PARADIGMA, No.2, 2026, səh.150-154
https://doi.org/10.30546/30015.2026.001.02.391

İNFORMASİYA TƏHLÜKƏSİZLİYİ SİSTEMLƏRİNİN SINAQ MÜHİTİNDƏ APARAT KOMPONENTLƏRİNİN VƏZİYYƏT MODELLƏRİNİN TƏTBİQİ

S.T. Əliyeva, N.R. Nəbiyev
Azərbaycan Universiteti, Ceyhun Hacıbəyli, 71, Bakı, Azərbaycan
e-mail: Nihad.Nabiyev@student.au.edu.az

Xülasə. Məqalədə informasiya təhlükəsizliyi sistemlərinin sınaq mühitində aparat komponentlərinin vəziyyət modellərinin tətbiqi araşdırılır. Modellər vasitəsilə sistem davranışı imitasiya olunur və aparat səviyyəli zəifliklərin aşkarlanması asanlaşdırılır. Nəticədə təhlükəsizlik sistemlərinin etibarlılığı artırılır.

Açar sözlər: İnformasiya təhlükəsizliyi, aparat komponentləri, vəziyyət modelləri, sınaq mühiti, modelləşdirmə.

Giriş

Müasir informasiya texnologiyaları sistemlərinin inkişaf tempi artdıqca informasiya təhlükəsizliyi məsələləri də daha kompleks və çoxsəviyyəli xarakter almağa başlamışdır. Artıq informasiya təhlükəsizliyi yalnız proqram təminatının qorunması ilə məhdudlaşmır, çünki müasir sistemlərin ümumi etibarlılığı həm proqram, həm də aparat komponentlərinin qarşılıqlı və düzgün fəaliyyətindən asılıdır. Rəqəmsal transformasiya nəticəsində təşkilatlar, dövlət qurumları və kritik infrastruktur sistemləri daha mürəkkəb hesablama arxitekturalarına keçmişdir və bu arxitekturalar yüksək inteqrasiya olunmuş aparat komponentləri üzərində qurulmuşdur.Bu sistemlərdə prosessorlar, operativ yaddaş modulları, daimi yaddaş qurğuları, şəbəkə interfeysləri və idarəetmə mikrokontrollerləri kimi komponentlər müxtəlif iş rejimlərində fərqli davranış sərgiləyir. Yükün artması, temperatur dəyişiklikləri, resurs çatışmazlığı və ya xarici müdaxilə halları bu komponentlərin vəziyyətində dəyişikliklərə səbəb olur. Bu dəyişikliklər isə birbaşa olaraq təhlükəsizlik mexanizmlərinin düzgün işləməsinə təsir göstərir və bəzi hallarda sistemin zəifliklərini üzə çıxarır.

Ənənəvi informasiya təhlükəsizliyi yanaşmalarında əsas diqqət proqram təminatına yönəldilir, aparat səviyyəsində baş verən hadisələr isə çox vaxt ya nəzərə alınmır, ya da sadələşdirilmiş formada qiymətləndirilir. Halbuki real hücumların və sistem nasazlıqlarının əhəmiyyətli hissəsi aparat səviyyəsində baş verən problemlərlə əlaqədardır. Bu səbəbdən aparat komponentlərinin vəziyyət modellərinin qurulması və onların sınaq mühitində tətbiqi müasir kibertəhlükəsizlik tədqiqatlarında mühüm istiqamət hesab olunur [1].

Aparat komponentlərinin vəziyyət modellərinin qurulması

Aparat komponentlərinin vəziyyət modellərinin qurulması informasiya sistemlərinin davranışını formal şəkildə təsvir etməyə imkan verən fundamental yanaşmadır. Bu

modelləşdirmə prosesində hər bir aparat komponenti üçün mümkün iş vəziyyətləri müəyyən edilir və həmin vəziyyətlər arasında keçidlərin necə baş verdiyi riyazi və ya məntiqi formalizm vasitəsilə ifadə olunur.Bu yanaşmada sistem "vəziyyətlər çoxluğu" kimi nəzərdən keçirilir. Məsələn, prosessor üçün vəziyyətlər aşağıdakı kimi təsnif oluna bilər: normal işləmə vəziyyəti, yüksək yüklənmə vəziyyəti, resurs çatışmazlığı, istilik səbəbindən performans azalması, donma vəziyyəti və xarici müdaxilə nəticəsində yaranan qeyri-stabil vəziyyət. Eyni yanaşma yaddaş sistemlərinə də tətbiq olunur, burada məlumat itkisi, yaddaş sızması, bloklanmış yaddaş sahələri və səhv oxuma/yazma əməliyyatları ayrıca vəziyyətlər kimi modelləşdirilir.

