STUDIA INFORMATICA 2003
Volume 24 Number 2B (54)

Jerzy KOROSTIL, Grzegorz ŚLIWIŃSKI
Politechnika Szczecińska, Wydział Informatyki

ANALIZA PARAMETRÓW OCENY PŁYNNEGO POZIOMU BEZPIECZEŃSTWA SIECI KORPORACYJNEJ

Streszczenie. Każda sieć korporacyjna posiada pewne informacje, które powinny być chronione. Jednak poziom zabezpieczeń w obecnym czasie określany jest w sposób statyczny, czyli przy budowie systemu określa się pewne parametry krytyczne systemu i na ich podstawie buduje się system bezpieczeństwa o ściśle określonym, nigdy niezmiennym poziomie. Często też nie prowadzi się weryfikacji zabezpieczeń (brak sprzężenia zwrotnego w systemie bezpieczeństwa), co powoduje, że informacje tam zgromadzone są zabezpieczone niedostatecznie.

Słowa kluczowe: bezpieczeństwo, sieci komputerowe, poziom bezpieczeństwa.

THE ANALYSIS OF THE PARAMETERS OF THE FLUID VALUATION OF THE SECURITY LEVEL IN THE CORPORATE NETWORKS

Summary. Every corporate network has some information that should be protected. However, nowadays security level is specified in the static mode, so some critical system parameters are specified while the system is built and based on that information the security system is created on the exactly specified and unchangeable level. Often, the verification of securities are not realised (there is no feedback in the security system) and that causes the information stored there are not sufficiently secured.

Keywords: security, computer networks, security level.

1. Wstęp

Główną cechą sieci korporacyjnych jest gromadzenie informacji celem jej późniejszego wykorzystania. Informacja ta powinna być należycie zabezpieczona, co czyni każda korporacja, jednak określenie poziomu zabezpieczeń najczęściej odbywa się jednorazowo w

trakcie tworzenia systemu bezpieczeństwa. Oznacza to, że dane zgromadzone w takim systemie niejednokrotnie są zabezpieczone niepoprawnie (zbyt mały poziom zabezpieczeń w stosunku do wartości ryzyka zgromadzonych danych) lub w najlepszym przypadku zabezpieczenia są „poważniejsze" niż wartości danych, które zabezpieczamy.

Istotą prawidłowego rozwiązania opisywanego problemu jest czynne wpływanie na zmianę poziomu zabezpieczeń poprzez automatyczne, płynne wpływanie systemu analizującego na system bezpieczeństwa.

Musimy jednak podać systemowi analizującemu pewne parametry, dzięki którym będzie w stanie określić aktualnie potrzebny poziom zabezpieczeń oraz zweryfikować już działający. Weryfikację aktualnie działającego systemu zabezpieczeń można przeprowadzić na podstawie trzech parametrów: odporność (ξ), otwartość (η), przeciążalność (μ). Parametry te są na tyle ogólne, że można je zastosować niemal do wszystkich dostępnych elementów zabezpieczających. Zakładamy również, iż istnieje możliwość wyznaczenia ryzyka systemu R(S)[1]. Działanie systemu analizującego sprowadzać się wówczas będzie do optymalizacji zgodnie z zależnością B(S)[2] = R(S). Wartość ta jest w rzeczywistości niemożliwa do uzyskania, dlatego mówić będziemy o wartości gwarantowanej w danym czasie jako różnicy B(S) – R(S) i określimy poprzez G(S), co sprowadza proces optymalizacji do wyznaczenia min{G(S)} [1].

2. Analiza parametrów

Zgodnie z [1] przedstawiamy w postaci matematycznej opisywane wcześniej współczynniki.

$$\xi = \frac{\sum_{i=0}^{n} k_i}{t(u)} \tag{1}$$

$$\eta = \alpha * \sum_{i=1}^{n} \left(\frac{M}{m} \right) \tag{2}$$

$$\mu = \frac{n * u_k}{\sum_{i=0}^{m} (z_i * t_i(u_k))} \tag{3}$$

[1] R(S) – ryzyko (koszt) utraty (ujawnienia) informacji chronionej w danym systemie.
[2] B(S) – wartość współczynnika bezpieczeństwa systemu chronionego.

