Nie tylko firewall, czyli zagadnienia bezpieczeństwa w sieciach komputerowych

Artur Opaliński
Sun Microsystems Polska

Abstrakt

Przechowywanie, przetwarzanie i przesyłanie danych komputerowych wymaga m.in. zapewnienia ich poufności oraz integralności. Ze względu na system rynkowy i uwarunkowania kulturowe istnieje rywalizacja podmiotów, która prowadzi m.in. do walki o dostęp do informacji.
Uwarunkowania techniczne, takie jak duża koncentracja danych i możliwości bardzo szybkiego ich przesyłania i przetwarzania w systemach komputerowych stwarzają szczególnie duże zagrożenie. Jednocześnie stniejące i przyszłe regulacje prawne klasyfikują dane i nakładają na użytkowników systemów komputerowych odpowiedzialność za zachowanie odpowiedniego poziomu ochrony.
Te i inne czynniki powodują, że problem ochrony informacji - do niedawna ograniczony do specjalnych instytucji, głównie rządowych - dotyczy nieomal wszytkich użytkowników systemów komputerowych.
Niniejszy referat w oparciu o prostą klasyfikację przedstawia przegląd wybranych środków technicznych oferowanych przez firmę Sun Microsystems do poprawy bezpieczeństwa danych w systemach i sieciach komputerowych.

Wstęp

Przechowywanie, przetwarzanie i przesyłanie danych komputerowych wymaga zapewnienia im bezpieczeństwa zgodnie z ich wrażliwością. Część danych podlega przepisom państwowym, regulującym zasady ich o chrony (DZ, 1998). W związku z dążeniem do Unii Europejsckiej, należy oczekiwać upodobnienia naszej legislacji do krajów zachodnich (Adamski, 1994; Cornwall, 1990; C-RC, 1990). Niemniej również te dane, które nie muszą byc chronione z punktu widzenia interesów państwa, moga być łakomym kąskiem dla konkurencji, prasy, nie powinny trafiać do wiadomości zewnętrznych firm np. konsultacyjnych i kontrolnych, ani niekiedy złośliwych osób postronnych.
Panujący w Polsce system rynkowy, zależności kulturowe i inne czynniki powodują, że występuje walka o dostęp do informacji.
Uwarunkowania techniczne, takie jak duża koncentracja danych i możliwości bardzo szybkiego ich przesyłania i przetwarzania w systemach komputerowych, czy rozległość publicznych sieci komputerowych oplatających cały świat, stwarzają szczególne zagrożenie. Lawinowy wzrost możliwości w dziedzinie komunikacji sprawia, że do wspólnej sieci dołączane są, bądź dołączają się, duże grupy użytkowników, którzy nie są bezpośrednio znani właścicielom dotychczas pracujących systemów i niekoniecznie realizują te same cele.
Pojawia się konieczność rozważenia zagadnienia bezpieczeństwa w firmie, określenia najcenniejszych zasobów i wyznaczenia środków ochrony. Do realizacji tych celów ważne są metryki, określające jakość bezpieczeństwa. Jedną z metryk może być zestaw kryteriów bezpieczeństwa i funkcjonalności przyjęty w IT Security Evaluation Criteria (ITSEC), który proponuje ropatrywać każdy system w rozbiciu na poniższe zagadnienia:

- Identyfikacja i uwierzytelnianie (Identification and Authentication)
- Kontrola dostępu (Access Control)
- Możliwość rozliczenia (Accountability)
- Audyt (Audit)
- Powtórne wykorzystanie (Object Reuse)
- Dokładność (Accuracy)
- Niezawodność (Relaibility of Services)
- Przesyłanie danych (Data Exchange)

Jest to bardo dobry, sformalizowany i bardzo złożony schemat, wykorzystywany raczej tylko przez instytucje o najwyższych wymogach bezpieczeństwa. Daje dobre wyobrażenie o skali problemu. Na potrzeby niniejszego referatu można pokusić się o prostsze przedstawienie kryteriów ochrony.

