STRESZCZENIA

Piotr HADAJ[1]
Marek NOWAK[2]

MPPT ALGORITHMS USED IN PHOTOVOLTAICS

Due to volatility of current-voltage characteristics of the photovoltaic module, MPPT algorithms are important element of photovoltaic power station. In most cases, MPPT algorithm controls power electronics converter, which receives power directly from one or more modules. Maximum power point changes its location together with insolation level temperature changes. There are also indirect, direct and artificial intelligence supported methods. Indirect methods are fractional methods and look-up table. Direct methods are Perturb & Observe and Incremental conductance. Direct algorithms are widely used, because of their ability to model maximum power point significantly better than indirect methods. Artificial intelligence supported methods obtain even better results in determining optimal operating conditions. Usage of these algorithms allows to increase the efficiency of energy production, and furthermore financial benefits. Investment payback time can also be shortened by using these methods, which are still being improved.

Keywords: MPPT, photovoltaics, perturb and observe, incremental conductance, direct algorithms, indirect algorithms.

ALGORYTMY MPPT STOSOWANE W FOTOWOLTAICE

S t r e s z c z e n i e

Ze względu na zmienność charakterystyki prądowo-napięciowej modułu fotowoltaicznego, algorytmy MPPT są ważnym elementem elektrowni fotowoltaicznej. Algorytm MPPT najczęściej steruje przekształtnikiem energoelektronicznym, który bezpośrednio odbiera moc z modułu lub grupy modułów. Punkt mocy maksymalnej zmienia swoje położenie, wraz ze zmianą nasłonecznia i temperatury pracy modułu. Istnieją metody pośrednie, bezpośrednie i wspomagane sztuczną inteligencją. Do metod pośrednich możemy zaliczyć m. in. metody ułamkowe i metodę look-up table, do bezpośrednich algorytm Perturb & Observe oraz Incremental conductance. Szerzej stosuje się algorytmy bezpośrednie, gdyż lepiej odwzorowują punkt mocy maksymalnej od metod pośrednich, a wspomagane sztuczną inteligencją pozwalają jeszcze lepszym stopniu wyznaczyć optymalne warunki pracy. Stosowanie tych algorytmów pozwala zwiększyć efektywność produkcji energii, a tym samym korzyści finansowe po może znacząco skrócić czas zwrotu inwestycji. Są one w dalszym ciągu udoskonalane.

Słowa kluczowe: MPPT, fotowoltaika, zaburz i obserwuj, konduktancja przyrostowa, algorytmy bezpośrednie, algorytmy pośrednie

DOI: 10.7862/re.2016.6

Tekst złożono w redakcji: maj 2016
Przyjęto do druku: czerwiec 2016

[1] Piotr Hadaj, Department of Power Electronics, Power Engineering and Complex Systems, Rzeszów University of Technology, ul. Wincentego Pola 2, 35-959 Rzeszów, 178651772, e-mail: piotr.hadaj@prz.edu.pl
[2] Corresponding author: Marek Nowak, Department of Power Electronics, Power Engineering and Complex Systems, Rzeszów University of Technology, ul. Wincentego Pola 2, 35-959 Rzeszów, 178651772, e-mail: mnowak@prz.edu.pl

Mariusz SZAREK[3]
Mariusz NYCZ[4]
Piotr HAJDER[5]

BADANIE SPRAWNOŚCI SYSTEMÓW IDS/IPS PRZED ATAKAMI DOS I DDOS

Tematem artykułu jest analiza sprawności systemów wykrywania i zapobiegania włamaniom przed atakami odmowy usługi. W początkowej cześć artykuł w oparciu o wynik analiz, zaprezentowano skalę problemu omawianych zagrożeń. W kolejnych paragrafach przedstawiono metodykę badań określenia podatności na ataki odmowy usługi. Następnie przeprowadzono symulacje wydajności i skuteczności obrony przed atakami dwóch sieciowych systemów wykrywania włamań w segmencie open-source Snort i Suricata. Analizowano rozwiązania pracując w trybach nfqueue i af-packet, przy zestawie tych samych reguł. Przeprowadzone testy porównawcze z wykorzystaniem dwóch najpopularniejszy zagrożeń tj. Land i SYN Flood, wykazały przewagę rozwiązania Suricata w skuteczności wykrywania analizowanych ataków. Artykuł jest adresowany do osób zajmujących się wdrażaniem i administracją systemów zabezpieczeń.

