Kompüter sistemlərinin təhlükəsizliyinin qiymətləndirilməsi metodları

Ramiz Şıxəliyev[1], Tural Yunusov[2]

AMEA İnformasiya Texnologiyaları İnstitutu

[1]ramiz@sciencez.az, [2]turaly@mail.ru

***Xülasə*— Məqalə kompüter sistemlərinin təhlükəsizliyinin qiymətləndirilməsinə həsr edilmişdir. Məqalədə kompüter sistemlərinin təhlükəsizliyinin qiymətləndirilməsinin bəzi standart və metodları, o cümlədən Ümumi Meyarlar standartı, sistemin zəiflik indeksi, çoxpilləli hücum modelləşdirməsi, Hücumun Aşkarlanması metodları analiz edilmiş və mövcud problemlər müəyyən edilmişdir. Həmçinin KS-nin təhlükəsizliyinin qiymətləndirilməsinə əsas yanaşmalar və qiymətləndirmə metrikaları analiz edilmişdir.**

Açar sözləri— kompüter sistemləri; təhlükəsizliyin qiymətləndirilməsi; təhlükəsizlik metrikaları; təhlükəsizliyin qiymətləndirilməsi metodları

I. GİRİŞ

Kompüter sistemləri (KS) enerji, rabitə, maliyyə və s. kimi əsas sənaye sektorlarında geniş istifadə olunur. Bu sektorlarda əsas əməliyyatlar KS ilə aparıldığından onlar bu sistemlərdən çox asılıdır. Nəticədə, bu sistemlərin təhlükəsizliyi əsas məsələlərdən birinə çevrilir. 2001-ci ildən etibarən müxtəlif sektorlarda KS təhlükəsizliyinə çəkilən xərclərin miqdarı əhəmiyyətli dərəcədə artmışdır [1]. Buna görə də KS təhlükəsizliyi sahəsində tədqiqatların aparılması çox vacibdir.

KS təhlükəsizlik səviyyəsi onlardan asılı olan hər bir şirkət və ya təşkilatın normal fəaliyyəti üçün əsasdır. Şirkət və təşkilatların maliyyə gəlirləri əhəmiyyətli dərəcədə KS-nin istifadəsinə əsaslandığı üçün təhlükəsizlik sistemlərinə böyük maliyyə xərclənir. Lakin təhlükəsizlik və xərclər arasında müəyyən kompromis olmalıdır. Çox yüksək təhlükəsizlik KS-ni əlçatmaz, qeyri-funksional edir və çox baha başa gəlir, lakin çox aşağı təhlükəsizlik ucuz başa gəlsə də, KS-ni hücumlara qarşı son dərəcə zəif edir və onun qeyri-funksionallığına gətirib çıxaracaqdır. Buna görə də, təhlükəsizliyi aşağı salmadan xərcləri azaltmaq məqsədilə hər bir hal üçün "nə qədər" təhlükəsizliyin tələb olunduğunun müəyyən edilməsinə böyük ehtiyac vardır.

KS-nin gündəlik həyat fəaliyyətlərimizə nüfuz etməsinə baxmayaraq, çox az adam təhlükəsizliyin əhəmiyyəti barədə məlumata malikdir. Hər gün müxtəlif növ KS-ləri (telefon, şəxsi kompüterlər, kredit kartları, bankomatlar və s.) istifadə olunsa da, istifadəçilər öz fəaliyyətləri ilə bağlı olan etibar və təhlükəsizlik məsələlərini başa düşmürlər. Bu sahədə məlumatlandırma çox vacibdir və KS təhlükəsizliyinin əhəmiyyətini göstərən bir üsul olmadıqda onun vacibliyi daha da artır. Təhlükəsizliyin qiymətləndirilməsi metodları bu istiqamətdə etibarın yaradılması vasitəsi rolunu oynaya bilər.

KS-nin mühasfizəsi zərurəti yeni olmadığından, kompüter təhlükəsizliyi termini artıq innovativ termin kimi səslənmir. Əksər müasir KS-lər onların və saxlanılan məlumatların təhlükəsizliyinin müəyyən səviyyədə təmin olunmasına imkan verən aparat və proqram təminatları ilə təchiz olunmuşdur.

