ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1996

Seria: INFORMATYKA z. 30 Nr kol. 1315

Stanisław CIEŚLA
Grzegorz HRYŃ

SYSTEMY WINDOWS NT I WINDOWS 95 – BEZPIECZEŃSTWO I ZARZĄDZANIE W SIECI

Streszczenie. W artykule przedstawiono możliwości współdzielenia zasobów poprzez sieć komputerów z systemem Windows 95, stosowanie różnych konfiguracji poziomów ochrony współdzielonych zasobów, tworzenie kont, określanie praw i przywilejów użytkowników w sieci oraz analizę możliwości zdalnego zarządzania i konfigurowania komputerów z systemem Windows 95.

WINDOWS 95 AND WINDOWS NT – NETWORK SECURITY AND ADMINISTRATION

Summary. In this paper we have described analysis of resource sharing in Windows95-based network using various sharing levels at different levels of security. We also reported creating new user accounts, defining their rights and evaluation of the possibility of remote management and configuration.

DIE OPERATIONSSYSTEME WINDOWS NT UND WINDOWS 95 – SICHERHEIT UND LEITEN IM KOMPUTERNETZ

Zusammenfassung. Der Artikel presentiert eine Möglichkeit der Mittailung der Vorräte im Komputernetz mit dem Operationssystem Windows 95, eine Anwendung der verschiedenen Konfigurationen der Schutzniveau, der mitgeteilten Vorräte, eine Gründung der Kontos, eine Bestimmung der Rechte und der Ausnachmerechte, der

Benutzer im Komputernetz und eine Analyse der Möglichkeiten des Vernleitens und der Konfigurierung der Komputers mit dem Windows 95.

1. Współdzielenie zasobów poprzez sieć

Każdy komputer wyposażony w system operacyjny Windows 95 i połączony z innymi komputerami w sieć może korzystać z zasobów przez nie udostępnianych poprzez sieć (drukarki, dyski, napędy CD-ROM) lub udostępniać im swoje zasoby.

Możemy tutaj rozpatrywać dwa rodzaje architektury sieci: sieć typu „każdy-z-każdym" bez wydzielonego serwera lub sieć działającą w oparciu o wydzielony serwer (Windows NT lub Novell NetWare) [1].

1.1. Korzystanie z udostępnianych w sieci zasobów

Komputer z systemem Windows 95, który może korzystać z udostępnianych w sieci zasobów, musi być wyposażony w oprogramowanie 32-bitowego klienta do sieci, dobrane odpowiednio do typu sieci, do jakiej komputer jest podłączony. Dla sieci Microsoft jest to oprogramowanie *Client for Microsoft Networks*, natomiast dla sieci NetWare jest to oprogramowanie *Client for NetWare Networks* pracujące w trybie chronionym 32-bitowym.

1.2. Udostępnianie innym komputerom własnych zasobów

Komputer, który może udostępniać swoje zasoby poprzez sieć innym komputerom, powinien być dodatkowo, oprócz zainstalowanego oprogramowania klienta danej sieci, wyposażony w oprogramowanie usługi udostępniania plików i drukarek *File and Print Sharing*, odpowiednie do typu sieci, do jakiej komputer jest podłączony.

Kiedy na danym komputerze uruchomiona jest usługa udostępniania zasobów, z innych komputerów można z tych zasobów korzystać pod warunkiem, że są one wyposażone w kompatybilne oprogramowanie klienta. Oznacza to, że komputer będący klientem sieci Microsoft Networks nie będzie mógł skorzystać z zasobów komputera udostępniającego oprogramowaniem dla sieci NetWare Networks.

1.3. Współdzielenie zasobów w architekturze bez wydzielonego serwera

Rozpatrując architekturę sieci bez wydzielonego serwera typu „każdy-z-każdym" co najmniej jeden komputer musi, ale każdy z komputerów może, pracować równocześnie jako klient i serwer, udostępniając swoje zasoby innym [4], [5]. Natomiast komputery skonfigurowane jedynie jako klienci mogą korzystać z zasobów udostępnianych przez inne komputery w sieci.

Dla takiej architektury współdzielenie zasobów jest możliwe jedynie przez sieć Microsoft Networks. Wszystkie komputery podłączone do tej sieci, które mają korzystać z udostępnianych zasobów, muszą być wyposażone w oprogramowanie klienta sieci Microsoft Networks, natomiast te komputery, które mają udostępniać swoje zasoby innym, muszą dodatkowo być wyposażone w oprogramowanie realizujące usługę udostępniania zasobów przez sieć Microsoft Networks.