Klasyfikacja zagadnień bezpieczeństwa

Sieci komputerowe to zgodnie z definicją dwa lub więcej urządzenia (węzły) połączone medium fizycznym w celu wspólnego użytkowania urządzeń lub przesyłania danych. W zastosowaniach praktycznych mamy do czynienia zazwyczaj z bardziej złozonymi strukturami, zawierającymi:

- medium fizyczne (np. kabel miedziany, świtłowód, fale radiowe)
- urządzenia pośredniczące w komunikacji (np. routery, switche, huby)
- urządzenia końcowe (np. komputery osobiste, serwery, drukarki sieciowe)

Aby zapewnić bezpieczeństwo danych w sieci trzeba oczywiście zapewnić bezpieczeństwo w każdym z jej elementów składowych. Niezabezpieczone media fizyczne stwarzają możliwość podsłuchu w czasie transmisji. Urządzenia pośredniczące w komunikacji mogą nieprawidłowo przesyłac dane. Urządzenia końcowe w których przechowuje się i przetwarza dane powinny udostępniac je w myśl ściśle okreslonych zasad, chronić przed niepowołanymi modyfikacjami i odseparować od ew. innych danych.

Oczywiście rozróżnić należy bezpieczeństwo fizyczne elementów składowych (zabezpieczenie przed kradzieżą, wpływem czynników środowiskowych, katastrof, itp.), oraz bezpieczeństwo „logiczne" - danych i informaji konfiguracyjnych. Poniższy referat pomija zagadnienia bezpieczeństwa fizycznego.

Ochronę danych realizuje się w dużej mierze od wieków w oparciu o te same mechanizmy, wykorzystując jedynie coraz bardziej zaawansowane środki techniczne. Owe mechanizmy ochrony to między innymi::

- Szyfrowanie danych

Polega na przedstawieniu informacji za pomocą symboli o znaczeniu znanym tylko zainteresowanym stronom. Szeroko znane są przykłady przekazywania zaszyfrowanej informacji poprzez ustawienie doniczki na oknie, czy użycie rzadkiego narzecza języka ludzkiego.

- Kontrola dostępu

Wymaga ona **identyfikacji** osoby korzystającej z informacji, oraz jej **uwierzytelnienia**, czyli potwierdzenia, że jest rzeczywiście tym, za kogo się podaje. Dodatkową korzyścią jest możliwość tworzenia spisów osób korzystających z dostępu do danej informacji. Przykładem uwierzytelnienia może być przedstawienie dowodu osobistego, przykładem kontroli dostępu - wypisywanie przepustek.

Ochronę dostępu bez identyfikacji osoby moga stanowiś solidne drzwi.

- Archiwizacja

Poprzez udostępnianie tylko kopii informacji można zapewnić ochronę przed zniszczeniem lub utratą spójności danych. Tradycyjnie udostępnia się kopie ważnych dokumentów.
Wszytstkie te i inne mechanizmy moga być stosowane także w ochronie danych w sieciach komputerowych, oczywiście z użyciem współczesnych środków technicznych.

Z powyższego krótkiego i niepełnego przeglądu wynika istotny wniosek co do natury problemu: zagadnienie ochrony informacji jest stare. Rozwiązania techniczne stosowane w sieciach komputerowych bazują w dużej mierze na wymienionych powyżej, dawnych metodach. Zatem w szczególności w ochronie danych w sieciach komputerowych - tak jak w zagadnieniach ochrony informacji czy dóbr w ogole - nie ma rozwiązań ostatecznych.

Stąd można mówić jedynie o „poprawie poziomu bezpieczeństwa", nie zaś o sieciach czy systemach bezpiecznych.
Istnieją organizacje i kryteria, które poprzez różne poziomy certyfikatów pozwalają w wymierny sposób określić poziom bezpieczeństwa danego systemu informatycznego (Trusted Computer Systems Evaluation Criteria, National Computer Security Agency, IT Security Evaluation Criteria, Common Criteria).
Należy pamietać, że nieuprawnione osoby skłonne sa włozyć w przełamanie systemu informatycznego wysiłki, czas i funusze, które są skorelowane z wagą chronionej informacji - w związku z czym zastosowanie środków bezpieczeństwa, których przełamanie wymaga większych nakładów niż może przynieść korzyści daje wysoka pewność, że dane znajdą się poza zakusami.