KS-nin informasiya təhlükəsizliyinin qiymətləndirilməsi zamanı bir çox amillər nəzərə alınmalıdır. Bu problemin dəqiq həlli üçün xüsusiyyətlərin və ölçülərin müfəssəl və son dərəcə dəqiq siyahısını tərtib edilməsi çox çətin məsələdir. KS-nin təhlükəsizliyinin qiymətləndirilməsi zamanı real irəliləyiş əldə etmək üçün eksperimental metodlar, təhlükəsizlik metrikaları və qabaqcadan xəbər vermək imkanına malik etibarlı təhlükəsizlik modelləri yaradılmalıdır.

KS-nin təhlükəsizliyinin qiymətləndirilməsi probleminin həllinə adətən nəzəri cəhətdən yanaşırlar. Çox zaman, təklif olunan nəzəri metodlar ilə real həyat arasındakı ziddiyyətin mövcud olması elmi tədqiqatın nəticələrini mübahisə mövzusuna çevirir. Hətta daha çox praktiki perspektivə malik olan tədqiqatlar belə bəzən lazımi nəticələr verə bilmir.

KS-nin təhlükəsizliyinin qiymətləndirilməsi problemini bir-biri ilə əlaqəli olan iki müxtəlif hissələrə ayırmaq olar: müvafiq təhlükəsizlik metrikasının müəyyən edilməsi və bu təhlükəsizlik metrikalarına uyğun olaraq KS təhlükəsizliyinin düzgün və dəqiq ölçüməsinə imkan verən metodların işlənməsi.

Bu gün, kompüter sistemlərin təhlükəsizliyinin qiymətləndirilməsi üçün müxtəlif metodlar təklif edilmişdir [2, 3, 4. 5]. Məqalənin əsas məqsədi bu metodların analizi və mövcud problemləri müəyyən etməkdir.

II. KOMPÜTER SİSTEMLƏRİNİN TƏHLÜKƏSİZLİYİNİN QİYMƏTLƏNDİRİLMƏSİ

KS təhlükəsizliyinin və onun elementlərinin qısa analizi onu tam olaraq müəyyənləşdirməyə imkan vermir. Heç sözsüz ki, onu qiymətləndirmək daha da çətindir. Buna baxmayaraq, KS-nin təhlükəsizliyini yoxlamaq üçün nəyi nəzərə almağın lazım olduğunu müəyyənləşdirmək istiqamətində işlər mövcuddur. [6]-cı işdə əsasən, təhlükəsizliyin qiymətləndirilməsi prosesinin müvəffəqiyyətli olması üçün vacib hesab edilən aşağıdakı aspektlər müəyyən edilmişdir:

- təhlükəsizliyin mənası;
- sistemin əhatə dairəsi;
- təhlükəsizliklə bağlı sistemin xüsusiyyətləri;
- qiymətləndirmə prosesinin əhatə dairəsi;
- qiymətləndirmənin etibarlılığı.

Yuxarıdakıların hamısı göstərir ki, qiymətləndirmə prosesinə başlamamışdan əvvəl kifayət qədər çox amil nəzərə alınmalıdır. KS-nin təhlükəsizliyinin ölçülməsi və qiymətləndirməsinin səbəbini, bu prosesin hansı şəraitdə

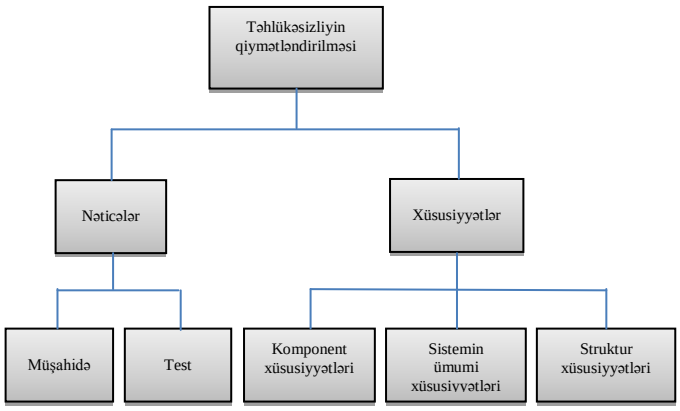
həyata keçirilməsi və hansı nəticələr verəcəyini bilmədən bu prosesə başlamaq yanlış olardı.

