helion.pl
KSIĘGARNIA INTERNETOWA · WYDAWNICTWO

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 w sieciach Windows



Autor: Marcin Szeliga
ISBN: 83-7361-180-0
Format: B5, stron: 386

Im cenniejsze dane udostępniane są za pomocą sieci komputerowych, tym istotniejsze staje się ich zabezpieczenie. Nie od dziś wiadomo, że sieci oparte na Microsoft Windows, mimo pozornej łatwości obsługi systemów operacyjnych z tej rodziny, nie należą do sieci łatwych do zabezpieczenia i wymagają od administratora bardzo rozległej, szczegółowej i często trudno dostępnej wiedzy. Znajdziesz ją w książce „Bezpieczeństwo w sieciach Windows". To obszerne kompendium zawiera zarówno informacje podstawowe, jak i techniczne szczegóły niezbędne każdemu administratorowi sieci.

Autor podzielił książkę na trzy części. W pierwszej, „Zagrożenia", opisane zostało ryzyko związane z podłączeniem komputera do sieci Microsoft Windows. Druga część zawiera opis podstawowych metod zabezpieczenia komputerów podłączonych do sieci MS Windows. Trzecia część książki, „Wykorzystanie kryptografii", zawiera opis bardziej skomplikowanych i trudniejszych do pokonania kryptograficznych metod zabezpieczenia danych.

Książka opisuje m.in.:

- Najczęstsze techniki używane przez hakerów
- Sposoby fizycznego zabezpieczania sieci
- Bezpieczne nadawanie uprawnień użytkownikom
- ActiveDirectory i DNS
- Metody autoryzacji
- Protokół RADIUS
- Udostępnianie zasobów w sieci
- Tworzenie i zabezpieczanie wirtualnych sieci prywatnych
- Zabezpieczenie komputerów przed atakami z internetu
- Monitorowanie i reagowanie na naruszenie zasad bezpieczeństwa
- Podstawowe techniki kryptograficzne
- Infrastrukturę kluczy publicznych, certyfikaty
- Zabezpieczanie usług internetowych

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

Spis treści

Wstęp 9

Część I Zagrożenia 17

Rozdział 1. Ataki lokalne 19
Proces startu komputera 19
Uruchomienie innego niż domyślny systemu operacyjnego 20
Uruchomienie domyślnego systemu operacyjnego 26
Zdobycie haseł logujących się lokalnie użytkowników 31
Odczytanie haseł użytkowników zapisanych w programach Internet Explorer, Outlook itd. 32
Śledzenie jakiejkolwiek aktywności lokalnych użytkowników 32

Rozdział 2. Wyszukiwanie celu 35
Model sieci Microsoft Windows 35
Protokół TCP 37
Protokół UDP 38
Protokół IP v4 38
Protokół ICMP 39
Wykrycie uruchomionych komputerów 40
Pobranie tablicy nazw NetBIOS 42
Zdobycie informacji o systemie operacyjnym 44
Skanowanie portów 45
Wyliczenie udostępnionych zasobów 51

Rozdział 3. Rozpoznanie 53
Nawiązanie anonimowego połączenia 54
Sesja CIFS/SMB 57
Etap 1. Nawiązanie połączenia TCP 58
Etap 2. Żądanie nawiązania sesji NetBIOS 58
Etap 3. Uzgodnienie protokołu sesji CIFS/SMB 58
Etap 4. Ustanowienie sesji 59
Etap 5. Połączenie z udostępnionym udziałem 59
Zdobywanie informacji o użytkownikach 61
Zdobywanie informacji o systemach 66

Rozdział 4. Podsłuchiwanie 71
Analiza przesyłanych danych 71
Hasła do serwerów FTP 73
Hasła do serwerów pocztowych 74

Hasła do serwerów IRC ... 76
Hasła do stron WWW ... 76
Hasła sesji LM i NTLM ... 77
Fałszywe serwery SMB/CIFS ... 80
Hasła sesji SNMP ... 83
Monitorowanie danych adresowanych do wybranego komputera ... 84
Wykrywanie komputerów nasłuchujących w trybie mieszanym ... 85

Rozdział 5. Włamanie ... 87
Usługa CIFS/SMB ... 87
Odgadywanie haseł ... 88
Klienty usług internetowych ... 92
Klienty poczty elektronicznej ... 92
Internet Explorer ... 95
Serwery ... 98
IIS ... 99
Microsoft SQL Server ... 100

Rozdział 6. Przejęcie kontroli ... 103
Konie trojańskie ... 103
Back Orifice ... 104
Prosiak ... 105
Zdobycie uprawnień administratora ... 106
Zdalny wiersz polecenia ... 107
Konsola administracyjna firmy Microsoft ... 107
Serwer Telnet ... 108
Sesja NetCat uruchamiana jako usługa ... 109
Zdalny wiersz polecenia ... 111
Uruchomienie programu na zdalnym komputerze ... 111
Zarządzanie zdalnym systemem ... 112
Wyświetlenie listy uruchomionych na zdalnym komputerze usług i programów ... 112
Zarządzanie usługami zainstalowanymi na zdalnym komputerze ... 112
Zatrzymanie wybranego procesu na zdalnym komputerze ... 113
Restart zdalnego komputera ... 113
Modyfikacja rejestru zdalnego komputera ... 114
Zarządzanie kontami użytkowników zdalnego systemu ... 115
Dodawanie kont użytkowników ... 116
Zdobycie haseł poszczególnych użytkowników ... 117
Zarządzanie zasobami zdalnego systemu ... 120
Wyszukiwanie plików ... 120

Rozdział 7. Ukrywanie ... 123
Inspekcja zdarzeń ... 123
Pliki ... 126
Usługi ... 129
Rejestr ... 130
Otwarte porty ... 131

Część II Zabezpieczenie sieci Microsoft Windows ... 133

Rozdział 8. Dostęp fizyczny ... 135
Zabezpieczenie budynku ... 136
Zabezpieczenie komputerów ... 136
Szyfrowanie danych zapisanych na lokalnych dyskach twardych ... 138
Nieodwracalne usuwanie usuniętych danych ... 141
Zabezpieczenie bazy kont lokalnych użytkowników ... 142

Bezpieczna administracja systemem ... 143
Ograniczenie dostępu użytkowników do komputerów ... 144
Wymuszenie stosowania skomplikowanych haseł ... 144
Ograniczenie dostępnych godzin logowania ... 145
Ograniczenie dostępnych komputerów ... 145
Minimalizowanie skutków ataku ... 146

Rozdział 9. Uprawnienia użytkowników ... 147
Protokoły potwierdzania tożsamości użytkownika ... 149
NTLM ... 149
Kerberos ... 150
Minimalizacja ryzyka zdobycia haseł przez hakera ... 150
Zasady konta ... 152
Nadawanie uprawnień użytkownikom ... 152
Zarządzanie kontami użytkowników ... 154
Zarządzanie kontami niskiego ryzyka ... 154
Szablony zabezpieczeń ... 155
Szablony administracyjne ... 159
Skrypty administracyjne ... 160
Przekazywanie argumentów ... 160
Skrypty logowania ... 161
Pliki i foldery ... 163
Rejestr ... 166
Monitorowanie wykonania skryptów ... 167
Monitorowanie aktywności użytkowników ... 169
Wybór zdarzeń podlegających inspekcji ... 169
Konfiguracja dziennika zabezpieczeń ... 170

Rozdział 10. Active Directory i DNS ... 173
Active Directory ... 173
Zagrożenia ... 174
DNS ... 174
Zagrożenia ... 176

Rozdział 11. Autoryzacja ... 179
Zagrożenia ... 179
Zabezpieczenie autoryzacji ... 180
Autoryzacja w sieci lokalnej ... 181
Wybór protokołu autoryzacji ... 181
Autoryzacja zewnętrznych użytkowników ... 184
Serwery WWW ... 184
Serwery RAS ... 188

Rozdział 12. RADIUS ... 193
Integracja z usługami sieciowymi ... 194
Serwer i klient RADIUS ... 194
Serwer RADIUS ... 194
Klient RADIUS ... 195
Bezpieczeństwo ... 195
Zasady dostępu zdalnego ... 195
Autoryzacja użytkowników ... 198
Szyfrowanie ... 199

Rozdział 13. Udostępnione zasoby 207
System plików NTFS 208
Uprawnienia NTFS 209
Szyfrowanie EFS 210
Udostępnione zasoby 213
Udziały administracyjne 213
Drukarki 214
Plik bufora wydruku 215
Przesyłanie danych do drukarki 216
Rejestr 216
Zdalna edycja rejestru 217
Kopie zapasowe 218

Rozdział 14. Transmisja 219
Protokoły niskiego poziomu 219
Zagrożenia 219
Zmniejszanie ryzyka 224
IPSec 225
Protokoły wyższych poziomów 233
Podpisywanie pakietów SMB 234
SSL/TLS 235
S/MIME 235
Sieci bezprzewodowe 236
Protokoły lokalnych bezprzewodowych sieci komputerowych 236
Zagrożenia 237
Zmniejszenie ryzyka 238

Rozdział 15. Wirtualne sieci prywatne 239
Routing w sieciach Microsoft Windows 240
Tabela routingu 240
Filtry 240
Statyczne trasy routingu zdalnych klientów 241
Dynamiczne trasy routingu 242
Adresowanie w sieciach VPN 243
Tworzenie połączeń VPN 246
Konfiguracja serwera VPN 246
Konfiguracja klienta VPN 248
Administracja sieciami VPN 250
Zarządzanie kontami i uprawnieniami użytkowników 250
Uwierzytelnianie zdalnych użytkowników i komputerów 250
Nadawanie adresów IP 250
Zmniejszanie ryzyka 251
Zablokowanie usług świadczonych przez serwer VPN 251
Blokada konta 252
Filtry połączeń PPTP 252
Filtry połączeń L2TP 253