Bu vəziyyətlər arasında keçidlər deterministik və ya ehtimallı ola bilər. Deterministik modellərdə keçidlər konkret şərtlərlə müəyyən olunur, məsələn, yüklənmə müəyyən həddi keçdikdə sistem "yük altında işləmə" vəziyyətinə keçir. Ehtimallı modellərdə isə keçidlər statistik ehtimallar əsasında baş verir və bu, real sistemlərin qeyri-müəyyən davranışını daha dəqiq əks etdirir.

Bu məqsədlə sonlu avtomatlar və Markov zəncirləri geniş istifadə olunur. Sonlu avtomatlar sistemin diskret vəziyyətlərini və keçidlərini formal şəkildə təsvir edir, Markov modelləri isə sistem davranışını ehtimallar əsasında modelləşdirərək daha realistik nəticələr əldə etməyə imkan verir [2]. Bu yanaşmalar aparat sistemlərinin mürəkkəb davranışını sadələşdirilmiş, lakin analitik baxımdan işlənə bilən formaya gətirir.

Sınaq mühitində aparat modellərinin tətbiqi

Sınaq mühiti informasiya təhlükəsizliyi sistemlərinin real iş şəraitinə yaxın şəraitdə yoxlanılması üçün istifadə olunan xüsusi test platformasıdır. Bu mühitin əsas məqsədi sistemin müxtəlif hücum ssenariləri, yüklənmə halları və nasazlıq vəziyyətləri altında necə davrandığını qiymətləndirməkdir.Aparat komponentlərinin vəziyyət modellərinin bu mühitə inteqrasiyası test prosesini daha strukturlaşdırılmış və sistemli edir. Modellər vasitəsilə sistemin bütün mümkün iş rejimləri əvvəlcədən müəyyən edilir və həmin rejimlər sınaq mühitində imitasiya olunur. Bu yanaşma test prosesinin təsadüfi xarakterdən çıxaraq planlı və analitik bir prosesə çevrilməsini təmin edir.

Məsələn, sınaq mühitində aşağıdakı hallar modelləşdirilə bilər: prosessorun maksimum yüklənməsi nəticəsində gecikmələrin yaranması, yaddaş modullarında məlumat pozulmaları, enerji təchizatında qeyri-sabitlik, şəbəkə paketlərinin itirilməsi və sistem komponentlərinin qismən nasazlığı. Bu ssenarilər vasitəsilə sistemin təhlükəsizlik mexanizmlərinin real şəraitdə necə işləyəcəyi qiymətləndirilir.

Bundan əlavə, aparat səviyyəli hücumların modelləşdirilməsi də bu mühitdə həyata keçirilə bilər. Yan kanal hücumları, elektromaqnit analizləri, enerji istehlakına əsaslanan

hücumlar və fiziki müdaxilə cəhdləri sistemin real təhlükələrə qarşı dayanıqlığını ölçməyə imkan verir. Bu isə ənənəvi proqram səviyyəli testlərin əhatə etmədiyi sahələrin analizinə şərait yaradır [3].

Sınaq prosesində vəziyyət modellərinin rolu

Vəziyyət modelləri sınaq prosesinin strukturlaşdırılmasında və optimallaşdırılmasında mühüm rol oynayır. Bu modellər əsasında sistemin bütün mümkün vəziyyətləri əvvəlcədən müəyyən edilir və test ssenariləri həmin struktura uyğun şəkildə hazırlanır.Bu yanaşma test prosesini təsadüfi yoxlamalardan çıxararaq sistemli və planlı bir mərhələyə çevirir. Hər bir vəziyyət ayrıca analiz olunur və sistemin həmin vəziyyətdə göstərdiyi davranış qiymətləndirilir. Bu isə daha dəqiq və etibarlı nəticələrin əldə edilməsinə imkan yaradır.

Eyni zamanda vəziyyət modelləri test prosesinin avtomatlaşdırılmasına şərait yaradır. Avtomatlaşdırılmış test sistemləri əvvəlcədən qurulmuş model əsasında müxtəlif vəziyyətlərə keçid edir və nəticələri qeydə alır. Bu yanaşma insan faktorundan qaynaqlanan səhvləri minimuma endirir, testlərin təkrarlanabilirliyini artırır və nəticələrin obyektivliyini yüksəldir [4].

Aparat səviyyəli zəifliklərin aşkarlanması

Aparat komponentlərinin vəziyyət modellərinin tətbiqi informasiya sistemlərində mövcud olan aparat səviyyəli zəifliklərin daha dərin və sistemli şəkildə analiz olunmasına imkan yaradır. Bu yanaşma xüsusilə kritik informasiya sistemlərində vacib hesab olunur, çünki bir çox təhlükəsizlik problemləri proqram təminatı səviyyəsində deyil, birbaşa aparat davranışında yaranan qeyri-sabitliklərdən qaynaqlanır. Aparat səviyyəli zəifliklərin aşkarlanması üçün yalnız funksional testlər kifayət etmir, sistemin fiziki və məntiqi davranışının paralel şəkildə araşdırılması tələb olunur.Belə zəifliklərə yan kanal hücumları, zamanlama əsaslı hücumlar, enerji istehlakının analizinə əsaslanan hücumlar, cache yaddaş strukturlarına müdaxilə və aparat resurslarının qeyri-normal və ya qeyri-stabil işləməsi kimi hallar daxildir. Bu cür zəifliklər çox vaxt sistemin daxili işləmə mexanizmlərini birbaşa pozmur, lakin dolayı yollarla məlumat sızmasına və ya sistem davranışının proqnozlaşdırılmaz hala gəlməsinə səbəb olur.

