Layihəni oxuyarkən qarşımıza çıxan və bizə maraqlı gələn fikirlər vardı. Və onları araşdırdıq. Məsələn:

Məlumatları hackerlərdən necə qorumaq olar?

Hal-hazırda hər bir təşkilat, hər bir müəssisə üçüncü tərəfin icazəsiz daxil olmasının və ya təhdidin qarşısını almaq üçün həssas məlumatların şifrələnməsini tələb edir. Şifrələmənin yeganə məqsədi kompüter sistemlərində saxlanan, internetdə və ya başqa bir şəbəkədə ötürülən rəqəmsal məlumatların məxfiliyini qorumaqdır (şifrələmə haqqında araşdırma edərkən, sizin bizə danışmış olduğunuz SİM kart məsələsi ağlımıza gəldi. Və məlumatlarımızı hackerlərdən necə qorumaq olar sualına SİM kartların şifrələmə alqoritmi və burada AES şifrələmə alqoritminin daha etibarlı olması fikrini də xatırladıq. Diqqət edilməsi, maraqlı və daima nəzərə alınacaq bir mövzu olduğunu da düşünürük). Eyni zamanda şifrələmə ilə əlaqəli protokollar vardır. Və onlar haqqında da kiçik bir araşdırma edərək öyrənmək istədik. Protokol məlumatların ötürülməsi üçün qaydalar və təlimatlar toplusudur. İki və ya daha çox kompüter arasında əlaqə zamanı hər addım və proses üçün qaydalar müəyyən edilir. Məlumatların uğurla ötürülməsi üçün şəbəkələr bu qaydalara əməl etməlidirlər. İndi isə şifrələmə protokollarına nəzər yetirək. Secure Socket Layer (SSL): Secure Socket Layer ən çox istifadə olunan təhlükəsizlik protololudur. İnternet üzərində işləyən iki maşın arasında etibarlı şifrəli bir kanal təmin edən protokoldur. SSL protokolu, ümumiyyətlə bir veb brauzerin etibarlı olmayan internet üzərindən bir veb serverə etibarlı bir şəkildə qoşulması lazım olduqda istifadə olunur. Və SSL sertifikatı vasitəsilə etibarlı əlaqə qurulacaqdır (qeyd etmək istəyirik ki, məsələn: özümüzdə olan web browser’dən axtarış hissəsinin yanında olan qıfıl işarəsinə daxil olaraq, daxil olduğunuz saytın SSL sertifikatı, etibarlı olub olmaması vəs. Haqqında da məlumat toplaya bilərsiniz).

Layer Two Tunneling Protocol (L2TP) : Layer Two Tunneling Protocol- u, virtual özəl şəbəkə (VPN) əməliyyatlarını təmin etmək üçün İnternet provayderləri tərəfindən istifadə olunan şəbəkə protokoludur. User Datagram Protocol (İstifadəçi Datagram Protokolu) portu L2TP rabitə üçün istifadə olunur çünki o, şifrələmə və məxfilik kimi məlumatlar üçün heç bir təhlükəsizlik təmin etmir, Internet Protocol (İnternet Protokolu) təhlükəsizliyi kimi şifrələmə protokolu tez-tez L2TP ilə istifadə olunur.

IPsec: Internet protocol security (IPsec) İnternet Protokolunun təhlükəsizliyini təmin edən protokollar dəstidir. Təhlükəsizliyi təmin etmək üçün kriptoqrafiyadan istifadə edə bilər. IPsec xüsusi bir şifrələmə alqoritmi deyil, IP protokolundakı paketlərin şifrələnməsi və təsdiqlənməsi üçün bir çərçivədir (framework). IPsec müxtəlif alqoritmlərdən istifadə edə bilər və tam və ya qismən həyata keçirilə bilər. Paket məzmununu şifrələmək üçün “public key” və “private key” kriptovalyutalarının birləşməsi istifadə olunur.

Vəs.