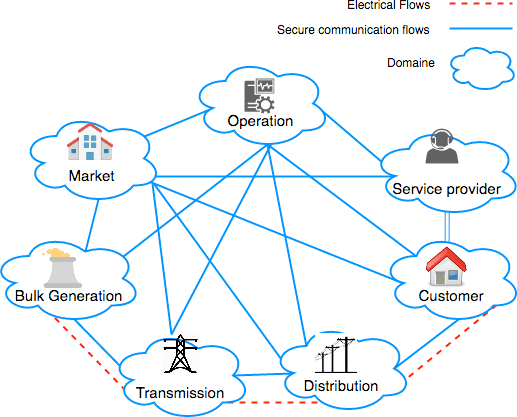
**Smart Grid**

Smart Grid, elektrik enerjisinin istehsalı, çatdırılması və istifadəsində kommunikasiya və informasiya texnologiyalarına əsaslanan bir sistemdir. Smart Grid-in əsas üstünlükləri şəbəkənin effektivliyinin artırılması və ətraf mühitin performansını yaxşılaşdırmaqdır. Smart Grid infrasturukturunda təhlükəsizliyə dair problemlərin həlli üçün bir neçə tədqiqat xarakterli məqalələr çap olunmuşdur. Onlar şəbəkə tipinə əsaslanan hücumlara görə siniflərə ayrılır: ev ərazisi şəbəkəsi(home area network HAN), yaxın ərazi şəbəkəsi(neighborhood area network NAN), qlobal şəbəkələr(wide area network WAN).

**Smart Gridin konseptual modeli**

Milli Standart və Texnologiya İnstitutunda aparılan tətqiqatlara (NIST) görə, smart grid yeddi məntiqi domaindən ibarətdir: kütləvi generasiya (bulk generation), ötürülmə (transmission), paylanma (distribution), müştəri (customer), marketlər (markets), servis təminatçısı (service provider) və əməliyyatlar (operations), bunların hər biri iştirakçı və tətbiqləri əhatə edir. İştirakçılar programlar, resurslar və sistemlərdir, tətbiqlər isə hər bir sahədə bir və ya bir neçə iştirakçının yerinə yetirdiyi tapşırıqlardır. Şəkil 1-də smart gridin konseptual modeli və təhlükəsiz kanal vasitəsilə müxtəlif domenlərdən qarşılıqlı əlaqəsi göstərilmişdir.