Słowa kluczowe: sieci, bezpieczeństwo, ochrona, testy, odmowa, usługi, wykrywanie, wtargnięcie, przeciwdziałanie

EFFICIENCY TEST OF IDS/IPS SYSTEMS AGAINST DOS AND DDOS ATTACKS

S u m m a r y

The theme of the article is to analyze the efficiency of detection systems and intrusion prevention against denial of service attacks. In the initial part of the article based on the analysis results, presented the scale of the problem of these threats. In the following paragraphs, the methodology of testing to determine susceptibility to denial of service attack. Then conducted simulations effectiveness and efficiency of defense against attacks by the two network intrusion detection systems in the segment of open-source Snort and Suricata. Analyzed solutions working modes nfqueue and af-packet, using the same set of rules. Comparative tests carried out using the two most common threats such Land and SYN Flood, showed superiority solutions Suricata the effectiveness of detection of the analyzed attacks. The article is addressed to people involved in the implementation and administration of security systems.

Keywords: networks, security, protection, tests, denial, service, detection, intrusion, counteraction

DOI: 10.7862/re.2016.7

Tekst złożono w redakcji: maj 2016
Przyjęto do druku: czerwiec 2016

[3] Mariusz Szarek, Politechnika Rzeszowska, 783535006, 132887@stud.prz.edu.pl
[4] Autor do korespondencji: Mariusz Nycz, Politechnika Rzeszowska, Katedra Energoelektroniki, Elektroenergetyki i Systemów Złożonych, mnycz@prz.edu.pl
[5] Piotr Hajder, Akademia Górniczo-Hutnicza, piootr.hajder@gmail.com

Paweł SZELIGA[6]
Mariusz NYCZ[7]
Sara NIENAJADŁO[3]

ANALIZA PODATNOŚCI SERWERÓW WWW W ODNIESIENIU DO ATAKÓW ODMOWY USŁUGI

Artykuł jest adresowany w głównej mierze do osób zajmujących się bezpieczeństwem serwerów WWW. Praca rozpoczyna się od przedstawienia statystycznego ujęcia problemu, jakim są ataki DDoS. Autorzy kładą szczególny nacisk na problematykę ochrony serwerów przed szybko rozwijającymi się atakami odmowy usługi. W pracy przeanalizowano odporności podstawowych konfiguracji dla najpopularniejszych obecnie serwerów web. Na potrzeby badań zostało opracowane wirtualne środowisko testowe, na którym zrealizowano badania podatności wybranych systemów WWW. Celem wykonanej analizy jest rozpoznanie oraz omówienie podstawowych podatności serwera Apache oraz serwera IIS. Dla każdego z omawianych serwerów WWW autorzy zaimplementowali podstawowe mechanizmy ochrony. Artykuł jest adresowany do osób zajmujących się analizą oraz bezpieczeństwem serwerów web.

Słowa kluczowe: DDoS, ochrona, bezpieczeństwo, podatność serwerów WWW, Apache, IIS.

VULNERABILITY ANALYSIS OF WEB SERVERS IN REFERENCE TO DENIAL-OF-SERVICE ATTACKS

S u m m a r y

The article is addressed primarily to those involved in the security of web servers. The work begins with the presentation of statistical treatment of the problem, which are DDoS attacks. The authors emphasize the problems of server protection against rapidly-evolving attacks denial of service. The study analyzed the resistance of the basic configuration for today's most popular web server. For the study, we have developed a virtual test environment, where the research was carried out vulnerability of selected sites. The aim of this analysis is to identify and discuss the fundamental vulnerability of Apache and IIS. For each of the Web servers authors have implemented the basic mechanisms of protection. The article is addressed to people involved in the analysis and the security of web servers.

Keywords: DDoS, security, protect, the vulnerability of web servers, Apache, IIS.