Środki poprawy bezpieczeństwa firmy Sun Microsystems

Firma Sun Microsystems należy do czołowych producentów sieciowych sysstemów komputerowych i oferuje całą game produktów do podniesienia poziomu bezpieczeństwa sieci.
Zgodnie z klasyfikacją przedstawioną uprzednio można przedstawić wybrane środki i produkty następująco:

- Rozwiązania do archiwizacji danych

  ⇒ Solstice Backup oraz Solstice Enterprise Backup

  Jest to oporgramowanie pozwalające na sporządzanie automatycznych, centralnych kopii bezpieczeństwa (backup) w określonym zakresie na serwerze z systemem operacyjnym Solaris. Można sporządzac kopie bezpieczeństwa danych znajdujących się na maszynach z systemami operacyjnymi: Solaris, Windows NT, Novell Netware, Macintosh. Można archiwizować zarówno dane zawarte w plikach, jak i w kilku rozproszonych bazach danych Oracle, Informix, Sybase, MS SQL Server - w tym również w trybie on-line (bez zatrzymywania bazy). Można też sporządzać kopie danych aplikacji, takich jak SAP/R3 i LotusNotes.
  Możliwe jest stosowanie bibliotek taśmowych (jukeboxów).

- Rozwiązania kontroli dostępu do danych i systemu komputerowego
  - identyfikacja/uwierzytelnienie w oparciu o:
    - hasła jednorazowe

    ⇒ Solstice FireWall-1

    Solstice FireWall-1 prowadzi uwierzytelnianie użytkowników kilkoma metodami: haseł jednorazowych S/Key, haseł jednorazowych SecurID, oraz

RADIUS i AssureNet Pathways Defender. Na podstawie przeprowadzonej identyfikacji i uwierzytlenienia Solstice FireWall-1 zezwala na realizację połączenia i korzystanie z serwisów sieciowych. Dodatkowo w oparciu o FireWall można prowadzić kontrolę antywirusową przesyłanych plików, blokowac dostęp do wybrancyh stron WWW, do stron WWW zawierających aplety w Java.

⇒ Solaris (p. metody biometryczne)

- karty z własną logiką (chipcards)

⇒ Sun Security Manager for Desktop
Oprogramowanie SSMD działające pod kontrolą systemów operacyjnych Solaris, Windows 3.x, Windows '95 i Windows NT, pozwala na jednokrotne logowanie (single sign-on) użytkowników przy korzystaniu z serwisów sieciowych i aplikacji bazodanowych z uzyciem haseł tradycyjnych, bądź z uzyciem kart z własną logiką (chipcard)

⇒ Solstice FireWall-1 (p. hasła jednorazowe)

⇒ Solaris (p. metody biometryczne)

- metody biometryczne

⇒ Solaris
System operacyjny Solaris od wersji 2,6, oprócz standardowej identyfikacji i uwierzytelniena w oparciu o identyfikator i stałe hasło użytkownika, posiada możliwośc włączenia dowolnego mechanizmu uwierzytelnienia poprzez stosowanie wymiennych modułów uwierzytelniających (Pluggable Autentication Modules). Daje to możliwość uwierzytelnienia w oparciu o Kerberos, DCE (Distributed Computing Environment), LDAP (Lightweight Directory Access Protocol) , karty z własna logiką i w szczególności również metody biometryczne.

- kontrola dostępu
  - rozpoczęcie sesji pracy w systemie

  ⇒ System operacyjny Solaris
  System operacyjny Solaris zapewnia rozpoczęcie sesji tylko użytkownikom, którzy zostali odpowiednio uwierzytelnieni. Duży wybór metod uwierzytelniania oferuje mechanizm PAM (wymmiennych modułów uwierzytelniających). Można wzbogacić te podstawowe mozliwości instalując dodatkowe oprogramowanie, takie jak Solstice FireWall-1, czy Sun Security Manager.

  - dostęp do danych (DAC, MAC)

  ⇒ system operacyjny Solaris
  Można precyzyjnie dopasować uprawnienia użytkownika po rozpoczęciu sesji pracy w systemie, poprzez prawa dla właściciela, grupy i świata, oraz poprzez listy dostępu (Access Control Lists) - standardowe mechanizmy systemu operacyjnego Solaris.