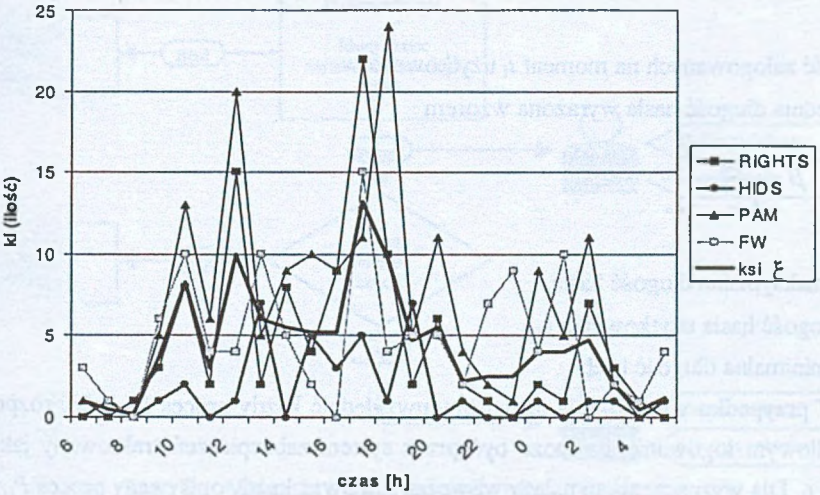
Zależności te w sposób ogólny mogą opisywać trzy główne cechy wszystkich elementów zabezpieczających. Na podstawie tych parametrów będziemy również określać wartość B(S) jako zależność:

$$B(S) = \sum_{i=1}^{n} \xi_i + \sum_{j=1}^{m} \eta_j + \sum_{r=1}^{k} \mu_r \tag{4}$$

Do analizy poszczególnych parametrów w badaniach wykorzystano aktualnie znane systemy zabezpieczające zintegrowane z systemem operacyjnym lub dostarczane w postaci dodatkowych modułów. Przeprowadzimy analizę sposobu obliczania wartości przedstawionych wcześniej współczynników.

2.1. Odporność

Wartość tego współczynnika jest miarą ilości nieprawidłowych zdarzeń z punktu widzenia systemu zabezpieczającego w jednostce czasu. Przeprowadzone badania określiły wartość średnią odporności w przedziale 5 – 11 zdarzeń na godzinę.



Rys. 1. Analiza odporności zabezpieczeń
Fig. 1. The analyse of the protections' resistance

Przedział ten został określony doświadczalnie (rys. 1) poprzez ogólnie dostępne analizatory rejestrów systemowych. Wartości średnie badanych zabezpieczeń (wyniki zaobserwowane w rejestrach) oscylowały właśnie w określonym przedziale i dlatego też autorzy przyjęli prezentowany przedział jako wyjściowy do dalszych badań.

2.2. Otwartość

Większość elementów zabezpieczających posiada jako podstawowy mechanizm bezpieczeństwa proces uwierzytelniający, który bazuje na identyfikatorze obiektu i haśle przypisanym do tego identyfikatora [2]. Opisywany współczynnik jest elementem, którego wyznaczenie wymaga poznania architektury wewnętrznej procesu chroniącego pod kątem posiadanych (gromadzonych) danych. W wyniku doświadczeń stworzono opis matematyczny, który pozwala wyliczyć wartości M i m potrzebne do prawidłowego przeliczenia współczynnika η, zgodnie ze wzorem (2).

$$M_{t_i} = N * \gamma \tag{5}$$

gdzie:

N – maksymalna ilość haseł w systemie

γ – współczynnik określony wzorem

$$\gamma = \frac{\sum_{i} \beta}{\varepsilon} \tag{6}$$

gdzie:

ε – ilość zalogowanych na moment t_i użytkowników

β – średnia długość hasła wyrażona wzorem

$$\beta = \frac{l_{max} - l_{\varepsilon_i}}{l_{max} - l_{min}} \tag{7}$$

gdzie:

l_{max} – maksymalna długość hasła

$l_{\varepsilon i}$ – długość hasła użytkownika ε_i

l_{min} – minimalna długość hasła.

