METODY ZABEZPIECZEŃ PRZESYŁU DANYCH W SIECI INTERNET

Mariusz Sojak, Szymon Głowacki, Paweł Policewicz
Katedra Podstaw Inżynierii, Szkoła Główna Gospodarstwa Wiejskiego w Warszawie

Streszczenie. Celem pracy było uświadomienie użytkownikom Internetu, na co są narażeni, gdy korzystają z komputera, który nie jest zabezpieczony przed atakami hakerów. Pokazanie, w jaki sposób dane przesyłane siecią mogą trafić w niepowołane ręce. Informacje te mogą być przydatne zarówno użytkownikom prowadzącym na przykład indywidualne gospodarstwa rolne, jak też innego typu przedsiębiorstwa. W pracy przedstawiono zarówno wybrane metody ataku na transmisję danych przesyłanych drogą internetową, jak też wybrane metody zabezpieczeń, których możemy używać do ochrony informacji.

Słowa kluczowe: metody zabezpieczeń, autoryzacja, uwierzytelnianie, szyfrowanie informacji, podpis cyfrowy, certyfikat cyfrowy

Wprowadzenie

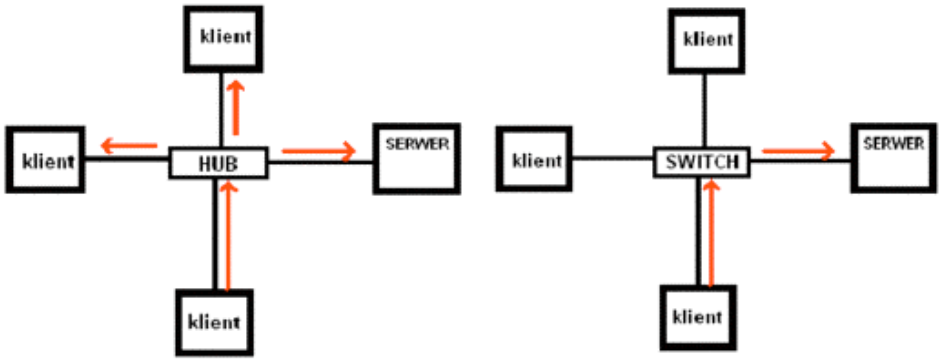
Sieć komputerowa jest to zbiór wielu wzajemnie ze sobą połączonych komputerów. Medium transmisyjnym stanowiącym łącze pomiędzy komputerami w sieci mogą być kable: skrętka ekranowana (STP), foliowana (FTP), foliowana ekranowana (SFTP), nieekranowana (UTP), koncentryczne (coaxial 50 Ω), linie telefoniczne, łącza światłowodowe (jednomodowe i wielomodowe), transmisja może odbywać się również drogą bezprzewodową (np. Wi-Fi, WiMAX, łącza satelitarne) [Sojak 2009]. W momencie korzystania z komputera w warunkach domowych nie zastanawiamy się nad jego fizycznym zabezpieczeniem oraz zagwarantowaniem toku pracy systemu. Firmy świadczące usługi, w tym produkujące dla sektora rolno-spożywczego oraz sektor gospodarki przetwórczej powinny dbać o bezpieczeństwo, bowiem czynnik bezpieczeństwa odgrywa ogromną rolę w serwerach komercyjnych. Systemy te powinny mieć ograniczony dostęp osób trzecich do bezpośredniego łączenia się z nimi.

Wybrane metody ataków na dane przesyłane przez sieć

Sniffing - jest ogólnie wykorzystywanym przez sieciowych włamywaczy sposobem przechwytywania i analizowania informacji przechodzących przez sieć TCP/IP. Technika ta polega na ustawieniu karty sieciowej w tryb promiscuous, przez co osoba niepowołana może zobaczyć wszystkie pakiety w sieci, również te, które nie są kierowane do niej. Gdy sniffer jest zainstalowany na routerze przestawienie trybu karty nie jest konieczne.

