

İNFORMATİKA

HTTP HÜCUMLARIN TANINMASI ÜÇÜN
GENETİK ALQORİTMLƏRİN TƏTBİQİ

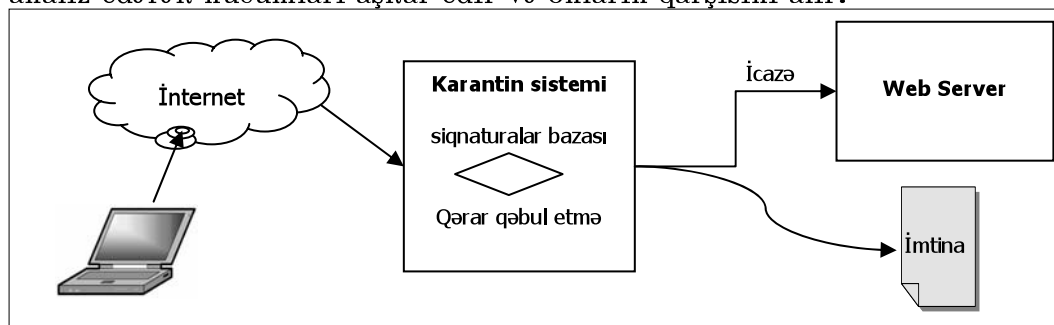
R.F.FƏRƏCULLAYEV

AMEA İnformasiya Texnologiyaları İnstitutu

Web-programların aktuallığı gündən-günə artır. Buna görə də onların təhlükəsizliyinin təmin edilməsi aktual məsələdir. Bu hücumları aşkar edən və onların qarşısını alan sistemlərdə istifadəçilərdən gələn HTTP sorğuların hücum olub-olmamasını təyin edən signaturaların yaradılması olduqca vacib məsələdir. Bu signaturalar adətən requlyar ifadələr dilində olub, hücumları identifikasiya edir və onların hansı sinfə mənsub olmasını müəyyən edir. Belə signaturaların mühəndislər tərəfindən yaradıldıqda yanlış qiymətləndirməyə (false positive, false negative) səbəb ola bilər. Buna görə də signaturaların yaradılması üçün haker hücumlarına məruz qalmış web-serverlərin loq fayllarını analiz etmək təklif edilir.

Loq fayllar ekspertlər tərəfindən nəzərdən keçirilir və orada özündə hücumu əks etdirən sorğular işarə edilir. HTTP hücum sorğularını əks etdirən requlyar ifadələrin avtomatik yaradılması üçün genetik alqoritmlər tətbiq edilmişdir. Genetik alqoritmlər loq faylları analiz edir, orada özündə hücumu əks etdirən sorğuların requlyar ifadələr dilində avtomatik ifadə edilməsini təmin edir. Modelin çıxışında HTTP hücum sorğularının ifadə edilməsi üçün requlyar ifadələr dilində signaturalar əldə edilir.

Giriş. Web texnologiyası əsasında işləyən istənilən informasiya portalının HTTP sorğularının [1] analiz edilməsinə və hücumlardan mühafizə olunmasına ehtiyacı var [2]. Belə bir mühafizəni təmin etmək üçün karantin sisteminin yaradılması və HTTP sorğuların analiz edilməsi təklif edilir. Karantin sistemi web-serverə edilən HTTP müraciətləri analiz edərək hücumları aşkar edir və onların qarşısını alır.



Şəkil 1. Karantin sisteminin konseptual sxemi

Hücumları identifikasiya etmək üçün istifadə edilən biliklər çoxluğuna siqnaturalar bazası deyilir. Bazanı təşkil edən siqnaturalar ekspertlər tərəfindən verilmiş requlyar ifadələrdən [3] ibarətdir.

Təhlükəsizliyin təmin edilməsi üçün təklif edilmiş karantin sisteminin gücü onun siqnaturalar bazasının böyüklüyündədir. Siqnaturalar bazası nə qədər güclü və dəqiq olarsa, karantin sistemi də sorğuları bir o qədər dəqiq qiymətləndirir və HTTP hücumlarını dayandıra bilər. Başqa sözlə, karantin sisteminin immuniteti siqnaturalar bazasının gücündədir.