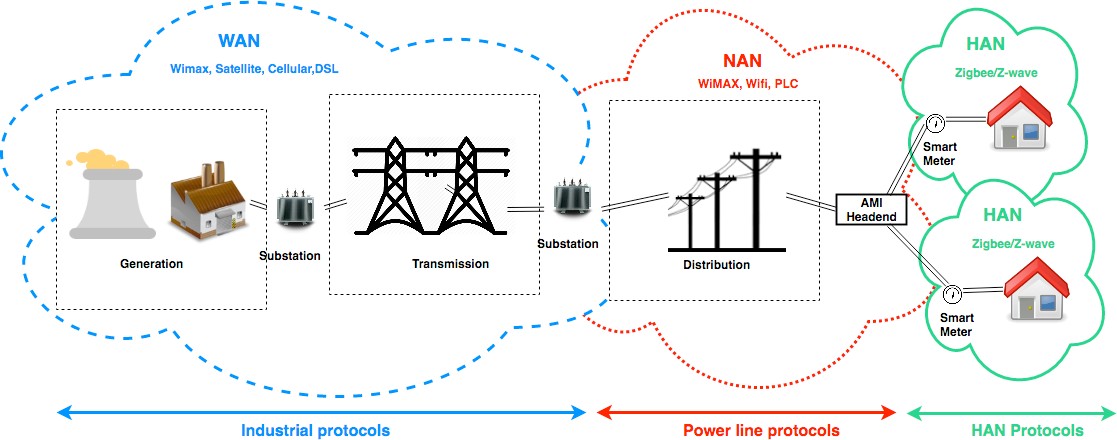


Şəkil 1. Smart Grid konseptual sxemi

* Müştəri domeni daxilində, əsas son istifadəçidir. Ümumiyyətlə, üç növ müştəri var: ev, ticarət / tikinti və sənaye. Elektrik istehlakı ilə yanaşı, bu aktyorlar enerji istifadəsini yarada, saxlaya və idarə edə bilərlər. Bu domen elektrik paylama domeninə qoşulur və paylanması, istismarı, xidmət təminatçısı və bazarda olan domenlərlə ünsiyyət qurur. Bu domen elektrik paylama domeninə qoşulur və paylanma, əməliyyat, servis təminatçı və market domenlərlə əlaqə qurur.
* Market domenində aktyorlar elektrik marketlərinin operatorlar və iştirakçılardır. Bu domen elektrik təchizatı və tələbat arasında balansı saxlayır.
* Servis provayderi domeninə elektrik müştərilərinə və kommunal servislərə xidmət edən təşkilatlar daxildir. Bu təşkilatlar hesabların tərtibi, müştəri hesabı və enerji istifadəsi kimi xidmətləri idarə edir. Servis provayderi situasiya bilikləri üçün əməliyyat domeni ilə qarşılıqlı fəaliyyət göstərir.
* Əməliyyatlar domenində fəaliyyət göstərən aktyorlar elektrik hərəkatının idarəçiləri olur. Bu domen ötürülmə və paylamada səmərəli və optimal əməliyyatları saxlayır. Ötürülmə zamanı enerji idarəetmə sistemləri (EMS), paylaşdırmada isə paylama idarəetmə sistemləri (DMS)istifadə edir.
* Kütləvi generasiya domenindəki aktyorlar, kütləvi miqdarda elektrik enerjisi generatorlarını əhatə edir. Enerji istehsalı son istifadəçiyə elektrik verilməsi prosesində ilk addımdır. Enerji neft, axan su, kömür, nüvə parçalanması və günəş radiasiyası kimi mənbələrdən istifadə edir.
* Ötürülmə domenində yaranan elektrik enerjisi, bir neçə substansiya vasitəsilə generasiya domenindən paylanma domeninə qədər uzun məsafələr keçir. Bu domen həmçinin elektrik enerjisi saxlaya və istehsal edə bilər.  Ötürülmə şəbəkəsi SCADA sistemi vasitəsilə izlənilir və nəzarət olunur, bu şəbəkə kommunikasiya şəbəkəsindən, nəzarət qurğularından və monitorinq qurğularından ibarətdir.
* Paylanma domeni son istifadəçi üçün elektrik verən distribyutorları əhatə edir. Elektrik paylama sistemlərinin radial, kontur və ya tor kimi müxtəlif strukturları vardır. Paylanma ilə yanaşı, bu domen enerji istehsalını və saxlanmasını da dəstəkləyə bilər.

Smart grid bir neçə paylanmış və hetrogen tətbiqlərdən ibarətdir, bura daxildir   inkişaf etmiş ölçü infrastrukturu (AMİ), avtomatlaşdırma yarımstansiyası, cavab tələbi, müşahidə nəzarəti və məlumatların əldə edilməsi (SCADA), elektrik vasitəsi (EV) və ev enerji idarəçiliyi (HEM).

Smart gridin paylanmış və hetrogen tətbiqləri fərqli kommunikasiya protokolları tələb edir. Şəkil 2 smart grid şəbəkəsinin arxitekturasını və hər bir şəbəkə üçün istifadə edilən protokolu göstərir. Ev sahəsi şəbəkəsində (HAN) ev alətləri ZigBee və Z-wave protokollarından istifadə edir. Qonşuluq ərazi şəbəkəsində (NAN) cihazlar, adətən, IEEE 802.11, IEEE 802.15.4 və ya IEEE 802.16 standartlar ilə əlaqələndirilir. Qlobal şəbəkələr(WAN) və müşahidə nəzarəti və məlumatların əldə edilməsi (SCADA) tətbiqlərində bir neçə sənaye protokolu, xüsusilə paylanmış şəbəkə protokolu 3.0 (DNP3) və modicon kommunikasiya avtobusu (ModBus) istifadə olunur. Yarımstansiyanın avtomatlaşdırılması prosesində IEC 61850 protokolu istifadə olunur.



Şəkil 2.Smart grid şəbəkə arxitekturasının nümunəsi

**Smart grid hücumlar**

Ümumiyyələ xakerlər tərəfindən Smart grid hücumların 4 addımı var. İlk addım kəşfiyyat zamanı, hücumçu öz məqsədi haqqında məlumat toplayır. İkinci mərhələdə, araşdırma zamanı, hücumçu sisteminin zəifliyini müəyyən etməyə çalışır. Bu tədbirlər açıq portları tapmaq və hər portda öz zəiflikləri ilə işləyən xidmətləri müəyyən etmək məqsədi daşıyır. İstismar addımı zamanı hücumçu, kompromisə və hədəfin tam nəzarətini almaq üçün çalışır. Təcavüzkarın hədəfə inzibati girişi olduqda, son mərhələyə daxil olur, hansı ki, bu girişin saxlanmasıdır. Bu addım gizli və təyin olunmayan proqramın qurulması yolu ilə əldə edilir. Beləliklə o, asanlıqla hədəf sistemə geri qayıda bilər.