1.4. Współdzielenie zasobów w architekturze z wydzielonym serwerem

Jeśli rozpatrujemy sieć, w której jest wydzielony serwer (Windows NT lub NetWare), to można stosować oprogramowanie klienta i usługi udostępniania zasobów odpowiednio dla sieci Microsoft Networks lub NetWare Networks.

Jeśli w sieci jest podłączony wydzielony serwer (Windows NT lub NetWare), to współdzielenie zasobów przez komputery z systemem Windows 95 odbywa się nadal jak w sieci typu „każdy-z-każdym", co oznacza, że każdy komputer w sieci, odpowiednio skonfigurowany, może udostępniać swoje zasoby pozostałym. Obecność serwera w takiej sieci rozszerza możliwości ochrony przed niepowołanym dostępem nakładanej na udostępniane zasoby.

Nie można uruchomić usługi udostępniania zasobów dla sieci NetWare Networks w systemie Windows 95, jeśli w sieci nie jest podłączony co najmniej jeden serwer NetWare. Nie jest możliwe zastosowanie usługi udostępniania zasobów jednocześnie dla sieci Microsoft i NetWare Networks [4], [5]. Decyzja, które oprogramowanie udostępniania zasobów zastosować, zależy przede wszystkim od stosowanego serwera, ale także od rodzaju konfiguracji komputerów, mających z tych usług korzystać, i tak:

a) jeśli większość użytkowników pracujących w sieci używa oprogramowania NETX, VLM lub oprogramowania klienta dla sieci NetWare Networks, wtedy należy zastosować udostępnianie zasobów na podstawie sieci NetWare Networks;
b) jeśli natomiast większość użytkowników pracujących w sieci używa oprogramowania klientów sieci Microsoft Networks, Windows NT, Windows for Workgroup lub

Workgroup for MS-DOS, wtedy należy zastosować udostępnianie zasobów w oparciu o sieć Microsoft Networks.

2. Bezpieczeństwo w systemie Windows 95

2.1. Zabezpieczenie komputera przed niepowołanym dostępem

Windows 95 nie dostarcza mechanizmów ochrony dysku, katalogów i plików na lokalnym komputerze za pomocą systemu praw i każdy użytkownik, pracujący na danym komputerze, ma dostęp do jego wszystkich zasobów. Można jednak ograniczyć dostęp użytkowników do systemu na dwa sposoby:

a) żądając autentyfikacji użytkownika przez serwer NT lub Novell NetWare;

b) zmieniając przywileje dla użytkownika domyślnego.

2.1.1. Autentyfikacja użytkownika przez serwer

Jeżeli opcja *Require Validation By Network for Windows Access* jest włączona, przy każdym logowaniu się użytkownika nazwa i hasło użytkownika są sprawdzane przez serwer. Zmiany tej opcji dokonuje się w bazie Registry za pomocą programu Policy Editor. Dodatkowo można nałożyć pewne ograniczenia dla zwiększenia poziomu bezpieczeństwa systemu: zarządać, aby hasło użytkownika zawierało również cyfry oraz wymusić minimalną długość hasła.

2.1.2. Zmiana przywilejów użytkownika domyślnego

W przypadku gdy nie można wprowadzić autentyfikacji użytkownika przez serwer, na przykład w przypadku sieci komputerów działających w systemie Windows 95 bez wydzielonego serwera NT lub NetWare, można ograniczyć przywileje użytkownika domyślnego. Za pomocą programu Policy Editor można zabronić wykonywania wszystkich aplikacji, czyli de facto uniemożliwić jakiekolwiek działanie. Dodatkowo można również ograniczyć dostęp do pewnych opcji Panelu Sterowania tak, aby uniemożliwić wprowadzanie zmian w konfiguracji systemu. Na podstawie danych o użytkowniku domyślnym tworzeni są nowi użytkownicy, tak więc każdemu, kto będzie usiłował uruchomić system, nie będąc zarejestrowanym użytkownikiem, zostaną przydzielone ograniczenia zdefiniowane dla użytkownika domyślnego. Jeśli zatem ograniczymy prawa użytkownika domyślnego, intruz nie będzie mógł skorzystać z systemu. W przypadku, gdy zostanie pominięte pytanie o nazwę użytkownika i hasło (podczas logowania się zostanie naciśnięty klawisz *Cancel*), Windows automatycznie

przydziela przywileje użytkownika domyślnego i tak zalogowany do systemu użytkownik również nie będzie mógł uruchomić żadnej aplikacji ani zmieniać ustawień systemowych.

2.2. Bezpieczeństwo w sieci

Gdy w systemie Windows 95 działa usługa *File and Printer Sharing*, możliwy jest dostęp innych użytkowników do współdzielonych zasobów: systemu plików, drukarek i napędów CD [1]. W celu ochrony współdzielonych zasobów w sieci system Windows 95 ustanawia dwa poziomy bezpieczeństwa: poziom dzielonego dostępu (ang. *share-level security*) i poziom dostępu specyfikowany dla poszczególnych użytkowników i grup na podstawie informacji przechowywanych na serwerze (ang. *user-level security*).

