Biuletyn WAT
Vol. LVII, Nr 4, 2008

O organizacji i implementacji mechanizmów dostępu do informacji wrażliwych przetwarzanych w systemach teleinformatycznych

KRZYSZTOF LIDERMAN

Wojskowa Akademia Techniczna, Instytut Teleinformatyki i Automatyki,
Zakład Systemów Komputerowych,
00-908 Warszawa, ul. S. Kaliskiego 2

Streszczenie. Artykuł zawiera omówienie, na przykładzie modelu Balla-LaPaduli, tematyki sterowania dostępem do informacji klasyfikowanej. W artykule przedstawiono m.in. zarys koncepcji systemu ochrony informacji i metod uwierzytelniania podmiotów oraz wnioski wynikające z praktycznego zastosowania modelu Bella-LaPaduli.
Słowa kluczowe: informatyka, uwierzytelnianie, autoryzacja, sterowanie dostępem, klasyfikacja informacji, model Balla-LaPaduli
Symbole UKD: 681.3.05

1. Wstęp

Problem przetwarzania informacji wrażliwych o różnych poziomach tajności był intensywnie badany już od początku lat 70. XX wieku [1, 2, 3]. Podstawy formalne tzw. ochrony wielopoziomowej (ang. *MultiLevel Security* — MLS) zostały przedstawione w pracach Bella-LaPaduli [2], a próby implementacji modelu, do przetwarzania informacji o różnych poziomach tajności w systemach informatycznych, były wykonane w korporacji MITRE w systemie Multics. Mówi się, że system lub urządzenie jest MLS (*multilevel secure* — zapewnia wielopoziomową ochronę), jeżeli potrafi przetwarzać informację z wielu poziomów tajności bez ujawnienia jej nieautoryzowanym podmiotom [10].

Wraz z rozwojem sieci komputerowych, w szczególności Internetu, problem ochrony wielopoziomowej przesunął się z pojedynczych systemów komputerowych na sieci komputerowe przetwarzające i wymieniające informacje z różnych poziomów tajności — w literaturze przedmiotu sieci takie są nazywane sieciami etykietowanymi (ang. *labeled networks*).

Zagadnienie omawiane w dalszej części tego artykułu można sformułować następująco: *jak skutecznie chronić informacje wrażliwe przed niepożądanym dostępem*. Ponieważ z założenia problem ma dotyczyć informacji wrażliwych z obszaru wojskowego, to do dalszych rozważań przyjmujemy, że ww. informacje wrażliwe są informacjami niejawnymi w rozumieniu ustawy o ochronie informacji niejawnych [13, 14, 15], a systemy teleinformatyczne, w których są przetwarzane, przechowywane i przesyłane, muszą, zgodnie z odpowiednimi regulacjami prawnymi, posiadać akredytację.

Dostęp do informacji można rozpatrywać na czterech, uzupełniających się, poziomach działań:
— organizacyjnych (przełożonych użytkownika);
— technicznych (administratora systemu i służb ochrony);
— operacyjnych (użytkownika w systemie);
— programowych i sprzętowych podsystemu kontroli dostępu systemu teleinformatycznego.

Działania organizacyjne przełożonych można przypisać do następujących procesów:
— **Opracowania i wdrożenia polityki i procedur bezpieczeństwa**.
— **Dopuszczenia użytkowników**, zgodnie z wymogami realizowanych zadań służbowych i z uwzględnieniem zasady „wiedzy koniecznej", do pracy z informacją niejawną. Wynikiem pomyślnego przejścia procesu dopuszczenia powinno być stwierdzenie „rękojmi bezpieczeństwa" i przyznanie użytkownikowi odpowiedniego certyfikatu osobowego, zawierającego podstawowe dane autoryzacyjne użytkownika.
— **Klasyfikacji informacji**, która ma być przetwarzana, przesyłana i przechowywana w systemie teleinformatycznym. Na zakończenie tego procesu cała informacja powinna mieć przypisane etykiety ze zbioru {*jawne, zastrzeżone, poufne, tajne, ściśle tajne*} oraz powinna być pogrupowana w odpowiednie kategorie (por. rozdz. 5).
— **Akredytacji systemu**, w którym mają być przetwarzane informacje niejawne. Warunkiem koniecznym otrzymania zgody na przetwarzanie informacji niejawnych (akredytacji) jest pomyślne zakończenie procesu oceny zdolności systemu do ochrony takich informacji, potwierdzone przyznaniem systemowi odpowiedniego certyfikatu.

Działania techniczne administratora systemu w zakresie ochrony dostępu do informacji polegają (oprócz właściwej konfiguracji sprzętu i oprogramowania) na:
— **rejestracji w systemie** użytkowników i ich uprawnień zgodnie z odpowiednimi procedurami;
— **skonfigurowaniu i uruchomieniu mechanizmów nadzoru** (w tym zapisu) działań użytkowników w systemie;
— **przydzieleniu haseł** początkowych użytkownikom.

Działania techniczne służb ochrony dotyczą **ograniczenia dostępu fizycznego** do elementów systemu teleinformatycznego przez umieszczenie ich w odpowiednio zaprojektowanych, wyposażonych i nadzorowanych strefach bezpieczeństwa oraz odpowiednie przedsięwzięcia organizacyjne (w tym współudział w działaniach organizacyjnych przełożonych).

Działania operacyjne użytkownika w zakresie uzyskania dostępu do informacji w systemie (po zmianie hasła początkowego) polegają na:
— **podaniu danych uwierzytelniających** (np. login i hasło);
— **podaniu kodu operacji** na informacji (obiekcie) w systemie.

Działania podsystemu kontroli dostępu systemu teleinformatycznego, po wykonaniu przez użytkownika ww. działań, to:
— **Identyfikacja użytkownika** (uwierzytelnienie) na podstawie danych uwierzytelniających i w zależności od wyników identyfikacji dopuszczenie użytkownika do dalszych działań w systemie lub zabronienie dostępu.
— W przypadku pomyślnego uwierzytelnienia użytkownika i podaniu przez niego kodu operacji na obiekcie, **sprawdzenie autoryzacji użytkownika**[1] i, w zależności od wyników tego sprawdzenia, dopuszczenie do wykonania danej operacji na wybranym obiekcie lub zabronienie jej wykonania.

W dalszej części artykułu będą omawiane działania z poziomu programowego i sprzętowego podsystemu kontroli dostępu systemu teleinformatycznego. Zakłada się przy tym, że działania z pozostałych poziomów zostały zrealizowane prawidłowo.

Warto zwrócić uwagę, że problem nieuprawnionego dostępu do systemów teleinformatycznych podlega różnym unormowaniom [12, 13, 14] także na forum międzynarodowym (por. przykład 1). W obszarze militarnym (NATO) takie unormowania zawiera Dyrektywa Bezpieczeństwa Zjednoczonego Dowództwa Europejskiego AD 70-1 PL [12].

[1] Potocznie ten proces jest nazywany *autoryzacją użytkownika w systemie.*

Przykład 1. Zalecenia formalno-prawne

DECYZJA RAMOWA RADY EUROPY 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne:

Artykuł 2
Nielegalny dostęp do systemów informatycznych:
1. Każde Państwo Członkowskie podejmuje niezbędne środki celem zapewnienia, że umyślny bezprawny dostęp do całości lub części systemu informatycznego jest karalny jako przestępstwo, przynajmniej w przypadkach, które nie są przypadkami mniejszej wagi.
2. Każde Państwo Członkowskie może zdecydować, że zachowanie, o którym mowa w ust. 1, jest objęte oskarżeniem jedynie w przypadkach, kiedy przestępstwo popełniane jest z naruszeniem zabezpieczenia.