DOI: 10.7862/re.2016.8

Tekst złożono w redakcji: maj 2016
Przyjęto do druku: czerwiec 2016

[6] Paweł Szeliga, Politechnika Rzeszowska im. Ignacego Łukasiewicza, Wydział Elektrotechniki i Informatyki, email: polozaq1@wp.pl
[7] Autor do korespondencji: Mariusz Nycz, Politechnika Rzeszowska im. Ignacego Łukasiewicza, Katedra Energoelektroniki, Elektroenergetyki i Systemów Złożonych, mnycz@prz.edu.pl
[3] Sara Nienajadło, Politechnika Rzeszowska im. Ignacego Łukasiewicza, Wydział Elektrotechniki i Informatyki, email: sara.n@op.pl

Michał DYMEK[8]
Mariusz NYCZ[2]
Alicja GERKA[3]

ANALIZA STATYCZNYCH METOD OBRONY PRZED ATAKAMI SQL INJECTION

W artykule zaprezentowano analizę podatności systemów bazodanowych na ataki typu SQL Injection. Praca rozpoczyna się od przedstawienia charakterystyki analizowanego ataku w kontekście baz danych. Bazy danych, pomimo kluczowego znaczenia w infrastrukturze wszelakich systemów odznaczają się niedostatecznym poziomom zabezpieczeń, co w konsekwencji może prowadzić do poważnych strat. Podstawowym zagrożeniem są ataki SQL Injection, na które obecnie nie występują zewnętrzne mechanizmy obrony. W tym celu zostało zaproponowane rozwiązanie zabezpieczające systemy bazodanowe polegające na odpowiednim przygotowaniu kodu, który obsługuje dynamiczne zapytania do bazy danych. Testy wykazały dużą skuteczność zabezpieczeń przed aktualnie znanymi atakami SQL Injection. Artykuł adresowany jest do administratorów baz danych w szczególności na potrzeby usług webowych.

Słowa kluczowe: bazy danych, bezpieczeństwo, podatność, sqlmap

ANALYSIS OF STATIC METHODS OF DEFENSE AGAINST SQL INJECTION

S u m m a r y

The article presents an analysis of SQL Injection vulnerabilities. The work begins with the presentation of the characteristics of the attack analyzed in the context of database. Databases, despite the key role in the infrastructure of many kinds of systems are characterized by insufficient level of security, which in turn can lead to serious loses. The main threat are SQL Injection attacks, which currently does not have external defense mechanisms. For this purpose, there is a solution to increase the security of database systems, involving the proper preparation of the code that supports dynamic database queries. Tests have shown high effectiveness of protection against currently known SQL Injection attacks. Article is aimed at database administrators in particular for Web services.

Keywords: databases; security; vulnerability; sqlmap;

DOI: 10.7862/re.2016.9

Tekst złożono w redakcji: maj 2016
Przyjęto do druku: czerwiec 2016

[8]Michał Dymek, Politechnika Rzeszowska, dymek.m@outlook.com
[2]Autor do korespondencji: Mariusz Nycz, Politechnika Rzeszowska, Katedra Energoelektroniki, Elektroenergetyki i Systemów Złożonych, mnycz@prz.edu.pl
[3]Alicja Gerka, Politechnika Rzeszowska, 137406@stud.prz.edu.pl

Dariusz KOWALSKI[9]
Paweł DYMORA[10]
Mirosław MAZUREK[11]

KLASTRY PRACY AWARYJNEJ W ŚRODOWISKU MICROSOFT WINDOWS SERVER 2012

W artykule poruszono temat klastrów pracy awaryjnej w środowisku Microsoft Windows Server 2012. Klastry tego typu działają w oparciu o tzw. elementy quorum (kworum). W Windows Server elementem quorum może zostać węzeł, dysk „świadek" lub plik współdzielony „świadek". Głównym celem artykułu jest porównanie czasów niedostępności usług świadczonych przez wymienione modele klastrów, w przypadku awarii elementów klastra, świadczących wybrane usługi. Analizie poddano architektury: Node Majority (elementy kworum w postaci węzłów klastra), Node and Disk Majority (elementy kworum w postaci węzłów klastra oraz dysku „świadka"), Node and File Share Majority (elementy kworum w postaci węzłów klastra oraz współdzielonego zasobu) oraz No Majority: Disk Only (element kworum w postaci dysku „świadka").