W przypadku wyznaczenia m musimy uwzględnić każdy proces P_i, który rozpoczyna się prawidłowym logowaniem i może być przez system zabezpieczeń traktowany jako atak na chwilę t_i. Dla wyznaczenia m należy wówczas sumować każdy opisywany proces P_i, zgodnie z zależnością.

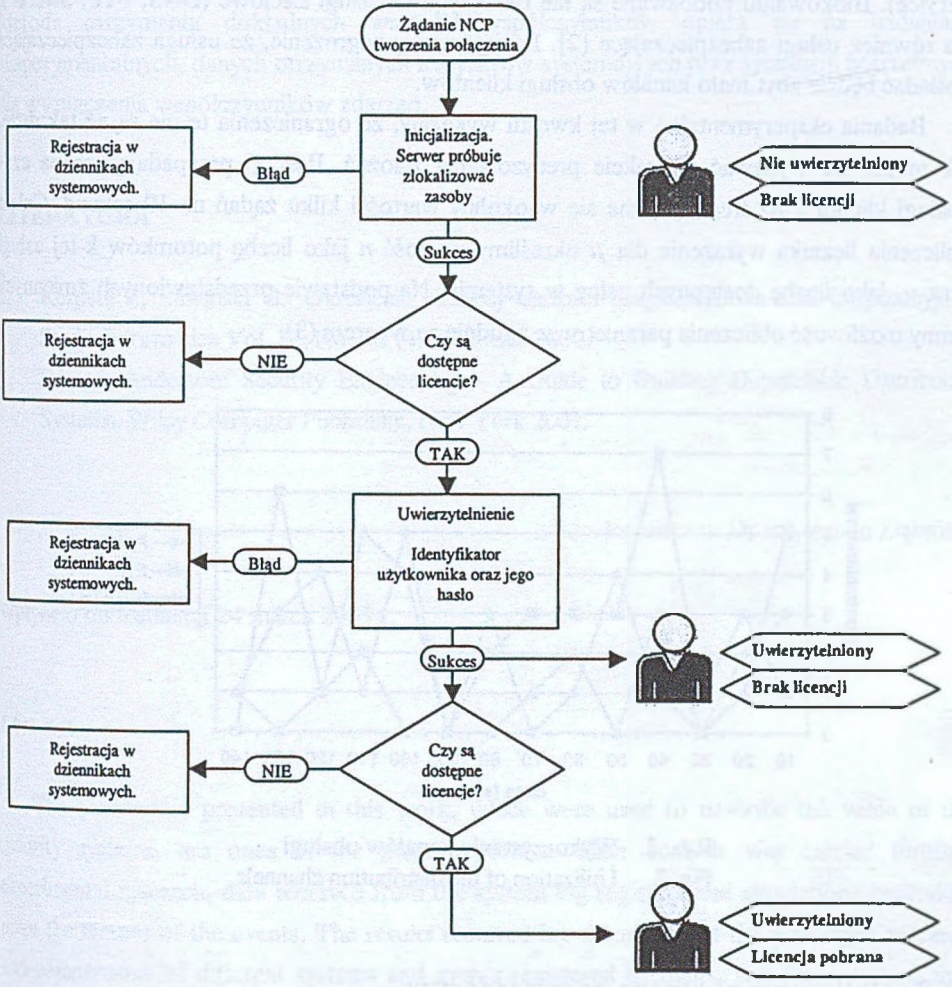
$$m = \sum_{i=1}^{n(t_i)} P_i \tag{8}$$

gdzie:

P_i – i-ty proces

n – ilość zdarzeń w czasie t_i.

Prześledźmy zatem proces weryfikacji użytkownika w systemie z rezerwacją licencji. Rysunek 2 przedstawia algorytm procesu uwierzytelniania w systemie sieciowym Novell NetWare.