⇒ system operacyjny Trusted Solaris
Bardziej wymagający użytkownicy mogą wykorzystać wersję systemu o zaawasowanych cechach bezpieczeństwa, która oprócz mechanizmów tradycyjnego systemu Solaris oferuje Mandatory Access Control. Przy określaniu praw dostępu uwzględnia się poziom wrażliwości informacji (np. ściśle tajna, tajna, poufna) i poziom uprawnień uzytkownika.

- ograniczenie dostępnych komend

⇒ system operacyjny Trusted Solaris
W systemie Trusted Solaris można ogarniczyć uprawnienia użytkownika do minimum, poprzez wyszczególnienie komend i aplikacji które wolno mu uruchamiać w jego profilu i dostepnych mu rolach.

- dostęp do mediów wymiennych

⇒ system operacyjny Trusted Solaris
W systemie Trusted Solaris można ograniczyć dostęp uzytkownika do mediów wymiennych i urządzeń wyjściowych (np. drukarek). Wyklucza się w ten sposób mozliwość wynoszenia danych na dyskietkach i wydrukach, jak też sprowadzania niekontrolowanego oprogramowania.

- filtrowanie pakietów

⇒ SunScreen SPF
Jest to kontekstowy filtr pakietów, niewidoczny w sieci (czarna skrzynka). Może filtrować pakiety innych protokołów niż IP. Posiada zaawansowane mozliwości w dziedzinie kryptografii (tworzenie wirtualnych sieci prywatnych). Korzysta z protokołu SKIP.

⇒ SunScreen EFS
Jest to typ firewalla. Realizuje zarówno kontekstowe filtrowanie pakietów IP, jak i usługi proxy i uwierzytelnianie urzytkowników. Posiada zaawansowane mozliwości w dziedzinie kryptografii (tworzenie wirtualnych sieci prywatnych). Korzysta z protokołu SKIP.

⇒ Solstice FireWall-1
Firewall o bogatej funkcjonalności, zawierającej filtrowanie kontekstowe IP, usługi proxy, uwierzytelnianie użytkowników, kontrolę antywirusową przesyłanych plików, blokowanie dostępu do stron WWW, i inne.

- Szyfrowanie danych

⇒ Sun Screen SKIP
SKIP .jest standardem IETF (Internet Engineering Task Force) stworzonym przez Sun Microsystems do szyfrowania informacji na poziomie trzecim standardu ISO/OSI (pakietów IP w protokole TCP/IP) oraz do zarządzania i dynamicznej zmiany symetrycznych i asymetrycznych kluczy szyfrujących. Interesujące cechy to możliwość stosowania dowolnego algorytmu szyfrującego (jako moduł) i dynamicznej zmiany kluczy.

Jednocześnie nazwą Sun Screen SKIP określa się oprogramowanie dostępne wiele platform, między innymi Solaris, JavaOS, Windows 3.x, Windows 95 i Windows NT, które służy do szyfrowanej komunikacji w sieciach publicznych z wykorzystanem protokołu SKIP.

⇒ SunScreen EFS, SunScreen SPF, SunScreen SKIP, oraz Solstice FireWall-1. Szeroko znane protokoły, takie jak DES, 3DES, SAFER, RC2, RC4 są stosowane są w produktach kryptograficznych Sun Microsystems do szyfrowania danych i kluczy. Ich implementację można znaleźć w SunScreen SKIP, SunScreen EFS, SunScreen SPF, oraz Solstice FireWall-1.

Referencje:

A.Adamski, „Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji", materiały z konferencji naukowej TNOiK, Torun, 1994

H.Cornwall, „Datatheft, Computer Fraud, Industrial Espionage and Information Crime", Manarin Paperbacks, London, 1990

C-RC, „Computer-Related Crime", Recommendation No R(89)9 on computer related crime and final report of the European Commitee on Crime Problems, Council of Europe, Strassbourg, 1990

DZ, Ustawa o ochronie danych osobowych, Dz.U. nr ... 1998

ITSEC, http://www.itsec.gov.uk