Implementacja powyższej decyzji ramowej w realiach polskich powoduje, że do polskiego Kodeksu Karnego jest przewidziane wprowadzenie stosowanych zmian:
Art. 267 Kodeksu Karnego (cytaty z projektu zmian z 24.04.2007 i 01.04.2008):
§1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nie przeznaczonej, otwierając zamknięte pismo, *podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie*, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
§2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

2. System ochrony informacji

Budując system ochrony informacji w systemach teleinformatycznych, należy uwzględniać dobrą praktykę inżynierską. Wynika z niej na przykład, że każdy ze znanych sposobów zabezpieczania można zakwalifikować do jednej z następujących grup:
1) **fizycznej i technicznej ochrony** przed nieupoważnionym dostępem fizycznym, ogniem i wodą, obejmującej nie tylko ludzi-strażników ale także skomputeryzowane systemy alarmowania o włamaniach, monitoringu, i ppoż., oraz środki mechaniczne (sejfy, zamki, przegrody budowlane itp.);
2) **sprzętowo-programowej**, obejmującej:
   — odpowiednią ochronę dostępu na poziomie logicznym,
   — odpowiedni poziom kryptograficznej ochrony tajności oraz integralność informacji,
   — monitorowanie przepływu pakietów w sieci i działań użytkowników,

— zapewnienie odpowiedniego poziomu dostępności informacji przez redundancje sprzętowe i programowe, w tym odpowiednio zbudowane systemy zasilania gwarantowanego,
— zapewnienie właściwego niszczenia informacji zapisanej na komputerowych nośnikach i na wydrukach z systemu komputerowego;

3) **organizacyjno-kadrowej**, obejmującej:
— właściwe udokumentowanie systemu ochrony informacji,
— klasyfikację informacji i przyznawanie praw dostępu do niej,
— szkolenia i treningi z zakresu bezpieczeństwa,
— właściwe przydzielenie zakresów odpowiedzialności za ochronę informacji,
— organizację nadzoru i kontroli w zakresie ochrony informacji,
— zasady reagowania na incydenty z zakresu bezpieczeństwa teleinformatycznego.

W zbiorze środków ochrony B_T można wyróżnić zatem zabezpieczenia:
— fizyczne i techniczne B_{TF},
— sprzętowo-programowe B_{TSP},
— organizacyjne i kadrowe B_{TO},
gdzie $B_T = B_{TF} \cup B_{TSP} \cup B_{TO}$.

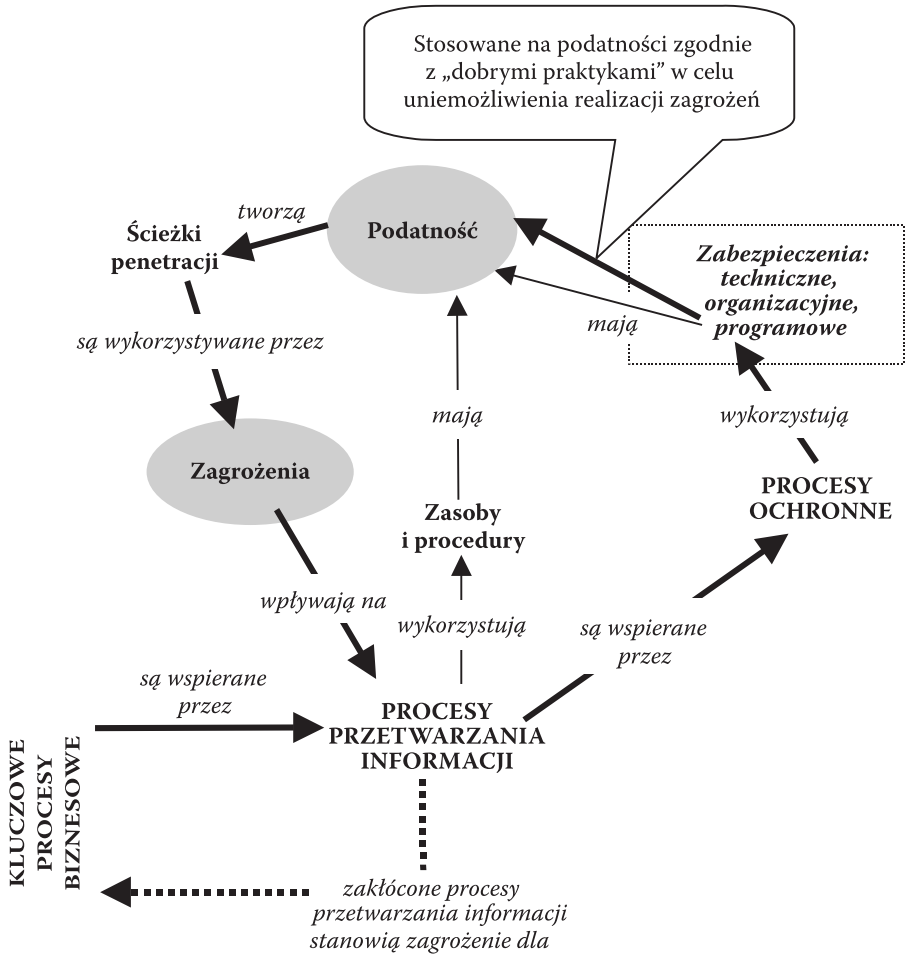
Na rysunku 1 są pokazane związki między procesami biznesowymi oraz zachodzącymi w systemie teleinformatycznym. Składają się na nie procesy przetwarzania informacji i — niejako „nałożone" na nie — procesy, których celem jest zapewnienie odpowiedniego poziomu ochrony informacji przetwarzanej w systemie teleinformatycznym. Do jego zapewnienia w procesach tych są wykorzystywane środki ochronne (zabezpieczenia) z trzech grup wymienionych na początku niniejszego rozdziału. Zatem zabezpieczenia można zdefiniować (przynajmniej na potrzeby tego opracowania) następująco:

Definicja

Termin **zabezpieczenia** oznacza elementy osobowe, techniczne, programowe lub organizacyjne wykorzystywane w procesach ochronnych do działań, których celem jest zapewnienie odpowiedniego poziomu ochrony logicznej i fizycznej informacji oraz elementów systemu teleinformatycznego.

Cechą poprawnego pod względem inżynierskim systemu bezpieczeństwa teleinformatycznego jest skuteczność. Jej podstawową przesłankę stanowi **kompleksowość** takiego systemu, rozumiana tutaj w następujący sposób:
— zastosowane zabezpieczenia powinny uwzględniać każdą z wymienionych w definicji grup (dywersyfikacja zabezpieczeń);

— zabezpieczenia powinny być zorganizowane tak, żeby zapewnić wykrycie naruszenia bezpieczeństwa oraz prób takich działań oraz skuteczną ochronę mimo przełamania części zabezpieczeń.



Rys. 1. Zależności przyczynowo-skutkowe w procesie identyfikacji procesów, zagrożeń, podatności i zabezpieczeń

Ostatni punkt oznacza, że zabezpieczenia powinny być zorganizowane według schematu tzw. *obrony w głąb*, której najlepszą wizualizacją jest średniowieczny zamek, odpowiednio umiejscowiony w terenie, otoczony fosą i kilkoma pasami murów obronnych wzmocnionych wieżami. Pokonanie fosy i przerwanie zewnętrznego pasa murów obronnych przez napastników zwykle nie prowadziło do utraty zamku,

ponieważ obrońcy wycofywali się za drugi, wewnętrzny pas murów obronnych i bronili się dalej. Warunkami dodatkowymi do wymogu kompleksowości są **spójność** (rozumiana jako brak luk w systemie ochrony, które mogłyby utworzyć ścieżki penetracji bez przełamywania zabezpieczeń) oraz **niesprzeczność** (rozumiana jako brak kolizji między zastosowanymi zabezpieczeniami).