Rozdział 16. Zabezpieczenie komputerów przed atakami z Internetu 255
Instalacja serwera ISA 255
Wymagania 255
Konfiguracja klientów serwera ISA 256
Konfiguracja 257
Zabezpieczenie serwera ISA 258
Zasady dostępu 258
Potwierdzanie tożsamości klientów 261
Klienci zdalni 262

Zapora połączenia internetowego ... 264
VPN ... 267
Serwer proxy ... 268
Monitorowanie ... 268
Zdarzenia ... 269
Dzienniki serwera ISA ... 270
Raporty ... 270

Rozdział 17. Monitorowanie i reagowanie na naruszenie zasad bezpieczeństwa ... 273
Zasady bezpieczeństwa ... 273
Analiza zabezpieczenia komputera ... 274
Wynikowe zasady bezpieczeństwa ... 274
MBSA ... 276
Monitorowanie naruszenia zasad bezpieczeństwa ... 278
Nieregularności w przesyłaniu danych ... 278
Nieregularności w pracy komputerów ... 278
Informacje o naruszeniu zasad bezpieczeństwa ... 279
Reagowanie ... 280
Poziom zagrożenia ... 280
Minimalizowanie skutków ataku ... 281

Rozdział 18. Sieci heterogeniczne ... 283
Klienty uniksowe ... 283
Potwierdzanie tożsamości użytkowników ... 284
Zasoby ... 285
Klienty Novell NetWare ... 285
Potwierdzanie tożsamości użytkowników ... 286
Zabezpieczenie komunikacji ... 286
Klienty AppleTalk ... 287
Potwierdzanie tożsamości użytkowników ... 287
Zasoby ... 287
Usługi sieciowe ... 288
DHCP ... 288
DNS ... 288
SNMP ... 289

Część III Wykorzystanie kryptografii ... 291

Rozdział 19. Metody szyfrowania danych ... 293
Algorytmy szyfrowania ... 293
Funkcje skrótu ... 293
Algorytmy symetryczne ... 294
Algorytmy asymetryczne ... 295
Algorytmy tajne ... 297
Algorytmy jawne ... 298
Klucze ... 298
EFS ... 298
Zastosowania kryptografii ... 299
Bezpieczeństwo szyfrogramów ... 299

Rozdział 20. Infrastruktura kluczy publicznych ... 303
Składniki PKI ... 303
Certyfikaty ... 304
Urzędy certyfikacji ... 305
Szablony certyfikatów ... 309
Narzędzia administracyjne PKI ... 310

Rozdział 21. Certyfikaty 311
Planowanie hierarchii urzędów certyfikacji 311
Typy hierarchii urzędów certyfikacji 312
Bezpieczeństwo PKI 313
Wytyczne końcowe 313
Tworzenie hierarchii urzędów certyfikacji 314
Główny urząd certyfikacji 314
Punkty dystrybucji certyfikatów i list CRL 315
Sprawdzanie ważności certyfikatów 317
Podrzędny urząd certyfikacji 318
Zarządzanie certyfikatami 319
Cykl życia certyfikatu 319
Zabezpieczenie CA 320
Rejestracja certyfikatów 322
Metody rejestracji certyfikatów 322
Rejestracja za pośrednictwem serwera WWW 323
Rejestracja za pośrednictwem konsoli Certyfikaty 325
Rejestracja za pośrednictwem programu Certreq 326
Automatyzacja rejestracji 326

Rozdział 22. Klucze 329
Strategie wykonywania i odtwarzania kopii zapasowych 330
Strategia kopii danych 330
Strategia kopii kluczy 330
Formaty plików 331
Eksportowanie certyfikatów 332
Konsola MMC Certyfikaty 332
Outlook Express 333
Zabezpieczenie plików kluczy prywatnych 333
Importowanie certyfikatów 334
Automatyczne zarządzanie kopiami kluczy prywatnych 335

Rozdział 23. Bezpieczeństwo usług internetowych 337
Zabezpieczenie serwera IIS 337
Zmiana domyślnej lokalizacji folderów serwera IIS 338
Zmniejszanie ryzyka 339
Komunikacja z serwerem IIS 339
Zabezpieczenie przeglądarki Internet Explorer 340
Strefy 340
Prywatność 341
Protokół SSL 343
Bezpieczna komunikacja z serwerem IIS za pośrednictwem SSL 345
Konfiguracja serwera IIS 346
Potwierdzane tożsamości użytkowników za pomocą certyfikatów 347
Zabezpieczenie serwera poczty elektronicznej 349
Środowisko Windows 2000 351
Środowisko Windows .NET 351
Bezpieczna komunikacja z serwerem Exchange 352
Zabezpieczenie klienta poczty elektronicznej 353
Zabezpieczenie komunikatorów internetowych 356

Skorowidz 359

Rozdział 23.

Bezpieczeństwo usług internetowych

Podłączenie lokalnej sieci komputerowej do Internetu zawsze zwielokrotnia ryzyko zaatakowania systemu przez hakera. Zapora połączenia internetowego (a w przypadku systemów wymagających wysokiego poziomu bezpieczeństwa dwie zapory, tworzące strefę zdemilitaryzowaną) to absolutne minimum, chroniące lokalne komputery przed atakami z Internetu. Jednak żadna zapora połączenia internetowego nie zabezpiecza systemu przed atakami na serwery i klienty usług internetowych, takie jak WWW czy poczta elektroniczna.

Zabezpieczenie serwera IIS

Microsoft Internet Information Services, wchodzący w skład systemów Windows 2000 Server i Windows .NET serwer WWW, FTP i NNTP, to jeden z najbardziej narażonych na ataki składników sieci Windows. Do najczęstszych typów ataków na ten serwer należą:

1. Uruchomienie przez hakera przykładowych programów serwera lub domyślnie instalowanych skryptów administracyjnych w celu przejęcia kontroli lub zmiany konfiguracji serwera.
2. Wykorzystanie domyślnej konfiguracji serwera, np. w celu uzyskania dostępu do folderu systemowego.
3. Wykorzystanie znanych słabych punktów tego serwera, np. przepełnienia bufora, w celu przejęcia nad nim kontroli.
4. Zdobycie poprzez sam serwer albo poprzez publikowane przez niego, a źle zabezpieczone, strony WWW informacji ułatwiających przeprowadzenie skutecznego ataku na system, np. haseł do serwera bazodanowego czy adresu IP wewnętrznego serwera DNS.
5. Zablokowanie serwera.

Zmiana domyślnej lokalizacji folderów serwera IIS

Instalując serwer IIS za pomocą panelu sterowania, administrator nie ma możliwości zmiany domyślnej lokalizacji folderów *ftproot* oraz *wwwroot* — zawsze ich lokalizacją będzie ścieżka *%SystemDisk%\InetPub*. Fakt ten w połączeniu z nieodpowiednim nadaniem uprawnień do systemowej partycji (o próbie zainstalowania serwera IIS na partycji FAT nawet nie wspominam) powoduje, że stosunkowo łatwo haker uzyskuje zdalny dostęp do dowolnego obiektu znajdującego się na tej partycji. Aby zmienić domyślną lokalizację tych folderów i zabezpieczyć się przed atakami tego typu, musimy przygotować **plik odpowiedzi instalacji nienadzorowanej** serwera IIS.

Instalacja systemu Windows 2000 i serwera IIS

Jeżeli serwer IIS ma zostać automatycznie zainstalowany podczas instalacji systemu operacyjnego:

- Przygotuj plik odpowiedzi instalacji nienadzorowanej systemu Microsoft Windows 2000 (plik *Unattend.txt*).



> Zagadnienia związane z automatyzacją instalacji systemu operacyjnego wykraczają poza zakres tej książki. Zainteresowani Czytelnicy znajdą opis tego zagadnienia np. w wydanej przez wydawnictwo Helion książce „Windows 2000 Server. Egzamin 70-215".

- Otwórz ten plik w dowolnym edytorze tekstowym i dodaj poniższą sekcję:

```
[InternetServer]
PathFtpRoot = lokalizacja_katalogu_FtpRoot
PathWwwRoot = lokalizacja_katalogu_WwwRoot
```

- Zapisz zmodyfikowany plik i rozpocznij proces automatycznej instalacji systemu Windows 2000.