Məsələnin qoyuluşu. Siqnaturaların əldə edilməsi üçün mənbə (cert.org, securityfocus.com) o qədər də böyük deyil. Bazada olan siqnaturalar isə ya müasir dövr üçün “köhnəlmiş” ola, ya da ki, bütün mümkün növ hücumların qarşısını almaq üçün kifayət etməyə bilər. Ekspertlər tərəfindən yeni siqnaturalar yaradılıb bazaya əlavə edilə bilər. Lakin bu üsul bir o qədər də effektiv deyil. Yeni yaradılacaq siqnaturaların “yanlış müsbət” (false positive) və “yanlış mənfi” (false negative) qiymətləndirilmələrindən yayınmasını əvvəlcədən demək çox çətin olacaq. Buna görə də web-sistemin hücumlardan mühafizə edən karantin sisteminin immunitetini gücləndirmək üçün hücumlara məruz qalmış web-serverlərin loq fayllarından istifadə etmək təklif olunur. Loq faylları analiz edərək hakerlərin göndərdiyi sorğuları öyrənmək və bu biliklər əsasında karantin sisteminin immunitetini həmin hücumla qarşı möhkəmləndirmək lazımdır.

Yeni hücum növlərinin dayandırılması üçün özündə hücumu əks etdirən sorğu tədqiq edilməli və requlyar ifadələr dilində ehtiva edən siqnatura yaradılmalıdır ki, göstərilmiş tip sorğuları mütləq tutsun və özündə heç bir hücum əks etdirməyən sorğuları isə web-serverə yönəlsin. Karantin sisteminin immunitetinin gücləndirilməsi üçün loq faylların avtomatik analizini həyata keçirmək üçün genetik alqoritmlərdən istifadə etmək təklif olunur.

Haker hücumuna məruz qalmış web-serverlərin loq fayllarını əvvəlcə ekspertlər xüsusi proqram təminatı ilə araşdırır və özündə hücumu əks etdirən sorğuları işarə edirlər. Adətən belə loq faylların həcmi 100-lərlə meqabayta bərabər olur. Bu isə ekspertlər üçün qiymətləndirməni həyata keçirməyə çətinliklər yaradır. Buna görə də təklif olunur ki, əvvəlcə loq fayllar statistik olaraq araşdırılsın və yalnız şübhəli sayılan sorğular onların içindən ayrılınsın. Bu filtrasiyanı həyata keçirmək üçün xüsusi alqoritmləri [4] istifadə etmək olar. Bundan sonra isə əldə edilmiş kiçik loq fayllar qiymətləndirilmək üçün ekspertlərə təqdim edilir.

Ekspertlər tərəfindən loqların qiymətləndirilməsi. Xüsusi proqram təminatından istifadə etməklə loq faylların sətirləri daha oxunaqlı şəkildə ekspertlərə təqdim edilir və ekspertlərə loq faylda heç bir dəyişiklik etmədən hücumları identifikasiya edirlər. Əks halda, loq faylda ediləcək hər hansı bir dəyişiklik yeni yaradılacaq siqnaturaya təsir göstərə bilər.

Ekspertin qiymətləndirməsinin nəticəsi kimi loq faylın hər bir sətiri aşağıdakı qiymətlərdən birini alacaq:

- Zəmanət verilir ki, hücum deyil;
- Ola bilər ki, hücumdur;

- Zəmanət verilir ki, hücumdur;
- Məlum deyil, qeyd edilməyib;

Sistemin işləməsində bu qeydlərin rolu daha sonra bu məqalədə qeyd ediləcəkdir. Qeyd etmək lazımdır ki, yaradılacaq siqnaturaların düzgünlüyü bu mərhələnin düzgün həyata keçirilməsindən asılıdır.

Sistem verilmiş sorğular üzərində onların qeydlərinə əsaslanaraq işləyir və genetik alqoritmlər [5] əsasında həmin sorğulara uyğun siqnaturalar yaradır. Başqa sözlə desək, ekspert əldə edilmiş loqları təsnif edir və ya riyazi dildə desək, “statuslar” çoxluğunda “sorğular” çoxluğunu göstərir. Məsələn, əgər sorğu əlifbası ASCİİ kodlardan təşkil olunmuş bir neçə sözdən ibarətdirsə, onda sorğunun bu və ya digər sinfə aid olmasını aşağıdakı funksiya ilə göstərmək olar:

$$\theta(Q) = \begin{cases} 1 & , \text{əgər hücum olmasına zəmanət verilsə;} \\ 0.5 & , \text{əgər hücum ola bilsə;} \\ 0 & , \text{əgər hücum olmamasına zəmanət verilsə.} \end{cases}$$

Artıq qeyd etdiyimiz kimi, biz siqnaturaları requlyar ifadələrin əsasında yaradacağıq. Bundan başqa bizdə siqnaturaların yaradılmasının düzgünlüyünü yoxlayan və seçilmiş sorğular üzrə keçərək bu siqnaturaların effektivliyini təyin edən requlyar ifadələr professoru vardır.