Sniffing najczęściej występuje w sieciach lokalnych LAN. W sieci LAN komputery łączą się z routerem poprzez hub lub switch. Metoda przeprowadzenia połączenia wyznacza kto będzie miał możliwość wglądu do wysyłanych i odbieranych przez nas wiadomości. W przypadku sieci wykorzystującej hub, z nadawanych przez nasz komputer pakietów mogą korzystać wszystkie komputery w sieci LAN. Włamywacz, chcąc przeprowadzić proces przechwytywania pakietów musi jedynie uruchomić program sniffujący [Szmit 2005].

W sieciach wykorzystujących przełączniki (switche), porozumiewanie komputerów sprowadza się do wysyłania pakietów między klientem a serwerem z wyeliminowaniem innych hostów. Powoduje to utrudnienie podsłuchu. Na rysunku 1 przedstawiono różnicę w przesyle pakietów w sieci z hubem i switchem.



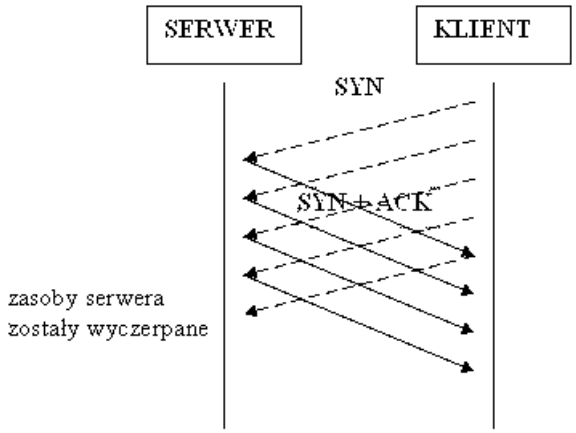
Rys. 1. Różnice w rozsyłaniu pakietów w sieci z hubem i switchem
Fig. 1. Differences in distribution of packages in the Web with hub and switch

Dobrą metodą zabezpieczającą nasze komputery przed sniffingiem jest zaszyfrowanie transmisji danych za pomocą protokołów SSL lub SSH. Możemy także bronić się poprzez wykrycie sniffujacego komputera za pomocą specjalnych programów zwanych antysniffe-rami.

Spoofing - polega na sfałszowaniu źródłowego adresu IP w pakiecie przesyłanym drogą internetową. Prowadzi to do ukrycia tożsamości nadawcy. Metoda ta używana jest w trakcie ataków odmowy dostępu tzw. DDoS (ang. Distributed Denial of Service) jako składnik SYN-floodingu. Zapory przeciwogniowe (firewall) starszego typu nie zabezpieczają przed spoofingiem, niemniej jednak nowe, które są wyposażone w mechanizmy analizujące pakiety od warstwy łącza danych po warstwę aplikacji modelu OSI umożliwiają już realizację złożonej polityki bezpieczeństwa.

SYN-flooding - jest popularnym atakiem sieciowym. Jego celem jest zablokowanie usług danego serwera. Polega on na ataku poprzez wysłanie do serwera dużej liczby pakietów. W każdym z pakietów ustawiona jest flaga synchronizacji (SYN), która informuje serwer o próbie komunikacji z nim. Serwer odpowiadając na pakiety SYN odsyła pakiety z ustawioną flagą synchronizacji i potwierdzenia (SYN, ACK) do komputera wywołujące-

go połączenie. Kolejnym etapem po wysłaniu pakietu jest oczekiwanie na odpowiedź komputera, który zapoczątkował połączenie. Odpowiedź jednak nie nastąpi. Zmusza to serwer do zapisywania w swojej tablicy stanów informacji o próbach uzyskania połączenia. Tablice te są przetrzymywane w pamięci RAM, dlatego ich wielkość jest ograniczona. Wysyłanie bardzo wielu pakietów z ustawiona flagą SYN prowadzi do wyczerpania zasobów serwera, przez co nie udziela on odpowiedzi innym nadawcom. Istnieją przypadki, kiedy atak prowadzi do zawieszenia systemu ofiary. Zasadę działania SYN-floodingu pokazano na rysunku 2.