Instalacja serwera IIS w działającym systemie Windows 2000

Aby zainstalować serwer IIS, zapisując w innej niż domyślna lokalizacji foldery *ftproot* oraz *wwwroot*, należy:

1. Upewnić się, czy serwer IIS nie jest zainstalowany i jeżeli tak — usunąć go z systemu. W takim przypadku należy również usunąć folder *%SystemDisk%\InetPub*.
2. Przygotować plik odpowiedzi instalacji serwera IIS. Na podstawie przykładowego pliku zostaną zainstalowane wszystkie składniki programu, a foldery *ftproot* i *wwwroot* zostaną przeniesione na dysk *D:*

```
[Components]
iis_common = on
iis_www = on
iis_ftp = on
iis_inetmgr = on
```

```
iis_htmla = on
iisdbg = on
iis_nntp = on
iis_nntp_docs = on
iis_smtp = on
iis_smtp_docs = on
iis_doc = on
[InternetServer]
PathFtpRoot = D:\InetPub\FtpRoot
PathWWWRoot = D:\InetPub\WwwRoot
```

3. Zapisać utworzony plik w głównym folderze dysku systemowego pod nazwą *iis.txt* i uruchomić instalator składników systemu Windows:

```
sysocmgr /i:%winnt%\inf\sysoc.inf /u:c:\iis.txt
```

Zmniejszanie ryzyka

Oprócz przeniesienia folderów, w których przechowywane są publikowane dokumenty, zmniejszyć ryzyko ataku na serwer IIS możemy poprzez:

- restrykcyjne ograniczenie uprawnień NTFS użytkowników, w tym użytkownika *IUSR_nazwa_serwera* do dysku, na którym zainstalowany został serwer IIS,
- wdrożenie restrykcyjnej polityki dotyczącej haseł i uprawnień użytkowników serwera IIS,
- uruchomienie na serwerze IIS minimalnej liczby usług sieciowych i zablokowanie wszystkich usług niewykorzystywanych (w szczególności serwer IIS nie powinien pełnić funkcji kontrolera domeny czy routera dostępowego),
- **wyłączeniu systemu NetBIOS przez TCP/IP**,
- systematyczne aktualizowanie serwera IIS (zautomatyzować tę czynność możemy np. dzięki dostępnemu w witrynie WWW firmy Microsoft programowi *HFNetChk* (ang. *Network Security Hotfix Checker tool*),
- zabezpieczenie przesyłanych danych protokołem SSL i wymaganie potwierdzania tożsamości klientów za pomocą certyfikatów — techniki te zostały opisane w dalszej części rozdziału.

Komunikacja z serwerem IIS

Dane pomiędzy serwerem IIS a jego klientami przesyłane są za pośrednictwem jednego z trzech protokołów:

1. Protokół HTTP umożliwia przeglądanie witryn WWW.
2. Protokół FTP — przesyłanie plików.
3. Protokół NNTP — wysyłanie i odbieranie wiadomości grup dyskusyjnych.

Podstawowe ryzyko związane z komunikacją za pośrednictwem protokołów FTP i NNTP polega na tym, że w przypadku umożliwienia nawiązywania połączeń anonimowych nie ma możliwości potwierdzenia tożsamości klienta, a w innym przypadku hasło użytkownika przesyłane jest do serwera jawnym tekstem (przykład przechwycenia przez hakera hasła do serwera FTP znajduje się w rozdziale 4.). Z tego powodu należy uruchomić usługi FTP i NNTP na innym serwerze IIS niż serwer pełniący usługi WWW. Chociaż możliwe jest ograniczenie listy adresów IP klientów serwerów FTP i NNTP, to jedynym gwarantującym względne bezpieczeństwo rozwiązaniem jest zabezpieczenie komunikacji z klientami protokołem SSH.

SSH

SSH (ang. *Secure Shell Protocol*), tak jak TELNET, jest protokołem umożliwiającym klientom zalogowanie się w zdalnym systemie poprzez sieć, ale w przeciwieństwie do protokołu TELNET, umożliwia zabezpieczenie przesyłanych informacji, w tym informacji uwierzytelniających użytkownika. Ponieważ pakiety innych protokołów, w tym protokołu PPP, mogą zostać „opakowane" w pakietach protokołu SSH, w rezultacie użytkownik ma możliwość nawiązania bezpiecznego połączenia z dowolnym serwerem, w tym z serwerem FTP czy NNTP.

Zabezpieczenie przeglądarki Internet Explorer

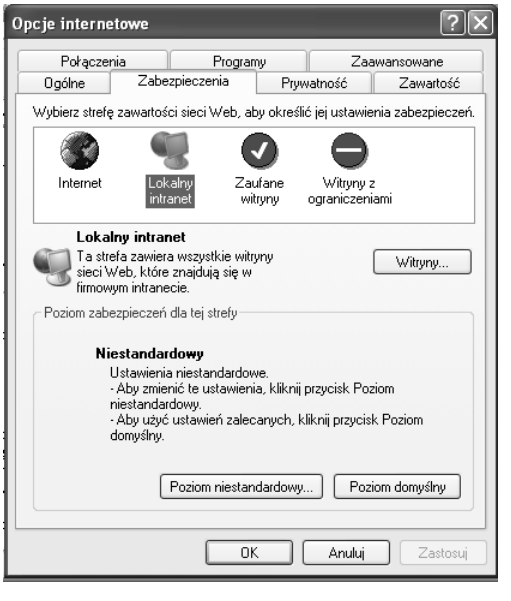
Równie duży wpływ na bezpieczeństwo systemu, co zabezpieczenie serwera IIS, ma zabezpieczenie programów klienckich tego serwera. Domyślnym, instalowanym wraz z systemem Windows klientem WWW, FTP i NNTP, jest przeglądarka Internet Explorer.

Statyczne strony WWW, czyli strony zapisane wyłącznie w postaci znaczników języka HTML, są już rzadkością. Dzisiaj prawie każda strona WWW jest tworzona z wykorzystaniem takich technologii, jak ASP, CGI czy języków skryptowych, takich jak JavaScript czy VBScript. Aby tak przygotowane strony były prawidłowo wyświetlane, przeglądarki internetowe muszą obsługiwać te technologie. A to z kolei powoduje wzrost zagrożenia związanego z możliwością uruchomienia na komputerze użytkownika wrogiego programu (szczególne znaczenie ma to w przypadku przeglądarki IE, która jest elementem systemu operacyjnego). Dlatego jednym z najskuteczniejszych sposobów obrony przed atakami na przeglądarkę IE jest ograniczenie możliwości automatycznego wykonywania potencjalnie niebezpiecznych programów.

Strefy

Internet Explorer umożliwia przypisanie konkretnych serwerów WWW do jednej z trzech **stref zabezpieczeń**:

1. W strefie *Lokalny intranet* znajdują się domyślnie wszystkie serwery WWW o prywatnych lub lokalnych adresach IP. Poziom bezpieczeństwa dla tej strefy ustawiany jest według szablonu *Średnio-niski*, co oznacza między innymi, że możliwe będzie automatyczne uruchamianie komponentów ActiveX i skryptów znajdujących się w przypisanych do tej strefy witrynach WWW.
2. Strefa *Zaufane witryny* domyślnie nie zawiera żadnych witryn. Po przypisaniu serwerów WWW do tej strefy obowiązywać je będzie szablon zabezpieczeń *Niski*, co oznacza między innymi, że możliwe będzie automatyczne uruchamianie również tych komponentów ActiveX i skryptów, które nie zostały oznaczone przez ich twórców jako bezpieczne.
3. Strefa *Witryny z ograniczeniami* również domyślnie nie zawiera żadnych witryn. Po przypisaniu serwerów WWW do tej strefy obowiązywać je będzie szablon zabezpieczeń *Wysoki*, co oznacza, że niemożliwe będzie uruchamianie i pobieranie wszelkich potencjalnie niebezpiecznych składników, takich jak komponenty ActiveX, skrypty czy pliki (rysunek 23.1).

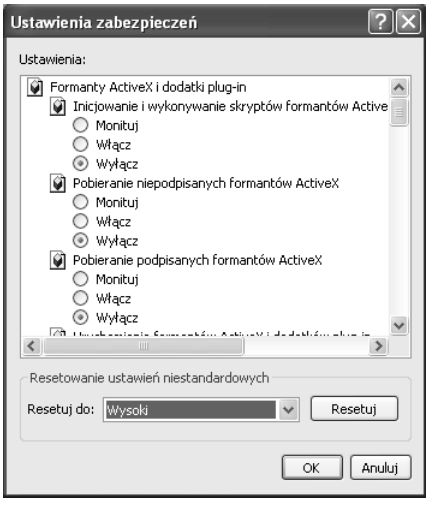


Rysunek 23.1. *Ponieważ stron WWW skopiowanych i otwieranych z lokalnego dysku twardego nie będą obowiązywały przypisania do poszczególnych stref, nie należy uruchamiać plików HTML z lokalnego dysku twardego*

Poziom zabezpieczeń obowiązujący w poszczególnych strefach może zostać dopasowany do indywidualnych wymagań użytkownika. W tym celu należy wybrać strefę i kliknąć przycisk *Poziom niestandardowy…*. Zostanie wyświetlone okno dialogowe *Ustawienia zabezpieczeń* (rysunek 23.2), umożliwiające dostosowanie poziomu zabezpieczeń do potrzeb użytkownika.