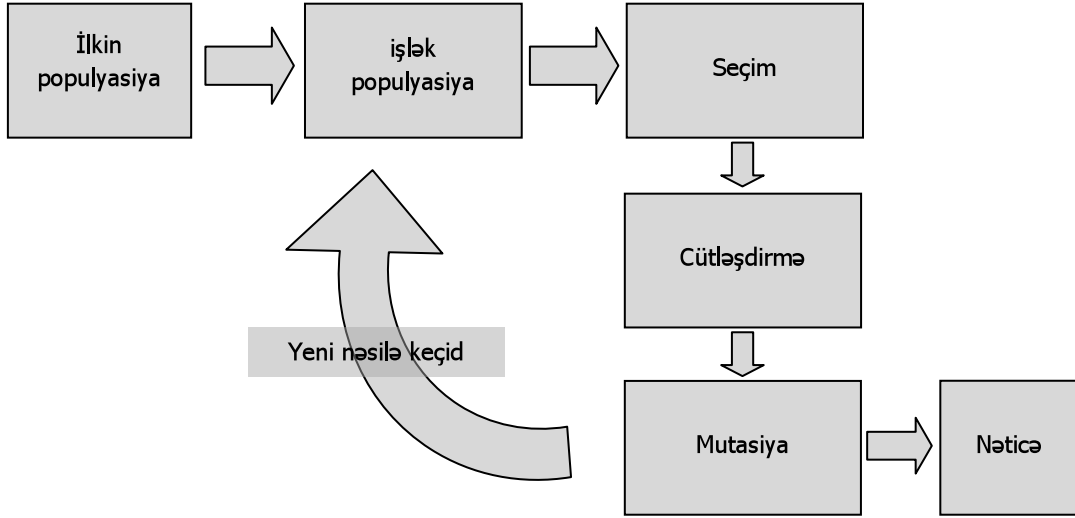
Bu halda, yuxarıda göstərilən terminlər ilə bu məsələnin formalaşdırılması, məsələn, belə bir şəkildə göstərilə bilər: requlyar ifadələr əlifbasındakı sözlə ASCİİ kodlar əlifbasındakı sözün elə təsvirini tapmaq lazımdır ki, müvafiq siqnaturaların effektivliyini maksimizasiya etsin.

Aydındır ki, siqnatura o vaxt maksimum effektiv sayılır ki, “hücum olmasına zəmanət verilən” sinifdən heç olmasa bir elementi tutur və “hücum olmamasına zəmanət verilən” sinifdən heç bir sorğunu tutmur.

Əsas nəticələr. Bu məsələnin həllinin tapılmasının avtomatlaşdırılması üçün axtarışın güclü və nisbətən sürətli metodu kimi, genetik alqoritmlərdən istifadə olunması təklif olunur. Təbii ki, bu metodun seçilməsi ortaya müəyyən tələblər qoyur [6]. Bu, sistemi çətinləşdirməkdən və ya zəiflətməkdənsə, onu daha güclü və daha effektiv edir. Məsələnin həllinin reallaşdırılmasının hər bir mərhələsini ayrı-ayrılıqda təsvir edək.

Əvvəlcə “hücum olmasına zəmanət verilən” sinifdən hər hansı bir Q sorğusunu seçək. İndi isə, güman edək ki, biz bir neçə W requlyar ifadəsini əvvəlcədən müəyyən etmişik. “Hücum olmasına zəmanət verilən” sinifdən tutulan sorğuların sayını $\lambda(w)$ ilə, “hücum olmamasına zəmanət verilən” sinifdən tutulan sorğuların sayını isə $\bar{\lambda}(w)$ ilə işarə edək. Onda sorğunun effektivliyi funksiyasını $f(w, Q, \lambda(w), \bar{\lambda}(w))$ və ya qısa-saca olaraq $f(w, Q)$ ilə işarə edək. İndi isə, bizim alqoritmin funksional blokunun təsvirinə keçmək olar.