Bundan başqa, [7]-ci işdə göstərilir ki, təhlükəsizliyin qiymətləndirilməsi prosesi dörd prinsipə əsasən həyata keçirilməlidir:

- sistemin müşahidə olunması – sistemin daxili funksiyaları təhlil edilmədən xaricdən təhlil edilir;
- sistemin kompleks yoxlanılması – sistemin təhlükəsizlik səviyyəsini yoxlamaq üçün əsas mənbə təhlükəsizlik sisteminin keçilməsi testidir (penetrasiya testi);
- sistem təhlükəsizliyinin funksionallığı – sistem təhlükəsizlik zəifliklərinin qarşısını almaq üçün təhlükəsizlik mexanizmləri və tədbirlərinin müəyyən olunması yolu ilə yoxlanılır;
- sistemin strukturu – sistem elementləri və həmin elementlər arasındakı əlaqələr toplusu kimi nəzərə alınır.

Bu yanaşmalar hal-hazırda mövcud olan müxtəlif metodlarda tətbiq olunur və bir-birinə rəqib olmaqdan daha çox tamamlayıcı kimi hesab edilə bilər. Onların bəziləri isə təhlükəsizliyin qiymətləndirilməsi prosesində istifadə oluna bilər.

[8]-ci işdə müəllif bu dörd sinfi iki əsas kateqoriyaya bölərək 1-ci şəkildə göstərilən beş yanaşmanı təklif etmişdir. Burada əsas yanaşma ondan ibarətdir ki, sistem ya daxili funksionallığı qeyri-məlum olan qara qutu (nəticələr) və yaxud da sistem xüsusiyyətləri məlum olan tərkib hissələri (xüsusiyyətlər) kimi göstərilir.



Şəkil 1: Təhlükəsizliyin qiymətləndirilməsinə əsas yanaşmalar

Təhlükəsizlik sisteminin keçilməsi testidir (penetrasiya testi) yanaşmasından istifadə zamanı sistemlər və şəbəkələr ya zəifliklərı yoxlayan skanerlərin (avtomatlaşdırılmış kompüter proqramı), ya da istifadəçilərin təhlükəsizlik təcrübəsindən istifadə edərək sistemlərə "əl ilə" nüfuz etməyə çalışan "qırmızı komandalar"-ın (təhlükəsizlik ekspertləri qrupu) köməyi ilə məlum proqram təminatı və ya potensial sistem konfiqurasiyası səhvləri yoxlanılır.

Bununla belə, bu metodun zəif cəhəti təkcə verilmiş məlumat və vaxt çərçivəsində sistemin və ya şəbəkənin nə dərəcədə təhlükəsiz olduğunu və həm də mövcud, lakin yoxlayıcılara məlum olmayan məlumatlardan istifadə etməklə gələcəkdə meydana çıxacaq təhlüklələrə qarşı necə təhlekəsiz olduğunu müəyyən edə bilməməsidir.

III. TƏHLÜKƏSİZLİYİN QİYMƏTLƏNDİRİLMƏSİ METRİKALARI

Təhlükəsizliyin qiymətləndirilməsinin müxtəlif tələb və aspektləri əhatə edən, təklif edilmiş bir neçə metrikalar mövcuddur [10, 11, 16]. Ümumi təyinatlı təhlükəsizlik metrikasını yaratmaq üçün göstərilən hər bir cəhd "ideal" metrika anlayışının bütün sistem və istifadəçilərə tətbiq oluna bilən metrikanı təşkil edən xüsusiyyətlər toplusunun olmadığını sübut etməyə yönəlmişdir [12].

Təhlükəsizlik metrikaları KS-nin təhlükəsizliyinin ölçülməsi və əldə olunan nəticələrin şərh edilməsini yerinə yetirir. Onlar təkcə emal üçün məlumatın toplanması üsulu deyil, həm də toplanmış məlumatların mənasının izah edilməsi üçün dəyərli bir vasitədir. Buna baxmayaraq, bu vaxta qədər aparılmış əksər tədqiqatlar təhlükəsizliyin idarə edilməsinə və yaxud insan davranışı aspektlərinə yönəlmişdir. Lakin, kifayət qədər qənaətbəxş texniki nəticə əldə olunmamışdır, bunun səbəbi də hələ də həll edilməmiş iki (ən azı) problemin olmasıdır. Birinci problem metrikanın müəyyən edilməsi və hesablanması üçün hansı məlumatdan istifadə edilməsi, ikinci problem isə etibarlı metrikanın müəyyən edilməsi ilə bağlıdır.