Rys. 2. Atak SYN-floodingu
Fig. 2. SYN-flooding attack

W przypadku SYN-floodingu sposobem na skuteczną obronę może być zainstalowanie dowolnej zapory przeciwogniowej. Innymi typami ataków polegającymi na tzw. przepełnieniu bufora są: *ICMP flooding (PING flooding)* – metoda ta polega na zalewaniu portów niepożądanymi pakietami ICMP, które z kolei generowane są np. przez program ping. *MAC flooding* - metoda ta wykorzystuje ograniczoną wielkość tablicy Content Addressable Memory (CAM), która po zapełnieniu sprowadza przełącznik (switch) do roli koncentratora (huba). W wyniku tego typu ataku agresor może wykorzystać daną sieć w celu łatwiejszego przeprowadzenia sniffingu.

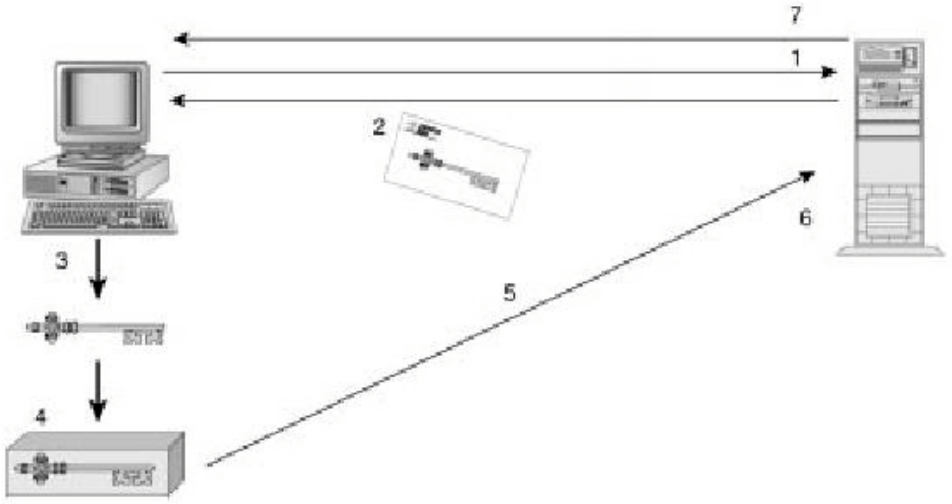
Skanowanie portów - przed włamaniem do komputera haker wyszukuje luki w zabezpieczeniach. Do tego celu służy mu skanowanie portów. Polega ono na wysłaniu pakietów TCP do jednego lub paru komputerów, aby uzyskać informacje o otwartych portach i dostępnych serwisach. Dzieje się to za pomocą skanera portów. Wysyła on pusty pakiet z ustawioną flagą SYN do badanego serwera, następnie czeka na potwierdzenie. W wyniku potwierdzenia otrzymuje pakiet zwrotny z ustawionymi flagami SYN/ACK. W pakiecie tym zawarte są informacje, poprzez które można zidentyfikować system i udostępnione na nim usługi. Do skanowania portów może posłużyć program nmap, którym można zidentyfikować system i zainstalowane na nim usługi.