3. Uwierzytelnianie i autoryzacja podmiotów, urządzeń i procesów

Wśród procesów ochronnych dwa mają znaczenie szczególne ze względu na kontrolę dostępu do elementów systemu teleinformatycznego i przetwarzanej w nim informacji.

Te procesy to:

— **uwierzytelnianie** — proces sprawdzający czy podmiot jest uprawniony do działania w systemie i, w razie pozytywnej identyfikacji, dopuszczający podmiot do dalszych działań w systemie.

— **weryfikacja autoryzacji** — proces sprawdzający, jakie uprawnienia w systemie ma podmiot i, w razie pozytywnej weryfikacji żądań podmiotu, dopuszczający go do dalszych działań w systemie.

Rozważając proces uwierzytelniania, nie należy mylić *uwierzytelniania podmiotów* z *uwierzytelnianiem danych*, tj. procesem wykorzystywanym do weryfikacji integralności danych, np. weryfikacji przeprowadzanej w celu stwierdzenia, czy dane otrzymane są identyczne z danymi wysłanymi.

Proces uwierzytelniania może dotyczyć nie tylko użytkownika (osoby), ale także stacji roboczej (wykorzystuje się adres fizyczny karty sieciowej), procesu w systemie oraz wymiennych nośników danych. Warto zwrócić także uwagę, że proces uwierzytelniania osób jest stosowany w systemach:

— kontroli dostępu fizycznego (np. do pomieszczeń) oraz

— kontroli dostępu logicznego (np. do określonej aplikacji).

Stosowane są trzy podstawowe metody, dzięki którym podmiot-użytkownik może uwierzytelnić swoją tożsamość:

— **weryfikacja przedmiotu posiadanego przez podmiot** (ang. *something he or she has*) — użytkownik otrzymuje dostęp do zasobów na podstawie identyfikacji przez system pewnego znacznika (ang. *tokena*), którym może być klucz, karta magnetyczna lub elektroniczna, a nawet specjalne urządzenie. Znacznik zawiera jednocześnie informacje o użytkowniku, co pozwala uniknąć wprowadzania ręcznego tej informacji. Obecnie wykorzystywane są głównie karty magnetyczne i mikroprocesorowe. W celu minimalizacji ryzyka związanego z nieupo-

ważnionym dostępem (np. w przypadku zagubienia lub pozostawienia go w miejscu dostępnym) użycie znacznika jest często połączone z koniecznością wprowadzenia przez użytkownika tzw. Osobistego Numeru Identyfikacyjnego (ang. *Personal Identification Number* — PIN), a po kilku nieudanych próbach wprowadzenia PIN, czytniki mogą zatrzymywać kartę;

— **weryfikacja cech fizycznych podmiotu** (ang. *something he or she is*) — metoda polega na identyfikacji biometrycznej (analiza odcisków palców, siatkówki oka, głosu, itd.), a zatem nadaje się wyłącznie do identyfikacji podmiotów-ludzi. Podstawowe problemy związane z wykorzystaniem praktycznym tej metody dotyczą ochrony baz wzorców biometrycznych[2], rozpoznania żywości podmiotu oraz minimalizacja fałszywych identyfikacji. Techniki stosowane w metodzie biometrycznej są obecnie intensywnie badane i udoskonalane. Urządzenia, w których są zaimplementowane, gwałtownie tanieją, co daje szansę na ich szersze zastosowanie;

— **weryfikacja wiedzy podmiotu** (ang. *something he or she knows*) — metoda ta polega na sprawdzaniu informacji znanej wyłącznie podmiotowi. Najprostszą i najczęściej stosowaną formą realizacji tej metody jest **sprawdzanie hasła**; znacznie rzadziej sprawdzanie innych informacji znanych uprawnionemu podmiotowi (np. imię matki, data urodzenia żony itp.), ze względu na brak akceptacji użytkowników i stosunkowo łatwe uzyskanie takich informacji.

Jak już wspomniano, uwierzytelnianie użytkowników w systemie teleinformatycznym jest dokonywane najczęściej przy pomocy *haseł* i *metod dialogowych*. Procedury uwierzytelniające wykonuje się raz na początku sesji lub w przypadku przerwania transmisji, więc nie muszą być zbyt oszczędne ale również nie powinny być zbyt skomplikowane, bo użytkownik będzie się starał je omijać.

Najczęściej stosowana procedura uwierzytelniania to tzw. *metoda prostych haseł*. Polega ona na podaniu przez jednego użytkownika hasła i sprawdzeniu jego poprawności przez system. W praktyce są też stosowane, dające silniejsze uwierzytelnianie, wariacje metody prostych haseł:

— podawanie wybranych znaków — system żąda podania nie całego hasła, lecz znaków ze wskazanych pozycji w haśle;

— hasła jednorazowe — użytkownik i komputer używają tylko raz kolejnego hasła z listy (wadą jest to, że przy błędach w transmisji nie wiadomo, czy jest złe hasło, czy transmisja).

[2] Baza z wzorcami biometrycznymi jest bazą z danymi osobowymi w rozumieniu ustawy o ochronie danych osobowych.

Przy posługiwaniu się hasłami, należy pamiętać że:

1) hasło, podobnie jak prywatny klucz kryptograficzny, powinno być skutecznie chronione przed nieuprawnionym wykorzystaniem;
2) hasło powinno być trudne do odgadnięcia — elementy, którymi można manipulować, to: *długość hasła, użyty do jego wytworzenia repertuar znaków (liczność zbioru znaków wpływająca na liczbę kombinacji), przypadkowość zestawienia znaków w hasło*;
3) im dłuższe hasło, tym skuteczniejsza ochrona *(ale efekt ten może zniweczyć zła implementacja systemu haseł — por. casus Windows NT i implementacji NTLM i LM)*;
4) im dłużej używane hasło, tym więcej czasu ma potencjalny intruz na jego złamanie i wykorzystanie;
5) hasła nie powinny być przechowywane w postaci jawnej *(również tak drukowane czy wyświetlane)*,

   ale (!)
   hasła osób o szczególnych uprawnieniach w systemie (np. administratorów) lub zarządzających aplikacjami i/lub systemami, do których dostęp jest ograniczony (np. administrator repozytorium projektowego systemu CASE), powinny być zapisane i przechowywane w bezpiecznym, znanym i dostępnym przełożonym miejscu[3];
6) współczesne systemy operacyjne udostępniają administratorowi szereg możliwości w zakresie zarządzania hasłami *(długość, częstość zmian, powtórzenia itd.)*.

Oprócz haseł można w procesie uwierzytelniania skorzystać z *metody dialogowej* (metody pytań i odpowiedzi). Polega ona na tym, że system utrzymuje zbiór pytań i odpowiedzi, a przy rozpoczęciu sesji zadaje losowo „n" z nich. Użytkownik musi udzielić właściwych odpowiedzi.

Innym sposobem uwierzytelniania podmiotów przy dostępie do systemu jest sposób dostępu wykorzystujący tzw. bilety. Najbardziej znanym jest opracowany w latach 80. XX wieku na Massachusetts Institute of Technology we współpracy z firmami IBM i DEC system (i protokół) Kerberos. Jego współczesne znaczenie wiąże się z faktem zaimplementowania wersji 5 tego protokołu przez firmę Microsoft jako podstawowego dla uwierzytelniania podmiotów w systemie operacyjnym Windows 2000. Kerberos w tym systemie operacyjnym został zaimplementowany zgodnie z otwartym standardem zawartym w dokumencie RFC1510. W celu potwierdzenia tożsamości podmioty muszą skorzystać z usługi centrum dystrybucji kluczy (KDC

[3] Np. w celu umożliwienia dostępu do danych w przypadku śmierci pracownika odpowiedzialnego za te dane.

