

IDŹ DO

PRZYKŁADOWY ROZDZIAŁ



SPIS TREŚCI

KATALOG KSIĄŻEK

KATALOG ONLINE

ZAMÓW DRUKOWANY KATALOG

TWÓJ KOSZYK

DODAJ DO KOSZYKA

CENNIK I INFORMACJE

ZAMÓW INFORMACJE
O NOWOŚCIACH

ZAMÓW CENNIK

CZYTELNIA

FRAGMENTY KSIĄŻEK ONLINE

Bezpieczeństwo sieci. Biblia

Autorzy: Eric Cole, Ronald L. Krutz, James Conley
Tłumaczenie: Marek Pętlicki (wstęp, rozdz. 1–10),
Wojciech Moch (rozdz. 11–14), Grzegorz Werner
(rozdz. 15, 17–19), Michał Grzegorzczak (rozdz. 16)
ISBN: 83-7361-946-1

Tytuł oryginału: [Network Security Bible](#)

Format: B5, stron: 625



Wszystkie najważniejsze zagadnienia związane z bezpieczeństwem sieci

- Opracowanie i wdrożenie polityki bezpieczeństwa w korporacyjnych systemach informatycznych
- Ochrona aplikacji i serwerów przed atakami z sieci
- Testowanie bezpieczeństwa systemów i interpretacja wyników badań

W czasach gdy dane kluczowe dla każdej firmy i organizacji są przechowywane w bazach danych na serwerach sieciowych, bezpieczeństwo systemów informatycznych jest sprawą niezwykle istotną. W wielu firmach pokutuje pogląd, że atak może nastąpić jedynie z zewnątrz – takie firmy posiadają zwykle doskonałe zabezpieczenia w postaci firewalli, skutecznie odstraszające potencjalnych włamywaczy. Jednakże ochrona danych to nie tylko zabezpieczenie ich przed atakiem z sieci – to także odpowiednia polityka postępowania wewnątrz firmy. Wielu spośród najgroźniejszych ataków hakerskich dokonano z wewnątrz korporacyjnej sieci. Dlatego też o wiele ważniejsza od urzędzeń jest świadomość użytkowników sieci. Dopiero ona, w połączeniu z odpowiednim sprzętem i oprogramowaniem, gwarantuje bezpieczeństwo systemu informatycznego.

„Bezpieczeństwo sieci. Biblia” to książka szczegółowo wyjaśniająca wszystkie kwestie związane z zabezpieczaniem firmowych sieci przed intruzami. Opisuje zasady i zalecane praktyki zabezpieczania sieci, przedstawia różne środki bezpieczeństwa przeznaczone dla różnych systemów oraz uczy, jak identyfikować zagrożenia i reagować na nie. Dzięki zawartym w niej wiadomościom będziesz w stanie oszacować poziom bezpieczeństwa sieci i wybrać najlepsze mechanizmy jej zabezpieczenia.

- Strategia zarządzania bezpieczeństwem systemu informatycznego
- Mechanizmy kontroli dostępu
- Zabezpieczanie systemów operacyjnych i aplikacji
- Bezpieczeństwo systemów Windows, Linux i Unix
- Rodzaje ataków
- Ochrona serwerów WWW i serwerów pocztowych
- Bezpieczeństwo protokołów sieciowych
- Kryptografia i steganografia
- Wykrywanie ataków i reagowanie na nie
- Ocena jakości zabezpieczeń systemów informatycznych

Informacja jest dziś najcenniejszym towarem. Naucz się ją ochraniać

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl



Spis treści

O autorach	19
Wstęp	21
Część I Podstawowe założenia bezpieczeństwa systemu informatycznego	29
Rozdział 1. Podstawowe założenia strategii bezpieczeństwa systemu informatycznego	31
Podstawowe założenia bezpieczeństwa sieci	32
Poufność	32
Integralność	32
Dostępność	32
Inne ważne terminy	33
Procesy formalne	33
Procesy inżynierii systemów	33
Zasady technicznego zabezpieczenia informacji	34
Proces inżynierii bezpieczeństwa systemu informatycznego	39
Cykl rozwoju systemu	48
Bezpieczeństwo systemu informatycznego i cykl rozwoju systemu (SDLC)	49
Zarządzanie ryzykiem	57
Definicje	58
Zarządzanie ryzykiem w ramach cyklu rozwoju systemu	59
Podsumowanie	68
Rozdział 2. Zarządzanie bezpieczeństwem systemu informatycznego	69
Polityka bezpieczeństwa	70
Oświadczenie polityki zarządu	70
Standardy, zalecenia, procedury i wzorce	72
Świadomość bezpieczeństwa	72
Szkolenie	73
Pomiary świadomości	73
Zarządzanie działaniami natury technicznej	74
Menedżer programu	74
Plan zarządzania programem	75
Plan zarządzania inżynierią systemów	75

Zarządzanie konfiguracją	81
Podstawowe funkcje zarządzania konfiguracją	83
Definicje i procedury	83
Planowanie ciągłości działań biznesowych oraz przywracania systemu po awariach	85
Planowanie ciągłości działań biznesowych	86
Planowanie przywracania systemu po awariach	90
Bezpieczeństwo fizyczne	94
Mechanizmy kontrolne	95
Czynniki środowiskowe	99
Zabezpieczenia przeciwpożarowe	100
Ponowne wykorzystanie zasobów i magnetyzm szczątkowy	101
Zagadnienia prawne i odpowiedzialność	102
Rodzaje przestępstw komputerowych	102
Monitorowanie elektroniczne	102
Odpowiedzialność	103
Podsumowanie	103
Rozdział 3. Kontrola dostępu	105
Modele kontroli	105
Uznaniowa kontrola dostępu	106
Obligatoryjna kontrola dostępu	106
Ogólna kontrola dostępu	107
Typy implementacji mechanizmów kontroli dostępu	107
Mechanizmy zapobiegawcze i środki administracyjne	107
Mechanizmy zapobiegawcze i środki techniczne	108
Mechanizmy zapobiegawcze i środki fizyczne	108
Mechanizmy wykrywające i środki administracyjne	108
Mechanizmy wykrywające i środki techniczne	109
Mechanizmy wykrywające i środki fizyczne	109
Scentralizowane i zdecentralizowane mechanizmy kontroli dostępu	110
Identyfikacja i uwierzytelnianie	110
Hasła	111
Biometryka	111
Mechanizm pojedynczego logowania	112
Bazy danych	116
Bazy relacyjne	116
Inne typy baz danych	118
Dostęp zdalny	119
RADIUS	119
TACACS oraz TACACS+	119
Protokół PAP	120
Protokół CHAP	120
Oddzwanianie	121
Podsumowanie	121
Część II Systemy operacyjne i aplikacje	123
Rozdział 4. Bezpieczeństwo systemów MS Windows	125
Bezpieczeństwo Windows w sercu systemu ochrony	127
Kto chciałby mnie skrzywdzić?	127
Należy się obawiać	129
Zalecenia firmy Microsoft	129

Wzmacnianie świeżo zainstalowanego systemu	132
Czynności wstępne	132
Ogólny opis procesu wzmacniania systemu	132
Przykład czystej instalacji systemu Windows 2003	135
Szczegółowe zagadnienia wzmacniania systemu	137
Zabezpieczanie typowej biznesowej stacji roboczej z systemem Windows	141
Zabezpieczanie systemu Windows przeznaczonego do gier	142
Instalacja aplikacji	143
Zabezpieczenie antywirusowe	143
Osobiste zapory sieciowe	145
Secure Shell (SSH)	145
Secure FTP	146
Pretty Good Privacy	147
Przyłączenie stacji roboczej do sieci	147
Testowanie wzmocnionej stacji	147
Bezpieczeństwo fizyczne	148
Architektura	148
Zapora sieciowa	149
Systemy detekcji włamań	149
Bezpieczne użytkowanie systemu Windows	150
Identyfikacja ryzykownych praktyk	150
Zagadnienia ochrony fizycznej	151
Konfiguracja	152
Kontrola konfiguracji	155
Zagadnienia operacyjne	157
Aktualizacja wersji systemu i poprawki	166
Aktualizacje wersji i poprawki oprogramowania firmy Microsoft	166
Utrzymywanie aktualności systemu przez instalacje aktualizacji i poprawek	167
Utrzymanie aktualności sygnatur antywirusowych	168
Wykorzystanie jak najnowszej wersji Windows	168
Utrzymanie i testowanie zabezpieczeń	169
Poszukiwanie słabych punktów	169
Testowanie niepewnych aplikacji	169
Nieoczekiwane zmiany wydajności systemu	170
Wymiana starych wersji systemu Windows	170
Okresowa analiza i przebudowa systemu	171
Monitorowanie	171
Dzienniki systemowe i audyt	172
Oczyszczanie systemu	172
Przygotowanie na wypadek ataku	173
Ataki na stacje robocze z systemem Windows	174
Wirusy	174
Robaki	175
Konie trojańskie	176
Oprogramowanie szpiegowskie i reklamowe	176
Oprogramowanie szpiegowskie typu „Wielki Brat”	178
Ataki fizyczne	178
Ataki TEMPEST	179
Tylne drzwi	179
Ataki typu DoS	180
Rozszerzenia nazw plików	181