Klassik genetik alqoritmlər aşağıdakı sxem üzrə işləyir:



Şəkil 2. Klassik genetik alqoritmlərin işləmə prinsipi.

Bizim məsələmizin terminləri ilə desək, bu təqribən belə görünür: Əvvəlcə biz başlanğıc populyasiyanı yaradırıq. Sonra bu populyasiyanın hər bir $f(w)$ fərdinin uyğunlaşma qabiliyyətini qiymətləndiririk. Bundan sonra isə daha çox uyğunlaşa bilən – nisbi uyğunlaşması maksimal olan elementləri seçimini həyata keçiririk. Onları cütləşdiririk və onların ən yaxşı keyfiyyətlərini özündə birləşdirən, lakin onlardan fərqlənən yeni nəsil əldə edirik. Sistemin parametrlərinə müvafiq olaraq mutasiyanı həyata keçiririk. Alınmış yeni fərdin uyğunlaşa bilmə qabiliyyətini qiymətləndiririk. Alınmış yeni fərddi populyasiyaya əlavə edirik. Ola bilər ki, bu zaman əvvəlki populyasiyada ən pis fərdləri ləğv edirik. Bununla isə biz yeni populyasiya əldə edirik. Bir daha populyasiyanın nisbi uyğunlaşa bilmə qabiliyyətini qiymətləndiririk və s. İndi isə bütün bunları daha ətraflı təsvir edək.

Dəyişənlərin kodlaşdırılması. Genetik alqoritmlərdə dəyişənlərin kodlaşdırılmasının ən effektiv formalarından biri binar (ikilik) formada kodlaşdırmaadır. Bunun üçün bizə requlyar ifadələr əlifbasının hərflərinin sayını bilmək lazımdır. Tutaq ki, bütün əlifbanı təsvir etmək üçün bizə M sayda bit kifayət edər. Bundan başqa fərz edək ki, son nəticədə alınacaq requlyar ifadənin uzunluğu L sayda hərfdən çox ola bilməz. Bu o deməkdir ki, alınacaq requlyar ifadəni kodlaşdıran xromosom $L \cdot M$ sayda bitdən ibarət olacaq. Bu halda isə bütün mümkün xromosomların sayı 2^{LM} olacaq. Aydınır ki, bu qədər variantların arasında ən yararlı xromosomun axtarılıb tapılması yalnız $L \cdot M$ hasilinin kiçik bir ədəd olması zamanı mümkündür.

Populyasiyanın yaradılması. Populyasiyanın ilkin yaradılması zamanı oraya bir neçə hücumlara qarşı artıq mövcud olan sadə signatura-

ları əlavə etmək yaxşı olar. Bu, gələcək nəsillərin yaradılması prosesinin düzgün istiqamətə yönəldilməsinə kömək edəcək. Lakin bunu etmək vacib deyil. Başlangıç populyasiya üçün böyük sayda müxtəlif fərdlər yaratmaq kifayət edər. Bu, axtarışı sürətləndirər və onun effektivliyini artırır.

Signaturaların effektivliyinin qiymətləndirilməsi. Artıq qeyd etdiyimiz kimi, signaturaların effektivliyinin qiymətləndirilməsi üçün $\lambda(w)$ və $\bar{\lambda}(w)$ qiymətlərini hesablamaq lazımdır. Ondan sonra isə artıq $f(w, Q) = f(w, Q, \lambda(w), \bar{\lambda}(w))$ qiymətini hesablamaq olar.

Tutaq ki, bizim populyasiyada fərdlərin sayı M , “hücum olmasına zəmanət verilən” sinifdə elementlərin sayı N və “hücum olmamasına zəmanət verilən” sinifdə isə elementlərin sayı \bar{N} -dir. Bu siniflərin elementləri müvafiq olaraq Q və \bar{Q} ilə işarə ediləcəklər. Bundan başqa, $[w \mapsto Q]$ predikatı w requlyar ifadəsinin Q sorgusunu tutması halında 1 qiyməti, əks halda isə 0 qiyməti alacaq. Onda populyasiyanın elementinin $f(w, Q)$ effektivliyini, məsələn, aşağıdakı düstur ilə hesablamaq olar:

$$\lambda(w) = \sum_{i=1}^N [w \mapsto Q_i]; \quad \bar{\lambda}(w) = \sum_{i=1}^{\bar{N}} [w \mapsto \bar{Q}_i]$$

$$f(w, Q^*) = [w \mapsto Q^*] \cdot (\lambda(w) - \bar{\lambda}(w)) - [w \mapsto \bar{Q}_i] \cdot \bar{N}$$