Zabezpieczenia

Autoryzacja i uwierzytelnianie - umożliwianie dostępu do zasobów komputerowych w Internecie niektórym użytkownikom udzielane jest po stwierdzeniu ich tożsamości. Autoryzacją (authorization) nazywamy proces utwierdzający w przekonaniu, że dany użytkownik jest osobą, za którą się podaje (po dokonaniu uwierzytelnienia) i posiada prawa do używania zasobów, o które zabiega. Użytkownicy, aby wejść np. na daną witrynę WWW muszą wykazać się swoją nazwą i prawidłowym hasłem. Po uwierzytelnieniu (authentication) zostają im przydzielone określone uprawnienia. Pewnym rodzajem uwierzytelnienia uwzględniającym hasło są numery PIN (ang. Personal Identification Number). Celem uwierzytelnienia jest stwierdzenie, czy właściciel karty jest jej legalnym użytkownikiem, czyli czy zna PIN. Innymi metodami uwierzytelnienia są sposoby: rozpoznawania linii papilarnych użytkownika lub układu żył w dłoni, ustalające tożsamość na podstawie obrazu siatkówki oka, rozpoznawania głosu [Wojciechowski 2006].

Szyfrowanie informacji - szyfrowanie jest procesem ochrony komunikacji i danych znajdujących się na dysku komputera w postaci plików. Tego typu ochronę powinny stosować firmy, których działalność związana jest z przetwarzaniem danych oraz ich przesyłem drogą internetową, w tym firmy z sektora gospodarki przetwórczej komunikujące się na przykład z indywidualnymi gospodarstwami rolnymi. Transfer informacji od indywidualnego producenta również powinien podlegać ochronie. W mechanizmie szyfrowania, jak i odczytywania tych danych niezbędne są tzw. klucze do algorytmu szyfrującego. Klucz zazwyczaj stanowi liczbę zapisaną w postaci wyrażenia lub ciągu znaków. Tajne informacje, podczas przesyłania ich poprzez sieć komputerową, powinny być zaszyfrowane. Tak samo należy postępować z plikami zapisanymi na dysku. Tajne dane będą mogły odczytać tylko osoby mające klucz deszyfrujący. Odbiorca informacji może odczytać przesłaną wiadomość tylko wtedy, kiedy zna klucz. Funkcjonowanie współczesnych algorytmów szyfrujących związane jest z dwoma kluczami znanymi jako klucz prywatny i publiczny. Charakterystyczną cechą algorytmów kryptograficznych jest niesymetryczność tych kluczy. Odczytanie informacji zaszyfrowanej kluczem prywatnym możliwe jest tylko wtedy, kiedy znamy klucz publiczny. Osoba nie posiadająca klucza prywatnego nie może zaszyfrować lub podpisać elektronicznie żadnego komunikatu. Szyfrowanie odbywa się także podczas komunikacji przeglądarki internetowej z serwerem WWW za pośrednictwem protokołu HTTPS (HyperText Transfer Protocol Secure). Połączenie szyfrowane zapewnia, że komunikacja serwera z naszym komputerem jest bezpieczna. Przeglądarka informuje nas o tym przez wyświetlenie ikony zamkniętej kłódki w dolnej części okna. Uniemożliwia to odczytanie naszych danych przez osoby niepowołane [Wojciechowski 2006].

Łącza SLL oraz związany z nimi HTTPS - stosuje się kilka metod do zabezpieczania informacji przesyłanych połączeniami HTTP. Do najpopularniejszych należą: SSL (Secure Socket Layer – warstwa gniazd bezpiecznych) zaprojektowany przez firmę Netscape oraz TLS (Transport Layer Security – zabezpieczenia warstwy transportu). SSL działa wraz z protokołami warstwy aplikacji m.in. takimi jak Telnet, HTTP, FTP, a także protokołem TCP/IP. SSL i TLS oparte są na szyfrowaniu transmisji danych i uwierzytelnianiu, zarówno klienta, jak i serwera. Funkcjonują jako dodatkowa warstwa pomiędzy warstwą transportową TCP/IP, a warstwą aplikacji. Wszystkie transmisje pomiędzy klientem a serwerem są szyfrowane jak i deszyfrowane przez warstwę SSL lub TLS. Szyfrowanie SSL i TLS opiera się na cyfrowych certyfikatach SSL. Typowy przebieg komunikacji SSL przedstawiono na rysunku 3.