2.2.1. Poziom współdzielonego dostępu

Poziom współdzielonego dostępu chroni zasoby za pomocą hasła indywidualnie nadawanego każdemu zasobowi, który ma być udostępniony innym użytkownikom w sieci. Na komputerze udostępniającym swe zasoby istnieje możliwość określenia hasła osobno dla różnych trybów dostępu. Niezdefiniowanie żadnego hasła powoduje, że zasób jest dostępny dla wszystkich użytkowników w sieci. Każdemu zasobowi, który jest udostępniany, nadaje się nazwę wraz z ewentualnym komentarzem, zaś ochrona może odbywać się w następujący sposób:

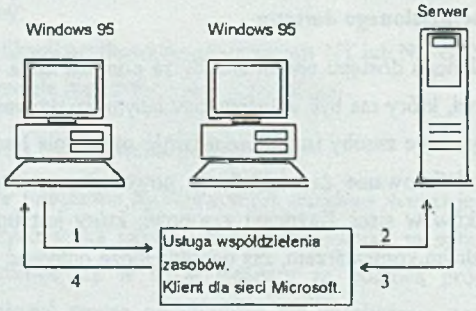
a) tylko do odczytu – użytkownicy w sieci mogą tylko czytać dane, natomiast nie mogą ich zmieniać ani zapisywać nic do współdzielonych katalogów;
b) pełny dostęp – użytkownicy w sieci mogą czytać dane, modyfikować je, tworzyć nowe pliki itp.;
c) w zależności od hasła – udostępniający zasób może zdefiniować dwa różne hasła, osobno dla dostępu tylko dla odczytu i osobno dla pełnego dostępu. Wtedy użytkownik chcący używać danego zasobu dostanie prawa zależnie od podanego hasła – albo tylko możliwość odczytu, albo pełny dostęp.

Możliwe jest udostępnienie katalogu tak, że nie jest on widoczny na liście zasobów udostępnianych przez dany komputer, natomiast można się do niego odwołać podając ścieżkę dostępu. Nazwa takiego katalogu musi kończyć się znakiem dolara *$*.

Ten poziom ochrony działa tylko w przypadku usługi *File and Printer Sharing for Microsoft Networks*, natomiast nie jest możliwe jego użycie dla Novell NetWare.

2.2.2. Poziom dostępu specyfikowany dla poszczególnych użytkowników

Ten sposób ochrony zabezpiecza dzielone zasoby za pomocą autentyfikacji użytkownika przez serwer – inaczej niż w poprzedniej metodzie, ponieważ tu dostęp do danego zasobu jest udzielany tylko danemu użytkownikowi lub grupie użytkowników. Sposób działania tej metody wyjaśnia rysunek 1. Gdy użytkownik usiłuje dostać się do dzielonego zasobu chronionego za pomocą tej metody (strzałka oznaczona numerem 1), żądanie jest przesyłane do serwera w celu autentyfikacji użytkownika (strzałka oznaczona numerem 2). Serwer odpowiada komputerowi, który udostępnia zasoby, potwierdzając lub nie czy hasło i nazwa użytkownika są poprawne (strzałka numer 3). W przypadku potwierdzenia Windows 95 udostępnia zasób na prawach uprzednio określonych dla danego użytkownika (strzałka numer 4).



Rys. 1. Poziom dostępu specyfikowany dla poszczególnych użytkowników
Fig. 1. User-level access control

Każdy zasób może być udostępniany za pomocą tej metody użytkownikom i grupom użytkowników na różnych prawach, których wybór zależy od udostępniającego zasób. Rodzaj praw, które są udzielane, zależy również od udostępnianego zasobu:

a) dla współdzielonych katalogów można zezwolić tylko na odczyt, udzielić wszystkich praw (ang. *full access*) lub zdefiniować, jakie prawa będą dotyczyły danego użytkownika;

b) dla drukarek użytkownik może mieć prawo dostępu do drukarki lub nie.

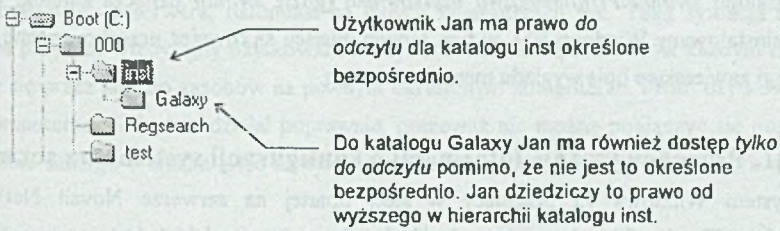
W przypadku współdzielonego katalogu prawa zdefiniowane dla danego katalogu dotyczą również wszystkich jego podkatalogów, nie można jednak udzielać praw dla poszczególnych plików tak, jak to jest w systemach Novell NetWare i Windows NT [6].