Xüsusilə yan kanal hücumları zamanı hücumçu sistemin birbaşa məlumatlarına çıxış etmədən, enerji sərfiyyatı, emal vaxtı və elektromaqnit siqnalları kimi dolayı göstəricilər vasitəsilə gizli məlumatları əldə edə bilər. Eyni zamanda cache strukturlarına edilən müdaxilələr sistem performansını aşağı sala və təhlükəsizlik mexanizmlərinin effektivliyini azalda bilər.Vəziyyət modelləri bu tip risklərin əvvəlcədən simulyasiya edilməsinə imkan verir. Modellər vasitəsilə sistem müxtəlif hücum ssenarilərinə salınır və aparat komponentlərinin bu

hallara reaksiyası analiz edilir. Bu yanaşma təhlükəsizlik sistemlərinin daha dayanıqlı dizayn edilməsinə, zəif nöqtələrin erkən mərhələdə müəyyən olunmasına və risklərin minimuma endirilməsinə şərait yaradır [5].

Nəticə. Aparat komponentlərinin vəziyyət modellərinin sınaq mühitində tətbiqi informasiya təhlükəsizliyi sistemlərinin daha dəqiq, sistemli və etibarlı şəkildə qiymətləndirilməsinə mühüm töhfə verir. Bu yanaşma ənənəvi test üsullarından fərqli olaraq sistemin yalnız statik deyil, dinamik davranışını da nəzərə alır və müxtəlif iş rejimlərində baş verə biləcək vəziyyət dəyişikliklərini əhatə edir.Belə modelləşdirmə sistemi daha real şəraitə yaxın test etməyə imkan yaradır, çünki aparat komponentlərinin davranışı müxtəlif yüklənmə, nasazlıq və hücum ssenariləri altında ayrıca analiz edilir. Nəticədə sistemin zəif nöqtələri daha erkən mərhələdə aşkar olunur, təhlükəsizlik mexanizmlərinin effektivliyi qiymətləndirilir və ümumi etibarlılıq səviyyəsi yüksəlir.Eyni zamanda bu yanaşma təhlükəsizlik sistemlərinin inkişafında proqnozlaşdırma imkanlarını genişləndirir. Yəni sistemin gələcəkdə müəyyən yük və ya hücum şəraitində necə davranacağı əvvəlcədən modelləşdirilə bilir. Bu isə risklərin idarə olunmasını daha effektiv edir.

Gələcək tədqiqat istiqamətlərində aparat modelləşdirilməsinin süni intellekt və maşın öyrənməsi metodları ilə inteqrasiyası xüsusi əhəmiyyət kəsb edir. Bu inteqrasiya vasitəsilə daha adaptiv, özünü öyrənən və real vaxtda qərar verə bilən təhlükəsizlik sistemlərinin yaradılması mümkün ola bilər. Beləliklə, aparat səviyyəli modelləşdirmə müasir kibertəhlükəsizlik sahəsində strateji əhəmiyyətə malik istiqamət kimi inkişaf etməkdədir.

Ədəbiyyat siyahısı

1. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Indianapolis, IN: John Wiley & Sons. 1232 p.
2. Bishop, M. (2019). Computer Security: Art and Science (2nd ed.). Boston, MA: Addison-Wesley. 1136 p.
3. Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.). Boston, MA: Pearson. 864 p.
4. Stallings, W. (2021). Cryptography and Network Security: Principles and Practice (7th ed.). Boston, MA: Pearson. 800 p.
5. Tanenbaum, A. S., & Bos, H. (2022). Modern Operating Systems (4th ed.). Boston, MA: Pearson. 1136 p.

APPLICATION OF STATE MODELS OF HARDWARE COMPONENTS IN THE TEST ENVIRONMENT OF INFORMATION SECURITY SYSTEMS

S.T. Aliyeva, N.R. Nabiyev
Azerbaijan University, Jeyhun Hajibeyli 71, Baku, Azerbaijan

Abstract: The article examines the application of state models of hardware components in the testing environment of information security systems. Through models, system behavior is simulated and hardware-level vulnerabilities are easier to detect. As a result, the reliability of security systems is increased.

Keywords: Information security, hardware components, situational models, test environment, modeling.