Birinci problemin həlli üçün xeyli sayda müxtəlif yanaşmalar təklif edilmişdir. Bəziləri hesab edir ki, müəyyən məlumatın müəyyən fraqmentlərinin toplanması daha spesifik və etibarlı nəticələr verəcəkdir. Digərləri hesab edir ki, toplanmış məlumatın ölçüsünü genişləndirməklə daha real və reallığa yaxın nəticələr əldə etmək olar və nəticədə, onlar daha dəqiq olar. Buna görə də KS-nin təhlükəsizliyinin qiymətləndirilməsi zamanı qarşıya qoyulan məsələdən asılı olaraq, müvafiq miqdarda və növdə məlumat toplanmalıdır.

Etibarlı metrikanın müəyyən edilməsi probleminin həlli üçün [13]-cü işdə yanaşma təklif edilmişdir. Müəlliflər etibarlı təhlükəsizlik metrikasının əldə edilməsi üçün beş xüsusiyyətin nəzərə alınmasını təklif edirlər:

- ardıcıl şəkildə ölçülməli, eyni məlumat blokundan istifadə etməklə müxtəlif insanlar eyni nəticələr əldə edə bilməlidir;
- toplanılması ucuz başa gəlir, asan toplanması və hesablama vaxtının çox olmaması;
- , yalnız nisbi məhsuldarlıq qiymətləndirilməsi üçün yaxşı olan formada (yüksək, orta, aşağı və s.) deyil, ədədi kəmiyyət və ya faiz kimi ifadə olunur;
- ən azı bir ölçü vahidindən istifadə etməklə ifadə olunur və nəticələr ölçülənlərin xüsusiyyətlərini ardıcıl şəkildə göstərməklə ifadə olunur;
- anlamaq üçün asan, yararlı, eyni zamanda mənalı və kifayət qədər spesifik olması üçün məzmun baxımından konkret olmalıdır.

IV. İNFORMASİYA TƏHLÜKƏSİZLİYİNİN QİYMƏTLƏNDİRİLMƏSİNİN MÖVCUD METODLARI

Təhlükəsizliyin qiymətləndirilməsi problemini tədqiq edən bir çox alimlər və bu məsələyə müxtəlif yanaşmalar mövcuddur. Ümumi Meyarlar (ÜM) kimi bu yanaşmaların

bəziləri, hətta, İSO (Beynəlxalq Standartlaşdırma Təşkilatı) standartlarına çevirilmişdir, lakin hələ də təhlükəsizliyin tam olaraq dəqiq qiymətləndirilməsi problemini həll etməmişdir, çünki onlar müxtəlif suallara müxtəlif şəkildə cavab verir. Təhlükəsizlik termininin müxtəlif izahlarını nəzərə alsaq, bunu başa düşmək elə də çətin olmaz.

Aşağıda kompüter sistemlərinin təhlükəsizliyinin qiymətləndirilməsinin bəzi metodlarının qısa analizi verilmişdir.

A. Ümumi Meyarlar

İnformasiya texnologiyaları (İT) məhsullarının (qurğu təminatı, proqram texniki təminatı, proqram təminatı) təhlükəsizlik səviyyəsini qiymətləndirmək və müqayisə etmək üçün geniş istifadə olunan bir standartdır. ÜM İSO beynəlxalq standartı kimi qəbul etdilmişdir (ISO 15408) və onun ən son variantı 3.1.CCv4-dir [17]. Onun əsas məqsədi izafi qiymətləndirmə fəaliyyətlərinin aradan qaldırılması, məhsulun zəmanətliyinə çox az təsir edən fəaliyyətlərin azaldılması/aradan qaldırılması, anlaşılmazlıqların azaldılması üçün ÜM terminologiyasının aydınlaşdırması, təhlükəsizlik zəmanətinin əldə olunduğu sahələrə qiymətləndirmə fəaliyyətlərinin strukturunun və istiqamətinin dəyişdirilməsi, həmçinin lazım olduqda yeni ÜM tələbləri əlavə etməkdir.