Specyfikując dostęp do danego katalogu określa się, co użytkownik może zrobić w tym katalogu:

Operacja	Wymagane prawa
Czytanie z pliku	read
Nazwa pliku jest widoczna w katalogu	list
Przeszukiwanie katalogu	list
Zapis do pliku	write, create, delete, change attributes
Uruchomienie programu	read, list
Utworzenie nowego pliku i zapis do niego	create
Kopiowanie plików z katalogu	read, list
Kopiowanie plików do katalogu	write, create, list
Tworzenie nowego katalogu	create
Skasowanie pliku	delete
Usunięcie katalogu	delete
Zmiana atrybutów pliku lub katalogu	change attributes
Zmiana nazwy pliku lub katalogu	change attributes
Zmiana praw dostępu	change access control

W zależności od tego, czy prawa do danego katalogu zostało przydzielone użytkownikowi bezpośrednio, czy pośrednio z tytułu przynależności do grupy użytkowników, rzeczywiste prawa dla danego zasobu są określane w następujący sposób:

a) jeśli dany użytkownik jest wymieniony na liście uprawnionych do dostępu do danego zasobu na określonych prawach, prawa te są mu przydzielane;
b) jeżeli użytkownik jest wymieniony pośrednio przez przynależność do grup, dla których są określone prawa dostępu, jego efektywne prawa są określane przez złożenie praw wszystkich grup, do których należy;
c) jeżeli żadna z grup, do których przynależy użytkownik, nie ma praw dostępu do danego zasobu, nie są mu przydzielane żadne prawa;



Rys. 2. Dziedziczenie praw
Fig. 2. Rights inheritance

Jeżeli dla danego katalogu prawa nie zostały określone bezpośrednio, Windows 95 stosuje prawa dziedziczone. Prawa dziedziczone to prawa najbliższego w hierarchii katalogu. Jeżeli żaden z katalogów na kolejnych, wyższych poziomach hierarchii (aż do głównego katalogu danego dysku) nie ma bezpośrednio określonych praw, to użytkownik nie będzie miał prawa dostępu. Dziedziczenie wyjaśnia rysunek 2.

3. System kont użytkowników i ograniczeń oparty na serwerze

System Windows 95 może pracować w trybie, w którym każdy użytkownik indywidualnie określa postać i sposób działania niektórych składników systemu – informacje te są zapisane w bazie Registry oraz w specjalnych katalogach. Mogą one dotyczyć następujących elementów:

a) ustawień Panelu Sterowania oraz interfejsu użytkownika dotyczących wyglądu ekranu, tła, ustawień czcionek, odwołań (ang. *shortcuts*), menu startowego itp.;
b) ustawień dla połączeń w sieci, informacji o ostatnio używanych zasobach, otwieranych dokumentach, portach drukarek itp.;
c) ustawień aplikacji potrafiących rejestrować się bezpośrednio w Registry, włączając w to akcesoria i aplikacje instalowane wraz z Windows 95.

Chociaż baza Registry logicznie tworzy jedną strukturę, to fizycznie jest podzielona na dwa pliki: USER.DAT i SYSTEM.DAT. Informacje dotyczące elementów indywidualnych dla użytkownika są zapamiętywane w pliku USER.DAT. Gdy w systemie włączy się opcję pozwalającą na indywidualizację ustawień dla użytkowników, każdy nowo utworzony użytkownik otrzymuje kopię pliku USER.DAT umieszczonego w głównym katalogu Windows (ustawienia domyślne). Pliki USER.DAT dla poszczególnych użytkowników są przechowywane w podkatalogu *$windir\Profiles\nazwa_użytkownika* (gdzie *$windir* oznacza katalog, w którym jest zainstalowany Windows 95), w tym samym miejscu są również przechowywane specjalne katalogi zawierające opis wyglądu menu startowego.

3.1. Przechowywanie informacji o konfiguracji systemu na serwerze

System Windows 95 pracujący w sieci opartej na serwerze Novell NetWare lub Windows NT umożliwia łatwe zarządzanie konfiguracją wszystkich komputerów w sieci w oparciu o dane przechowywane na serwerze.