Źródło: Komar 2002

Rys. 3. Proces wymiany potwierdzeń SSL
Fig. 3. The process involving exchange of SSL acknowledgements

Wiele mechanizmów szyfrowania korzysta z systemu klucza prywatnego i klucza publicznego. Pakiet zaszyfrowany przy użyciu klucza prywatnego można odszyfrować tylko przy użyciu odpowiedniego klucza publicznego i odwrotnie, pakiet zaszyfrowany przy użyciu klucza publicznego można odszyfrować jedynie kluczem prywatnym. Szyfrowanie i deszyfrowanie wszelkich dalszych danych odbywa się przy użyciu klucza głównego przesłanego serwerowi. Stosowanie innego klucza sesji dla każdej transmisji uniemożliwia hakerowi użycie danych zdobytych podczas jednej transmisji do ataku na kolejną. Szyfrowanie odbywa się za pomocą szyfru 128 bitowego. Przez to liczba operacji wymagana do rozszyfrowania danych jest tak wysoka, że odstrasza włamywaczy. W USA stosowany mechanizm szyfrowania korzysta z 512 bitów, przez co zapewnia wyższy poziom bezpieczeństwa.

Wszystkie strony WWW wyposażone w mechanizm SSL posiadają adres URL rozpoczynający się od HTTPS://. Witryny nierozpoczynające się takim adresem nie są szyfrowane, dlatego używając ich nie należy podawać cennych informacji np. numerów kart kredytowych. Przeglądarki WWW posiadają, także dodatkowe wskaźniki bezpiecznego połączenia SSL. W przeglądarkach internetowych takich jak Internet Explorer u dołu okna pojawia się kłódka, a w Netscape Navigator przy dolnej krawędzi okna pojawia się kluczyk. Od tej pory dane wymieniane między użytkownikiem Internetu a serwerem są kodowane i zabezpieczone [Bowen 2009].

Podpis cyfrowy - podpis cyfrowy, nazywany jest inaczej podpisem elektronicznym. Umożliwia on dołączanie do podpisywanego dokumentu informacji utworzonych na podstawie klucza prywatnego osoby podpisującej dokument. Prawidłowość składanego podpi-

su może ustalić właściciel klucza publicznego osoby podpisującej. Podpis realizuje trzy istotne funkcje: gwarantuje kontrolę spójności – umożliwia znalezienie każdej niezatwierdzonej zmiany w treści informacji oraz jej załącznikach; gwarantuje niezaprzeczalność – autor wiadomości nie może zakwestionować, że ją wysłał i podpisał; przekonuje o autentyczności nadawcy – tylko właściciel jedynego klucza prywatnego może wysłać wiadomość (uwierzytelnienie) [Wojciechowski 2006].

PGP (Pretty Good Privacy) jest programowym systemem szyfrowania. Wykorzystywany jest do ochrony listów e-mail i załączników. Programy pocztowe tj. Microsoft Outlook Express, Eudora i Microsoft Outlook mogą korzystać z modułów rozszerzających PGP. Moduły te instalowane są w programie pocztowym i występują w opcjach menu lub jako przyciski w oknie programu pocztowego. PGP daje możliwość podpisania listów cyfrowo, przez co zagwarantowana jest autentyczność wysyłanych listów elektronicznych. Każdy dokument i użytkownik posiadają jedyny w swoim rodzaju podpis cyfrowy. W sytuacji, kiedy jeden użytkownik będzie wysyłać dwa różne dokumenty, wówczas będą one dysponować innymi podpisami cyfrowymi, ponieważ ich skróty (na podstawie których tworzone są sumy kontrolne) będą inne [Karbowski 2007].