ÜM üç hissədən ibarətdir. Birinci hissə texnologiyaya giriş verir və ümumi modeli təqdim edir, ikincisi hissə İT məhsullarının təhlükəsizliyi üçün zəruri olan tələblər toplusunu təsvir edir, üçüncü hissə isə qiymətləndirmə prosesi zamanı həmin məhsullara tətbiq olunan zəmanətlik tədbirlərini təmin edir.

ÜM-ın 2-ci hissəsi geniş təhlükəsizliyin funksional tələblərinin (TFT) müəyyən edilməsi ilə başlayır. İT məhsulun növləri kateqoriyasından (məsələn, aparat şəbəkələrarası ekranı, müdaxilələrin aşkarlanması üzrə proqram təminatı, rəqəmsal müəllif hüquqlarının tətbiqi və s.) asılı olaraq arzu olunan formanı və təhlükəsizlik baxımından bu məhsulların tətbiqini təsvir edən müdafiə profili (MP) yaradılır. Növbəti addım qiymətləndirilən spesifik məhsulun arzuolunan təhlükəsizlik funksionallığını təmin edəcək təhlükəsizlik hədəfinin (TH) təsvir edilməsindən ibarətdir. TH MP tərəfindən verilən ümumi təsvirə əsaslanaraq məhsulun yekun qiymətləndirilməsi və onun TH-nin qoyduğu funksiyalar və qaydalara əsaslanaraq təsdiq olunub-olunmamasını yoxlamaq üçün istifadə olunur. Əvvəlcədən müəyyən olunmuş qiymətləndirmə zəmanəti səviyyələrinə (QZS) uyğun olaraq qiymətləndirməni başa çatdırmaq məqsədilə ÜM-a ümumi qiymətləndirmə metodologiyası adlı standartlaşdırılmış metod əlavə olunur. QZT-nin səkkiz səviyyəsi mövcuddur (QZS 0-dan QZS7-yə qədər) və onlar TFT-nə uyğunluq səviyyəsinin ölçüsüdür.

B. Sistemin Zəiflik İndeksi (SZİ) metodu

Təhlükəsizliyi qiymətləndirmək üçün [3]-cü işdə SZİ metodu təklif edilmişdir. Sistemin zəifliyinə səbəb olan üç müxtəlif kateqoriyalı amil formalaşdırılır və sistemin zəifliyinin abstrakt ölçülməsi barədə qərar qəbul edilir. Bu üç kateqoriya aiddir: sistemin xüsusiyyətləri, potensial etinasızlıq hərəkətləri və potensial qərəzli hərəkətlər.

Metodun kəmiyyətcə ifadəsi üçün SZİ 0 və 1 arasında ədədi kəmiyyətlər təyin edilir, lakin bu, imtiyazlı istifadəçilər üçün heç bir statistik və ehtimal əhəmiyyəti kəsb etmir. Bu, növbəti qaydada hesablanır. Müəyyən bir amilin sistemin təhlükəsizliyinə təsirinin əminliyini göstərən əminlik indeksi (Əİ) ilə ölçülür. Başqa sözlə, əgər müəyyən bir amil sistemdə varsa, onda sistemin zəifliyinin olmasına dair Əİ əminliyi mövcuddur. Sonra SZİ müxtəlif Əİ ilə ayrı-ayrılıqda hesablanır. Nəticədə, müəlliflər SZİ-nin qiymətini dörd qrupa bölürlər və bu qrupların hər bir sistemin zəifliyinin müxtəlif spektrlərini göstərir.

C. Çoxpilləli Hücum Modelləşdirməsi (ÇPHM) metodu

Sistemin təhlükəsizliyini onun hücumlara müqaviməti baxımından da qiymətləndirmək olar. Bu yanaşma [4]-cü işdə göstərilmişdir. ÇPHM metodu konkret şəbəkəyə sistemin boşluğunun istifadəsinə imkan verən hücumun modelləşdirməsinə əsaslanır. Şəbəkənin, zəifliyin və hücüm edənin imkanlarının sistemli ekspertizası vasitəsi ilə şəbəkənin məruz qaldığı təsirin effektinin analizi verilir. Hücum və təsirlərin mürəkkəbliyi və təhlükəsizliyi pozulmuş şəbəkə elementlərinin şəbəkənin digər sistemləri ilə qarşılıqlı əlaqəsi nəticəsində şəbəkənin təhlükəsizliyində ciddi hadisələr baş verə bilər. Bu hadisələr hücum zəncirləri adlanır. Bu hücumlardan potensial zəifliklərin və hücum yollarını müəyyən etmək üçün istifadə edilə bilər. Bu yolla şəbəkədə hücumun yayılması modelləşdirilir. Hər bir mümkün hücum üçün ehtimal müəyyən etməklə, ehtimal nəzəriyyəsindən istifadə etməklə hücumun hücum zəncirinin hər bir mərhələsinə çatmaq ehtimalını hesablamaq olar.