3.1.1. Standardowe profile użytkownika

W celu ułatwienia zarządzania siecią komputerów z zainstalowanym systemem Windows 95 wprowadzono możliwość przechowywania profili użytkownika (informacji indywidualnych dla danego użytkownika) na serwerze Novell NetWare lub Windows NT. W przypadku serwera Novell NetWare profile są przechowywane w katalogu *MAIL\ID_użytkownika*, ponieważ ten katalog zawsze istnieje, natomiast na serwerze NT są przechowywane w katalogu odpowiednim dla danego użytkownika. Na komputerach, na których mają być dostępne profile przechowywane na serwerze, musi być, w zależności od rodzaju serwera, odpowiednie oprogramowanie dostarczane wraz z systemem Windows 95:

a) *Client for NetWare Networks*;

b) *Client for Microsoft Networks*.

Pełne udostępnienie walorów takiej konfiguracji wymaga, by serwer miał możliwość zapisu i odczytu długich nazw plików. Jeśli taka możliwość nie będzie dostępna, na serwerze będzie można przechowywać tylko informacje zawarte w bazie Registry (plik USER.DAT). Ponadto wszystkie komputery, które mają korzystać z informacji przechowywanych na serwerze, muszą mieć tę samą nazwę dla katalogu, w którym jest zainstalowany system Windows 95 (np. C:\WIN95) i musi on być zainstalowany na dysku oznaczonym tą samą literą, w przeciwnym przypadku niektóre ustawienia nie będą działać. Dodatkowo oprogramowanie *Client for Microsoft Networks* musi być wybrane jako obsługujące proces logowania się użytkownika.

Jeżeli te wszystkie założenia będą spełnione, to w trakcie logowania się użytkownika nastąpi sprawdzenie autentyczności jego nazwy oraz hasła i indywidualne ustawienia zostaną automatycznie odczytane z serwera. Umożliwia to komfortową sytuację, gdy użytkownik na każdym komputerze w sieci może pracować w znanym sobie środowisku operacyjnym. Po zakończeniu pracy plik USER.DAT jest automatycznie uaktualniany tak, że na serwerze znajdują się zawsze aktualne ustawienia (profil) danego użytkownika.

Czasem może zajść konieczność, aby na jednym z komputerów profil danego użytkownika nie był wczytywany z serwera, natomiast na innych komputerach tak. Taka sytuacja może powstać na przykład wtedy, gdy użytkownik korzysta z kilku komputerów, za każdym razem odwołując się przez sieć do zasobów na pewnym określonym komputerze. Profil użytkownika na tym komputerze nie będzie działał poprawnie, ponieważ nie można podłączyć się poprzez sieć do siebie samego – trzeba więc na tym komputerze za pomocą Registry Editora dodać w kluczu:

Hkey_Local_Machine\Network\Logon

nową wartość typu DWORD o nazwie *UseHomeDirectory* równą 0. Spowoduje to wyłączenie możliwości wczytania konfiguracji z serwera.

3.1.2. Działanie systemu profili użytkownika

Za każdym razem, kiedy użytkownik loguje się do systemu na dowolnym komputerze w sieci, na którym jest włączona opcja profili użytkownika, Windows 95 sprawdza w bazie Registry, czy użytkownik ma zdefiniowany własny profil lokalny. Ponadto Windows 95 określa również, czy na serwerze istnieje katalog tego użytkownika i czy zawiera on odpowiedni profil.

Jeżeli wersja na serwerze jest nowsza, wszystkie informacje z serwera są kopiowane na dysk lokalny, a następnie ustawienia zawarte w tej lokalnej kopii pliku USER.DAT są wprowadzane do Registry. Podobnie postępuje system w przypadku braku lokalnej kopii profilu. Jeżeli ani na serwerze ani na lokalnym dysku nie ma tych danych, Windows 95 automatycznie tworzy nowy profil użytkownika na lokalnym komputerze, wykorzystując ustawienia domyślne (lokalny plik USER.DAT w głównym katalogu Windows 95).

Obydwie kopie ustawień użytkownika są automatycznie uaktualniane podczas opuszczania systemu. Jeżeli użytkownik jest zalogowany do systemu na więcej niż jednym komputerze równocześnie, to zmiany w profilu użytkownika dokonane przez komputer, na którym użytkownik wylogował się wcześniej, zostaną utracone, ponieważ podczas wylogowania się z drugiej maszyny zostanie zapamiętany ten właśnie profil.

3.1.3. Profile obowiązkowe

Windows 95 umożliwia również stworzenie tzw. profili obowiązkowych. Zmiana w stosunku do uprzednio omawianych polega na tym, że użytkownik ma możliwość dokonywania zmian w aktualnych ustawieniach systemu, natomiast jest pozbawiony możliwości zapisu dokonanych poprawek. Może być to korzystne w przypadku początkujących użytkowników, którzy często mogą wprowadzić nieświadomie zmiany w systemie, które spowodowałyby konieczność interwencji administratora systemu. W przypadku istnienia profilu obowiązkowego, wystarczy opuścić system, a następnie uruchomić go powtórnie i standardowe ustawienia zostaną przywrócone.