— ang. *Key Distribution Center*). KDC zostaje zainstalowane w systemie Windows 2000 Server wraz z instalacją usługi Active Directory[4]. W procesie uwierzytelniania wykorzystywana jest baza skrótów haseł użytkowników, która jest zawarta właśnie w Active Directory. Podstawowe słabości systemu Kerberos to:

— system Kerberos wymaga bezpiecznego serwera Kerberos — nieuprawniony dostęp do takiego serwera grozi przejęciem przez intruza głównej bazy haseł systemu;
— system Kerberos wymaga ciągłej dostępności serwera Kerberos.

Podstawowa niedoskonałość koncepcji uwierzytelniania za pomocą haseł polega na tym, że w przypadku wymaganego dostępu chronionego do różnych obiektów uwierzytelnianie, zgodnie z regułami sztuki, powinno się odbywać z wykorzystaniem różnych haseł. Wymaga to od użytkownika pamiętania nieraz wieloelementowego zbioru haseł. Dodatkowym utrudnieniem jest to, że zbiór ten, ze względu na stosowane reguły bezpieczeństwa, powinien być zbiorem zmieniającym się w czasie. Także sam fakt nieraz wielokrotnego w czasie jednej sesji podawania danych uwierzytelniających, może frustrować użytkownika i powodować próby obejścia mechanizmów kontroli dostępu.

Dlatego we współczesnych systemach teleinformatycznych próbuje się stosować tzw. *jeden punkt uwierzytelniania* (SSO — ang. *Single Sign-On*) — mechanizm, z pomocą którego jedna akcja uwierzytelniania oraz autoryzacji umożliwia użytkownikowi uzyskanie dostępu do wszystkich komputerów oraz systemów, do których dany użytkownik ma uprawnienia dostępu, bez konieczności wielokrotnego wprowadzania haseł[5]. Odmiany SSO to:

1. Jeden zestaw poświadczeń, np. *Kerberos*.
2. Wiele zestawów poświadczeń, np. *Credential Manager* (Win 2003 i XP).

Mechanizm SSO należy do modnego trendu rozwoju metod uwierzytelniania podmiotów, tzw. *zarządzania tożsamością*.

Uwierzytelnianie tożsamości podmiotów i systemów ma także istotne znaczenie w sieciach, jako sposób przeciwdziałania atakowi intruza przez linie transmisji danych. Podstawowe, stosowane w praktyce, zabezpieczenie, to korzystanie z protokołów dostarczających mechanizmów uwierzytelniania w połączeniach komutowanych (por. przykład 2).

[4] Serwerem kluczy może być każdy kontroler domeny.

[5] Warto zauważyć, że *jeden punkt uwierzytelniania* to także *jeden punkt awarii* skutecznie unieruchamiający cały system lub pozwalający intruzowi na dostęp do wszystkich chronionych zasobów.

Przykład 2. Protokoły dostarczające mechanizmów uwierzytelniania:[6]

1. **TACACS** (*TAC Access Control Server*) jest protokołem klient-serwer (demon serwera nasłuchuje zwykle na porcie 49) firmy TAC. **TACACS+** jest unowocześnionym przez CISCO protokołem TACACS; do transportu wykorzystuje TCP. Klientem TACACS+ jest zwykle serwer dostępowy, a serwerem proces-demon działający na komputerze z systemem UNIX lub NT. Protokół TACACS+ umożliwia:
   — wymianę uwierzytelnień o narzuconej długości i zawartości, co umożliwia w klientach TACACS+ zastosowanie dowolnego mechanizmu uwierzytelniania (Kerberos, karty znacznika, PAP PPP, itd.);
   — autoryzację (może dostosować usługę do danego użytkownika);
   — rozliczanie użytkowników (są zapisywane ich działania).
2. **RADIUS** (*Remote Adress Dial-In User Service*) jest protokołem klient-serwer (demon serwera nasłuchuje zwykle na porcie 1812); do transportu wykorzystuje UDP. Klientem RADIUS jest zwykle serwer dostępowy, a serwerem proces-demon działający na komputerze z systemem UNIX lub NT. Podobnie jak TACACS+ umożliwia uwierzytelnianie, autoryzację i rozliczanie użytkowników.
3. **IPSec** (*IP Scecurity*) — jest to zbiór protokołów opracowywanych od 1992 roku przez IETF w celu podwyższenia bezpieczeństwa komunikacji w sieciach TCP/IP. IPSec jest opisany w dokumentach RFC 2401-2411, 2451 i 2709. Obecna zalecana wersja IPSec v.6 obejmuje zestaw protokołów:
   — AH (*Authentication Header)* — uwierzytelniający;
   — ESP (*Encapsulation security Payload*) — zabezpieczenia zawartości pakietu;
   — SA (*Security Associations*) — bezpiecznych połączeń. Protokół ten umożliwia dwa tryby pracy: *transportowy* (do transmisji w sieciach LAN: komputer-komputer i komputer-bramka IPSec) i *tunelowy* (głównie do komunikacji firewall-firewall; umożliwia budowę VPN);
   — IKE (*Internet Key Management*) — zarządzania kluczami.

Ze względu na kluczowe znaczenie dla ochrony przed niepożądanym dostępem, system uwierzytelniania jest szczególnie narażony na różnego rodzaju ataki. Oprócz nadużyć[7] na poziomie organizacyjnym i technicznym (por. wstęp) należy się liczyć z atakami na system uwierzytelniania. Można je sklasyfikować jako:

1. Bezpośrednie — polegają na przejęciu elementu uwierzytelniającego (np. pliku haseł, tokena, przepustki), ewentualnej obróbce (np. rozszyfrowaniu pliku haseł, zamiany zdjęcia na przepustce) i nieuprawnionym wykorzystaniu.

[6] Bardzo dobre omówienie tej tematyki zainteresowany Czytelnik znajdzie w [6] i [11].

[7] Od strony formalnej, takie nadużycia można traktować jak ataki.

2. Pośrednie — polegają na wykorzystaniu podatności systemu uwierzytelniania związanych z przesyłaniem informacji uwierzytelniających. Do podstawowych technik ataku należą:
   a) podsłuch sieciowy;
   b) podsłuch ulotu elektromagnetycznego;
   c) przechwytywanie i odtwarzanie informacji uwierzytelniającej (atak powtórzeniowy);
   d) przejęcie uwierzytelnionej sesji.
3. Typu „social engineering" — polegają na obserwacji i oddziaływaniu na użytkowników systemu uwierzytelniania oraz przeszukiwaniu środowiska pracy atakowanego użytkownika w celu przejęcia informacji lub elementu uwierzytelniającego.

W celu zminimalizowania możliwości ataku na system uwierzytelniania, stosuje się m.in. metody kryptograficzne. Sposoby realizacji kryptograficznych usług ochrony przesyłanej informacji (nie tylko) uwierzytelniającej są następujące:

1) integralność zawartości — przez dołączenie do wiadomości znacznika integralności, będącego ciągiem bitów obliczonych na podstawie wiadomości. Dla wykluczenia możliwości podszycia się intruza pod innego użytkownika sieci, usługa ta nie powinna być realizowana samodzielnie, lecz zawsze jako część składowa usług uwierzytelniania i niezaprzeczalności;
2) integralność sekwencji[8] — nadawca zawiera w wiadomości, a odbiorca sprawdza numer sekwencyjny wiadomości lub nadawca może zażądać potwierdzenia odebrania wiadomości;
3) wykrycie powielonych lub przechwyconych i przesłanych z opóźnieniem wiadomości:
   — nadawca zawiera w wiadomości, a odbiorca sprawdza numer sekwencyjny,
   — nadawca zawiera w wiadomości, a odbiorca sprawdza znacznik czasu;
4) uwierzytelnianie nadawcy — przez dołączenie do wiadomości znacznika uwierzytelniania wiadomości (ang. MAC — *Message Authentication Code*), którego wartość jest funkcją wiadomości i tajnego klucza, znanego tylko nadawcy i odbiorcy;
5) niezaprzeczalność nadania — przez zastosowanie podpisu cyfrowego;
6) utajnianie zawartości — przez zaszyfrowanie zawartości wiadomości.