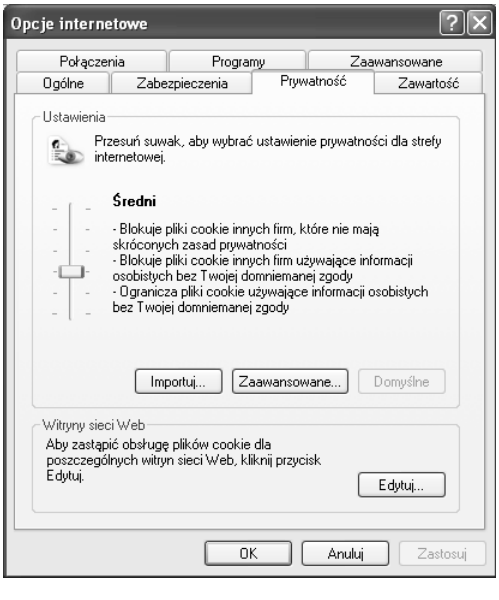
Prywatność

Ponieważ serwery WWW umożliwiające dostęp anonimowym użytkownikom nie są w stanie zidentyfikować użytkowników, którzy łączą się ponownie z tą samą stroną (np. w celu dopasowania wyglądu strony do preferencji danego użytkownika), zapisują



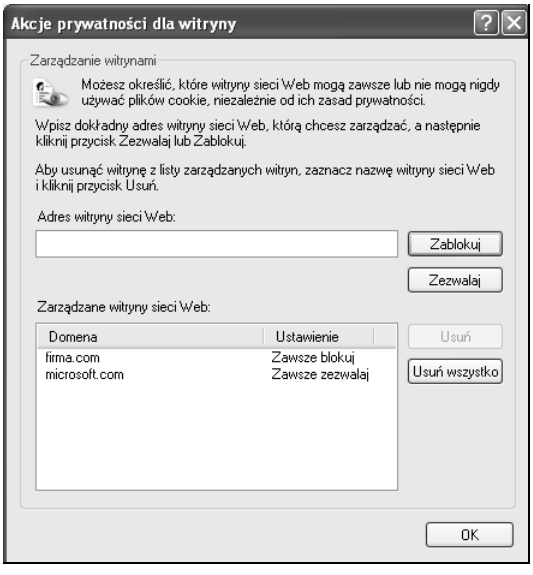
Rysunek 23.2. *Okno dialogowe umożliwiające konfigurację poziomu zabezpieczeń obozujących w danej strefie*

one w tym celu na **komputerze użytkownika** pliki cookie. Przeglądarka IE umożliwia skonfigurowanie zasad pobierania tych plików: pliki cookie mogą być automatycznie pobierane, ich pobranie może zależeć od tego, kto próbuje wysłać nam taki plik lub od jawnej bądź domniemanej (na podstawie konfiguracji IE) odpowiedzi użytkownika, możliwe jest również zablokowanie plików cookie. Ta ostatnia opcja, zastosowana w odniesieniu do wszystkich serwerów internetowych, spowoduje, że niektóre witryny, np. witryny banków internetowych, nie będą poprawnie wyświetlane (rysunek 23.3).



Rysunek 23.3. *Domyślnie obowiązujący średni poziom zabezpieczeń w zabezpieczonych systemach powinien zostać podniesiony do poziomu wysokiego*

Ponieważ wysoki poziom prywatności może uniemożliwić poprawne wyświetlanie niektórych stron WWW, po jego ustawieniu należy jawnie określić domeny, z których pochodzące pliki cookie będą zawsze akceptowane (rysunek 23.4).

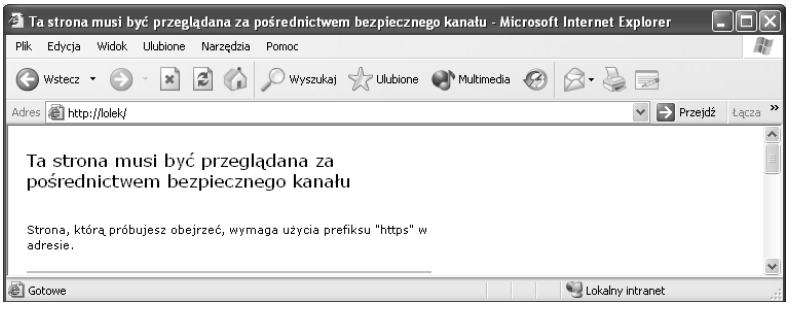


Rysunek 23.4. *IE pozwala nie tylko na określenie poziomu prywatności, ale również na jawne podanie domen, z których pliki cooki będą zawsze akceptowane lub odrzucane*

Protokół SSL

Warstwa zabezpieczeń łączy (ang. *Secure Sockets Layer*, SSL) to najpopularniejszy w Internecie protokół warstwy aplikacji, służący do zabezpieczenia przesyłanych poprzez publiczną sieć danych. Ponieważ domyślnie dane w pakietach protokołu HTTP przesyłane są jawnym tekstem, w zabezpieczonych systemach komunikacja z serwerami WWW powinna odbywać się za pośrednictwem protokołu SSL. Dodatkowo protokół ten umożliwia potwierdzanie tożsamości klienta i serwera na podstawie wydanych im certyfikatów.

Aby nawiązać bezpieczne połączenie z serwerem WWW, po stronie klienta nie jest wymagana instalacja żadnego dodatkowego oprogramowania — wystarczy, że podając adres URL, użytkownik zastąpi nazwę protokołu HTTP nazwą protokołu HTTPS. Natomiast po stronie serwera WWW konieczne jest zainstalowanie certyfikatu serwera WWW. Na przykład aby nawiązać bezpieczne połączenie z serwerem WWW *lolek*, użytkownik powinien wpisać adres *https://lolek* (rysunek 23.5).

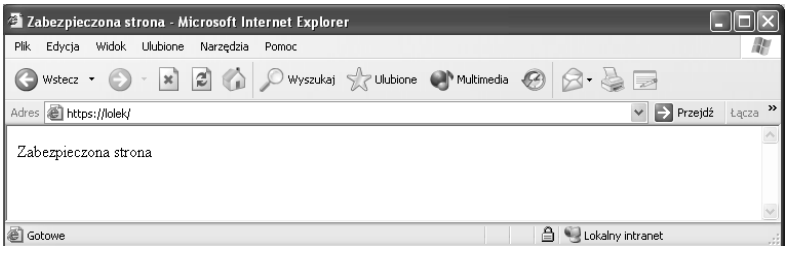


Rysunek 23.5. *Niektóre strony muszą być przeglądane za pośrednictwem protokołu SSL*

Po wpisaniu poprawnego adresu zabezpieczonej strony serwer WWW wysyła do klienta swój certyfikat zawierający klucz publiczny serwera WWW. Klucz ten będzie wykorzystywany przez klienta do deszyfrowania przesłanych danych.

Następnie następuje wynegocjowanie długości klucza sesji używanego do szyfrowania wszystkich przesyłanych danych. Z uwagi na moc obliczeniową współczesnych komputerów, serwer WWW nie powinien zgadzać się na wynegocjowanie podatnego na ataki siłowe 40-bitowego klucza. Zabezpieczone serwery WWW, publikujące poufne lub ważne dane, powinny wymagać szyfrowania za pomocą klucza o długości 128 bitów.

Po wynegocjowaniu długości klucza sesji klient generuje ten klucz, szyfruje go otrzymanym wcześniej kluczem publicznym serwera WWW i odsyła go do serwera. Ponieważ do odszyfrowania klucza sesji niezbędny jest klucz prywatny serwera WWW, klient może mieć pewność, że zaszyfrowane dane będą dostępne tylko dla serwera WWW, z którym nawiązano połączenie (rysunek 23.6).



Rysunek 23.6. *Ikona kłódki wyświetlona na pasku zadań IE świadczy o pomyślnym nawiązaniu bezpiecznego połączenia z serwerem WWW. Ponieważ nie można wykluczyć, że haker podszywa się pod serwer WWW o określonym adresie, przed wysłaniem np. hasła do konta założonego w banku internetowym należy, klikając na tę ikonę, sprawdzić poprawność certyfikatu danego serwera WWW*

O ile nawiązanie bezpiecznego połączenia z serwerem WWW w żadnym wypadku nie jest możliwe, jeżeli dany serwer nie posiada własnego certyfikatu, o tyle serwer WWW może dodatkowo wymagać potwierdzenia tożsamości użytkownika za pomocą wystawionego temu użytkownikowi certyfikatu (serwer IIS może **akceptować** lub **wymagać** certyfikatu klienta).

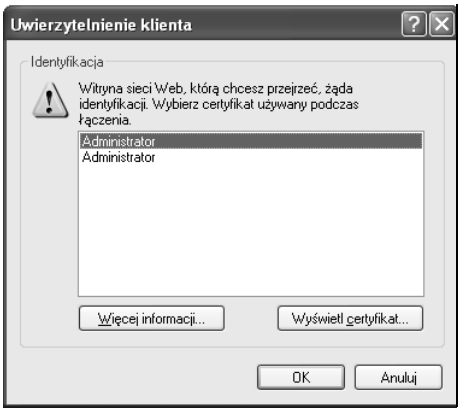


Certyfikat serwera WWW może zostać wystawiony przez prywatny urząd certyfikacji lub wykupiony w firmie świadczącej usługi tego typu.

Jeżeli po stronie serwera włączone zostanie mapowanie pomiędzy certyfikatami a nazwami upoważnionych do przeglądania stron WWW użytkowników systemu, a dany użytkownik posiada kilka certyfikatów umożliwiających nawiązywanie bezpiecznych połączeń, przed nawiązaniem połączenia będzie on musiał wybrać certyfikat, którym posłuży się w tym przypadku (rysunek 23.7).



Ważność wykorzystanego do nawiązania połączenia certyfikatu musi zostać potwierdzona przez główny urząd certyfikacji organizacji, która wystawiła certyfikat serwera WWW.



Rysunek 23.7. *Certyfikaty są najbezpieczniejszym sposobem potwierdzenia tożsamości klienta. Jeżeli użytkownik posiada kilka certyfikatów, będzie mógł wybrać, którym z nich w tym wypadku potwierdzi swoją tożsamość*

Bezpieczna komunikacja z serwerem IIS za pośrednictwem SSL

Koniecznym warunkiem, umożliwiającym nawiązywanie bezpiecznych połączeń z serwerem IIS, jest zarejestrowanie certyfikatu serwera WWW. W tym celu należy:

1. Uruchomić konsolę MMC *Internetowe usługi informacyjne*.
2. Wyświetlić właściwości wybranej witryny WWW.



Aby zabezpieczyć się przed przesyłaniem haseł jawnym tekstem, należy zabezpieczać całe witryny, a nie poszczególne strony WWW.