Aby wprowadzić profile obowiązkowe, należy w katalogach użytkowników na serwerze zapisać pliki USER.DAT i zmienić rozszerzenie na *.MAN. Jeśli system podczas startu wykryje plik USER.MAN w katalogu logującego się użytkownika na serwerze, automatycznie wprowadzi ustawienia zawarte w tym pliku do bazy Registry, pomijając istniejącą lokalną kopię USER.DAT. Jeśli użytkownik wprowadzi jakiekolwiek zmiany w konfiguracji menu startowego, wyglądu ekranu itp., zmiany te nie zostaną zapisane w pliku USER.MAN.

3.2. Ograniczenia (ang. system policies)

Windows 95 oferuje mechanizm zarządzania kontami użytkowników poprzez wprowadzenie pewnych ograniczeń lub narzucenie niektórych ustawień systemu centralnie przez administratora bez konieczności modyfikacji Registry dla każdego użytkownika z osobna. Informacje o tych ograniczeniach są przechowywane na serwerze w specjalnym pliku, którego edycję przeprowadza się za pomocą programu Policy Editor, dostarczanego z systemem Windows w wersji na nośniku CD ROM.

3.2.1. Przygotowanie systemu ograniczeń

Za pomocą programu Policy Editor administrator tworzy plik CONFIG.POL, zawierający przywileje i ograniczenia dla poszczególnych użytkowników lub ich grup i umieszcza go na serwerze.

Dla każdego użytkownika i każdej grupy użytkowników można wprowadzić następujące zmiany:

a) ograniczyć dostęp do opcji Panelu Sterowania;
b) narzucić ustawienia dotyczące tła i kolorów okien;
c) ograniczyć możliwości udostępniania zasobów komputera poprzez sieć;
d) wprowadzić ograniczenia dotyczące menu startowego;
e) uniemożliwić użytkownikowi edycję Registry za pomocą programu Registry Editor;
f) wyłączyć możliwość otwarcia sesji systemu DOS w okienku (ang. *DOS prompt*);
g) wyłączyć możliwość przejścia do systemu DOS opuszczając system Windows (ang. *DOS mode*);
h) pozwolić użytkownikowi na wykonywanie tylko niektórych, wymienionych przez administratora aplikacji.

W celu automatycznego wczytywania informacji o ograniczeniach z serwera muszą być spełnione następujące warunki:

a) dla serwera NT, oprogramowanie *Client for Microsoft Networks* musi być wyspecyfikowane jako *Primary Network Logon*, tzn. logowanie do sieci ma odbywać się za pomocą oprogramowania klienta dla sieci Microsoft do określonej uprzednio domeny. Plik CONFIG.POL musi się znajdować w katalogu NETLOGON na serwerze;
b) dla serwera Novell NetWare, oprogramowanie *Client for NetWare Networks* musi być wyspecyfikowane jako *Primary Network Logon* i dodatkowo musi być określony serwer, z którego będzie odczytywany plik CONFIG.POL. Musi się on znajdować na wolumenie SYS w katalogu PUBLIC.

Możliwe jest umieszczenie pliku CONFIG.POL w innym katalogu na serwerze lub nawet na innym komputerze, na którym jest uruchomiony system Windows 95. W tym celu trzeba za pomocą Policy Editora włączyć opcję *Remote Update* w bazie Registry tego komputera, dla którego system ograniczeń ma być wczytywany z innego katalogu lub innego komputera i podać położenie pliku CONFIG.POL.

W momencie zalogowania się użytkownika system Windows 95 sprawdza, gdzie umieszczony jest plik zawierający ograniczenia i kopiuje te ograniczenia do Registry, stosując następujące zasady:

a) jeżeli włączone są profile użytkowników, sprawdza się czy istnieją ograniczenia zdefiniowane dla danego użytkownika i jeśli tak, to są one nakładane, w przeciwnym przypadku stosowane są ograniczenia dla użytkownika domyślnego;
b) Jeśli na danym komputerze istnieje możliwość odczytu ograniczeń nakładanych dla grup użytkowników (tzn. jest zainstalowana biblioteka GROUPPOL.DLL), sprawdza się czy użytkownik należy do którejkolwiek z wymienionych grup. Jeśli tak, wczytywane są ograniczenia począwszy od grupy użytkowników o najniższym priorytecie. Proces ten jest przeprowadzany dla wszystkich grup, do których należy dany użytkownik. Wczytywanie ograniczeń dla grup użytkowników nie odbędzie się, jeśli są bezpośrednio zdefiniowane ograniczenia dla danego użytkownika.