4. Sterowanie dostępem do informacji — realizacja praktyczna

Podstawowe znaczenie dla skutecznej ochrony informacji przetwarzanej, przesyłanej i przechowywanej w systemie teleinformatycznym ma **sterowanie**

[8] W celu wykrycia utraty wiadomości lub zmiany kolejności wiadomości.

dostępem na poziomie fizycznym i logicznym do informacji i elementów systemu teleinformatycznego (obiektów, w tym zabezpieczeń). Sterowanie takie jest realizowane na bazie procesów ochronnych:

1. Uwierzytelniania (opisanego bardziej szczegółowo w rozdziale 3):
   — w systemach dostępu logicznego do systemu teleinformatycznego;
   — w systemach dostępu fizycznego do obiektów.
2. Wykrywania:
   — nieuprawnionych działań;
   — zagrożeń środowiskowych (np. pożar, zalanie). Te zagrożenia można traktować także w kategoriach niepożądanego „dostępu" ognia lub wody do elementów systemu komputerowego.
3. Autoryzacji osób i/lub procesów (którego formalna strona jest przedstawiona w rozdziale 5).

Procesy uwierzytelniania wykorzystują zabezpieczenia (por. rozdz. 2):

— wbudowane w systemy operacyjne (integralne procesy uwierzytelniania w systemach operacyjnych), czyli z grupy B_{TSP};
— dodane do systemu w ramach budowy systemu ochrony (autonomiczne systemy kontroli dostępu do danych), czyli z grupy B_{TSP} w wypadku dostępu logicznego i B_{TF} w wypadku dostępu fizycznego.

Ale zabezpieczenia te nie będą skuteczne, jeśli nie zostaną wsparte odpowiednio dobranymi zabezpieczeniami z grupy B_{TO}, takimi jak:

— procedury nadawania i odbierania praw dostępu do informacji ($B_{TO} \rightarrow B_{TSP}$)[9];
— procedury nadawania i odbierania praw dostępu do pomieszczeń i urządzeń ($B_{TO} \rightarrow B_{TF}$);
— procedury działania służb nadzoru i prewencji w zakresie obsługi skomputeryzowanych systemów wykrywania włamań i reakcji na wykryte zagrożenia ($B_{TO} \rightarrow B_{TF}$);
— szkolenia ($B_{TO} \rightarrow B_{TSP}$, B_{TF}).

Procesy wykrywania obejmują podprocesy:

— monitorowania;
— alarmowania (powiadamiania)[10];
— zapisu (rejestracji) zdarzeń;
— analizy zapisów.

[9] $B_{TO} \rightarrow B_{TSP}$ czytaj: zabezpieczenie organizacyjne wspierające zabezpieczenie...

[10] Ten podproces należy interpretować jako przekazywanie informacji/sygnałów do ustalonych elementów systemu komputerowego — plików, innych procesów lub elementów wykonawczych.

Procesy wykrywania wykorzystują zabezpieczenia:
- — w zakresie nieuprawnionych działań: IPS (*Intrusion Prevention System*), skomputeryzowane narzędzia do analizy zapisów w dziennikach zdarzeń systemów operacyjnych i urządzeń (B_{TSP});
- — w zakresie zagrożeń środowiskowych: systemy ppoż., systemy wykrywania wilgoci (B_{TF}).

Ale zabezpieczenia te nie będą skuteczne, jeśli nie zostaną wsparte odpowiednio dobranymi zabezpieczeniami z grupy B_{TO}, takimi jak:
- — procedury reakcji na incydenty nieuprawnionych działań w sieci komputerowej ($B_{TO} \rightarrow B_{TSP}$);
- — procedury działania służb nadzoru i prewencji w zakresie obsługi skomputeryzowanych systemów wykrywania zagrożeń środowiskowych i reakcji na wykryte zagrożenia ($B_{TO} \rightarrow B_{TF}$);
- — szkolenia ($B_{TO} \rightarrow B_{TSP}$, B_{TF}).

Procesy autoryzacji osób/procesów wykorzystują zabezpieczenia:
- — wbudowane w systemy operacyjne (integralne procesy autoryzacji działań w systemach operacyjnych), czyli z grupy B_{TSP};
- — dodane do systemu teleinformatycznego w ramach budowy systemu ochrony (autonomiczne systemy kontroli dostępu do danych), czyli z grupy B_{TSP} w wypadku dostępu logicznego i B_{TF} w wypadku dostępu fizycznego.

Ale zabezpieczenia te nie będą skuteczne, jeśli nie zostaną wsparte odpowiednio dobranymi zabezpieczeniami z grupy B_{TO}, takimi jak:
- — procedury autoryzacji praw dostępu do informacji ($B_{TO} \rightarrow B_{TSP}$);
- — procedury autoryzacji praw dostępu do pomieszczeń i urządzeń ($B_{TO} \rightarrow B_{TF}$);
- — procedury działania służb nadzoru i prewencji w zakresie obsługi błędów w autoryzacji praw dostępu do informacji ($B_{TO} \rightarrow B_{TSP}$) i pomieszczeń lub urządzeń ($B_{TO} \rightarrow B_{TF}$);.
- — szkolenia ($B_{TO} \rightarrow B_{TSP}$, B_{TF}).

5. Sterowanie dostępem do informacji — model formalny

Stosowane do ochrony przed nieuprawnionym dostępem, opisane w rozdz. 2, zabezpieczenia fizyczne i techniczne, osobowe, sprzętowo-programowe oraz odpowiednie rozwiązania organizacyjne, pozwalają na zorganizowanie różnych sposobów wymuszania i kontroli dróg dostępu[11]. Wyróżnia się trzy podstawowe sposoby sterowania dostępem:

1. **Uznaniowe sterowanie dostępem** (ang. *Discretionary Access Control*, DAC).

[11] W tym kontekście mówi się często o *sterowaniu* dostępem.

Środki ochronne, ograniczające dostęp do obiektów wykorzystują atrybut **własności** obiektu, umożliwiający podmiotowi nadanie lub odebranie innemu podmiotowi (lub grupie podmiotów) prawa dostępu do obiektu, którego jest właścicielem.

2. **Obowiązkowe sterowanie dostępem** (ang. *Mandatory Access Control*, MAC).
   Środki ochronne, ograniczające dostęp do obiektów wykorzystują przypisane do obiektu etykiety określającej **poziom tajności** (ang. *security level,* nazywanej też *etykietą wrażliwości* lub, jak to ma miejsce w modelu Bella-LaPaduli, *klasą bezpieczeństwa*) oraz formalnie nadane podmiotom **poziomy uprawnień** (ang. *clerance level*).
3. **Sterowanie dostępem wykorzystujące role** (ang. *Role Based Access Control*, RBAC).
   Uprawnienia dostępu do obiektów zamiast podmiotowi przypisane są **rolom**. Podmiot może pełnić różne role, ale zawsze powinien posiadać tylko takie uprawnienia, jakie są niezbędne do wypełnienia aktualnej roli.

Do dalszych rozważań, z tego względu że taki typ sterowania dostępem jest związany z omawianym w tym artykule modelem Bella-LaPaduli, przyjętym jako obowiązujący w unormowaniach z zakresu militarnego (por. np. [12]), będzie przyjęte obowiązkowe sterowanie dostępem.