Podsluchiwanie pakietów	181
Przechwytywanie i wznowianie sesji	181
Socjotechnika	182
Podsumowanie	182
Rozdział 5. Bezpieczeństwo systemów Unix i Linux	185
Zadania zabezpieczeń systemów Unix i Linux	185
Unix jako cel ataku	186
Unix i Linux jako trudny cel ataków	188
Otwarty kod źródłowy — zagadnienia	189
Bezpieczeństwo fizyczne	191
Ograniczanie dostępu	191
Wykrywanie zmian sprzętowych	193
Podział dysku na partycje	194
Przygotowanie na ewentualny atak	195
Kontrola konfiguracji	196
Zainstalowane pakiety	197
Konfiguracje jądra	198
Bezpieczna obsługa systemu Unix	205
Kontrola procesów	205
Kontrola użytkowników	218
Szyfrowanie i certyfikaty	225
Wzmacnianie systemu Unix	227
Konfiguracja	227
TCP wrapper	229
Sprawdzanie siły haseł	230
Filtrowanie pakietów z użyciem iptables	230
Podsumowanie	231
Rozdział 6. Bezpieczeństwo przeglądarek i klientów WWW	233
Ryzyko powodowane przez przeglądarki WWW	233
Prywatność a bezpieczeństwo	234
Wygoda przeglądarek WWW	234
Wszechstronność i popularność przeglądarki WWW	235
Ewolucja przeglądarek	236
Zagrożenia przeglądarek WWW	236
Czynniki działające na niekorzyść napastnika	237
Sposób działania przeglądarek WWW	237
HTTP — protokół stron WWW	237
Cookies	240
Utrzymanie stanu	241
Buforowanie	243
SSL	243
Ataki na przeglądarki WWW	247
Atak przechwytyjący	247
Atak powtórzenia	248
Pasożyty przeglądarek	249
Bezpieczne użytkowanie przeglądarek	250
Instalacja poprawek	250
Unikanie wirusów	251
Wykorzystanie bezpiecznych stron WWW	251

Zabezpieczanie środowiska sieciowego	253
Zastosowanie bezpiecznego serwera pośredniczącego	253
Unikanie ujawniania prywatnych danych	254
Zalecenia ogólne	254
Konfiguracja przeglądarki WWW	256
Cookies	256
Wtyczki	257
Zagadnienia specyficzne dla przeglądarek Mozilla Firefox	261
Zagadnienia specyficzne dla przeglądarek Internet Explorer	262
Podsumowanie	267
Rozdział 7. Bezpieczeństwo WWW	269
Protokół HTTP	269
Mechanizm działania HTTP	271
Implementacja HTTP	274
Połączenia trwałe	276
Model klient-serwer	278
PUT	279
GET	280
Burstable TCP	280
HTML	282
Obsługa aktywnej zawartości po stronie serwera	282
Skrypty CGI	283
Strony PHP	283
Obsługa aktywnej zawartości po stronie klienta	284
JavaScript	284
Java	285
ActiveX	287
Stan	290
Stan w aplikacji WWW	290
Związek stanu z protokołem HTTP	290
Aplikacje wymagające śledzenia stanu	290
Śledzenie stanu	291
Cookies	291
Pluskwy stron WWW	294
Śledzenie adresów URL	294
Ukryte ramki	295
Ukryte pola formularza	295
Ataki wykorzystujące strony WWW	296
Zbieranie danych o użytkownikach	296
Wymuszanie kodu SQL	297
Projektowanie serwisu e-commerce	298
Lokalizacja fizyczna	298
Podsumowanie	300
Rozdział 8. Bezpieczeństwo poczty elektronicznej	301
Ryzyko związane z pocztą elektroniczną	301
Podatność danych	301
Prosta poczta elektroniczna a mechanizmy pracy grupowej	302
Spam	313
Poufność poczty elektronicznej	316

Integralność poczty elektronicznej	316
Dostępność poczty elektronicznej	317
Protokoły poczty elektronicznej	317
SMTP	317
POP	320
IMAP	322
Uwierzytelnianie w poczcie elektronicznej	322
Proste logowanie	322
Logowanie uwierzytelniane	323
APOP	324
NTLM, czyli SPA	324
POP before SMTP	325
Kerberos oraz GSSAPI	326
Bezpieczne użytkowanie poczty elektronicznej	326
Zachować czujność	326
Konfiguracja programu pocztowego	327
Wersje aplikacji	328
Architektura systemu	328
Tunel SSH	329
PGP oraz GPG	333
Podsumowanie	333
Rozdział 9. DNS	335
Zadania DNS	336
Zapytania proste	341
Zapytania odwrotne	341
Alternatywne sposoby odwzorowania nazw	343
Problemy bezpieczeństwa związane z DNS	344
Błędy konfiguracji	344
Transfery stref	346
Przewidywalne identyfikatory zapytań	349
Zapytania rekurencyjne i iteracyjne	350
Ataki na usługę DNS	351
Proste ataki na usługę DNS	351
Zatrucie pamięci podręcznej	352
Projektowanie usługi DNS	353
Podzielony DNS	353
Krzyżowy DNS	353
Serwery DNS nadrzędne i podrzędne	353
Szczegóły architektury DNS	355
Podsumowanie	356
Rozdział 10. Bezpieczeństwo serwerów	357
Ogólne zagrożenia serwerów	357
Projektowanie z myślą o bezpieczeństwie	358
Właściwe podejście do zagadnień bezpieczeństwa	359
Pozyskanie bezpiecznego środowiska rozwoju aplikacji	364
Bezpieczne praktyki rozwoju oprogramowania	368
Testy, testy, testy	375

Bezpieczne użytkowanie serwerów	377
Kontrola konfiguracji serwera	377
Kontrola użytkowników i dostępu	379
Hasła	380
Monitorowanie, audyty i dzienniki systemowe	381
Zastosowania serwerów	381
Wymiana danych	382
Sieci peer to peer	385
Komunikatory internetowe i chat	386
Podsumowanie	387

Część III Podstawy bezpieczeństwa sieciowego 389

Rozdział 11. Protokoły sieciowe 391

Protokoły	391
Model ISO OSI	392
Warstwy modelu ISO OSI	392
Warstwa aplikacji	392
Warstwa prezentacji	394
Warstwa sesji	394
Warstwa transportowa	395
Warstwa sieci	396
Warstwa łącza danych	397
Warstwa fizyczna	398
Model TCP/IP	399
Warstwy modelu TCP/IP	400
Translacja adresów sieciowych (NAT)	400
Podsumowanie	402

Rozdział 12. Bezpieczeństwo sieci bezprzewodowych 403

Spektrum fal elektromagnetycznych	403
Sieć telefonów komórkowych	405
Wykonywanie połączeń w telefonii komórkowej	407
Systemy bezprzewodowej transmisji danych	408
Wielodostęp w dziedzinie czasu	408
Wielodostęp w dziedzinie częstotliwości	409
Wielodostęp kodowy	409
Typy bezprzewodowych systemów transmisji danych	409
Technologie sieci bezprzewodowych	413
Technologia widma rozproszonego	413
Podstawy działania technologii widma rozproszonego	415
Specyfikacje bezprzewodowych sieci lokalnych IEEE	418
Warstwa fizyczna PHY	419
Warstwa kontroli dostępu do nośnika MAC	419
Bezpieczeństwo sieci bezprzewodowych 802.11	420
WEP	421
Podnoszenie bezpieczeństwa protokołu WEP	423
802.11i	428
Bluetooth	433
Protokół WAP	434
Podsumowanie	436

Rozdział 13. Podstawy architektury sieci	437
Segmenty sieci	438
Sieci publiczne	438
Sieci półprywatne	439
Sieci prywatne	439
Ochrona zewnętrzna	439
Translacja adresów sieciowych	440
Podstawowe elementy architektury	441
Podsieci, przełączanie i sieci typu VLAN	444
Adresy MAC i protokół ARP	446
Protokół DHCP i kontrola adresów	447
Zapory sieciowe	448
Zapory sieciowe filtrujące pakiety	449
Filtrowanie pakietów na podstawie stanu	451
Pośredniczące zapory sieciowe	453
Wady zapór sieciowych	453
Systemy wykrywania włamań	454
Rodzaje systemów wykrywania włamań	455
Metody i tryby wykrywania włamań	458
Reakcje na wykrycie włamania	461
Typowe ataki	462
Podsumowanie	463
 Część IV Komunikacja	 465
Rozdział 14. Komunikacja utajniona	467
Ogólne pojęcia	468
Historia kryptografii	469
Szyfry podstawieniowe	469
Szyfry, które tworzyły historię	475
Cztery podstawowe elementy kryptografii	475
Generatory liczb losowych	476
Obsada	479
Szyfrowanie symetryczne	480
Szyfry strumieniowe	482
Szyfry blokowe	483
Współużytkowanie kluczy	485
Szyfrowanie asymetryczne	487
Wykorzystywanie certyfikatów	488
Sieci zaufania	489
Podpisy cyfrowe	490
Funkcje mieszające	491
Funkcje mieszające korzystające z kluczy	493
Łączenie podstawowych elementów kryptografii w celu uzyskania CIA	493
Różnice pomiędzy algorytmem a implementacją	495
Algorytmy własnościowe i otwarte	496
Podsumowanie	497