Bu metodun çatışmayan cəhəti ondan ibarətdir ki, şəbəkəni kifayət qədər təhlil edilməli və şəbəkəyə olan bütün hücumlar və hallar nəzərə alınmalıdır.

D. Hücumun Aşkarlanması Metodu (HAM)

[5]-ci işdə müəlliflər təhlükəsizlik nöqteyi-nəzərindən eyni sistemin iki müxtəlif versiyasını müqayisə etmək məqsədi ilə təhlükəsizliyin qiymətləndirilməsi üçün yeni metrika təqdim ediblər. Onların tədqiqatı [14]-cü işə əsaslanır, hansında ki, bu metod Microsoft Windows əməliyyat sistemlərinin müxtəlif versiyalarında sınaqdan keçirilmiş və onun cari inkişaf mərhələsi texniki hesabatda təqdim edilmişdir [15]. Hücumun aşkarlanması sistemdə baş verən hərəkətlər və onların təsir etdiyi sistem resursları ilə müəyyən olunur. Hər bir hərəkət potensial hücum ola bilər. Bu resurslar giriş və çıxış nöqtəsi adlanır və resurslara hücumun aşkarlanmasını təsvir etmək üçün əlavə olaraq hücum qabiliyyəti anlayışı daxil olunur. Hücum sinfi termini həmçinin resurslar çoxluğu (metodlar, kanallar və yaxud məlumat elementləri) şəkilində təqdim olunur ki, onları hücum qabiliyyətindən asılı olaraq təsnif etmək olsun. Bu metod kod səviyyəsində işləyir, yəni proqram təminatının hissələrinin əsas kodundakı boşluqları yoxlayır. O, təhlükəsizliyin pozulmasına səbəb olan potensial problemli resursların tapılmasına yönəlir və nəzərə alınmış resurslar nəticəsində üçlü dəyərlər formasında kəmiyyət nəticələri verir.

Üç növ resurs mövcuddur:

- giriş və çıxış nöqtələri (sistemə/proqram təminatına daxil olmaq üçün icazə verən metod və ya funksiyalar);

- açıq kanallar çoxluğu (proqram təminatının xarici mühitlə əlaqə yaratmasına imkan yaradan şəbəkə portları);
- etibarsız məlumat elementləri çoxluğu (təyin olunmuş daxilolma səviyyəsinə görə təhlükəsizlik problemlərinə səbəb olan məlumatlar/fayllar).

Bu metod proqram təminatının təhlükəsizlik keyfiyyətinə dair nəticələr çıxarmaq məqsədilə, iki səbəbdən proqram təminatı səhvlərini nəzərə alınmır. Bəzi səhvlər yoxlama prosesi zamanı gözdən yayına bilər və bütün proqram təminatı səhvlərinə bərabər əhəmiyyət verilir. Əksinə, hücumun aşkarlanması təkcə kodun təhlükəsizliyini deyil, həm də hər bir fərdi tətbiq zamanı rast gəlinən konfiqurasiya parametrlərini də yoxlayır. Bununla belə, problem ondadır ki, müəyyən olunmuş göstəricilər olmadığından onlar yalnız müqayisəli metrika kimi istifadə oluna bilər. İstifadə olunan işarələmələr müəyyən proqramlara uyğun gəlir və proqram təminatının bir hissəsinin iki giriş nöqtəsi və ya məlumat elementlərinin digər proqram hissənin ekvivalent resursları ilə eyni çəkiyə malik olunduğunu düşünmək yanlış olardı. Bundan başqa, əvvəlcədən verilmiş üçlükdə ikidən artıq dəyərlər olduqda (giriş nöqtələri, kanallar, məlumat elementləri), hətta eyni proqram təminatının iki müxtəlif versiyaları arasında hansının daha təhlükəsiz olmasına dair nəticə çıxarmaq asan olmur. Bu metodun elmi cəhətdən güclü olmasına baxmayaraq, yalnız xüsusi hallarda tətbiq oluna bilər.