Burada Q^* hər hansı bir sorgudur. Onun hücum olması və ya olmaması burada nəzərə alınmır. Yuxarıdakı düsturu nəzərə alaraq, bütün populyasiyanın uyğunlaşa bilmə qabiliyyətini aşağıdakı düsturla hesablamaq olar:

$$f(Q^*) = \max_{j=1, M} f(w_j, Q^*)$$

Onda populyasiyanın hər bir fərdinin nisbi uyğunlaşa bilmə qabiliyyəti aşağıdakı düsturla hesablanmalıdır:

$$\mu(w, Q^*) = \begin{cases} \frac{f(w, Q^*)}{f(Q^*)} & , \text{əgər } f(Q^*) \neq 0 \\ 0 & , \text{əgər } f(Q^*) = 0 \end{cases}$$

Seçim. Genetik alqoritmlərdə seçimin həyata keçirilməsi alqoritmləri olduqca müxtəlifdir [7]. Bu metodların əksəriyyətində fərdin seçilməsinin ehtimalı onun nisbi uyğunlaşa bilmə qabiliyyətinə proporsionaldır. Bunu həyata keçirməyin ən sadə üsulu populyasiyanın elementlərinin nisbi uyğunlaşa bilmə qabiliyyətinə görə azalan sıra ilə düzülməsi və bu sıradan ilk C elementin seçilməsidir.

Cütləşdirmə, mutasiya və yeni nəslin yaradılması. Cütləşdirmə crossover operatoru [8] ilə həyata keçirilir. Bu operatorun da variasiyaları müxtəlifdir. Məsələn, birnöqtəli, çoxnöqtəli, bircinsli və s. Krosso-

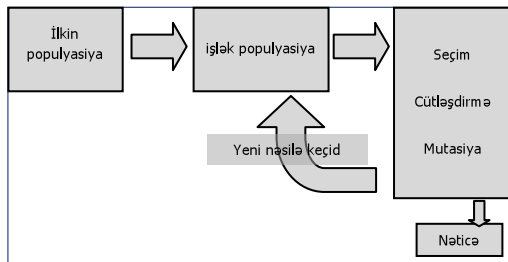
ver operatorunun tətbiqi nəticəsində 1, 2 və ya daha çox övlad alınabilir.

Yeni alınmış övladların hər birini mutasiyaya düşür etmək olar. Mutasiya operatorları da sayına görə çoxdur. Amma yeni alınmış xromosomun mutasiyaya uğradılması üçün onun müxtəlif pozisiyalarındakı təsadüfi bitlər invertasiya edilir. Adətən yeni alınmış övladları dərhal populyasiyaya daxil edirlər. Bəzən isə onları populyasiyaya əlavə etməzdən əvvəl onların effektivliyini yoxlayır və yalnız ən effektivləri populyasiyaya daxil edirlər. Bu zaman köhnə nəslin ən az uyğunlaşa bilən fərdlərini ləğv edirlər.

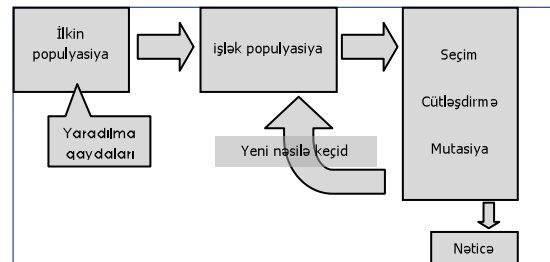
Dayandırılma kriteriyası. Adətən dayandırılma kriteriyası kimi populyasiyanın heç olmasa bir fərdinin məsələnin həllinə yararlılığı şərtini ödəməsi götürülür. Bizim baxdığımız halda şərtin ödənməsi kimi requlyar ifadənin “hücum olmasına zəmanət verilən” sinifdən axtarılan sorğunu tutması və “hücum olmamasına zəmanət verilən” sinifdən heç bir sorğunu tutmaması hesab edilə bilər. Lakin əvvəlcədən təyin olunmuş sayda populyasiyanın yaradılması həyata keçirilir və yenə də axtarılan requlyar ifadə tapılmırsa, onda son ana qədər yaradılmış populyasiyanın fərdləri arasından ən yararlısı seçilir. Bu halda ekspertlər özləri tətbiq olunmuş alqoritmlərin hansını dəyişmək və ya axtarılan requlyar ifadənin L uzunluğunu necə dəyişmək lazım olduğunu müəyyən etməlidirlər. Bundan sonra isə şəkil 2-də göstərilən proses yenidən başlandı.