Obowiązkowe sterowanie dostępem oznacza, że każdemu podmiotowi (może nim być człowiek lub proces) i zasobowi systemu (może to być informacja, np. w postaci pliku komputerowego lub papierowego dokumentu) nadaje się **klasę bezpieczeństwa**. Jest ona wyznaczana na podstawie **poziomu tajności**, opisywanego *etykietą ochrony* (np. ściśle tajne, tajne, poufne, zastrzeżone)[12] i **kategorii**, określającej klasę informacji, do której podmiot może uzyskać dostęp zgodnie z regułą „wiedzy niezbędnej". Nadawanie klas bezpieczeństwa potocznie nazywa się klasyfikacją. Klasyfikacja zasobów polega zatem na wyznaczaniu par:

$$\{poziom\ tajności, kategoria\ tajności\}$$

Należy zauważyć, że wprowadzenie, np. w firmie lub organizacji, klasyfikacji zasobów automatycznie wymusza wprowadzenie „klasyfikacji" (ang. *clearance*) pracowników (podmiotów) przez nadanie im odpowiednich uprawnień dostępu do zasobów klasyfikowanych. Klasyfikacja podmiotów odzwierciedla stopień zaufania klasyfikującego do podmiotu i obszar działania podmiotu (klasę informacji lub, szerzej, zbiór zasobów, do której może mieć dostęp). Klasyfikacja zasobów

[12] Jest to przykład etykiet ochrony stosowanych w Polsce na postawie ustawy o ochronie informacji niejawnych. Podobna czterostopniowa klasyfikacja jest przyjęta w całej Unii Europejskiej.

odzwierciedla ich wrażliwość, czyli jest miarą ważności, przypisaną zwykle do informacji zawartych w obiekcie (zasobie).

Na podstawie opisanej wyżej klasyfikacji informacji, w Dyrektywie Bezpieczeństwa Zjednoczonego Dowództwa Europejskiego AD 70-1 PL [12] zdefiniowano tzw. *bezpieczne tryby pracy systemów komputerowych*:

1. Tryb dedykowany (ang. *dedicated mode)*
   Wszyscy użytkownicy, posiadający dostęp do systemu komputerowego, są upoważnieni do najwyższej klauzuli tajności informacji przetwarzanej, przechowywanej i przesyłanej przez ten system komputerowy i mają dostęp do całej informacji (przy zachowaniu zasady „*wiedzy koniecznej*"[13] — oznacza to, że wymagania bezpieczeństwa nie narzucają obowiązku separacji danych wewnątrz systemu komputerowego).
2. Tryb wysokiego poziomu (ang. *system high mode*)
   Wszyscy użytkownicy, posiadający dostęp do systemu komputerowego są upoważnieni do najwyższej klauzuli tajności informacji przetwarzanej przechowywanej i przesyłanej przez ten system komputerowy, natomiast **nie wszyscy** posiadający taki dostęp i upoważnienie będą mieli dostęp do konkretnej informacji (zgodnie z zasadą „*wiedzy koniecznej*" — zastosowane środki bezpieczeństwa muszą zapewniać selektywny dostęp i separację informacji wewnątrz systemu komputerowego).
3. Tryb wielopoziomowy (ang. *multilevel mode*)
   Nie wszyscy użytkownicy, posiadający dostęp do systemu komputerowego, posiadają upoważnienie odpowiadające najwyższej klauzuli tajności informacji przetwarzanej, przechowywanej i przesyłanej przez dany system komputerowy i **nie wszyscy** posiadający taki dostęp i upoważnienie będą mieli dostęp do konkretnej informacji (zgodnie z zasadą „*wiedzy koniecznej*"). Ten tryb pracy pozwala na jednoczesne przechowywanie, przetwarzanie lub transmisję informacji o różnych klasyfikacjach i różnych kategoriach przeznaczenia.

Jedną z podstawowych konstrukcji formalnych, wykorzystywanych w modelu Bella-LaPaduli, jest **macierz dostępu** (nazywana też macierzą uprawnień). Składa się ona z wierszy reprezentujących *podmioty* (np. użytkowników) i kolumn reprezentujących *obiekty* (np. pliki, ale w ogólnym przypadku do zbioru O mogą należeć także podmioty). Zawiera podzbiory zbioru dopuszczalnych w systemie *uprawnień* $A(s_j, o_k)$, tzn. na przecięciu wiersza *j* i kolumny *k* znajduje się zbiór praw dostępu, jakie posiada podmiot *j* względem obiektu *k* (por. tab. 1).

[13] Zasada wiedzy koniecznej (w polskiej literaturze używane jest też określenie „wiedza niezbędna"): pracownik powinien wiedzieć tylko tyle, ile jest mu niezbędne do rzetelnego wykonywania jego obowiązków służbowych.

Tabela 1

Macierz dostępu

	Obiekty			
Podmioty	o_1	o_2	...	o_m
s_1	$A(s_1, o_1)$	$A(s_1, o_2)$		$A(s_1, o_m)$
s_2	$A(s_2, o_1)$	$A(s_2, o_2)$		$A(s_2, o_m)$
...				
s_n	$A(s_n, o_1)$	$A(s_n, o_2)$		$A(s_n, o_m)$

Aktualny stan ochrony modelowanego systemu opisuje trójka:

$$(S, O, A)$$

gdzie: S — jest zbiorem podmiotów $S = \{s_i \mid i \in \overline{1,n}\}$;

O — jest zbiorem obiektów $O = \{oj \mid j \in \overline{1,m}\}$;

A — jest macierzą dostępu (uprawnień).

Mechanizm autoryzacji sprawdza, czy dostęp r_{ij}, który podmiot s_i próbuje zastosować do obiektu o_j, należy do podzbioru praw dostępu określonego dla s_i i o_j w macierzy A, czyli czy na przecięciu kolumny odpowiadającej o_j i wiersza odpowiadającego s_i, znajduje się taki zbiór $A(s_j, o_j)$, że $r_{ij} \in A(s_j, o_j)$. Jeżeli ten warunek zachodzi, to podmiot s_i ma dostęp do obiektu o_j (w przeciwnym przypadku nie ma).

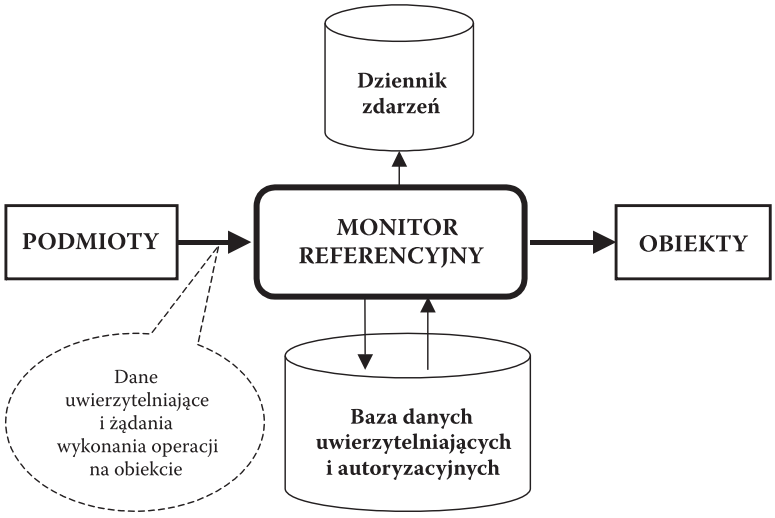
W modelu Bella-LaPaduli wprowadza się pojęcia:

— poziomu bezpieczeństwa dla obiektu i podmiotu (tzw. *poziom autoryzacji*), opisywanego za pomocą dwóch elementów: *klasyfikacji*, tj. elementu zbioru klas bezpieczeństwa i zbioru *kategorii*. Zbiór L poziomów bezpieczeństwa tworzy kratę;
— stanu bezpiecznego;
— podmiotu zaufanego (gwarantuje utrzymanie bezpieczeństwa);
— monitora referencyjnego (nadzoruje żądania wykonania operacji — por. rys. 2).