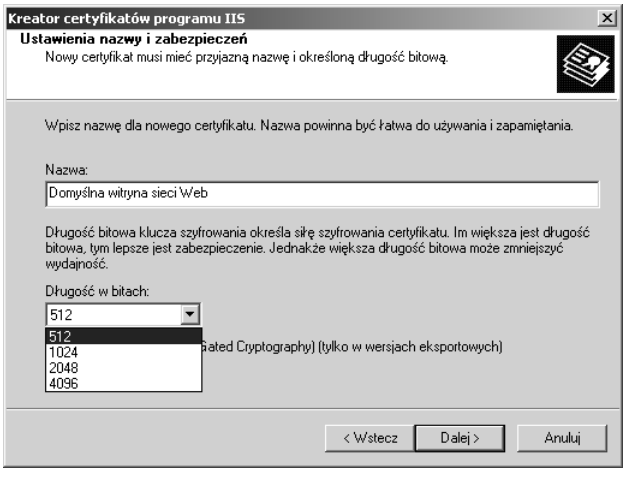
3. Kliknąć znajdujący się w zakładce *Zabezpieczenia katalogów* przycisk *Certyfikat serwera...*.
4. Odpowiadając na pytanie *Kreatora certyfikatów serwera IIS*, wybrać opcję *Utwórz nowy certyfikat*.
   a) Jeżeli CA, do którego zostanie wysłane żądanie, jest prywatnym urzędem CA, należy następnie wybrać opcję *Wyślij żądanie natychmiast do urzędu certyfikacji online*.



Instalacja i konfiguracja urzędów certyfikacji zostały opisane w rozdziale 21.

   b) Jeżeli certyfikat zostanie wystawiony przez publiczny urząd certyfikacji, należy wybrać opcję *Przygotuj żądanie teraz, ale wyślij później*. W efekcie żądanie certyfikatu zostanie zapisane w pliku formatu PKCS#10. Plik ten należy następnie, za pomocą poczty elektronicznej, wysłać do wybranej firmy, oferującej certyfikaty.

5. Podać opisową nazwę certyfikatu i określić długość klucza prywatnego serwera WWW (rysunek 23.8).



Rysunek 23.8. *Ze względu na wydajność, w większości wypadków serwery WWW używają klucza prywatnego o długości 512 lub 1024 bitów*

6. Następnie należy podać nazwę i podstawowe dane firmy ubiegającej się o certyfikat. Po zakończeniu pracy kreatora albo żądanie będzie automatycznie rozpatrzone przez prywatny CA, albo trzeba będzie zainstalować przesłany przez publiczny CA certyfikat serwera WWW.

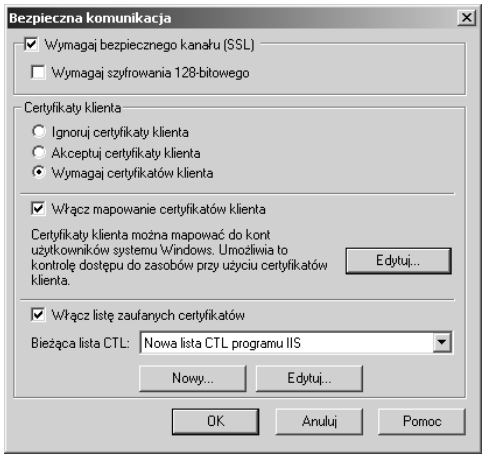


Jeżeli określona w certyfikacie nazwa domeny nie będzie odpowiadać nazwie domeny serwera WWW, klienci podczas nawiązywania połączenia będą każdorazowo ostrzegani o prawdopodobnym podszywaniu się serwera WWW pod serwer, dla którego wystawiono certyfikat.

Konfiguracja serwera IIS

Po zainstalowaniu certyfikatu możliwa jest konfiguracja zabezpieczeń publikowanej poprzez serwer IIS witryny. Administrator systemu ma możliwość:

- uniemożliwiania nawiązywania połączeń za pośrednictwem protokołu HTTP (po wybraniu tej opcji możliwe będzie wyłącznie nawiązywanie połączeń za pośrednictwem protokołu HTTPS),
- wymuszenia stosowania 128-bitowego klucza sesji (po wybraniu tej opcji przeglądarki internetowe nie obsługujące tak silnego szyfrowania nie umożliwią przeglądania witryny),
- potwierdzania za pośrednictwem certyfikatów tożsamości klientów, w tym powiązania certyfikatów z określonymi kontami użytkowników lokalnej domeny (rysunek 23.9),
- zmienienia (opcja dostępna jest w zakładce *Witryna sieci Web*) portu wykorzystywanego do nawiązywania bezpiecznych połączeń (domyślnie protokół SSL wykorzystuje port 443).



Rysunek 23.9. *Implementacja PKI umożliwia nie tylko szyfrowanie przesyłanych danych, ale również potwierdzanie tożsamości klientów zdalnych*

Potwierdzane tożsamości użytkowników za pomocą certyfikatów

Po skonfigurowaniu bezpiecznej komunikacji z serwerem IIS za pośrednictwem protokołu SSL administrator może dodatkowo podnieść poziom bezpieczeństwa systemu, wymuszając potwierdzanie tożsamości użytkowników za pomocą certyfikatów. W ten sposób, zamiast sprawdzać poprawność wprowadzonego przez użytkownika hasła, serwer IIS przeprowadzi autoryzację na podstawie powiązań certyfikatów z lokalnymi lub domenowymi kontami użytkowników.

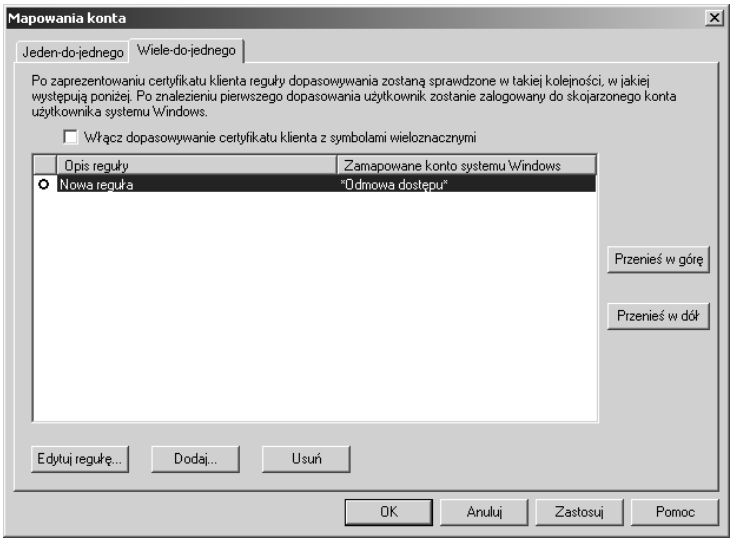
Metody uwierzytelniania

Wersja 6.0 serwera IIS umożliwia potwierdzenie tożsamości zdalnego użytkownika na podstawie jednej z poniższych, uszeregowanych według ich bezpieczeństwa, metod:



Serwer IIS zezwala również na dostęp użytkownikom anonimowym. W takim przypadku poznać tożsamość użytkownika można jedynie, analizując dzienniki zabezpieczeń serwera IIS i zapory połączenia internetowego.

1. Przesłanego jawnym tekstem hasła użytkownika (uwierzytelnianie podstawowe).
2. Przesłanej wyliczonej na podstawie hasła użytkownika wartości funkcji skrótu (uwierzytelnianie skrócone).
3. Przesłania paszportu .NET (wszystkie informacje w paszporcie .NET użytkownika przechowywane są w postaci zaszyfrowanej).
4. Wymiany komunikatów wyzwania i odpowiedzi (zintegrowane uwierzytelnienie systemu Windows).
5. Przesłania poprawnego certyfikatu. W tym przypadku administrator może utworzyć powiązania typu jeden do jednego lub wiele do jednego pomiędzy certyfikatami a kontami użytkowników (rysunek 23.10).



Rysunek 23.10. *Tworzenie powiązań typu wiele do jednego ułatwia zarządzanie większą liczbą użytkowników serwera IIS*

Konfiguracja uwierzytelniana za pomocą certyfikatów

Aby serwer IIS mógł potwierdzić tożsamość użytkownika, administrator musi zainstalować w nim certyfikaty poszczególnych użytkowników. Zadanie to może zostać zrealizowane na poziomie serwera IIS lub domeny (czy jednostki organizacyjnej) Active Directory.

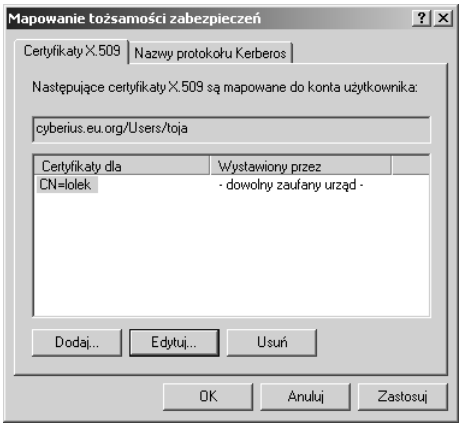
W pierwszym wypadku administrator powinien za pomocą konsoli MMC *Certyfikaty* wyeksportować certyfikaty użytkowników do plików w formacie Base64 (plików o rozszerzeniach *.cer*, *.crt*, *.spc*, lub *.key*). Po upewnieniu się, że serwer IIS ufa głównemu urzędowi certyfikacji, który wystawił te certyfikaty, pozostaje jeszcze przygotować hasła użytkowników. Administrator musi **znać hasła użytkowników**, dla których będzie tworzył powiązania pomiędzy kontem a certyfikatem.