Certyfikat cyfrowy - (ang. Digital Certyficate) jest dokumentem zawierającym informacje wraz z kluczem publicznym. Certyfikaty są wydawane przez tzw. Instytucje Certyfikujące, które odgrywają rolę godnej zaufania trzeciej strony. Certyfikat zapisywany jest na określonym nośniku, np. karcie mikroprocesorowej. Dzięki certyfikatowi cyfrowemu możemy zidentyfikować osobę, która posługuje się podpisem cyfrowym. Program komputerowy, tworząc parę kluczy asymetrycznych, korzysta tylko z informacji zapisanych przez samego użytkownika i w ogóle nie może ich sprawdzić. Kontrolowanie kluczy polega na stwierdzeniu autentyczności sygnatury osoby trzeciej przez osobę zasługującą na zaufanie. Użytkownik po wytworzeniu swojej pary kluczy asymetrycznych przesyła klucz publiczny do osoby udzielającej certyfikacji. Po skontrolowaniu prawdziwości danych użytkownika, jednostka udziela mu właściwy certyfikat cyfrowy. Certyfikat jest nierozłącznie połączony z kluczem publicznym. Weryfikacja certyfikatu polega na sprawdzeniu podpisu cyfrowego za pomocą jego klucza publicznego. Klucz także powinien być certyfikowany, by zapobiec podszyciu się hakera pod centrum certyfikacji. W certyfikacie zapisane są następujące informacje: określenie nazwy użytkownika, stowarzyszenia lub serwera, dla których certyfikat był przeznaczony (w zależności od rodzaju certyfikatu), klucz publiczny posiadacza certyfikatu, nazwa organu, który wydał certyfikat, identyfikator wystawcy, numer seryjny certyfikatu, termin ważności certyfikatu, podpis elektroniczny centrum certyfikacji [krystian.jedrzejczak.webpark.pl]

Firewall - powiązanie sieci lokalnej z Internetem wiąże się z niebezpieczeństwami pochodzącymi z zewnątrz. Firewall, czyli zapora przeciwogniowa, jest systemem zabezpieczenia sieci informatycznych przed włamaniem. Firewalle chronią przed dostępem osób nieupoważnionych do sieci lokalnej, dlatego instalowane są między sieciami. Niektóre zapory przeciwogniowe zupełnie nie dopuszczają do ruchu pakietów z zewnątrz. Dają jednak dostęp pakietom używanym przez program poczty elektronicznej, a także umożli-

wiają bezpieczną komunikację użytkownika z siecią zewnętrzną. Kolejną pozytywną cechą firewalli jest wprowadzanie i przeglądanie wszystkich nadchodzących pakietów. Pozycjami, przez które przechodzą wszystkie dane do sieci lokalnej i na zewnątrz są stacje zwane bastion host. Zajmują one pierwsze miejsce na linii obrony. Zapora przeciwogniowa zabezpiecza przed podsłuchiwaniem i podszywaniem się przez nieuprawnione osoby, oraz zabezpiecza przed wirusami i koniami trojańskimi.

Firewalle dzielą się na programowe i sprzętowe. Firewalle programowe to specjalne programy. Za pomocą ich możemy kontrolować cały ruch pakietów wchodzących i wychodzących z naszego komputera do Internetu. Zaliczyć do nich możemy programy ZoneAlarm, Outpost Firewall, Sygate Personal Firewall, Ashampoo FireWall, Comodo Personal, GeSWall, Jetico Personal, Kerio Personal Firewall. Zapory sprzętowe są to specjalne urządzenia zewnętrzne. Urządzenia te filtrują i analizują pakiety za pomocą układów scalonych i wewnętrznego oprogramowania. Wyodrębniamy trzy typy zapór przeciwogniowych: zaporę na poziomie sieci; zaporę na poziomie aplikacji; zaporę na poziomie transmisji.