İdeyanın gələcək inkişafı. Təklif edilmiş modelin işinin effektivliyinin artırılması üçün populyasiyanın yaradılması zamanı xüsusi qaydalara [9] riayət edilməsi tövsiyə edilir. Bu qaydalar **ilkin populyasiyada** istifadəyə yararsız, mənasız xromosomların olmasının qarşısını alacaq. Qaydaları həmçinin cütləşdirmə və mutasiya proseslərindən sonra əldə edilmiş xromosomları yeni populyasiyaya əlavə etməzdən əvvəl də tətbiq etmək olar. Amma onu da qeyd etmək lazımdır ki, bu qaydalar lazımsız xromosomları populyasiyadan silməməlidirlər. Bu qaydalar requlyar ifadədəki kritik səhvləri aradan qaldıraraq xromosomun işə yararlılığını artırmağa xidmət etməlidirlər. Əgər tətbiq ediləcək qaydalar populyasiyadan yararsız hesab etdiyi xromosomları silərsə, populyasiya zəifləyər və ya tamamilə məhv ola bilər.

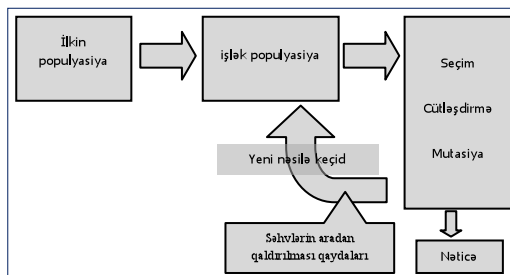
Təklif edilmiş metodda qaydaları iki yerdə tətbiq etmək olar: ilkin populyasiyanın yaradılması zamanı və mutasiyadan sonra. Bununla da sistemdə qaydaların tətbiqinin 4 müxtəlif versiyası ola bilər:



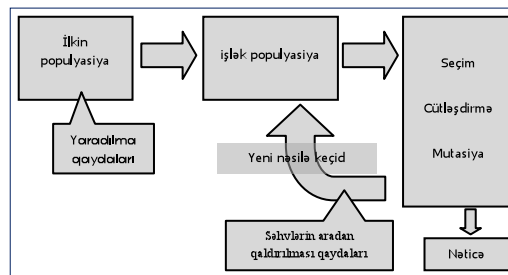
Şəkil 3. Heç bir qayda yoxdur.



Şəkil 4. Yaradılma qaydaları var.



Şəkil 5. Səhvləri aradan qaldıran qaydaları var.



Şəkil 6. Qaydalar hər iki yerdə tətbiq edilir.

İlkin populyasiyanın yaradılması zamanı qaydaları təklif edilmiş metoda generator kimi və ya filter kimi əlavə etmək mümkündür. Təvsiyə olunur ki, ilkin populyasiyanın yaradılması zamanı qaydalar generator kimi tətbiq edilsin. Filterə nisbətən generator daha qısa zamanda daha işə yararlı genlər verir.

Nəticə. Bütün prosesin sona çatması və müvafiq requlyar ifadələrin əldə edilməsindən sonra, həmin ifadələr bir daha “qeyd edilməyən” sorğular sinfinə daxil olan elementlər üzərində bir daha sınaqdan keçirilir və karantin sisteminin signaturalar bazasına daxil edirlər. Bazaya daxil edilərkən yeni signaturaların çəki əmsalları kimi onların nisbi uyğunlaşa bilmə əmsalı seçilir.