Jeżeli w ramach domeny działa kilka serwerów IIS, administrator może utworzyć powiązania pomiędzy certyfikatami a kontami użytkowników za pomocą konsoli MMC *Użytkownicy i komputery usługi Active Directory*. W tym celu należy:

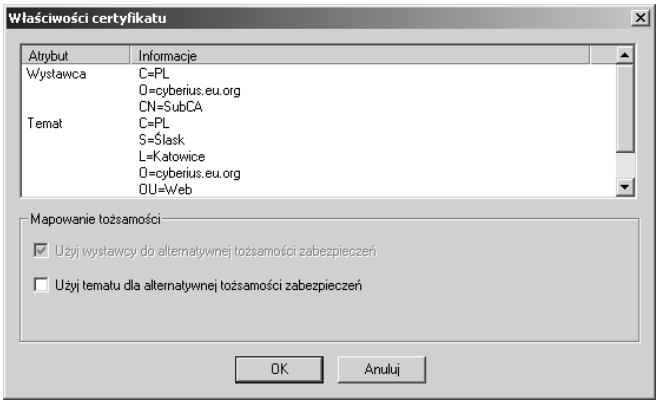
1. Zaznaczyć dostępną w menu *Widok* tej konsoli pozycję *Opcje zawansowane*.
2. Zaznaczyć konto wybranego użytkownika i z menu kontekstowego wybrać polecenie *Mapowanie nazw…*.
3. Zaimportować certyfikat danego użytkownika (rysunek 23.11).
4. Jeżeli utworzone ma zostać powiązanie typu wiele do jednego, należy wyczyścić pole wyboru *Użyj tematu dla alternatywnej tożsamości zabezpieczeń* (rysunek 23.12).



W obu przypadkach usunięcie powiązanego z certyfikatem konta użytkownika uniemożliwi tej osobie nawiązanie połączenia z zabezpieczoną witryną WWW.



Rysunek 23.11. *Konsola Użytkownicy i komputery usługi Active Directory umożliwia dodatkowo importowanie certyfikatów zapisanych w formacie DER (ang. Distinguished Encoding Rules)*



Rysunek 23.12. *Precyzyjne powiązanie certyfikatów do konta użytkownika za pomocą reguł jest możliwe wyłącznie za pomocą konsoli MMC Internetowe Usługi Informacyjne*

Zabezpieczenie serwera poczty elektronicznej

Równie popularne, co ataki na serwery i klienty WWW, są ataki na serwery i klienty poczty elektronicznej. Zadaniem serwera poczty elektronicznej jest wysyłanie, odbieranie i filtrowanie wiadomości przesyłanych pomiędzy klientami. Do realizacji tego zadania wykorzystywane są następujące protokoły sieciowe:

- SMTP (ang. *Simple Mail Transfer Protocol*) jest wykorzystywany do wysyłania i odbierania wiadomości e-mail. Do zaszyfrowania pakietów tego protokołu należy wykorzystać technologię S/MIME (ang. *Secure Multipurpose Internet Mail Extensions*) oraz jeden z dwóch protokołów: IPSec lub SSL.
- POP3 (ang. *Post Office Protocol 3*) jest wykorzystywany do zapisywania wiadomości w znajdujących się na serwerze pocztowym skrzynkach klientów. Klienci łącząc się z serwerem, mogą pobrać zapisane w ich skrzynkach wiadomości. Do zaszyfrowania pakietów tego protokołu należy wykorzystać jeden z dwóch protokołów: IPSec lub SSL.

- IMAP (ang. *Internet Message Access Protocol*) podobnie jak protokół POP3, wykorzystywany jest do zapisywania wiadomości w skrzynkach odbiorców, ale ze jego pośrednictwem klient może traktować serwer pocztowy jak serwer plików i np. przeglądać wiadomości przed ich pobraniem. Do zaszyfrowania pakietów tego protokołu należy wykorzystać zgodną z nim technologię szyfrowania.

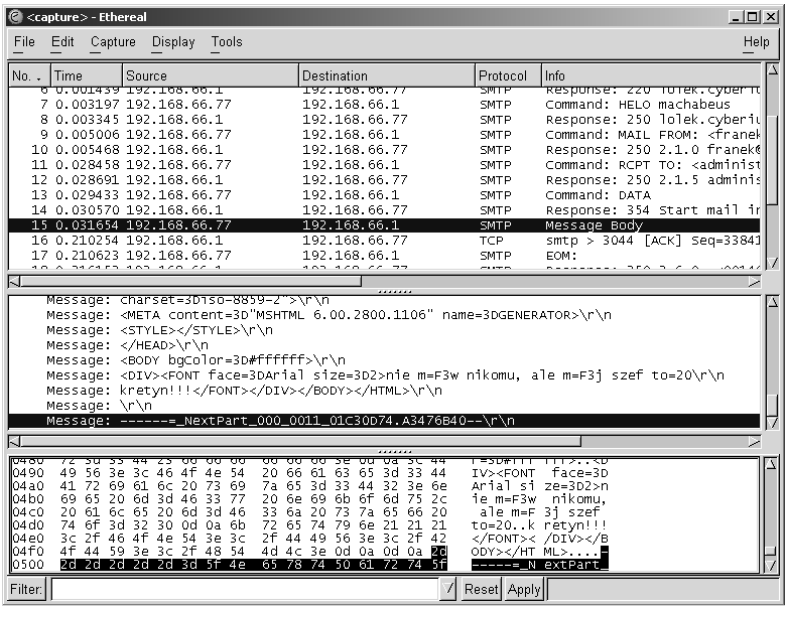


Popularną techniką zabezpieczenia wiadomości e-mail jest wykorzystanie technologii PGP (ang. *Pretty Good Privacy*). Technologia ta wykorzystuje asymetryczne protokoły szyfrowania i podpisywania wiadomości, tak więc każdy użytkownik musi dysponować parą kluczy: prywatnym i publicznym. Technologia **ta nie jest zgodna** z oferowaną w ramach PKI technologią S/MIME.

Do najczęstszych typów ataków na serwery należą:

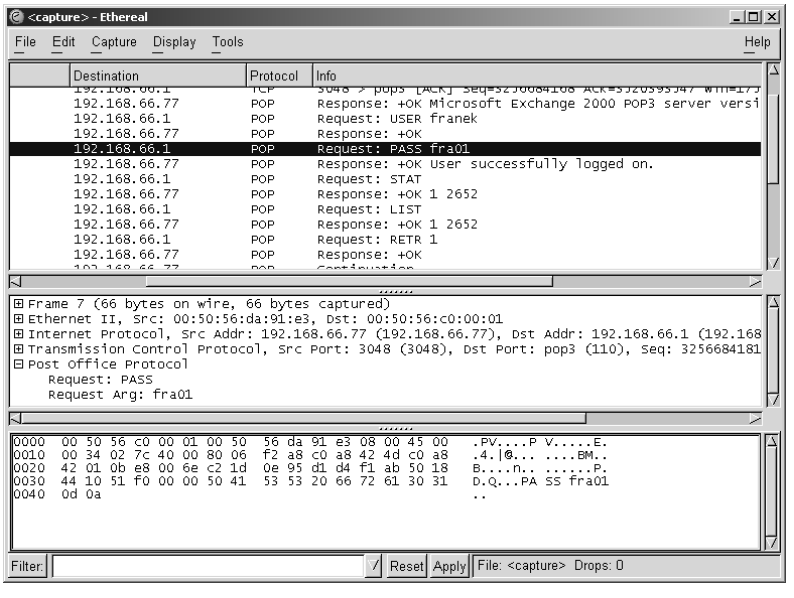
1. Podsłuchiwanie lub przechwytywanie przesyłanych wiadomości e-mail. Ponieważ domyślnie wiadomości te przesyłane są jawnym tekstem, hakerowi do poznania treści wszystkich wiadomości wystarczy dostęp do segmentu sieci, w którym znajduje się serwer pocztowy lub komputer nadawcy bądź odbiorcy wiadomości (rysunek 23.13).

Rysunek 23.13. *Wiadomości wysyłane jako HTML są mniej czytelne niż wiadomości wysyłane jako tekst, ale i tak wszyscy wiedzą, co ten pracownik myśli o swoim szefie*



2. Wykorzystanie serwera pocztowego do nieautoryzowanego przesyłania wiadomości.
3. Zablokowanie pracy serwera poprzez wysyłanie dużej liczby nieprawidłowych pakietów.
4. Wykorzystanie serwera pocztowego do automatycznego rozsyłania wirusów.

5. Podsłuchiwanie przesyłanych jawnym tekstem haseł użytkowników (rysunek 23.14).



Rysunek 23.14. *Ponieważ w domenie Windows hasło do serwera pocztowego często jest hasłem do systemu, haker nie tylko może podszyć się pod użytkownika i odczytać adresowane do niego wiadomości lub wysyłać wiadomości jako on, ale również uzyska dostęp do systemu Windows*



Zabezpieczeniem przed podsłuchiwaniem przesyłanych haseł i wiadomości e-mail oraz przed podszywaniem się pod użytkowników systemu jest wdrożenie infrastruktury kluczy publicznych.