Monitor referencyjny to koncepcja wyrażona w formie zalecenia, aby wszystkie próby dostępu do obiektów uwierzytelniać i autoryzować na podstawie informacji zawartych w specjalnej bazie danych. Ponieważ jest to koncepcja (pewna idea), nie wspiera ona żadnego zbioru reguł dostępu ani konkretnej implementacji. Podstawowe wymagania, które musi spełniać każda implementacja monitora referencyjnego, są następujące:

— kompletność — każdy dostęp musi odbywać się przez monitor (nie można go obejść);

— izolowanie — musi być odporny na manipulacje;
— weryfikowalność — musi być możliwość wykazania jego poprawnej implementacji.



Rys. 2. Koncepcja monitora referencyjnego

Biorąc pod uwagę wymagania na systemy wojskowe eksploatowane w NATO można stwierdzić, że monitor referencyjny powinien być zaimplementowany jako element tzw. **wiarygodnej platformy komputerowej** (*TCB — Trusted Computer Base*), którą jest (cytat za [12]): *... całokształt mechanizmów bezpieczeństwa w systemie komputerowym obejmujący sprzęt i oprogramowanie sprzętowe i systemowe, których połączenie realizuje wdrożenie polityki bezpieczeństwa. Tworzy to podstawowe środowisko zabezpieczeń i dostarcza dodatkowych usług dla użytkowników. Zdolność wiarygodnej platformy komputerowej do właściwego wymuszania polityki bezpieczeństwa zależy wyłącznie od mechanizmów w niej zawartych i od właściwego wprowadzania parametrów przez personel administracyjny (np. upoważnienie i weryfikacja użytkowników), zgodnie z polityką bezpieczeństwa*.

W modelu Bella-LaPaduli rozważa się cztery podstawowe uprawnienia:
r — czytanie zawartości;
w — zmiana zawartości;
ap — dopisywanie zawartości[14];
x — wykonywanie programu.

[14] Warto zauważyć, że podmiot dopisujący nie widzi (dokładniej: zgodnie z założeniami dla modelu nie powinien widzieć) zawartości dokumentu (pliku), do którego coś dopisuje.

W modelu zapewnia się także zdecentralizowane administrowanie uprawnieniami do obiektów przez możliwość przypisania uprawnienia *n* zarządzania obiektami. Twórca obiektu jest uważany za jego właściciela i posiada uprawnienie do przekazywania i cofania uprawnień do tego obiektu innym użytkownikom (wyjątek stanowi uprawnienie *n*, które nie podlega przekazaniu).

W modelu Bella-LaPaduli *stanem systemu* nazywa się czwórkę:

$$\mathbf{(D, A, \lambda, H),}$$

gdzie: D — zbiór aktualnych uprawnień podmiotów do obiektów; trójka $(s_i, o_j, r_{ij}) \in D$ oznacza że podmiot s_i posiada aktualnie uprawnienie r_{ij} do obiektu o_j.
A — macierz uprawnień.
λ — funkcja poziomu, która jest przekształceniem $\lambda: O \cup S \rightarrow L$.
Symbol λ_{ok}, gdzie element $\lambda_{ok} \cup L$ oznacza poziom bezpieczeństwa obiektu o_k. Analogicznie, symbol λ_{sl}, gdzie element $\lambda_{sl} \cup L$ oznacza poziom bezpieczeństwa podmiotu s_l (nazywanego często w tym przypadku poziomem autoryzacji).
H — bieżąca hierarchia obiektów; jest to drzewo skierowane z korzeniem, w którym wierzchołki odpowiadają obiektom.
Poziom bezpieczeństwa danego obiektu nie może być niższy niż poziom bezpieczeństwa jego rodzica.

Stan systemu Q może ulec zmianie na Q' w wyniku wykonania operacji *op*, tj. *op*: Q→Q'. Zbiór OP operacji[15], powodujących zmianę stanu systemu, jest następujący:

get_access_r_{new},
release_access_ r_{new},
give_access_r_{ij},
rescind_access_r_{ij},
create_object,
delete_object,
change_user_security_level,
change_object_security_level.

Właściwości systemu opisuje się formalnie za pomocą sześciu aksjomatów.

Aksjomat_1 (bezpieczeństwa prostego)

Podmiot może mieć uprawnienia r lub w do obiektu tylko wtedy, gdy poziom autoryzacji podmiotu jest poziomem bezpieczeństwa równym lub wyższym niż poziom bezpieczeństwa obiektu.

[15] Interpretację wymienionych operacji zainteresowany Czytelnik znajdzie w [2] i [7].

Aksjomat_2 (gwiazdki)

Stan Q = (D, A, λ, H) systemu spełnia aksjomat gwiazdki wtedy i tylko wtedy, gdy dla każdego podmiotu s∈ S', przy czym S'⊆S jest zbiorem podmiotów nie będących zaufanymi i dla każdego obiektu o∈ O są spełnione trzy warunki:

$$ap \in A(s,o) \Rightarrow \lambda_o(o) \geq \lambda_s(s)$$
$$r \in A(s,o) \Rightarrow \lambda_o(o) \leq \lambda_s(s)$$
$$w \in A(s,o) \Rightarrow \lambda_o(o) = \lambda_s(s)$$

Aksjomat_3 (stałości)

Żaden podmiot nie może modyfikować klasyfikacji aktywnego obiektu.

Aksjomat_4 (bezpieczeństwa uznaniowego)

Stan systemu spełnia aksjomat bezpieczeństwa uznaniowego wtedy i tylko wtedy, gdy dla każdego podmiotu s, każdego obiektu o i każdego uprawnienia r jest spełniona implikacja:

$$(s, o, r) \in D \Rightarrow r \in A(s,o)$$

tzn. podmiot może korzystać tylko z tych uprawnień, do których ma autoryzację.

Aksjomat_5 (niedostępności obiektu nieaktywnego)

Stan Q = (D, A, λ, H) systemu spełnia aksjomat niedostępności obiektu nieaktywnego wtedy i tylko wtedy, gdy dla każdego podmiotu s i dla każdego obiektu nieaktywnego o zachodzi implikacja:

$$(s, o, r) \in D \Rightarrow r \neq r \wedge r \neq w$$

Aksjomat_6 (niezależności stanu początkowego)

Nowo aktywowany obiekt ma stan początkowy Q_0 niezależny od poprzednich aktywacji tego obiektu.

Z przedstawionych aksjomatów wynikają następujące wnioski:

1. Aksjomat bezpieczeństwa prostego ma zapobiec temu, że podmioty będą miały uprawnienia do informacji, będących na wyższym poziomie bezpieczeństwa niż poziom autoryzacji podmiotu.
2. Aksjomat gwiazdki oznacza że:

a) podmiot nie będący zaufanym może mieć uprawnienie *ap* (dopisywania) do obiektu, jeżeli poziom bezpieczeństwa obiektu jest nie niższy niż bieżący poziom bezpieczeństwa podmiotu;
b) podmiot nie będący zaufanym może mieć uprawnienie *r* (czytania) do obiektu, jeżeli bieżący poziom bezpieczeństwa podmiotu jest nie niższy niż poziom bezpieczeństwa obiektu;
c) podmiot nie będący zaufanym może mieć uprawnienie *w* (zmiany zawartości) do obiektu, jeżeli poziom bezpieczeństwa obiektu jest równy bieżącemu poziomowi bezpieczeństwa podmiotu.

3. Aksjomat bezpieczeństwa prostego oraz aksjomat gwiazdki są podstawą następujących reguł, dających pewność, że dostęp do informacji klasyfikowanej nie będzie możliwy dla podmiotów, które nie przeszły wymaganej weryfikacji:
   a) podmiot ma uprawnienia do czytania informacji klasyfikowanych z tych obiektów, których poziom bezpieczeństwa jest zdominowany przez poziom bezpieczeństwa podmiotu;
   b) podmiot ma uprawnienia do zapisywania informacji klasyfikowanych do tych obiektów, których poziom bezpieczeństwa dominuje nad poziomem bezpieczeństwa podmiotu.