Do głównych zalet firewalli zaliczymy: zabezpieczanie systemu, pozwalanie całej sieci na korzystanie z jednego wspólnego adresu IP (serwer proxy), umożliwianie systemom z protokołami innymi niż TCP/IP podłączenie do Internetu, monitorowanie połączeń WAN i ruchu w sieci, Proxy Cache Server optymalizuje obciążenie na łączu WAN, przy intensywnej pracy z www.

Wady firewalli: wymagają częstych uaktualnień, utrudniają zdalne sterowanie siecią, mała wydajność serwerów pośredniczących zmniejsza wydajność sieci [Pieńkowski 2003].

Wnioski

1. Działanie sieci Internet jest uzależnione od wielu mechanizmów, takich jak protokoły internetowe, serwery DNS oraz DDNS, routery.
2. Korzystając z Internetu użytkownik narażony jest na wiele niebezpieczeństw, takich jak: sniffing, spoofing, syn-flooding, skanowanie portów, niemniej jednak istnieją metody przeciwdziałania im, takie jak: autoryzacja i uwierzytelnianie, szyfrowanie informacji, podpis cyfrowy, certyfikat cyfrowy i firewall.
3. Z uwagi na niski stopień informatyzacji obszarów wiejskich oraz rozproszony charakter sieci sektora rolno-spożywczego istnieje tam szczególna potrzeba wdrażania zagadnień związanych z zabezpieczeniem przesyłu danych. Niestety problem ten jest bagatelizowany przez większość użytkowników sieci.
4. Pomimo stosowania różnego rodzaju zabezpieczeń (ww. oraz programów antyspamowych, antyspyware) komputer nigdy nie będzie zabezpieczony w pełni, dlatego podczas przesyłania różnego rodzaju informacji w sieci komputerowej należy zachować zdrowy rozsądek.

Bibliografia

Bowen R., Coar K. 2009. Apache. Receptury. Wyd. 2. Helion. ISBN: 978-83-246-1549-0.
Jędrzejczak K. Bankowość elektroniczna. [Online]. [dostęp 11.07.2008]. Dostępny w internecie http://krystian.jedrzejczak.webpark.pl/podpis.htm.
Komar B. 2002. TCP/IP dla każdego. Helion. ISBN: 83-7197-782-4.
Karbowski M. 2007. Podstawy kryptografii. Wyd. 2. Helion. ISBN: 978-83-246-1215-4.

Sojak M., Głowacki Sz. 2009. Wi-Fi networks in small and medium sized businesses (SMB). Studia Informatica, Systems and information technology. 1(12). s. 55-66.
Szmit M., Gusta M., Tomaszewski M. 2005. 101 zabezpieczeń przed atakami w sieci komputerowej. Helion. ISBN: 83-7361-517-2.
Wojciechowski A. 2006. Usługi w sieciach informatycznych. Mikom, Warszawa. ISBN:978-83-01-14751-8.
Praca zbiorowa. 2003. Administrator PC Przewodnik Telepracy, skład: Jerzy Pieńkowski, Fundacja Pomocy Matematykom i Informatykom Niepełnosprawnym Ruchowo, Wydanie I, Warszawa.

PROTECTION METHODS FOR DATA TRANSFER VIA THE INTERNET

Abstract. The purpose of the work is to make Internet users aware of hazards they are exposed to while using a computer, which is not protected against hackers' attacks, and to show how data transferred via the Internet may get into the wrong hands. This information may be useful for users who e.g. run their own, individual farms, and for other types of businesses as well. The paper presents both selected methods used to attack transmission of data transferred via the Internet, and selected protection methods, which may be used to secure information.

Key words: protection methods, authorisation, authentication, information coding, digital signature, digital certificate

Adres do korespondencji:
Mariusz Sojak; e-mail: mariusz_sojak@sggw.pl
Zakład Podstaw Nauk Technicznych
Szkoła Główna Gospodarstwa Wiejskiego w Warszawie
ul. Nowoursynowska 164
02-787 Warszawa