Rozdział 15. Tajna komunikacja	499
Gdzie kryją się ukryte dane?	499
Skąd wzięła się steganografia?	501
Dokąd zmierza steganografia?	501
Przegląd steganografii	501
Do czego jest potrzebna steganografia?	503
Zalety steganografii	503
Wady steganografii	504
Porównanie z innymi technikami	504
Historia steganografii	506
Steganografia w walce o imperium rzymskie	507
Steganografia podczas wojen	507
Podstawowe aspekty bezpieczeństwa sieci i ich związek ze steganografią	508
Poufność	508
Integralność	509
Dostępność	509
Dodatkowe cele steganografii	509
Zasady steganografii	510
Steganografia a kryptografia	511
Przykład z zabezpieczaniem pierścionka	511
Składanie elementów	511
Typy steganografii	513
Pierwotny system klasyfikacji	513
Nowy system klasyfikacji	515
Tablice kolorów	518
Produkty implementujące steganografię	519
S-Tools	519
Hide and Seek	522
Jsteg	523
EZ-Stego	526
Image Hide	526
Digital Picture Envelope	527
Camouflage	529
Gif Shuffle	530
Spam Mimic	532
Steganografia a cyfrowe znaki wodne	533
Co to jest cyfrowy znak wodny?	534
Do czego potrzebne są cyfrowe znaki wodne?	534
Cechy cyfrowych znaków wodnych	534
Typy cyfrowych znaków wodnych	535
Niewidoczne znaki wodne	535
Widoczne znaki wodne	535
Cele stosowania cyfrowych znaków wodnych	536
Cyfrowe znaki wodne a steganografia	536
Zastosowania cyfrowych znaków wodnych	537
Usuwanie cyfrowych znaków wodnych	537
Podsumowanie	539

Rozdział 16. Aplikacje bezpiecznej i tajnej komunikacji 541

E-mail	542
Protokoły POP/IMAP	542
PGP	542
Kerberos	544
Serwery uwierzytelniające	545
Model praktyczny	546
PKI — infrastruktura klucza publicznego	549
Klucze prywatne i publiczne	549
Zarządzanie kluczami	551
Sieć zaufania	552
Wirtualne sieci prywatne	553
Problemy projektowania	553
Sieci VPN wykorzystujące protokoły IPsec	555
Tryby pracy protokołu IPsec	556
Wirtualne sieci prywatne związane z protokołami PPTP/PPP	558
SSH	559
SSL/TLS	560
Protokół uzgodnień SSL — SSL handshake	560
Podsumowanie	564

Część V Zagrożenia i reakcja 565**Rozdział 17. Wykrywanie włamań i reagowanie na atak 567**

Szkodliwy kod	567
Wirusy	567
Przegląd popularnych ataków	569
Blokada usług i rozproszona blokada usług	569
Tylne drzwi	570
Fałszowanie adresu	570
Człowiek w środku	570
Odtworzenie	571
Przejmowanie sesji TCP	571
Fragmentacja	571
Słabe klucze	572
Ataki matematyczne	572
Inżynieria społeczna	572
Skanowanie portów	573
Nurkowanie w śmieciach	573
Atak metodą dnia urodzin	574
Odgadywanie haseł	574
Wykorzystywanie luk w oprogramowaniu	575
Niewłaściwe wykorzystanie systemu	575
Podśluch	576
Rozpoznanie mobilne	576
Ataki z wykorzystaniem numerów sekwencyjnych TCP/IP	576
Rozpoznanie telefoniczne	576
Mechanizmy wykrywania włamań	576
Systemy antywirusowe	577
Wykrywanie włamań i reagowanie na atak	577
Systemy IDS oparte na sieci	578

Garnki miodu	581
Cele	582
Kategorie garnków miodu	583
Kiedy należy używać garnka miodu?	583
Kiedy nie należy używać garnka miodu?	584
Obecne rozwiązania	585
Honeynet Project	585
Reakcja na incydenty	586
Zalecenia CERT/CC	587
Zalecenia Internet Engineering Task Force	591
Ochrona wielowarstwowa a systemy IDS	592
Zespoły ds. bezpieczeństwa komputerowego i reakcji na incydenty	593
Proces powiadamiania o incydentach naruszenia bezpieczeństwa	594
Zautomatyzowane mechanizmy powiadamiania o atakach i usuwania ich skutków	595
Podsumowanie	596
Rozdział 18. Szacowanie, testowanie i ocena zabezpieczeń	597
Metodologie oceny poziomu bezpieczeństwa informacji	597
Systems Security Engineering Capability Maturity Model (SSE-CMM)	597
Infosec Assessment Methodology (IAM)	598
Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)	600
Federal Information Technology Security Assessment Framework (FITSAF)	600
Certyfikacja i akredytacja	601
National Information Assurance Certification and Accreditation Process (NIACAP)	601
Cztery fazy procesu NIACAP	602
DoD Information Technology Security Certification and Accreditation Process (DITSCAP)	603
Cztery fazy procesu DITSCAP	604
Federal Information Processing Standard 102	604
Okólnik OMB A-130	605
Wytyczne oceny opracowane przez National Institute of Standards and Technology	606
SP 800-14	607
SP 800-27	607
SP 800-30	608
SP 800-64	610
Testowanie penetracyjne	611
Wewnętrzny test penetracyjny	612
Zewnętrzny test penetracyjny	612
Test z pełną wiedzą o sieci	612
Test z częściową wiedzą o sieci	612
Test bez wiedzy o sieci	612
Test na systemie zamkniętym	613
Test na systemie otwartym	613
Inspekcje i monitorowanie	613
Inspekcje	613
Monitorowanie	614
Podsumowanie	615
Rozdział 19. Łączenie wszystkiego w całość	617
Kluczowe problemy, z którymi zmagają się organizacje	617
Jak przekonać kierownictwo, że bezpieczeństwo jest ważne i że warto za nie zapłacić?	617
Jak radzić sobie ze zwiększoną liczbą ataków?	618

Jak sprawić, aby pracownicy byli częścią rozwiązania, a nie częścią problemu?	619
Jak analizować dane z dzienników?	619
Jak poradzić sobie z różnymi systemami w moim przedsiębiorstwie i upewnić się, że są bezpieczne?	620
Skąd mam wiedzieć, czy jestem celem szpiegostwa korporacyjnego albo innych ataków?	621
Dziesięć najczęstszych pomyłek	621
Ogólne wskazówki dotyczące zabezpieczania sieci	623
Dogłębna ochrona	623
Zasada minimalnych przywilejów	624
Wiedza o oprogramowaniu działającym w systemie	624
Prewencja to ideał, ale wykrywanie to konieczność	625
Stosowanie i testowanie poprawek	625
Regularne kontrolowanie systemu	626
Podsumowanie	626

Dodatki 627

skorowidz 629

Rozdział 3.

Kontrola dostępu

Zagadnienia omówione w tym rozdziale:

- ◆ modele kontroli dostępu;
- ◆ typy mechanizmów kontroli dostępu;
- ◆ identyfikacja, uwierzytelnianie i autoryzacja;
- ◆ bazy danych i ich bezpieczeństwo;
- ◆ implementacje zdalnego dostępu.

Kontrola dostępu do sieci i związanych z nią zasobów jest kluczowym zagadnieniem bezpieczeństwa sieciowego. W przypadku obecnie spotykanych rozproszonych środowisk informatycznych, gdy na dyskach twardych poszczególnych komputerów spoczywa krytyczna dla istnienia organizacji własność intelektualna, kontrola dostępu staje się jeszcze ważniejszym problemem.

Ten rozdział opisuje modele służące do określania metod kontroli dostępu, różne typy mechanizmów kontrolnych oraz środki służące do implementacji bezpiecznych i wiarygodnych mechanizmów zdalnego oraz lokalnego logowania się użytkowników w systemach.

Modele kontroli

Kontrola dostępu ma na celu zmniejszenie zagrożenia wynikającego ze słabych punktów zabezpieczeń, co jest związane z zagrożeniami sieci wskutek możliwości uzyskania dostępu do systemów przez różnych użytkowników. **Zagrożenie** definiuje się jako zdarzenie lub działanie, które potencjalnie może powodować szkody w systemie sieciowym. W tym przypadku zagrożenie jest związane z możliwością pokonania lub oszukania mechanizmów kontroli dostępu, co pozwala napastnikowi na uzyskanie nieautoryzowanego dostępu do sieci. **Podatność** (słaby punkt) systemu na ataki jest cechą, która może zostać wykorzystana przez zagrożenie i w efekcie spowodować szkodę w sieci. Prawdopodobieństwo, że zagrożenie spowoduje rzeczywiste straty, jest określane mianem **ryzyka**. Ponadto przy omawianiu zagadnień kontroli dostępu są wykorzystywane pojęcia obiektu i podmiotu. **Podmiotem** jest aktywna jednostka (na przykład osoba lub proces), natomiast **obiektem** nazywa się jednostkę pasywną (taką jak plik).

Modele kontroli dostępu można podzielić na indywidualne, obowiązkowe i ogólne.

Uznaniowa kontrola dostępu

Jednostka uwierzytelniająca lub podmiot uwierzytelniania w pewnym zakresie ma możliwość określania obiektów kontroli dostępu. Jednym ze sposobów opisywania indywidualnej kontroli dostępu jest *tablica*. Tablica uwzględnia podmioty, obiekty i uprawnienia dostępu, przydzielane podmiotom do poszczególnych obiektów. Tabelę taką czasem określa się mianem **listy kontroli dostępu** (ang. *access control list*, ACL). Przykład listy kontroli dostępu przedstawia tabela 3.1.