Aksjomat stałości, wprowadzony w oryginalnym modelu Bella i LaPaduli, został z niego usunięty — w nowszych wersjach modelu dopuszcza się modyfikację klasyfikacji obiektów aktywnych według reguł formułowanych w zależności od rozpatrywanego systemu.

Model opisany w tym rozdziale został opracowany na potrzeby systemów operacyjnych, chociaż sprawdza się też w systemach baz danych (por. np. modele *Wooda* i *SeaView* [8]). Warto zauważyć, że model Bella-LaPaduli zapewnia **tajność** informacji, ale jednocześnie nie zabrania podmiotom pisać do obiektów o etykiecie wrażliwości dominującej nad poziomem uprawnień podmiotu — narusza to **integralność** informacji. Model ten identyfikuje także tzw. *ukryte kanały wycieku informacji* (ang. *covert channel*) — podmiot może wykryć istnienie obiektu o wyższym (niż jego) poziomie tajności, gdy zostanie mu zabroniony dostęp typu ***r***. Przegląd modeli formalnych wraz z ich podstawowymi charakterystykami jest zamieszczony w tabeli 2.

6. Podsumowanie

Problematyka ochrony przed niepożądanym dostępem jest nadal, pomimo upływu ponad trzydziestu lat od podjęcia pierwszych prac formalnych nad tym zagadnieniem [1, 2], przedmiotem intensywnych badań na całym świecie. Jako przykład można wskazać prace prowadzone w ramach projektu SECURE sponsorowanego przez Unię Europejską [9], a związane z zapewnianiem ochrony informacji

Tabela 2

Charakterystyka modeli ochrony informacji (za [7])

MODEL	Ochrona informacji w:		Sterowanie dostępem			Kontrola dostępu	Kontrola przepływu informacji lub dostępu pośredniego
	bazie danych	systemie operacyjnym	uznaniowe	obowiązkowe			
				poufność	integralność		
macierzowy	✓	✓	✓			✓	
„take-grant”	✓	✓	✓			✓	
Wooda	✓		✓			✓	
Bella-LaPaduli		✓	✓	✓		✓	
Biby		✓	✓	✓	✓	✓	✓
Diona		✓		✓	✓	✓	✓
Sea View	✓		✓	✓	✓	✓	✓
Jajodii-Sandhu	✓			✓		✓	✓
Smitha-Winslett	✓			✓		✓	✓
kratowy		✓					✓

w sieciach (głównie telefonii mobilnej). W ramach tego projektu wykorzystano sterowanie dostępem wykorzystujące role (por. rozdz.3) oraz pojęcia „zaufania” (ang. *trust*) i analizy ryzyka jako kluczowych elementów decydujących o przyznaniu dostępu podmiotom do określonych obiektów.

Powołując się na model Bella-LaPaduli [2, 3, 10], można stwierdzić, że do „należytej staranności” w zakresie ochrony dostępu do informacji należy spisanie, wdrożenie i przestrzeganie reguł bezpieczeństwa w zakresie utrzymania odpowiedniego poziomu tajności, w tym:

— reguły przydzielania dostępu do informacji zgodnie z zasadą „wiedzy niezbędnej”;
— reguły zabraniającej „pisania w dół”;
— reguły zabraniającej „czytania w górę”;
— reguł (i działań) zapewniających zaufanie do podmiotu-administratora.

Niestety, zaimplementowanie w systemach i sieciach komputerowych wymienionych reguł (czyli zbudowanie wielopoziomowego „wojskowego” systemu ochrony informacji) jest niezmiernie trudne i kosztowne. W praktyce okazało się także, a ma to konkretne przełożenie na pieniądze wykładane na badania i zakupy przez przemysł, że w systemach komercyjnych, w odróżnieniu od systemów wojskowych, większą wagę przywiązuje się do integralności niż tajności informacji (por. model

Clarka-Wilsona [5]). Dlatego rozwój „bezpiecznych" systemów komputerowych dla przemysłu poszedł własną drogą – por. np. politykę „chińskiego muru" [5], model Brewera-Nasha [4] czy ww. prace w ramach projektu SECURE.

Artykuł wpłynął do redakcji 25.07.2008 r. Zweryfikowaną wersję po recenzji otrzymano we wrześniu 2008 r.

LITERATURA

[1] J. P. Anderson, *Computer Security Technology Planning Study*, vol. 2 ESD-TR-73-51, Electronic System Division, Air Force System Command, Hansom Field, Bedford, MA, 01730, 1973.

[2] D. D. Bell, L. J. La Padula, *Secure Computer System: Unified Exposition and Multics Interpretation*, ESD-TR-75-306, Bedford, MA: ESD/AFSC, Hanscom AFB, 1974; available at: http://csrc.nist.gov/publications/history/bell76.pdf.

[3] D. E. Bell, *Looking Back at the Bell-La Padula Model*, Reston VA, 20191, Dec. 7. 2005.

[4] D. Brewer, M. Nash, *The Chinese Wall Security Policy*, Proc. IEEE Computer Society Symposium on Research in Security and Privacy, 1989, 215-228.

[5] D. Clark, D. R. Wilson, *A Comparison of Commercial and Military Computer Security Policies*, Proc. IEEE Symposium on Research in Security and Privacy, 1987, 184-194.

[6] J. Furtak, *Mechanizmy zabezpieczeń transmisji danych w środowisku Spiec*, w: Liderman K. (red.), Bezpieczeństwo teleinformatyczne. Problemy formalne i techniczne, Warszawa, 2006, 119-132.

[7] K. Liderman, *Podręcznik administratora bezpieczeństwa teleinformatycznego*, MIKOM, Warszawa, 2003.

[8] J. Stokłosa, T. Bilski, T. Pankowski, *Bezpieczeństwo danych w systemach informatycznych*, PWN, Warszawa–Poznań, 2001.

[9] J. M. Seigneur et al.: *SECURE Framework Architecture* (Beta), IST-2001-32486 SECURE project, part of the EU Global Computing Initiative.

[10] R. Smith, *Introduction to Multilevel Security*, artykuł dostępny pod: http://w.cs.stthomas.edu/faculty/rsmith/r/mls.

[11] Z. Świerczyński, *Wybrane metody uwierzytelniania użytkownika sieci komputerowej*, w: Liderman K. (red.): Bezpieczeństwo teleinformatyczne. Problemy formalne i techniczne, Warszawa, 2006, 209-235.

[12] Dyrektywa Bezpieczeństwa Zjednoczonego Dowództwa Europejskiego AD 70-1 PL (z dn. 1.01.97, ze zmianami z 16.02.01; część V: *Bezpieczeństwo ADP/INFOSEC*).

[13] Ustawa z dnia 22.01.1999*: O ochronie informacji niejawnej*, Dz. U. 11/99 poz. 95, znowelizowana.

[14] Rozporządzenie Prezesa Rady Ministrów z dn. 25.02.1999: *w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformacyjnych*. Dz. U. 18/99 poz. 162.

[15] Rozporządzenie MSWiA oraz ON z dn. 26.02.1999: *w sprawie sposobu oznaczania materiałów, w tym klauzulami tajności, oraz sposobu umieszczania klauzul na tych materiałach*. Dz. U. 18/99 poz. 167.

K. LIDERMAN

On organization and implementation of access control mechanisms to sensitive information in computer systems

Abstract. The paper discusses — on the example of Bell-LaPadula model — questions of access control to categorized information. Also the concepts of information security system and methods of subject authentication and conclusions arising from Bell-LaPadula model practical application are given.
Keywords: authentication, authorization, access control, categorization of information, Bell-LaPadula model
Universal Decimal Classification: 681.3.05