şifrələmə səviyyəsindən keçib.

Kaspersky-də qeyd olunan antivirus və son nöqtə təhlükəsizliyi mütəxəssisləri şifrələməni “...məlumatların oxuna bilən formatdan yalnız şifrəsi açıldıqdan sonra oxuna və ya emal edilə bilən kodlaşdırılmış formata çevrilməsi” kimi müəyyən edir.

Onlar daha sonra deyirlər ki, şifrələmə məlumat təhlükəsizliyinin əsas bloku hesab olunur, iri təşkilatlar, kiçik müəssisələr və fərdi istehlakçılar tərəfindən geniş istifadə olunur. Bu, son nöqtələrdən serverlərə keçən məlumatları qorumaq üçün ən sadə və vacib vasitədir.

Bu gün kibercinayətkarlıq riskinin artdığını nəzərə alsaq, internetdən istifadə edən hər bir şəxs və qrup, ən azı, əsas şifrələmə üsulları ilə tanış olmalı və onları özündə birləşdirməlidir.

Məlumatların idarə edilməsində üstün olmaq istəyirsiniz? Simplilearn-ın məlumatların idarə edilməsi kursları müvəffəqiyyət üçün ekspert fikirləri və praktiki biliklər təklif edir.

Kibertəhlükəsizlik təhsili sahəsində hərtərəfli kibertəhlükəsizlik bootcamp məlumat şifrələməsinin incəliklərinə dalmaq imkanı təqdim edir. İştirakçılar simmetrik və asimmetrik şifrələmə kimi müxtəlif şifrələmə üsulları və onların həssas məlumatların qorunmasında əhəmiyyəti haqqında anlayışlar əldə edirlər.

**Məlumatların Şifrələnməsi Necə İşləyir?**

Şifrələnməsi lazım olan məlumatlar açıq mətn və ya aydın mətn adlanır. Açıq mətni bəzi şifrələmə alqoritmləri vasitəsilə ötürmək lazımdır ki, bunlar əsasən xam məlumat üzərində aparılacaq riyazi hesablamalardır. Çoxlu şifrələmə alqoritmləri var, onların hər biri tətbiqi və təhlükəsizlik indeksi ilə fərqlənir.

Alqoritmlərdən başqa, bir şifrələmə açarı da lazımdır. Sözügedən açardan və uyğun bir şifrələmə alqoritmindən istifadə edərək, açıq mətn şifrəli mətn kimi də tanınan şifrələnmiş məlumat parçasına çevrilir. Açıq mətni qəbulediciyə göndərmək əvəzinə, şifrəli mətn etibarlı olmayan rabitə kanalları vasitəsilə göndərilir.

Şifrə mətni nəzərdə tutulan qəbulediciyə çatdıqdan sonra o, şifrəli mətni orijinal oxuna bilən formatına, yəni açıq mətnə çevirmək üçün deşifrə açarından istifadə edə bilər. Bu deşifrə açarı hər zaman məxfi saxlanmalıdır və mesajın şifrələnməsi üçün istifadə olunan açara bənzəyir, ya da olmaya bilər. Eyni şeyi bir nümunə ilə başa düşək.