NƏTİCƏ

KS-nin təhlükəsizliyi binar xüsusiyyətə malik deyil. Onun qiymətləndirilməsi zamanı çoxlu sayda faktorlar nəzərə almaq lazımdır. KS-nin təhlükəsizliyinin qiymətləndirilməsi üçün müfəssəl, dəqiq funksiyalar və ölçmələr bu gün də problem olaraq qalmaqdadır. KS-nin təhlükəsizliyinin qiymətləndirilməsi sahəsində real irəliləyişə nail olmaq üçün problemlərin müəyyən edilməsi və eksperimental metodların, dəqiq təhlükəsizlik metrikalarının və modellərinin yaradılması zəruridir.

Məqalədə KS-nin təhlükəsizliyinin qiymətləndirilməsinin bəzi standart və metodları, o cümlədən ÜM standartı, SZİ, ÇHM, HAM metodları analiz edilmiş və mövcud problemlər müəyyən edilmişdir. Həmçinin KS-nin təhlükəsizliyinin qiymətləndirilməsinə əsas yanaşmalar və qiymətləndirmə metrikaları analiz edilmişdir. Bu analizin nəticəsi KS-nin təhlükəsizliyinin qiymətləndirilməsi sahəsində mövcud olan bəzi problemlərin həll edilməsinə imkan verəcək.

ƏDƏBİYYAT

[1] Olsen, F., (2005) Input: IT security spending to catch its breath, Retrieved July 13, 2005 at URL: http://www.fcw.com/article89546-07-13-05

[2] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Information, Part 2: Security Functional Requirements, Part 3: Security Assurance Requirements, Version 3.1 Revision 1, September 2006

[3] A.J. ‑ Foss, Barbosa S., Assessing Computer Security Vulnerability, Operating Systems Review, v 29, n 3, July 1995, pp. 3 ‑ 13.

[4] Clark, K., Tyree, S., Dawkins, J., Hale, J., Qualitative and Quantitative Analytical Techniques for Network Security Assessment, In Proceedings of the 2004 IEEE Workshop on Information Assurance and Security, June 10-11, 2004, United States Military Academy, West Point, NY

[5] Howard, M., Pincus, J. Wing, J., Measuring Relative Attack Surfaces, In Proceedings of Workshop on Advanced Developments in Software and Systems Security, December, 2003, Taipei, Taiwan, Republic of China

[6] Hallberg, J., Hunstad, A., Peterson, A Framework for System Security Assessment, In Proceedings of the 2005 IEEE Workshop on Information Assurance, June, 2005, West Point, New York, USA

[7] Hallberg, J., Hunstad, A., Bond, A., Peterson, M., Pålsson, N., System IT Security Assessment, Scientific Report, Swedish Research Agency, Linköping, FOI-R--1468—E

[8] Gacic, D., FSA – Framework for Security Assessment of Distributed Information Systems. Master's thesis, Royal Institute of Technology, Stockholm, Sweden.

[9] Bishop, M., Introduction to Computer Security, Addison-Wesley Professional, ISBN 0-321- 24744-2

[10] Schudel, G., Wood, B., Adversary Work Factor as a Metric for Information Assurance, In Proceedings of the New Security Paradigm Workshop, September 18-22, 2002, Ireland

[11] Swanson, M., Bartol, N., Sabato, J., & Hash, J. (2003). Security metrics guide for information technology systems. Technical Report NIST Special Publication 800-55, NIST, July 2003.

[12] http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf.

[13] Vaughn, R., Henning, R., Siraj, A. Information Assurance Measures and Metrics – State of Practice and Proposed Taxonomy, In Proceedings of the 36th Hawaii International Conference on System Sciences, January 6-9, 2003, Big Island, HI, USA.

[14] Howard, M., Fending Off Future Attacks by Reducing Attack Surface, Retrieved January 29, 2007.

[15] Jaquith, A., Metrics are nifty, In Proceedings of the MetriCon 1.0 Workshop in conjunction with the USENIX Association's Security Symposium, August 1, 2006, Vancouver, British Columbia, Canada.

[16] P. Manadhata, J. Wing, An Attack Surface Metric, Carnegie Mellon University, CMU-CS-05-155, 2005.

[17] http://www.commoncriteriaportal.org/cc/