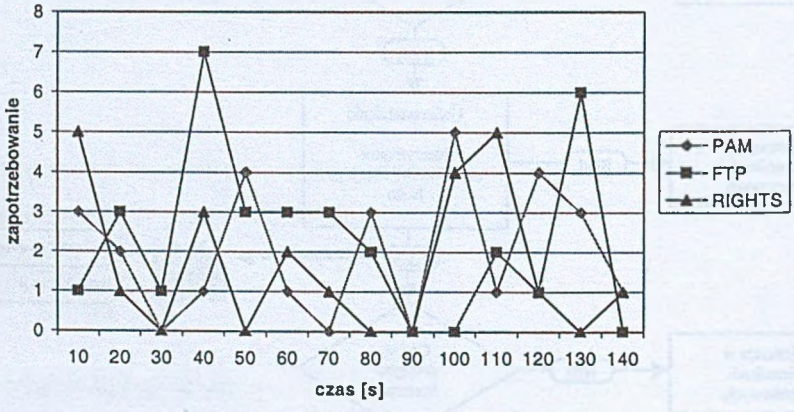
Rys. 2. Algorytm uwierzytelnienia użytkownika
Fig. 2. The algorithm of user's authentication

W kwestii przedstawianego współczynnika potrzebne są dalsze badania, celem których będzie wyznaczenie dokładnych wartości η innych elementów systemu zabezpieczającego.

2.3. Przeciążalność

Współczesne sieci komputerowe narażone są na dość częste ataki typu DoS (Denial of Service). Blokowaniu poddawane są nie tylko typowe usługi sieciowe (DNS, FTP, SMTP[3]), ale również usługi zabezpieczające [2]. Istnieje zatem zagrożenie, że usługa zabezpieczająca posiadać będzie zbyt mało kanałów obsługi klientów.

Badania eksperymentalne w tej kwestii wykazały, że ograniczenia te nie są aż tak duże, jak mogło się wydawać w trakcie precyzowania założeń. Ilość z_i przypadających na czas obsługi klienta $t(u_k)$ średnio waha się w okolicy wartości kilku żądań na 10 sekund. Celem obliczenia licznika wyrażenia dla μ określimy wartość n jako liczbę potomków k-tej usługi oraz u_k jako liczbę dostępnych usług w systemie. Na podstawie przedstawionych zmiennych mamy możliwość obliczenia parametru μ, zgodnie ze wzorem (3).



Rys. 3. Wykorzystanie kanałów obsługi
Fig. 3. Utilization of the distribution channels

3. Obliczanie płynnego bezpieczeństwa

Zgodnie ze wzorem (4) wartość wielkości płynnego bezpieczeństwa można obliczyć na podstawie wyników przeprowadzonej powyżej analizy metod wyznaczenia współczynników.

[3] Usługi internetowe – DNS (Domain Name System), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol).

4. Podsumowanie

W referacie przedstawiono możliwość obliczenia poszczególnych współczynników ξ, η, μ. Metoda otrzymania dokładnych wartości współczynników opiera się na badaniach eksperymentalnych, danych otrzymanych z rejestrów systemowych oraz symulacji potrzebnych dla wyznaczenia współczynników zdarzeń.

LITERATURA

1. Korostil J., Śliwiński G.: Określenie bieżącej wartości bezpieczeństwa sieci korporacyjnej. Studia Informatica Vol. 23, No. 2B (49), Gliwice 2002.
2. Ross J. Anderson: Security Engineering – A Guide to Building Dependable Distributed Systems. Wiley Computer Publishing, New York 2001.

Recenzent: Dr inż. Adam Ziębiński

Wpłynęło do Redakcji 24 marca 2003 r.

Abstract

The parameters presented in this work, which were used to describe the value of the security systems, are ones of the most important. Their analysis was carried through experimental research, data received from the system log registers and simulations needed to point the factors of the events. The results received are the effects of the prolonged research and comparisons of different systems and events registered by them. The authors claim that there is a possibility to describe a proper method allowing the influence of the system security level using the factors presented. The use of such a method would cause a greater reliability laid in the security systems that should always adequately protect the information stored in the system in relation to the value of the risk of the protected system.

Adresy

Jerzy KOROSTIL: Wydział Informatyki Politechniki Szczecińskiej, ul. Żołnierska 49, 71-210 Szczecin, Polska, ikorostil@wi.ps.pl .

Grzegorz ŚLIWIŃSKI: Wydział Informatyki Politechniki Szczecińskiej, ul. Żołnierska 49, 71-210 Szczecin, Polska, gsliwinski@wi.ps.pl .