Praktika göstərir ki, genetik alqoritmlər axtarış aparmaq üçün mövcud olan digər alqoritmlərə nisbətən məsələnin həllini əhəmiyyətli dərəcədə tez tapırlar. Bu metodun əsas üstün və eyni zamanda mənfi cəhəti ondadır ki, genetik alqoritmlərin çoxsaylı tipləri və strukturları arasında böyük seçim etmək lazım gəlir. Bu isə metodların praktiki tətbiqi zamanı müəyyən çətinliklər törədir. Lakin onu da qeyd etmək lazımdır ki, bir dəfə yaxşı təyin olunmuş və axtarılan requlyar ifadələri təyin edən struktur, ondan sonra həmişə düzgün işləyəcək və məsələnin həlli üçün lazım olan güclü signaturaları təyin edəcək. Bununla da, təklif edilmiş metod sistem administratoruna karantin sisteminin immunitetini gücləndirməyə böyük kömək göstərəcək.

ƏDƏBİYYAT

1. R.Fielding et al. Hypertext Transfer Protocol – HTTP/1.1. RFC 2616, June 1999
2. W.Lee and S.Stolfo. A Framework for Constructing Features and Models for Intrusion Detection Systems. ACM Transactions on Information and System Security, 3(4), November 2000
3. Jeffrey Friedl, Mastering Regular Expressions, August 2006. ISBN: 9780596528126 (0596528124). 512 p.
4. Christopher Kruegel, Giovanni Vigna. Anomaly Detection of Web-based Attacks. October 27–31, 2003, Washington, DC, USA: ACM. 251-261
5. Darrel Whitley "A Genetic Algorithm Tutorial", 1993.
6. Mitchell M. An Introduction to Genetic Algorithms. Cambridge, MA: The MIT Press, 1996.
7. Holland J.H. Adaptation in natural and artificial systems. An introductory analysis with application to biology, control, and artificial intelligence.— London: Bradford book edition, 1994 —211 p.

8. Вороновский Г.К., Махотило К.В., Петрашев С.Н., Сергеев С.А., Генетические алгоритмы, искусственные нейронные сети и проблемы виртуальной реальности, Харьков, ОСНОВА, 1997. – 112с.
9. M.J.FOSTER. Avoiding Latch Formation in Regular Expression Recognizers. IEEE TRANSACTIONSON COMPUTERS, VOL.38, NO.5, MAY 1989. IEEE Log Number 8825684. 3 p.

ПРИМЕНЕНИЕ ГЕНЕТИЧЕСКИХ АЛГОРИТМОВ ДЛЯ РАСПОЗНАВАНИЯ HTTP-АТАК

Р.Ф.ФАРАДЖУЛЛАЕВ

РЕЗЮМЕ

Актуальность веб-программ повышается с каждым днём. Поэтому актуальной является и задача обеспечения их безопасности. Важной задачей является создание сигнатур для определения в системах выявления того, является ли идущий от пользователя HTTP-запрос атакой, или нет и предотвращения этих атак. Обычно эти сигнатуры создаются на языке регулярных выражений, идентифицируют атаки и определяют класс, к которому они относятся. Создание таких сигнатур инженерами вручную может привести к неверной оценке (фалсе позитиве, фалсе негативе). Поэтому для создания сигнатур предлагается анализировать лог-файлы веб-сервера, подвергшегося атаке хакера.

Лог-файлы проверяются экспертами и отмечаются запросы, отражающие в себе атаки. Были применены генетические алгоритмы для автоматического создания сигнатур на языке регулярных выражений, отражающих запросы, являющимися HTTP-атаками. Генетические алгоритмы анализируют лог-файлы, обеспечивают автоматическое выражение на языке регулярных выражений запросов, отображающих атаки. В результате получается сигнатуры на языке регулярных выражений для выдачи запросов, являющимися HTTP-атаками.

APPLYING GENETIC ALGORITHMS TO RECOGNIZE HTTP ATTACKS

R.F.FARADJULLAYEV

SUMMARY

Topicality of web applications is growing day by day. That is why providing their security is a very topical problem. Creating signatures for estimating HTTP queries coming from users which detect and prevent attacks is a very important issue. These signatures are usually in the language of regular expressions and identify attacks and determine their class they belong to. Such signatures may cause false positive and false negative estimations when they are created by engineers manually. Hence, for automatic formation of these signatures it's offered to analyze log files of web servers suffered from hacker attacks.

Log files are looked through by experts and HTTP queries reflecting threats are marked. Genetic algorithms have been applied for automatic creation of regular expressions reflecting HTTP queries. Genetic algorithms analyze log files and supply automatic expression in the language regular expressions of HTTP queries reflecting attacks. As the output of the suggested model, signatures in the language of regular expressions reflecting attacks are obtained.