Tabela 3.1. *Lista kontroli dostępu*

Podmiot	Obiekt 1	Obiekt 2	Obiekt 3
	Plik z bazą płac	Plik z analizą zysków	Proces „Analiza”
Program „Płace”	Zapis i odczyt	Odczyt	Wykonanie
Kowalski	Brak	Odczyt	Brak
Nowak	Zapis i odczyt	Zapis i odczyt	Brak

Tabela 3.1 przedstawia informacje dotyczące programu „Płace”, w którym można definiować prawa odczytu i zapisu pliku z bazą płac oraz prawa odczytu z pliku zawierającego analizę zysków. Program „Płace” uwzględnia również prawo wykonywania procesu „Analiza”.

Użytkownik, który ma prawo modyfikacji przywilejów dostępu do określonych obiektów, działa w ramach indywidualnej kontroli dostępu **definiowanej przez użytkownika**. Inna odmiana indywidualnej kontroli dostępu opiera się na **identyfikacji użytkownika**.

Obligatoryjna kontrola dostępu

Model obowiązkowej kontroli dostępu wymaga formalnego dopasowania uprawnień podmiotów z poziomem znaczenia obiektów, które stanowią cel kontroli dostępu. Jednym z takich rozwiązań jest wykorzystanie **etykiety**. Uwierzytelnienie obiektu może odbywać się z wykorzystaniem formy **przepustki**, porównywanej z **wzorcem** zabezpieczenia obiektu. W USA dokumenty militarne są klasyfikowane jako jawne, poufne, tajne i ściśle tajne. Analogicznie, dana osoba może otrzymać przepustkę o uprawnieniach poufnych, tajnych i ściśle tajnych i na podstawie tej przepustki uzyskać dostęp do dokumentów na określonym lub niższym poziomie poufności. W ten sposób osoba z przepustką na poziomie „tajne” może mieć dostęp do dokumentów zaklasyfikowanych jako poufne, lecz z ograniczeniem określanym jako **potrzeba zapoznania**. Ograniczenie to oznacza, że podmiot może uzyskać dostęp do dokumentu, jeśli jest to niezbędne w celu realizacji jego obowiązków. Jedną z form obowiązkowej kontroli dostępu jest **kontrola dostępu oparta na regulach**, w której przywileje dostępu regulują zdefiniowane reguły (podobnie jak dopasowanie etykiety przepustki do etykiety klasyfikacji dokumentu), nie zaś wyłącznie identyfikacja podmiotu i obiektu.

Ogólna kontrola dostępu

Ogólna kontrola dostępu definiuje przywileje dostępu bazując na roli danej osoby w organizacji (**kontrola oparta na rolach**) lub obowiązkach i odpowiedzialności podmiotu (**kontrola oparta na zadaniach**). Kontrola dostępu oparta na rolach jest stosowana w organizacjach, w których następują częste zmiany personalne. W ten sposób nie ma potrzeby dokonywania częstych zmian przywilejów poszczególnych osób w przypadku zmiany ich ról.

Kontrola dostępu może być również zależna od kontekstu oraz zależna od treści. **Kontrola dostępu zależna od kontekstu** wykorzystuje takie zagadnienia jak lokalizacja, pora dnia oraz historia dostępu. Ma ścisły związek z otoczeniem, czyli kontekstem danych. **Kontrola dostępu zależna od treści** jest określana na podstawie zawartości informacji w momencie próby uzyskania dostępu.

Typy implementacji mechanizmów kontroli dostępu

Mechanizmy kontroli dostępu są stosowane do zapobiegania atakom lub detekcji przeprowadzonych ataków bądź ich prób oraz w celu przywrócenia sieci do stanu sprzed ataku w przypadku, gdy atak był skuteczny. Wyróżnia się trzy typy mechanizmów kontrolnych: **zapobiegawcze**, **wykrywające** oraz **korekcyjne**. Do implementacji tych mechanizmów są stosowane środki administracyjne, techniczne (logiczne) oraz fizyczne. **Środki administracyjne** obejmują działania formalne, takie jak definicja polityki, procedur, szkolenia kształtujące świadomość bezpieczeństwa oraz kontrola historii pracowników. **Środki techniczne (logiczne)** uwzględniają wykorzystanie mechanizmów kryptograficznych, kart procesorowych i protokołów transmisyjnych. **Środki fizyczne** są najpowszechniej znane, obejmują zatrudnienie strażników czy zabezpieczenie budynków i komputerów przenośnych. Połączenie tych środków bezpieczeństwa w zastosowanej implementacji pozwala na realizację różnych kombinacji mechanizmów kontrolnych. Przykłady takich kombinacji zostały omówione poniżej.

Mechanizmy zapobiegawcze i środki administracyjne

Mechanizmy zapobiegawcze wykorzystujące administracyjne środki bezpieczeństwa obejmują:

- ♦ politykę bezpieczeństwa i procedury organizacyjne;
- ♦ kontrolę historii pracowników;
- ♦ procedury towarzyszące rozwiązywaniu umów o pracę z pracownikami;
- ♦ umowy o pracę;
- ♦ szkolenia kształtujące świadomość bezpieczeństwa;
- ♦ klasyfikację niejawnych materiałów;
- ♦ planowanie urlopów.

Mechanizmy zapobiegawcze i środki techniczne

Mechanizmy zapobiegawcze wykorzystujące środki techniczne polegają na stosowaniu zdobyczy technologicznych do zapobiegania pogwałceniom polityki bezpieczeństwa organizacji. Środki techniczne są znane również pod nazwą środków logicznych i mogą być wbudowane w system operacyjny, występować w postaci aplikacji lub dodatkowego sprzętu bądź oprogramowania. Przykłady zapobiegawczych środków technicznych obejmują:

- ♦ protokoły;
- ♦ techniki biometryczne;
- ♦ kryptografię;
- ♦ karty procesorowe;
- ♦ menu;
- ♦ ograniczenia interfejsów użytkownika;
- ♦ hasła;
- ♦ ograniczenia klawiatur.

Ograniczenia interfejsów użytkownika polegają na przykład na dezaktywowaniu („wyszarzeniu”) niedostępnych dla użytkownika opcji w menu aplikacji. Ograniczenia klawiatur są związane z zablokowaniem funkcji dostępnych przez naciśnięcie odpowiednich klawiszy na klawiaturach.

Mechanizmy zapobiegawcze i środki fizyczne

Ta kategoria wiąże się z ograniczaniem fizycznego dostępu do tych stref w organizacji, w których są zlokalizowane systemy obsługujące poufne informacje. Do środków fizycznych implementacji mechanizmów zapobiegawczych zalicza się:

- ♦ strażników;
- ♦ śluzy (przejścia pomiędzy strefami w postaci podwójnych, oddzielnych drzwi. Przed otwarciem jednych drzwi drugie muszą zostać zamknięte);
- ♦ ogrodzenia;
- ♦ urządzenia kontroli dostępu oparte na technikach biometrycznych;
- ♦ zabezpieczenia środowiskowe (temperatura, wilgoć, energia elektryczna);
- ♦ identyfikatory.

Mechanizmy wykrywające i środki administracyjne

Do środków administracyjnych implementujących mechanizmy wykrywające zalicza się:

- ♦ analizę zapisu audytów;
- ♦ podział odpowiedzialności;
- ♦ politykę i procedury administracyjne;
- ♦ kontrolę historii pracowników;
- ♦ planowanie urlopów;
- ♦ kategoryzację poufnych materiałów;
- ♦ świadomość związana z zachowaniem się.

Mechanizmy wykrywające i środki techniczne

Środki techniczne implementujące mechanizmy wykrywające służą do detekcji włamań lub innych form pogwałcenia polityki bezpieczeństwa organizacji. Poniżej wymieniono te środki.

- ♦ **Mechanizmy detekcji włamań** (ang. *intrusion detection systems*, IDS). Mechanizmy te podlegają dalszemu podziałowi z uwagi na zastosowane technologie. Przykładowo, system detekcji włamań scentralizowany dla danego systemu jest zainstalowany w tym systemie i służy do wykrywania ataków na tę jedną maszynę. Tego typu mechanizmy IDS nie są jednak skuteczne w wykrywaniu włamań do całej sieci. Sieciowe mechanizmy IDS z kolei mają konstrukcję pasywną i służą do wykrywania włamań w czasie rzeczywistym. Są to mechanizmy mniej obciążające zasoby od mechanizmów IDS scentralizowanych systemowo. Mechanizm detekcji włamań opiera się na dwóch podstawowych metodach. Jedną z nich polega na profilowaniu „normalnych” sytuacji w sieci w systemach i wykrywaniu wszelkich odchyłeń od tego stanu. Drugie podejście jest związane z pozyskiwaniem „sygnatur” ataków i z monitorowaniem systemów pod kątem ich wystąpienia, co sygnalizuje zagrożenie.
- ♦ **Generowanie raportów o pogwałceniu bezpieczeństwa z wykorzystaniem danych pochodzących z audytów**. Raporty tego typu mogą zawierać różne informacje, które dotyczą zarówno dozwolonych operacji, których przebieg z różnych przyczyn odbiegał od normy, jak i przypadków wykrycia znanych sygnatur zdarzeń związanych z próbami nieautoryzowanego dostępu. Można również zdefiniować poziomy **odcinka** (ang. *clipping*), czyli liczby zdarzeń danego typu, poniżej której dane zdarzenie nie jest raportowane.