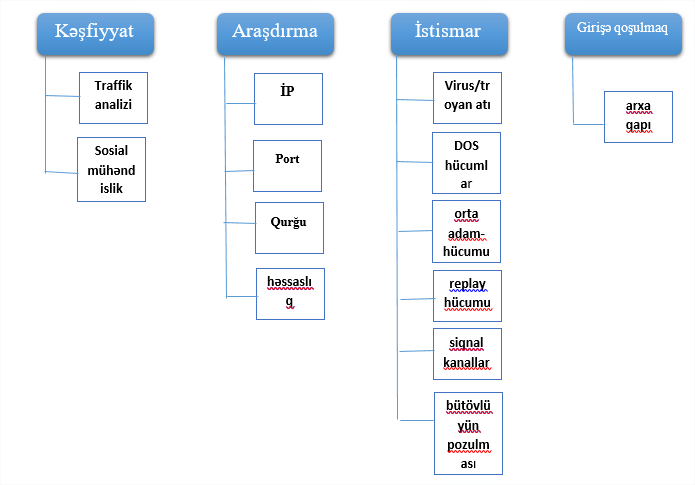
Girişə qoşulmaq

Araşdırma

Kəşfiyyat

İstismar

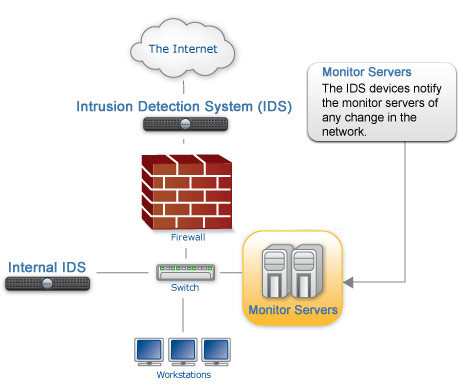
Şəkil 3. Bir sistem üzərində nəzarəti ələ almaq üçün hackerlər tərəfindən təqib edilən hücum dövrü



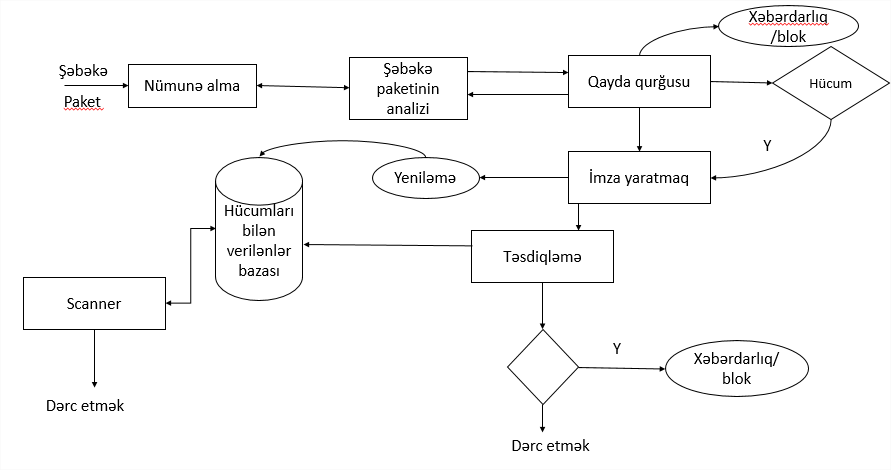
Şəkil 4. Hücum dövrünə əsaslanan smart griddə kiber hücumların təsnifatı

**Smart griddə şəbəkə təhlükəsizliyi**

Şəbəkə smart gridin əsasını təşkil edir. Beləliklə, şəbəkə təhlükəsizliyi bütün sistemi təmin etməkdə mühüm rol oynayır. Smart grid şəbəkəsini təmin etmək üçün monitorinq və yoxlama texnologiyaları ilə təchiz edilmiş firewalllardan istifadə edilməsi tövsiyə olunur. Firewall xüsusi qaydalara və siyasətlərə əsasən şəbəkə əlaqələrini təmin etməyi və ya inkar etməyi nəzərdə tutur. Ancaq bilinməyən və ya inkişaf etmiş bir hücum üsulu, bir çox firewall üsulunu asanlıqla atlaya bilər. Buna görə də firewalllar müdaxilənin aşkarlanması sistemi (IDS), təhlükəsizlik məlumatları və hadisələri idarəetmə sistemləri (SIEM) və şəbəkə məlumatlarının itirilməsinin qarşısının alınması (DLP) kimi digər təhlükəsizlik texnologiyaları ilə əlaqəli  olmalıdır.