Środowisko Windows 2000

Składnikiem serwera Microsoft Exchange 2000, umożliwiającym rejestrowanie użytkowników oraz tworzenie i odtwarzanie ich kluczy prywatnych, jest KMS (ang. *Key Managment Service*). Usługa ta nie tylko zgłasza do urzędu certyfikacji przedsiębiorstwa w imieniu użytkowników żądania wystawienia certyfikatów, ale również zapisuje kopie ich kluczy w bazie KMS i sprawdza ważność certyfikatów poprzez porównanie ich z publikowaną przez CA listą CRL.

Środowisko Windows .NET

W systemie Windows .NET Server Enterprise Edition rolę usługi KMS przejął urząd certyfikacji przedsiębiorstwa (następca serwera Exchenge 2000, serwer Microsoft Titanium, nie zawiera już usługi KMS). Dzięki takiej integracji usług związanych z zarządzaniem certyfikatami ułatwione zostało zarządzanie systemami, w ramach których działało wiele serwerów pełniących tę samą funkcję, np. kilka serwerów pocztowych. Największą zaletą nowego rozwiązania jest możliwość automatycznego wydawania i wycofywania certyfikatów S/MIME wydanych na podstawie drugiej wersji szablonów certyfikatów.



Niemożliwe jest zainstalowanie serwera Microsoft Exchange w wersji 2000 lub wcześniejszej w środowisku systemu Windows .NET.

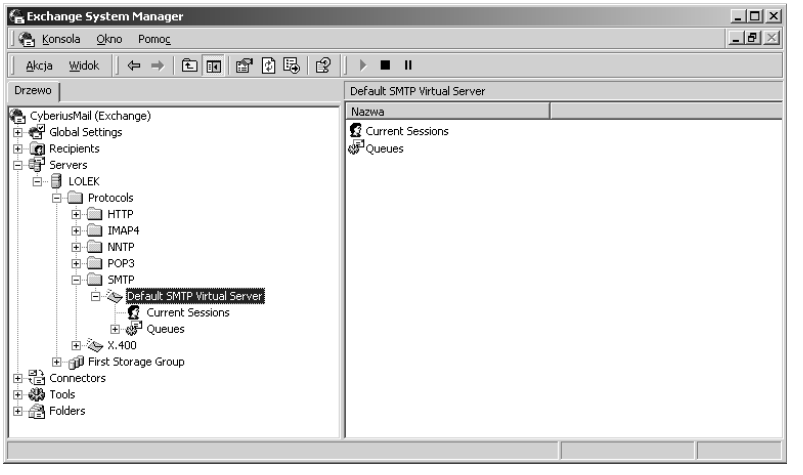
Bezpieczna komunikacja z serwerem Exchange

Zabezpieczyć dane przesyłane jako pakiety protokołów SMTP, POP3 i IMAP4 w sieciach Windows możemy dzięki PKI. W tym celu należy:

1. Zainstalować certyfikaty serwera Exchange, umożliwiające mu zabezpieczanie danych przesyłanych za pośrednictwem poszczególnych protokołów. Aby wykonać to zadanie:

   a) Uruchom konsolę MMC *Exchange System Manager* i kolejno wybierz *Servers/Nazwa serwera Exchange/Protocols/SMTP/Default SMTP Virtual Server* i z menu kontekstowego wybierz *Właściwości* (rysunek 23.15).

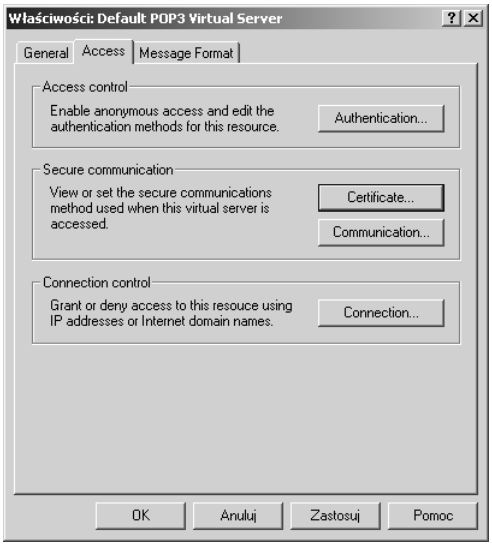
Rysunek 23.15. *Główna konsola administracyjna serwera Exchange 2000*



   b) Przejdź do zakładki *Access* i kliknij przycisk *Ceryficate*.... Uruchomiony zostanie *Kreator certyfikatów serwera sieci Web* (rysunek 23.16).

2. Wymuś nawiązywanie bezpiecznych połączeń przez klientów poczty elektronicznej. W tym celu, po zainstalowaniu certyfikatu, kliknij przycisk *Communication* (zostanie wyświetlone okno dialogowe pokazane na rysunku 23.17).

3. Powtórz te czynności dla pozostałych protokołów. W rezultacie serwer pocztowy będzie nasłuchiwał na portach o następujących numerach: protokół SMTP — port TCP 25 (bez zmian), protokół POP3 — port TCP 995 (zamiast TCP 110), protokół IMAP — port TCP 993 (zamiast TCP 143), protokół NNTP — port TCP 563 (zamiast TCP 119).



Rysunek 23.16. *Serwer Exchange korzysta z certyfikatów tego samego typu i wystawianych za pomocą tego samego kreatora, co serwer IIS*



Rysunek 23.17. *Po zaznaczeniu opcji Require secure chanell serwer Exchange umożliwi wyłącznie nawiązywanie połączeń klientom posługującym się certyfikatami*

Zabezpieczenie klienta poczty elektronicznej

Następnym etapem w procesie zabezpieczenia wymiany poczty elektronicznej jest konfiguracja programów klienckich (domyślnym, instalowanym wraz z systemem Windows, klientem poczty elektronicznej jest program Outlook Express). Zabezpieczona powinna zostać cała komunikacja z serwerem pocztowym (zaszyfrowane i podpisane cyfrowo powinny zostać nie tylko wiadomości e-mail, ale również przesyłane do serwera pocztowego hasła użytkowników). W efekcie zminimalizowane zostaje ryzyko związane z odebraniem wiadomości e-mail wysłanej przez hakera podszywającego się pod użytkownika systemu (problem ten dotyczy w szczególnym stopniu klientów pocztowych firmy Microsoft, które są podatne na ataki związane z automatycznie uruchamianymi wirusami i elementami wiadomości wysłanych jako HTML).

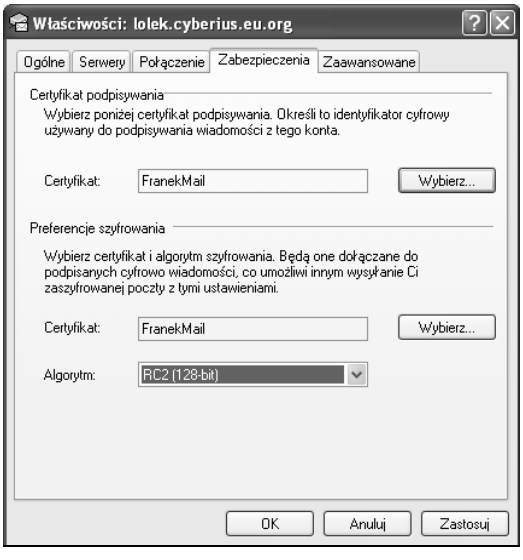
Aby umożliwić klientom korzystającym z programu Outlook Express korzystanie z usług zabezpieczonego serwera poczty elektronicznej:

1. Uruchom program Outlook Express i z menu *Narzędzia* wybierz *Opcje*.
2. Przejdź do zakładki *Zabezpieczenia* i zainstaluj certyfikat danego użytkownika, następnie zaznacz oba pokazane na rysunku 23.18 pola wyboru.



Rysunek 23.18. *Po zaznaczeniu pól szyfrowania i podpisywania wszystkie wiadomości będą domyślnie zabezpieczane przed odczytaniem przez niepowołane osoby*

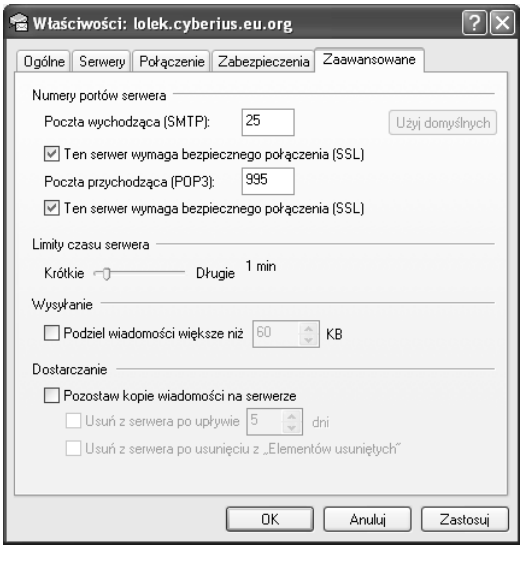
3. Wyświetl właściwości konta utworzonego na zabezpieczonym serwerze pocztowym.
4. Przejdź do zakładki *Zabezpieczenia* i z listy certyfikatów użytkownika wybierz certyfikat używany do szyfrowania i podpisywania wiadomości e-mail.
5. Określ algorytm, który będzie wykorzystywany do szyfrowania wysyłanych do tego użytkownika wiadomości (rysunek 23.19). Na liście dostępnych algorytmów szyfrowania programu Outlook 2002 znajdują się:
   - SHA1 (ang. *Secure Hash Algorithm version 1*) — wykorzystywana do podpisywania funkcja skrótu, która dla danych o maksymalnej długości 2^{64} zwraca wynik o długości 160 bitów.
   - MD5 (ang. *Message Digest version 5*) — wykorzystywana do podpisywania funkcja skrótu, która dla danych o dowolnej długości zwraca wynik o długości 128 bitów.
   - DES (ang. *Data Encryption Standard*) — algorytm szyfrowania wykorzystujący klucz o długości 56 bitów.
   - 3DES (ang. *Triple DES*) — zmodyfikowana wersja algorytmu DES, w której te same dane zostają trzykrotnie zaszyfrowane za pomocą trzech różnych, 56-bitowych kluczy.