Mechanizmy wykrywające i środki fizyczne

Środki fizyczne implementujące mechanizmy wykrywające wymagają ingerencji człowieka w celu dokonania oceny danych wejściowych z czujników oraz określenia potencjalnego zagrożenia. Przykłady takich środków mogą być następujące:

- ♦ kamery wideo;
- ♦ wykrywacze ruchu;
- ♦ czujniki temperatury.

Scentralizowane i zdecentralizowane mechanizmy kontroli dostępu

Scentralizowane mechanizmy kontroli dostępu z reguły charakteryzują się zasobami zarządzanymi centralnie przez profesjonalne kadry o dużym stopniu doświadczenia w obsłudze różnorodnych mechanizmów kontrolnych. Scentralizowane systemy kontrolne i protokoły to między innymi RADIUS oraz TACACS+, które zostaną omówione w dalszej części rozdziału.

Zdecentralizowane mechanizmy kontroli dostępu są implementowane bliżej użytkownika i w konsekwencji powinny zapewniać lepszą obsługę elementów związanych z użytkownikami i ich wymaganiami. Paradygmat zdecentralizowanej kontroli dostępu wykorzystuje pojęcie **dziedzin bezpieczeństwa**, których użytkownicy podlegają temu samemu zarządowi i przestrzegają wspólnych zasad bezpieczeństwa (polityki).

Systemy zdecentralizowane charakteryzują się zapotrzebowaniem na silną kontrolę dostępu. Przykładem takiej kontroli może być wykorzystanie WWW do zapewnienia komunikacji i współpracy pomiędzy poszczególnymi jednostkami (podsieciami) organizacji. Taki system w dużym uogólnieniu powinien mieć następujące cechy:

- ♦ szyfrowanie haseł i identyfikatorów;
- ♦ zdefiniowanie formalnych reguł kontroli dostępu;
- ♦ każda jednostka samodzielnie uwierzytelnia swoich użytkowników;
- ♦ do sieci można dodawać nowe jednostki.

Identyfikacja i uwierzytelnianie

Identyfikacja jest procedurą zgłoszenia systemowi tożsamości użytkownika, z reguły w postaci identyfikatora logowania. Proces ten uruchamia również procedurę zapisu w pliku dziennika informacji o działaniach użytkownika w systemie. **Uwierzytelnianie** polega na weryfikacji tożsamości użytkownika i z reguły jest implementowane w postaci konieczności podania hasła podczas logowania w systemie. Uwierzytelnianie może być również realizowane przez inne mechanizmy, od różnych form haseł po analizę charakterystyki biometrycznej. Ogólnie ujmując, uwierzytelnianie jest realizowane przez sprawdzenie jednej lub kilku z poniższych cech:

- ♦ informacji, która powinna być znana wyłącznie autoryzowanemu użytkownikowi, jak osobisty numer PIN (ang. *personal identification number*). Ten element jest znany jako uwierzytelnianie typu 1. (ang. *Type 1 authentication*);
- ♦ urządzenia, które powinno być w posiadaniu wyłącznie autoryzowanego użytkownika, jak karta magnetyczna (z mikroprocesorem i z pamięcią). Ten element jest znany jako uwierzytelnianie typu 2. (ang. *Type 2 authentication*);
- ♦ unikalnych cech biometrycznych autoryzowanego użytkownika, jak odcisk palca lub wzór siatkówki. Ten element jest znany jako uwierzytelnianie typu 3. (ang. *Type 3 authentication*).

Oczywiście zastosowanie więcej niż jednego mechanizmu uwierzytelniającego zwiększa wiarygodność procesu. Na przykład **dwuetapowe uwierzytelnianie** może wykorzystywać takie elementy jak numer PIN w połączeniu z kartą magnetyczną.

Po uwierzytelnieniu użytkownik uzyskuje dostęp do określonych zasobów komputera i informacji. Taka alokacja uprawnień jest określana mianem autoryzacji.

Hasła

Hasła są najpopularniejszym sposobem uwierzytelniania użytkowników. Z tego powodu skuteczne zabezpieczanie haseł przed niepowołanym dostępem jest kluczowym aspektem polityki bezpieczeństwa.

Najwyższy poziom bezpieczeństwa zapewniają **hasła jednorazowe**. W takim modelu przy każdym logowaniu jest wymagane inne hasło, dzięki czemu napastnik nie może wykorzystać zdobytego w nielegalny sposób hasła, które było wykorzystane przy poprzednim logowaniu. Często zmieniane hasło nazywa się **hasłem dynamicznym**. Hasło, które pozostaje identyczne przy każdym logowaniu nazywa się **hasłem statycznym**. W organizacji może istnieć wymóg okresowych zmian haseł, na przykład raz na miesiąc, raz na kwartał lub w innych odstępach czasu, w zależności od stopnia poufności danych zabezpieczanych tymi hasłami.

W niektórych przypadkach zamiast hasła może być stosowana **fraza** (ang. *passphrase*). Fraza jest ciągiem znaków, z reguły dłuższym od dopuszczalnej długości hasła. Fraza jest konwertowana przez system na formę wirtualnego hasła.

Hasła mogą być generowane w sposób automatyczny z użyciem kart pamięci o rozmiarach karty kredytowej, kart magnetycznych lub urządzeń przypominających niewielki kalkulator (tzw. **token**). Generatory haseł stanowią implementację uwierzytelniania typu 2.

Biometryka

Biometryka jest zdefiniowana jako zautomatyzowane techniki identyfikacji lub uwierzytelniania osób z wykorzystaniem ich charakterystyki fizjologicznej lub behawioralnej. Biometryka należy do mechanizmów uwierzytelniających typu trzeciego. Biometryka znajduje zastosowanie zarówno do identyfikacji, jak i do uwierzytelniania.

W celu identyfikacji biometryka jest stosowana w wyszukiwaniach typu „**jeden do wielu**”, gdzie cechy biometryczne są odnajdywane w większej bazie danych zapisanych cech biometrycznych. Przykładem takiego wyszukiwania może być próba dopasowania odcisków palców sprawcy za pomocą bazy danych, zawierającej odciski palców wszystkich obywateli. Uwierzytelnianie obejmuje wyszukiwanie typu „**jeden do jednego**”, ponieważ polega na sprawdzeniu, czy użytkownik poddany sprawdzeniu jest tym, za kogo się podaje. Przykładem takiego wyszukiwania może być porównanie odcisków palców danej osoby z jej odciskami palców, zapisanymi w bazie danych pracowników firmy. Biometryka w zastosowaniach kontroli dostępu jest wykorzystywana do identyfikacji w mechanizmach kontroli fizycznej i do uwierzytelniania w mechanizmach kontroli logicznej.

System biometryczny posiada kilka cech, które określają jego skuteczność i wydajność. Należą do nich cechy techniczne, lecz również subiektywne poczucie komfortu użytkowników zmuszonych do poddania się badaniom. Przykłady cech pomiaru skuteczności są następujące:

- ♦ **Współczynnik fałszywych odrzuceń** (ang. *false rejection rate*, FRR), zwanych błędami typu pierwszego (*Type I*) — procentowy współczynnik błędnych odrzuceń prawidłowych prób zalogowania.
- ♦ **Współczynnik fałszywych akceptacji** (ang. *false acceptance rate*, FAR), zwanych błędami typu drugiego (*Type II*) — procentowy współczynnik błędnych akceptacji nieprawidłowych prób logowania.
- ♦ **Skrzyżowany współczynnik błędu** (ang. *crossover error rate*, CER) — procent przypadków, w których FRR jest równy FAR. Im mniejsza wartość CER, tym skuteczniejszy jest system biometryczny.
- ♦ **Czas pobrania** (ang. *enrollment time*) — czas, który jest potrzebny do pobrania próbek biometrycznych. Akceptowalny czas analizy wynosi około dwóch minut.
- ♦ **Przepustowość systemu** (ang. *throughput rate*) — liczba użytkowników w jednostce czasu, których dane mogą być przetworzone przez system po pobraniu próbek do analizy. Akceptowalna przepustowość to około 10 podmiotów na minutę.
- ♦ **Akceptowalność** (ang. *acceptability*) — dotyczy zagadnień prywatności, inwazyjności i względów psychologicznych, czyli ogólnie rozumianego komfortu korzystania z systemu. Na przykład skanowanie siatkówki może się wiązać z naruszeniem płynów ustrojowych na powierzchni oka. Inne zagadnienie związane z tą techniką może dotyczyć zmian w siatkówce związanych ze stanem zdrowia użytkownika, na przykład z początkowymi stadiami cukrzycy lub podwyższonym ciśnieniem krwi.

Typowe cechy biometryczne obejmują:

- ♦ skanowanie siatkówki;
- ♦ skanowanie tęczówki;
- ♦ linie papilarne;
- ♦ skanowanie twarzy;
- ♦ skanowanie dłoni;
- ♦ geometria dłoni;
- ♦ głos;
- ♦ dynamika ręcznego podpisu.

Mechanizm pojedynczego logowania

W systemach wykorzystujących mechanizm pojedynczego logowania (ang. *Single Sign-On*, SSO) użytkownik podaje nazwę użytkownika i hasło tylko raz, na początku swojej sesji, po czym jest automatycznie logowany we wszystkich systemach, zasobach sieciowych

i aplikacjach. Bez mechanizmu SSO użytkownik musiałby wpisywać różne hasła w celu pracy z różnymi zasobami sieciowymi. W SSO hasła dla bezpieczeństwa są przesyłane w sieci i przechowywane w postaci zaszyfrowanej. Dzięki SSO administracja siecią jest łatwiejsza, mogą być wykorzystane mocniejsze hasła a dostęp do zasobów jest szybszy.