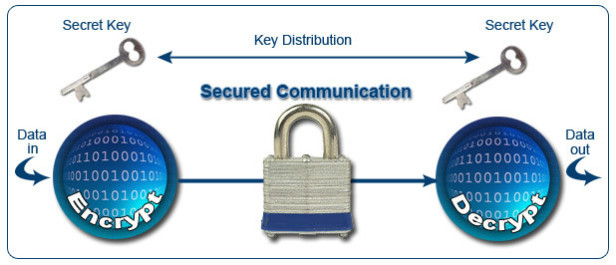


İDS qurğuların monitor serverləri şəbəkədə bəzi dəyişikliklər üçün istifadə olunur



Şəkil 5. İDS sistemlərin arxitekurası

Şifrələnmə mexanizmləri məlumatların məxfiliyini, bütövlüyünü və qeyri-bərabərliyini təmin etmək məqsədi daşıyır.



Əsas şifrələrin iki növü vardır: Simetrik və asimmetrik. Simmetrik şifrələmə və ya tək-açarlı şifrələmə məlumatları şifrələmək və ya deşifrələmək üçün tək açardan istifadə edir. Simmetrik şifrələmədə istifadə edən ən çox istifadə edilən alqoritmlər inkişaf etmiş şifrələmə standartı (AES) və məlumat şifrələmə standartıdır (DES). Asimmetrik şifrələmə məlumatları şifrələmək və ya deşifrələmək üçün iki açardan istifadə edir: fərdi və ictimai açar. RSA (Rivest, Shamir və Adleman) geniş şəkildə istifadə edilən asimmetrik alqoritmdir. Smart griddə müxtəlif hesablama qabiliyyətinə malik müxtəlif komponentlər mövcuddur. Buna görə də seçim kriteriyaları, vaxt məhdudiyyətləri və hesablama resursları daxil olmaqla bir neçə faktordan aslı olaraq həm simmetrik, həm də asimmetrik əsas şifrələmə istifadə edilə bilər.

**Konfidensiallıq, bütövlük, əlçatanlıq**

NİST hər bir hücumun informasiya təhlükəsizliyinə təsirini təqdim edir: konfidensiallıq, bütövlük və əlçatanlıq (confidentiality, integrity, and availability CIA).

****

**Konfidensiallıq**- Ümumiyyətlə konfidensiallıq(gizlilik) məlumata giriş və açıqlama ilə əlaqədar olan məhdudiyyətləri qoruyur. Başqa sözlə, gizlilik meyarları həm şəxsi gizlilik həm də xüsusi məlumatların icazəsiz şəxslər, fərdlər və ya proseslər tərəfindən əldə edilməsinin və ya ifşa edilməsinin qarşısını almağı tələb edir. İcazəsiz məlumat ifşa edildikdə, məxfilik itirilər. Məsələn, müştəri və müxtəlif təşkilatlar arasında göndərilən vacib məlumatlar gizlədilməli və qorunmalıdır; Əks təqdirdə müştərinin məlumatı digər zərərli məqsədlər üçün manipulyasiya edilə, dəyişdirilə və ya istifadə edilə bilər.

**Bütövlük**- Smart griddə bütövlük, məlumatların səhv şəkildə dəyişdirilməsi və ya məhv edilməsinə qarşı qoruma mənasını verir. Bütövlüyün pozulması, məlumatın icazəsiz bir şəkildə dəyişdirilməsi və ya məlum olmayan bir şəkildə məhv edilməsidir. Bütövlüyün qorunub saxlanılması üçün həm imtina edilməməsi, həm də məlumatın orijinallığı tələb olunur. Qeyri-imtina fərdlərin, müəssisə və ya təşkilatın müəyyən bir hərəkəti həyata keçirə bilməməsi və daha sonra imtina etməsi mənasını verər. Orijinallik, məlumatların qanuni bir qaynaqdan alınmasıdır.

**Əlçatanlıq** - Məlumatın vaxtında və etibarlı şəkildə əldə edilməsi, istifadəsinin təmin edilməsi kimi müəyyən edilir. Bu, smart griddə ən mühüm təhlükəsizlik kriteriyası hesab olunur, çünki əlçatanlığın pozulması smart şəbəkədəki məlumatlara girişin dayandırılması deməkdir. Məsələn, əlçatanlığın pozulması şəbəkənin məlumat axınıın qarşısını alaraq idarəetmə sisteminin fəaliyyətini poza bilər.