Słowa kluczowe: failover, HA, wysoka dostępność, serwer, klaster

FAILOVER CLUSTERING IN MICROSOFT WINDOWS SERVER 2012

S u m m a r y

The article is all about failover clusters in Microsoft Windows Server 2012. Failover clusters called as well High-Availability Clusters creates a group of servers working together to provide high availability of provided by the cluster services and applications. Client devices see the cluster as a single system. Clusters of this type - in the family of Microsoft Windows Server - are based on element quorum. Quorum in failover clusters is considered as a parts of cluster witch has to be active to allow the cluster to work. Thanks to this each individual node of the cluster can check - by the single query - if the whole cluster can be active. In the MS Windows Server Environment component of a quorum may be for example: node, disk quorum, shared file quorum. The clusters models discussed in the article - provided by MS Windows Server 2012 - include: Node Majority, Node and Disk Majority, Node and File Share Majority and No Majority: Disk Only. The main purpose of the article is to compare the unavailability time of the services provided by these models of clustering in the case of cluster component failure.

Keywords: failover, HA, high availability, server, cluster

DOI: 10.7862/re.2016.10

Tekst złożono w redakcji: maj 2016
Przyjęto do druku: czerwiec 2016

[9] Autor do korespondencji: Dariusz Kowalski, Politechnika Rzeszowska, darkowalski@windowslive.com
[10] Paweł Dymora, Politechnika Rzeszowska, Katedra Energoelektroniki, Elektroenergetyki i Systemów Złożonych, pawel.dymora@prz.edu.pl
[11] Mirosław Mazurek, Politechnika Rzeszowska, Katedra Energoelektroniki, Elektroenergetyki i Systemów Złożonych, miroslaw.mazurek@prz.edu.pl

Bartosz KOWAL[12]
Paweł DYMORA[13]
Mirosław MAZUREK[14]

WYBRANE ATAKI NA SYSTEMY BAZODANOWE

Systemy bazodanowe oraz zawarte w nich dane są jednym z najważniejszych elementów współczesnego świata informatyki. W obecnych czasach rośnie zagrożenie związane z bezpiecznym przechowywaniem danych. Celem tego artykułu jest dokonanie klasyfikacji oraz analizy wybranych typów ataków na system zarządzania bazami danych. W artykule dokonano klasyfikacji ataków, scharakteryzowano i przeprowadzono wybrane ataki na RDBMS w szczególności ataki DoS, wnioskowanie, ataki socjotechniczne, testy penetracyjne, podsłuchiwanie pakietów oraz ataki z wykorzystaniem luk w programach - SQL Injection.

Słowa kluczowe: systemy bazodanowe, ataki na DBMS, SQL Injection, sniffing

ATTACKS ON DATABASES SYSTEMS

S u m m a r y

Database systems and the data they contain, are one of the most important elements of the modern world of computer science. Nowadays, threat greatly increases for the safe storage of data. The purpose of this article is to classify and analyze the selected types of attacks on the database management system. At the beginning selected attacks on the DBMS are classified and described. Afterwards, exemplary attacks were carried out in the test environment. The attacks on the DBMS includes: DDoS attacks, inference, social engineering, penetration test, packet sniffing and attacks using vulnerabilities in programs like SQL Injection.

Keywords: database systems, attacks on DBMS, SQL Injection, sniffing

DOI: 10.7862/re.2016.11

Tekst złożono w redakcji: maj 2016
Przyjęto do druku: czerwiec 2016

[12] Autor do korespondencji: Bartosz Kowal, Politechnika Rzeszowska, b.kowal.1991@gmail.com
[13] Paweł Dymora, Politechnika Rzeszowska, Katedra Energoelektroniki, Elektroenergetyki i Systemów Złożonych, pawel.dymora@prz.edu.pl
[14] Mirosław Mazurek, Politechnika Rzeszowska, Katedra Energoelektroniki, Elektroenergetyki i Systemów Złożonych, miroslaw.mazurek@prz.edu.pl

Maksymilian BURDACKI[15]
Paweł DYMORA[16]
Mirosław MAZUREK[17]

PROGRAMY ANTYWIRUSOWE TYPU KLIENT/CHMURA – PERSPEKTYWY ROZWOJU, WYDAJNOŚĆ, ZAGROŻENIA

W artykule omówiono działanie oprogramowania antywirusowego typu klient/chmura oraz różnice pomiędzy standardowym oprogramowaniem antywirusowym działającym w oparciu o „ciężkiego klienta". Przedstawiono perspektywy rozwoju oprogramowania tego typu. W części badawczej porównano działanie obu typów programów. Dokonano oceny wpływu oprogramowania antywirusowego na wykorzystanie pamięci RAM, użycie procesora oraz wpływu na szybkość działania systemu i wykrywalności złośliwego oprogramowania przez testowane programy antywirusowe.