Główna wada implementacji SSO polega na tym, że po uzyskaniu dostępu do systemu po początkowym zalogowaniu się, użytkownik może bez ograniczeń korzystać z różnych zasobach sieciowych.

Mechanizm SSO może być zaimplementowany na kilka sposobów.

- ♦ W postaci skryptów dokonujących automatycznego logowania się użytkownika w sieci.
- ♦ Z użyciem mechanizmu *Enterprise Access Management* (EAM). EAM udostępnia mechanizmy zarządzania kontrolą dostępu, między innymi SSO, który działa z wykorzystaniem systemów WWW. Jedno z tego typu rozwiązań wykorzystuje SSO w postaci szyfrowanych, nietrwałych plików tekstowych zwanych *cookies* (ang. *cookies*) przesyłanych do przeglądarki WWW. Pliki te służą do automatycznego uwierzytelniania użytkownika w różnych serwerach WWW organizacji.
- ♦ Z wykorzystaniem serwerów uwierzytelniania, które weryfikują tożsamość użytkownika, po czym udostępniają mu tzw. bilet uwierzytelniający, dający mu możliwość korzystania z usług systemowych.

Popularnym rozwiązaniem SSO wykorzystującym serwery uwierzytelniania jest mechanizm Kerberos.

Kerberos

Kerberos nosi swoją nazwę na pamiątkę trójgłowego psa z mitologii greckiej, strzegącego wejścia do świata podziemnego. Kerberos stosuje technikę kryptografii z użyciem kluczy symetrycznych, opracowaną przez Project Athena w Massachusetts Institute of Technology. Jest to zaufany protokół uwierzytelniający, który działa w sieci i zapewnia bezpieczny sposób kontroli dostępu do jej zasobów.

Mechanizmy Kerberos opierają się na założeniu, że komputery przyłączone do sieci stanowią publicznie dostępne, niegodne zaufania lokalizacje. Z tego wynika, że komunikaty mechanizmu Kerberos przesyłane w sieci mogą być przechwytywane przez intruzów. Twórcy Kerberos uważali jednak, że niektóre lokalizacje można zabezpieczyć na tyle, aby działały jako zaufane mechanizmy uwierzytelniające, dostępne dla wszystkich klientów i usług w sieci. Te scentralizowane serwery nazywa się centrami dystrybucji kluczy (ang. *Key Distribution Center*, KDC), usługami przyznawania biletów (ang. *Ticket Granting Service*, TGS) oraz usługami uwierzytelniania (ang. *Authentication Service*, AS).

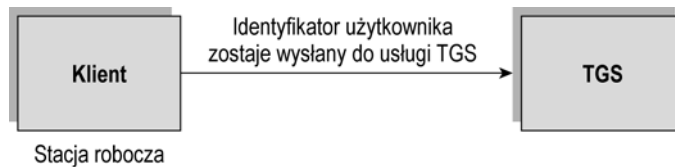
Podstawowe zasady mechanizmu uwierzytelniania systemu Kerberos są następujące:

1. KDC posiada informacje o tajnych kluczach wszystkich klientów i serwerów w sieci.
2. KDC wymienia z klientem informacje inicjalizujące z wykorzystaniem właśnie tych tajnych kluczy.

3. Kerberos uwierzytelnia klienta żądającego usługi serwera. W tym celu wykorzystuje się serwer TGS, który generuje tymczasowe symetryczne klucze sesji na potrzeby komunikacji pomiędzy klientem a KDC, serwerem a KDC oraz pomiędzy klientem a serwerem.
4. Teraz rozpoczyna się komunikacja pomiędzy klientem a serwerem, w trakcie której wykorzystuje się wcześniej wspomniane, tymczasowe symetryczne klucze sesji.

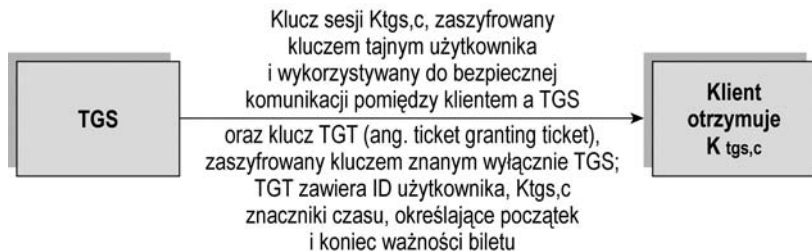
Wymiana danych w systemie Kerberos rozpoczyna się od wpisania przez użytkownika hasła na jednej ze stacji skonfigurowanej w tym systemie. W stacji hasło użytkownika jest przekształcane na klucz tajny użytkownika. Ten klucz tajny jest zapisywany tymczasowo w stacji. Następnie klient przesyła identyfikator użytkownika w postaci nieszyfrowanej do usługi przyznającej bilety (TGS), jak to przedstawia rysunek 3.1.

Rysunek 3.1.
Wymiana danych klienta z TGS



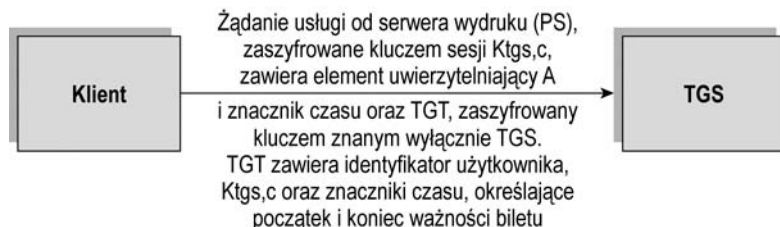
W odpowiedzi na to żądanie TGS wysyła klientowi klucz sesji TGS-klient — $K_{tgs,c}$ — zaszyfrowany kluczem tajnym klienta. Ponadto TGS wysyła bilet dający prawo do otrzymywania innych biletów (ang. *ticket granting ticket*, TGT) zaszyfrowany kluczem znanym tylko TGS. Schemat tej wymiany został zaprezentowany na rysunku 3.2.

Rysunek 3.2.
Wymiana klucza sesji i biletu TGT pomiędzy klientem a TGS



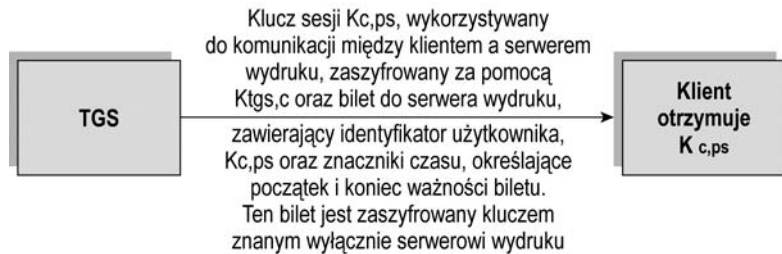
Po otrzymaniu tych komunikatów klient odszyfrowuje $K_{tgs,c}$ używając klucza tajnego użytkownika. Na potrzeby przykładu założmy, że klient żąda dostępu do drukarki PS. Użytkownik wysyła zatem żądanie do TGS w celu uzyskania biletu do serwera wydruku. To żądanie, którego schemat zaprezentowano na rysunku 3.3, składa się z elementu uwierzytelniającego A oraz znacznika czasu — obydwa te elementy są zaszyfrowane kluczem $K_{tgs,c}$. Wysyłany jest również TGT zaszyfrowany kluczem znanym wyłącznie TGS.

Rysunek 3.3.
Klient wysyła żądanie



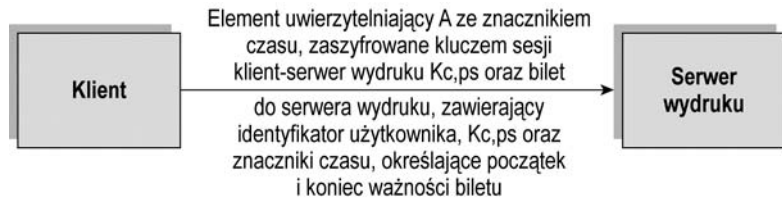
Na kolejnym etapie sekwencji TGS przesyła klientowi klucz sesji klient-serwer wydruku $K_{c,ps}$. Ten klucz sesji jest zaszyfrowany kluczem $K_{tgs,c}$. TGS również wysyła klientowi bilet przeznaczony dla serwera wydruku, który z kolei jest zaszyfrowany kluczem znanym wyłącznie serwerowi wydruku. Ta wymiana została zilustrowana na rysunku 3.4.

Rysunek 3.4.
Transmisja klucza
sesji klienta
i serwera wydruku



W celu uzyskania dostępu do serwera wydruku, klient wysyła do serwera wydruku element uwierzytelniający A opatrzony znacznikiem czasu i zaszyfrowany kluczem $K_{c,ps}$. Klient wysyła również bilet zaszyfrowany kluczem znanym wyłącznie serwerowi wydruku. Serwer wydruku odszyfrowuje bilet i uzyskuje $K_{c,ps}$, czyli klucz sesji klient-serwer wydruku. Od tego momentu serwer wydruku wykorzystuje $K_{c,ps}$ do bezpiecznej komunikacji z klientem. Tę wymianę pokazano na rysunku 3.5.