Rysunek 23.19. *Zanim możliwe będzie wysyłanie zaszyfrowanych wiadomości, konieczne jest zainstalowanie kluczy publicznych ich odbiorców*

- RC2 (40-bit) (ang. *Rivest's Cipher version 2*) — algorytm szyfrowania wykorzystujący klucz o zmiennej długości, do którego dodana jest losowa, 40-bitowa liczba. Dane zostają zaszyfrowane kluczem o zwiększonej w ten sposób długości.
- RC2 (128-bit) — zmodyfikowana wersja algorytmu RC2, w której długość dołączanej do klucza liczby została zwiększona do 88 bitów.

6. Przejdź do zakładki *Zaawansowane* i zaznacz pola wyboru, umożliwiające nawiązywanie bezpiecznych połączeń z serwerem pocztowym (rysunek 23.20). W ten sposób nie tylko wiadomości e-mail, ale wszystkie wymieniane z serwerem dane (np. hasła) będą przesyłane w postaci zaszyfrowanej.

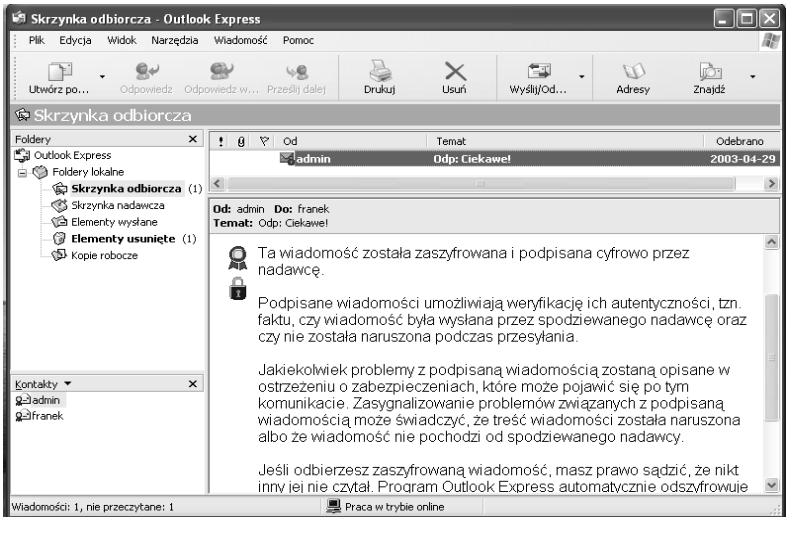


Rysunek 23.20. *O ile do szyfrowania i podpisywania wiadomości nie jest wymagane zabezpieczenie serwera pocztowego (a więc możemy szyfrować wiadomości wysyłane i odbierane ze skrzynki znajdującej się na dowolnym, w tym darmowym, serwerze pocztowym), o tyle nawiązywanie bezpiecznych połączeń, a więc zabezpieczenie przesyłanego hasła, wymaga zmiany konfiguracji serwera pocztowego*



Zanim możliwe będzie szyfrowanie wiadomości, wszyscy użytkownicy muszą zainstalować wystawione przez zaufany CA i zawierające klucze publiczne certyfikaty pozostałych użytkowników.

Po odebraniu pierwszej podpisanej lub zaszyfrowanej wiadomości program kliencki wyświetli krótką informację o zastosowanych zabezpieczeniach (rysunek 23.21).



Rysunek 23.21. *Odpowiedź administratora na wiadomość pokazaną na rysunku 23.13 została i zaszyfrowana, i podpisana kluczem prywatnym administratora*

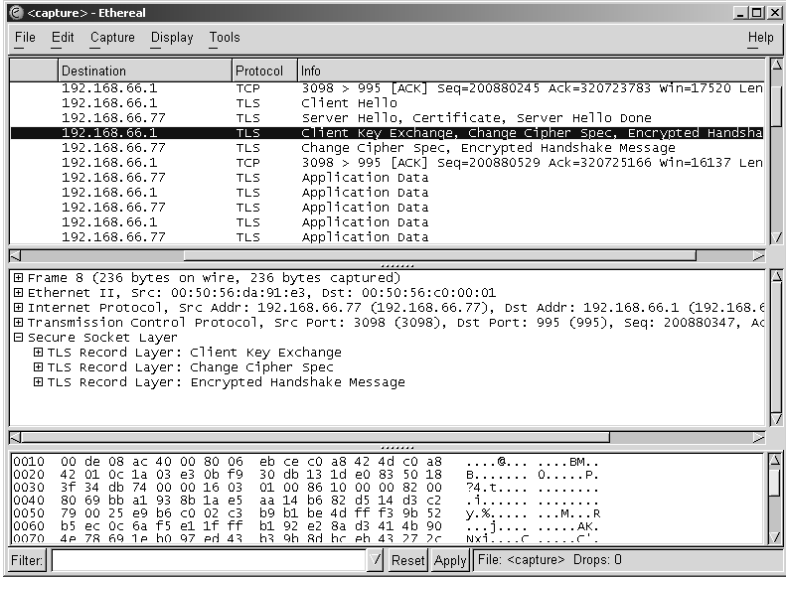
Podpisanie wiadomości gwarantuje, że jej treść nie została zmodyfikowana i że wiadomość została wysłana przez użytkownika, dla którego wystawiono dany certyfikat, a nie przez hakera, który podszywając się pod niego, zalogował się na serwer pocztowy. Natomiast jej zaszyfrowanie uniemożliwia osobom, które nie dysponują kluczem prywatnym, odpowiadającym kluczowi publicznemu wykorzystanemu do jej zaszyfrowania, jej odczytanie (rysunek 23.22).



Wdrożenie infrastruktury kluczy publicznych jest najskuteczniejszym sposobem zagwarantowania poufności i autentyczności przesyłanych wiadomości e-mail, ale nie chroni przed wszystkimi typami ataków. W tak zabezpieczonych systemach nadal konieczne jest systematyczne aktualizowanie oprogramowania i stosowanie skanerów antywirusowych (z aktualnymi bazami wirusów) na wszystkich komputerach klienckich.

Zabezpieczenie komunikatorów internetowych

Coraz popularniejsze **komunikatory internetowe** (takie jak ICQ czy Gadu-Gadu) są odmianą systemów poczty elektronicznej, umożliwiającą wymianę wiadomości pomiędzy zarejestrowanymi użytkownikami. Po zalogowaniu się użytkownika na serwerze



Rysunek 23.22. *Odpowiedź administratora będzie znana tylko jemu i adresatowi wiadomości*

może on odbierać wysyłane do niego wiadomości i wysyłać, za pośrednictwem serwera lub bezpośrednio do komputera odbiorcy, wiadomości do pozostałych użytkowników.

Poziom bezpieczeństwa obecnie oferowany przez różne typy komunikatorów internetowych jest bliski zeru — dane przesyłane są jawnym tekstem, a wdrożenie technologii ich szyfrowania pomiędzy użytkownikami zdalnych systemów często jest niemożliwe (w ramach sieci lokalnej dane mogą zostać zaszyfrowane protokołem IPSec) albo wymaga wykorzystania technologii firm trzecich. Ponadto mechanizm potwierdzania tożsamości klientów, choć dzisiaj nie spotyka się już rozwiązań polegających na przesyłaniu haseł jawnym tekstem, jest bardzo prosty i nawet dla początkującego hakera zdobycie haseł innych użytkowników serwera nie jest specjalnym wyzwaniem (przykład ataku tego typu znajduje się w rozdziale 4.).



Szczególnym zagrożeniem bezpieczeństwa systemu jest możliwość przesyłania danych bezpośrednio pomiędzy komputerami użytkowników — tak jak w przypadku innych zdecentralizowanych technologii przesyłania danych, również to rozwiązanie jest bardzo trudne do zarządzania i w konsekwencji — do zabezpieczenia przez administratorów systemów.

W czasie pisania tej książki zmniejszyć ryzyko związane z komunikatorami internetowymi można było przede wszystkim poprzez uświadomienie ich użytkownikom skali zagrożenia — przesyłane jawnym tekstem dane mogą zostać odczytane i zmodyfikowane przez każdego użytkownika Internetu, a podszycie się pod użytkownika i wysyłanie informacji w jego imieniu również nie wymaga specjalnych umiejętności od hakera. Paradoksalnie, ogromna większość użytkowników tych komunikatorów jest przeświadczona o swojej anonimowości — nic bardziej błędnego. Przechwycone pakiety jednoznacznie identyfikują i nadawcę, i odbiorcę przesyłanych komunikatów.