Słowa kluczowe: architektura klient/chmura, program antywirusowy, sygnatury wirusowe, chmury obliczeniowe.

CLIENT/CLOUD ARCHITECTURE ANTIVIRUS SOFTWARE - DEVELOPMENT PROSPECTS, PERFORMANCE, RISKS

S u m m a r y

The presented article describes issues referring to cloud computing, history of antivirus software, kinds of malicious software and client/cloud antivirus software. The aim of the thesis is comparison of client/cloud antivirus software and standard "fat client" antivirus software. Two "fat client" antiviruses and two client/cloud antiviruses were compared. Influence on system performance and malicious software detection rate were checked during testing. After the research it was possible to draw conclusions about each type of antivirus software.

Keywords: client/cloud antivirus software, cloud computing, computer viruses.

DOI: 10.7862/re.2016.12

Tekst złożono w redakcji: maj 2016
Przyjęto do druku: czerwiec 2016

[15] Autor do korespondencji: Maksymilian Burdacki, Politechnika Rzeszowska, maxb931@gmail.com
[16] Paweł Dymora, Politechnika Rzeszowska, Katedra Energoelektroniki, Elektroenergetyki i Systemów Złożonych, pawel.dymora@prz.edu.pl
[17] Mirosław Mazurek, Politechnika Rzeszowska, Katedra Energoelektroniki, Elektroenergetyki i Systemów Złożonych, miroslaw.mazurek@prz.edu.pl

Bartosz BROŻEK[18]
Paweł DYMORA[19]
Mirosław MAZUREK[20]

BADANIE WYDAJNOŚCI SYSTEMU OPERACYJNEGO ZAINFEKOWANEGO ZŁOŚLIWYM OPROGRAMOWANIEM Z WYKORZYSTANIEM ANALIZY SAMOPODOBIEŃSTWA

W artykule przedstawiono wpływ oprogramowania złośliwego na wydajność systemu operacyjnego z wykorzystaniem aplikacji zbierającej dane oraz analizy obciążenia systemu z użyciem elementów statystyki nieekstensywnej w szczególności samopodobieństwa procesów. Badano wpływ oprogramowania złośliwego w postaci: wirusów, trojanów oraz adware. Zainfekowane systemy operacyjne Windows 8.1 przebadano pod względem ich wpływu na wykorzystanie procesora, pamięci RAM oraz dysku twardego. Wykorzystano wykładnik Hursta do analizy zebranych danych.

Słowa kluczowe: badania wydajnościowe, złośliwe oprogramowanie, analiza samopodobieństwa, Windows Performance Analyzer.

PERFORMANCE TESTING OF THE OPERATING SYSTEM INFECTED BY MALICIOUS SOFTWARE WITH USING OF SELF-SIMILARITY ANALYSIS

S u m m a r y

The purpose of presented article is to show the analysis of the impact of malicious software on operating system performance using application which can collect data about computer resources and it's further analysis with self-similarity. All studies were about viruses, trojans and adware programs. Infected Windows 8.1 Pro were studied by their impact on CPU, RAM memory and HDD, then they were compared with not infected system. For self-similarity tests Hurst exponent was used.

Keywords: performance tests, malicious software, self-similarity analysis, Windows Performance Analyzer.

DOI: 10.7862/re.2016.13

Tekst złożono w redakcji: maj 2016
Przyjęto do druku: czerwiec 2016

[18] Autor do korespondencji: Bartosz Brożek, Politechnika Rzeszowska, bartekbrozek@gmail.com
[19] Paweł Dymora, Politechnika Rzeszowska, Katedra Energoelektroniki, Elektroenergetyki i Systemów Złożonych, pawel.dymora@prz.edu.pl
[20] Mirosław Mazurek, Politechnika Rzeszowska, Katedra Energoelektroniki, Elektroenergetyki i Systemów Złożonych, miroslaw.mazurek@prz.edu.pl