Rysunek 3.5.
Wymiana kluczy
pomiędzy klientem
a serwerem wydruku



Podstawowym celem stosowania mechanizmu Kerberos jest zabezpieczenie poufności i integralności informacji. Z powodu braku zaufania do stacji roboczych i kabli sieciowych nie ma bezpośredniej możliwości zabezpieczenia dostępności. Skoro wszystkie tajne klucze klientów i innych zasobów sieciowych są zapisane na serwerach KDS i TGS, więc te serwery są podatne na ataki i stanowią potencjalny pojedynczy punkt uszkodzenia (ang. *single point of failure*). Dzięki wykorzystaniu w określonym czasie biletów wygenerowanych w sposób nielegalny, można uzyskać nieautoryzowany dostęp do zasobów. Również z uwagi na przesyłanie hasła użytkownika do serwera Kerberos jawnym tekstem na początku sesji, mechanizm Kerberos jest podatny na techniki zgadywania haseł. Tajny klucz klienta jest zapisywany tymczasowo na stacji klienta, a więc jest potencjalnie podatny na naruszenie bezpieczeństwa.

SESAME

Kryptografia z użyciem technik klucza publicznego znacznie się rozpowszechniła, pojawiła się zatem koncepcja wykorzystania technik tego typu do bezpiecznego przesyłania kluczy tajnych, wykorzystywanych w systemach uwierzytelniania kluczem symetrycznym. Takie hybrydowe podejście jest stosowane przez inną implementację mechanizmu SSO, zwaną SESAME (*Secure European System for Applications in a Multivendor*

Environment — bezpieczny europejski system dla aplikacji działających w środowiskach wielu dostawców). SESAME wykorzystuje protokół autentykacji Needhama-Schroedera i zaufany serwer uwierzytelniania w każdym systemie klienckim, co ma na celu ograniczenie wymogów zarządzania kluczami. SESAME wykorzystuje również dwa certyfikaty lub bilety, które służą do obsługi uwierzytelniania i określania przywilejów dostępu. System SESAME jest niestety również podatny na odgadywanie haseł.

KryptoKnight

Podobnie jak Kerberos, system SSO firmy IBM znany pod nazwą KryptoKnight wykorzystuje zaufany serwer KDC, przechowujący sieciowy tajny klucz klienta. Jedną z różnic pomiędzy Kerberosem a KryptoKnight jest równorzędna (ang. *peer-to-peer*) zależność pomiędzy klientami a serwerami KDC. Implementacja mechanizmów SSO polega na początkowym wysłaniu od klienta do KDC nazwy użytkownika i wartości, będącej wynikiem funkcji hasła oraz jednorazowego elementu uwierzytelniającego, generowanego metodą losową (tzw. *nonce*). KDC uwierzytelnia użytkownika i wysyła mu bilet zaszyfrowany jego tajnym hasłem. Użytkownik odszyfrowuje ten bilet i od tej pory może używać go do autoryzacji usług w innych systemach w sieci.

Bazy danych

Jednym ze środków wykorzystywanych w mechanizmach kontroli dostępu są bazy danych, w których zapisuje się informacje dostępne różnym użytkownikom na różnych zasadach uprawnień. Szczególną popularnością w aplikacjach sieciowych cieszy się model relacyjny, opracowany przez E. F. Codd'a w firmie IBM (około roku 1970).

Bazy relacyjne

Model relacyjnych baz danych składa się ze struktur danych w postaci tabel i powiązań, więzów integralności określających dopuszczalne wartości w tabelach oraz operacji na danych w tabelach. **Baza danych** może być formalnie zdefiniowana jako trwała kolekcja wzajemnie powiązanych elementów danych. Trwałość jest uzyskana dzięki zachowaniu integralności i zastosowaniu nieulotnych nośników danych. Poniżej wymieniono kilka ważnych aspektów baz danych:

- ♦ **Schemat** — opis bazy danych.
- ♦ **Język opisu danych** (ang. *Data Description Language*, DDL) — definiuje schemat struktury danych.
- ♦ **System zarządzania bazą danych** (ang. *database management system*, DBMS) — oprogramowanie zarządzające bazą danych i dostępem do niej. Wykorzystuje własną kontrolę dostępu, w której każdemu użytkownikowi można przyznać lub zablokować dostęp do określonych informacji.
- ♦ **Relacja** — tabela dwuwymiarowa, będąca podstawowym kontenerem danych w bazie relacyjnej. **Wiersze** tabeli reprezentują **rekordy** lub **krotki**, natomiast kolumny stanowią **atrybuty**.

- ♦ **Liczność** — liczba wierszy w tabeli.
- ♦ **Stopień** — liczba kolumn w relacji.
- ♦ **Dziedzina** — zestaw prawidłowych wartości atrybutu w relacji.

W relacji każdy wiersz jest jednoznacznie reprezentowany przez **klucz główny**. Jeśli atrybut jednej z relacji zawiera klucz wskazujący klucz główny w innej relacji, atrybut ten nazywa się **kluczem obcym**. Klucz obcy nie powinien być kluczem głównym relacji, w której występuje.

Przykłady operacji w relacyjnych bazach danych

W algebrze relacyjnych baz danych zdefiniowano kilka operacji, za pomocą których można budować nowe relacje i wykonywać operacje na danych. Oto kilka przykładów operacji obsługiwanych przez relacyjne bazy danych:

- ♦ **wybór** (ang. *select*) — definiuje nową relację opartą na formule wyboru;
- ♦ **unia** (ang. *union*) — definiuje nową relację przez połączenie dwóch innych relacji;
- ♦ **złączenie** (ang. *join*) — dokonuje wyboru wierszy z różnych relacji na podstawie wspólnych wartości wybranych atrybutów.

Istnieje jeszcze jedna ważna operacja w relacyjnych bazach danych, której zastosowanie ma związek z bezpieczeństwem. Chodzi o tworzenie **perspektyw** (ang. *view*). Perspektywa (zwana też widokiem) nie istnieje fizycznie, lecz można ją uznać za wirtualną tabelę, którą tworzy się z kilku tabel. Relację, która istnieje fizycznie w bazie danych, określa się mianem **relacji bazowej** (ang. *base relation*). Tabele, z których buduje się perspektywę, mogą być właśnie takimi relacjami bazowymi, mogą też być innymi widokami. Perspektywy mogą być wykorzystywane do ograniczania dostępu do określonych informacji w bazie danych. Może to mieć na celu ukrycie atrybutów oraz implementację ograniczeń dostępu z uwagi na zawartość danych. Osoba żądająca dostępu do bazy danych może korzystać z perspektywy zawierającej informacje, do których ma prawo. Widok może również ukrywać informacje, do których dany użytkownik nie powinien mieć dostępu. W ten sposób, za pomocą tej techniki można zaimplementować zasadę minimalnych przywilejów (ang. *Least Privilege*).

W zapytaniach statystycznych można posłużyć się ograniczeniem minimalnego rozmiaru zestawu danych, zabraniając również wykonywania zapytań statystycznych na wszystkich oprócz jednego wierszach w bazie. Dzięki temu zapobiega się atakom ukierunkowanym na zdobycie określonych danych. Atak taki polega na zdobyciu informacji statystycznej na temat M wierszy (gdzie M jest równe lub większe od minimalnego zestawu wierszy w zapytaniu) a następnie wysłaniu żądania statystycznego na temat $M + 1$ wierszy w tabeli. Drugie z tych zapytań może być zaprojektowane w taki sposób, aby objęło dodatkowo poszukiwane dane. Z tego powodu należy zabezpieczyć indywidualne informacje przed odczytem za pomocą zapytań statystycznych. Wymóg minimalnego zestawu wierszy (większego od jednego) pozwala na zabezpieczenie się przed zdobyciem informacji o określonej jednostce.

Normalizacja danych

Normalizacja jest ważnym elementem projektu bazy danych, zapewniającym zależność atrybutów tabel wyłącznie od kluczy głównych. Dzięki temu zarządzanie danymi jest łatwiejsze i raporty uzyskiwane z bazy danych są bardziej jednoznaczne. Normalizacja danych w bazie składa się z trzech kroków:

- ♦ eliminacja powtarzalnych grup informacji przez umieszczenie ich w osobnych tabelach;
- ♦ eliminacja nadmiarowych danych (występujących w więcej niż jednej tabeli);
- ♦ eliminacja atrybutów w tabeli, które nie są zależne od klucza głównego tej tabeli.

Inne typy baz danych

Relacyjne bazy danych zostały bardzo szeroko przeanalizowane pod kątem zastosowań związanych z bezpieczeństwem. Zostały bardzo dobrze przystosowane do zastosowań związanych z przetwarzaniem tekstów. Istnieją również inne typy baz danych o zastosowaniach multimedialno-tekstowych, multimedialnych lub związanych z bezpieczeństwem. Dwa typy z tych baz danych zostaną omówione w kolejnych podrozdziałach.