4. Zdalne zarządzanie w systemie Windows 95

4.1. Przegląd narzędzi służących do zdalnego zarządzania

Narzędzia służące do zdalnego zarządzania w sieci komputerami z systemem operacyjnym Windows 95 zostały stworzone po to, by ułatwić administratorowi zdalne identyfikowanie i usuwanie problemów, jakie mogą pojawić się na komputerach użytkowników.

Dostępne narzędzia zdalnej administracji i ich charakterystyka:

a) *System Policy Editor* – narzędzie umożliwiające zdalne modyfikowanie niektórych opcji Registry użytkownika, odpowiadających za to, co użytkownik może zmodyfikować na desktopie, w konfiguracji sieci w panelu sterującym;
b) *Registry Editor* – umożliwia zdalną, pełną edycję Registry użytkownika, pozwalając na modyfikowanie wszystkich wpisów, dodawanie nowych i usuwanie istniejących;

c) *System Monitor* – umożliwia zdalne monitorowanie pracy komputera użytkownika w następujących kategoriach: system zbiorów, protokół IPX/SPX, jądro systemu, zarządzanie pamięcią operacyjną, usługi udostępniania zasobów, oprogramowanie klienta do sieci, wydajność sieci Microsoft Networks;

d) *Net Watcher* – pozwala na zdalne monitorowanie i modyfikowanie udostępnianych przez użytkownika zasobów, jeśli na komputerze użytkownika jest uruchomiona usługa udostępniania zasobów, pozwala także na zarządzanie systemem zbiorów użytkownika.

4.2. Konfiguracja systemu umożliwiająca zdalne zarządzanie

Skonfigurowanie systemu Windows 95 tak, by umożliwić korzystanie ze zdalnego zarządzania, wymaga spełnienia poniższych wymogów.

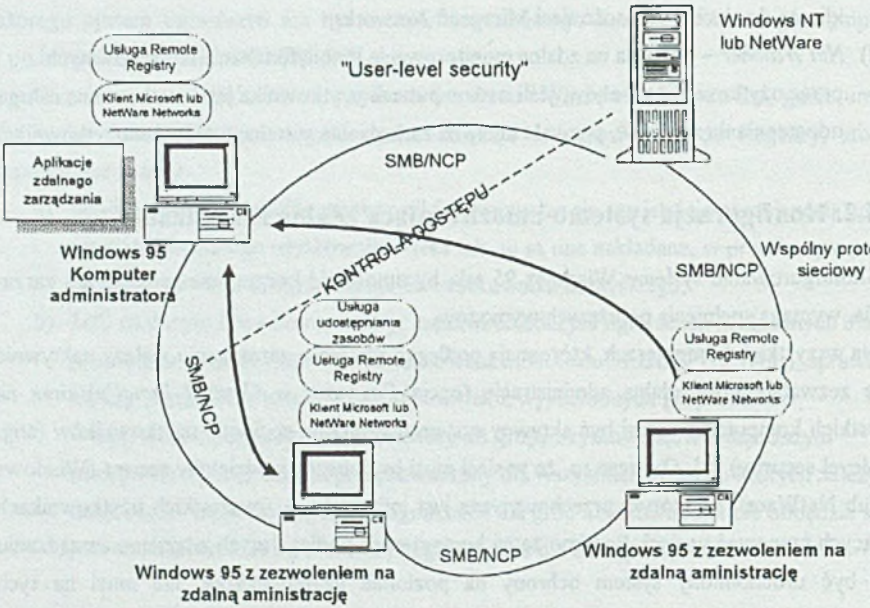
Na wszystkich komputerach, które mają podlegać zdalnemu zarządzaniu, należy uaktywnić opcję zezwalającą na zdalną administrację (opcja *Password* w *Control Panel'u*) oraz na wszystkich komputerach musi być aktywny system ochrony na poziomie użytkowników (ang. user-level security) [2]. Oznacza to, że w sieci musi być obecny wydzielony serwer (Windows NT lub NetWare), na którym przechowywana jest informacja o wszystkich użytkownikach mogących pracować w sieci. Pomimo że na komputerach podlegających zdalnemu zarządzaniu musi być uruchomiony system ochrony na poziomie użytkowników, nie musi na tych komputerach być zainstalowana usługa udostępniania zasobów.

Chcąc używać do zdalnej administracji następujących narzędzi: *Registry Editor*, *System Policy Editor* i *System Monitor*, należy zainstalować na komputerach podlegających administracji usługę Microsoft Remote Registry, umożliwiającą realizację zdalnego manipulowania systemem użytkownika.