Bazy danych zorientowane obiektowo

Bazy zorientowane obiektowo (ang. *object-oriented databases*, OODB) mają wiele zastosowań, między innymi w multimediami, projektowaniu wspomaganym komputerowo, przetwarzaniu materiałów wideo, grafiki i systemach eksperckich. Bazy danych zorientowane obiektowo mają kilka cech charakterystycznych, z których część stanowi zalety, inne zaś wady:

- ♦ łatwość ponownego użycia kodu i analizy;
- ♦ nie ma ograniczeń w stosunku do rozmiarów elementów danych, co ma miejsce w przypadku baz relacyjnych;
- ♦ zmniejszone potrzeby związane z utrzymaniem;
- ♦ łatwiejsze przejście od analizy problemu do projektu i implementacji;
- ♦ intensywny proces nauki;
- ♦ duży nakład sprzętowy i programowy wymagany do rozwoju i działania.

Bazy danych obiektowo-relacyjne

Bazy danych obiektowo-relacyjne łączą w sobie cechy baz danych zorientowanych obiektowo oraz relacyjnych baz danych. Model obiektowo-relacyjny został wprowadzony w roku 1992 wraz ze zunifikowanym obiektowo-relacyjnym systemem UniSQL/X. Następnie firma Hewlett Packard wprowadziła produkt OpenODB (później znany pod nazwą Oadapter), który stanowił rozszerzenie produktu *AllBase relational Database Management System*.

Dostęp zdalny

Uwierzytelnianie, autoryzacja i księgowanie stanowią ważne wymogi podczas sesji zdalnego dostępu. Do implementacji tego typu możliwości wykorzystuje się kilka usług i protokołów. Najpopularniejsze usługi i protokoły zostały omówione poniżej.

RADIUS

Jest to usługa scentralizowanego uwierzytelniania dla użytkowników systemów wdzwanianych (ang. *Remote Authentication and Dial-In User Service*). RADIUS wykorzystuje serwer uwierzytelniania oraz technikę dynamicznych haseł. Protokół wykorzystywany przez RADIUS jest otwarty, lekki, oparty na protokole UDP, który można zmodyfikować w taki sposób, aby działał z innymi systemami bezpieczeństwa. Zapewnia uwierzytelnianie, autoryzację i rejestrowanie pracy routerów, serwerów modemowych i aplikacji bezprzewodowych. Opis standardu RADIUS znajduje się w dokumencie RFC 2865.

RADIUS składa się z następujących trzech elementów głównych:

- ♦ **Serwer dostępu sieciowego** (ang. *network access server*, NAS) — przetwarza żądania połączenia i inicjalizuje z klientem wymianę danych połączenia, wykorzystując protokoły PPP (*Point-to-Point Protocol*) lub SLIP (*Serial Line Internet Protocol*). W wyniku działania tej usługi zostaje ustalona nazwa użytkownika, hasło, identyfikator NAS itd. Następnie NAS wysyła te informacje do serwera RADIUS w celu uwierzytelnienia. Hasło użytkownika jest zabezpieczone przez szyfrowanie w ramach protokołów PAP (*Password Authentication Protocol*) lub CHAP (*Challenge Handshake Authentication Protocol*).
- ♦ **Klient** — urządzenie (router) lub użytkownik łączący się z dostawcą usług internetowych.
- ♦ **Serwer RADIUS** — porównuje informacje przesłane przez NAS z danymi zapisanymi w bazie danych i zwraca informacje uwierzytelniające i autoryzujące. NAS przesyła do serwera RADIUS informacje księgowania zdarzeń w celach dokumentacyjnych.

TACACS oraz TACACS +

System TACACS (*Terminal Access Controller Access Control System*) jest protokołem usług uwierzytelniania, obsługującym proces zdalnego uwierzytelniania i związane z tym usługi, takie jak rejestracja zdarzeń. W systemie TACACS hasła użytkowników są przechowywane w centralnej bazie danych, a nie w poszczególnych routerach, dzięki czemu można tworzyć łatwo rozszerzalne konfiguracje zabezpieczeń sieciowych. Urządzenie sieciowe z aktywnym mechanizmem TACACS wysyła do zdalnego użytkownika żądanie podania nazwy użytkownika i statycznego hasła, a następnie przesyła zdobyte w ten sposób informacje do serwera TACACS z żądaniem weryfikacji. Mechanizm TACACS nie obsługuje mechanizmu zmian haseł przez użytkowników ani mechanizmów dynamicznych haseł (tokenów). System TACACS został wyparty przez TACACS+, który obsługuje dynamiczne hasła, uwierzytelnianie dwuetapowe i posiada ulepszone funkcje audytu.

System TACACS+ składa się z następujących elementów, których role są dość podobne do analogicznych części systemu RADIUS:

- ♦ **Klient** — osoba lub urządzenie łączące się z dostawcą usług internetowych.
- ♦ **Serwer dostępu sieciowego** (ang. *network access server*, NAS) — serwer przetwarzający żądania połączenia. NAS przeprowadza z klientem wymianę informacji uwierzytelniających, zdobywając takie informacje, jak nazwa użytkownika, hasło oraz numer portu NAS. Następnie dane te są przesyłane do serwera TACACS+ w celu uwierzytelnienia.
- ♦ **Serwer TACACS+** — serwer dokonujący uwierzytelnienia żądania dostępu i autoryzacji usług. Otrzymuje również informacje księgujące i inne dane statystyczne od serwera NAS.

Protokół PAP

Kolejnym protokołem uwierzytelniającym jest PAP (ang. *Password Authentication Protocol*). Użytkownik podaje niezaszyfrowaną nazwę użytkownika i hasło, które następnie są porównywane z odpowiednią informacją w bazie danych autoryzowanych użytkowników. Nazwa użytkownika i hasło są z reguły przesyłane w nieszyfrowanej postaci, zatem metoda ta nie jest bezpieczna i jest podatna na przechwycenie poufnych informacji. Protokół PAP został zdefiniowany w dokumencie RFC 1334.

Po nawiązaniu połączenia pomiędzy zdalnym użytkownikiem a usługą PAP identyfikator użytkownika i hasło są przesyłane co jakiś czas aż do zakończenia procesu uwierzytelniania lub zerwania połączenia.

Protokół PAP jest podatny na odgadywanie identyfikatorów użytkownika i haseł oraz na ataki typu powtórzeniowego (ang. *replay*).

Poprawioną wersją protokołu PAP jest protokół CHAP.

Protokół CHAP

Protokół CHAP (*Challenge Handshake Authentication Protocol*) został zdefiniowany w dokumencie RFC 1994. Usługa polega na uwierzytelnianiu po nawiązaniu połączenia pomiędzy użytkownikiem a serwerem CHAP. Uwierzytelnianie CHAP odbywa się na podstawie trzetałkowej procedury potwierdzeń.

1. Po ustanowieniu połączenia komunikacyjnego mechanizm uwierzytelniający CHAP wysyła użytkownikowi wyzwanie (ang. *challenge*).
2. Użytkownik odpowiada na wyzwanie ciągiem znaków utworzonym w wyniku jednokierunkowej funkcji mieszającej (ang. *hash*).
3. Wynik działania funkcji mieszającej jest wysyłany przez użytkownika i porównywany z ciągiem znakowym, wyliczonym za pomocą identycznej funkcji przez mechanizm uwierzytelniający. Jeśli obie wartości są identyczne, użytkownik zostaje uwierzytelniony. W przeciwnym przypadku następuje zerwanie połączenia.

4. W celu zwiększenia bezpieczeństwa etapy od 1. do 3. są powtarzane co losowe odstępy czasu. Ta procedura stanowi zabezpieczenie przed atakami powtórzeniowymi.

Oddzwanianie

Inną metodą zdalnego uwierzytelniania jest oddzwanianie. W przypadku tej usługi zdalny użytkownik dzwoni do serwera uwierzytelniającego, przedstawia identyfikator i hasło, po czym rozłącza się. Serwer uwierzytelniający sprawdza podany identyfikator użytkownika w bazie danych i odczytuje z niej numer telefonu. Warunkiem koniecznym powodzenia takiej operacji jest łączenie się użytkowników z ustalonych lokalizacji. Serwer uwierzytelniający dzwoni na ustalony numer, użytkownik akceptuje połączenie i uzyskuje dostęp do systemu. W niektórych implementacjach mechanizmu oddzwaniania użytkownik musi podać inne hasło przy oddzwonieniu serwera. Wadą tego systemu jest konieczność łączenia się ze stałych lokalizacji, których numery telefonu są znane serwerowi uwierzytelniającemu. Zagrożenie w przypadku stosowania tej metody polega na tym, że napastnik może skonfigurować automatyczne przekierowanie połączenia na swój numer telefonu przejmując dostęp do systemu.

Podsumowanie

Kontrola dostępu jest kluczowym zagadnieniem zabezpieczania sieci i jej zasobów. W architekturze kontroli dostępu warto zadbać o ograniczenie liczby obszarów administracji. Rozwiązania jednorazowego logowania (SSO), takie jak Kerberos czy SESAME pozwalają na wdrożenie tego typu koncepcji. Paradygmat obowiązkowej kontroli dostępu jest szczególnie użyteczny w celu zabezpieczenia informacji i zapobieganiu naruszenia własności intelektualnej.

Kolejnym ważnym narzędziem są bazy danych, które posiadają własne mechanizmy kontroli dostępu i implementacji zasady minimalnych przywilejów. Do tego służą perspektywy. Systemy i protokoły zdalnego dostępu, jak RADIUS czy CHAP zapewniają bezpieczne sposoby uwierzytelnienia użytkowników za pomocą dynamicznych haseł i procedur opartych na metodzie wyzwanie-odpowiedź (ang. *challenge-response*).