Wszystkie komputery pracujące w sieci, które mają być poddane zdalnemu zarządzaniu, muszą posiadać wspólny protokół sieciowy (wersja firmy Microsoft protokołu IPX/SPX, TCP/IP lub NetBEUI). Schematyczny sposób, w jaki należy skonfigurować sieć, by móc zastosować mechanizmy zdalnej administracji przedstawia rysunek 3.

Wyjątkiem od powyższych reguł jest program Net Watcher, który umożliwia zdalne gospodarowanie zasobami udostępnianymi przez komputer użytkownika. Tę usługę można zainstalować i stosować w sieci bez wydzielonego serwera. Należy w takim przypadku skonfigurować komputery mające podlegać zdalnemu zarządzaniu w następujący sposób. Uaktywnić opcję zezwalającą na zdalną administrację i podać hasło, jakim powinien posłużyć się administrator oraz uraktywnić system ochrony zasobów na poziomie współdzielonym (*share-level security*). Oczywiście komputery podlegające zarządzaniu programem NetWatcher muszą

być wyposażone w usługę udostępniania zasobów, gdyż w innym przypadku stosowanie programu NetWatcher nie ma sensu.



Rys. 3. Konfiguracja sieci umożliwiająca zdalne zarządzanie
Fig. 3. Network configuration for remote administration

Tak jak w poprzedniej konfiguracji tak i dla zdalnego zarządzania zasobami wszystkie komputery w sieci muszą posługiwać się tym samym protokołem sieciowym.

Wszystkie podejmowane czynności zdalnej administracji muszą odbywać się przy włączonym komputerze użytkownika i uruchomionym systemie Windows 95. Jednocześnie wszelkie modyfikacje zbiorów systemowych dotyczą aktualnego użytkownika. Jeśli na komputerze użytkownika dopuszcza się tworzenie różnych profili, należy pamiętać, że modyfikowany jest zbiór np. Registry aktualnego użytkownika a nie wybranego z listy dostępnych użytkowników.

Niektóre modyfikacje dokonywane u użytkownika uwidaczniają się natychmiast (np. odłączenie udostępnianego zasobu lub utworzenie nowego folderu), natomiast inne wymagają ponownego restartu systemu i wpisania się użytkownika do systemu (np. modyfikacje Registry lub uprawnień użytkownika).

Poniżej zestawiono informację o tym, jaka jest niezbędna konfiguracja zdalnego zarządzania, by wykonać odpowiednie czynności administracyjne [1]. Rozpatrywany jest jedynie szero-

ki zakres usług, stąd wszędzie występuje konieczność aktywowania systemu ochrony na poziomie użytkowników, co powoduje, że niezbędna jest obecność serwera (Windows NT lub NetWare).

Czynność administracyjna wykonywana zdalnie	Konfiguracja komputera zarządzanego zdalnie
Przeglądanie i zarządzanie udostępnianymi zasobami zdalnego komputera z użyciem programu Net Watcher	Uaktywnienie poziomu ochrony user-level i zezwolenie na zdalną administrację; zainstalowanie usługi udostępniania zasobów; nadanie praw zdalnemu administratorowi do zarządzania komputerem
Modyfikowanie systemu zbiorów zdalnego komputera programem Net Watcher	Uaktywnienie poziomu ochrony user-level i zezwolenie na zdalną administrację; nadanie praw zdalnemu administratorowi do zarządzania komputerem
Modyfikowanie zdalne Registry użytkownika z użyciem programów Registry Editor lub System Policy Editor	Uaktywnienie poziomu ochrony user-level i zezwolenie na zdalną administrację; zainstalowanie usługi Microsoft Remote Registry
Monitorowanie pracy zdalnego systemu z użyciem programu System Monitor	Uaktywnienie poziomu ochrony user-level i zezwolenie na zdalną administrację; zainstalowanie usługi Microsoft Remote Registry

Nadanie zdalnemu administratorowi praw do zarządzania komputerem oznacza wyspecyfikowanie go w liście zdalnych administratorów i wiąże się z nadaniem mu praw do pełnej kontroli nad całym systemem użytkownika.

Domyślnymi administratorami dla usługi zdalnej administracji przy poziomie ochrony „user-level security" są dla Windows NT administratorzy domeny, natomiast dla NetWare Supervisor (NetWare 3.x) lub Admin (NetWare 4.x).

5. Podsumowanie

W pracy omówiono systemy Windows 95 i Windows NT pod kątem bezpieczeństwa i zarządzania w sieci komputerowej, opartej na różnych protokołach.

Uwagi i sugestie zawarte w opracowaniu mogą pomóc administratorowi we właściwym skonfigurowaniu i dopasowaniu sieci komputerów opartych na systemie Windows 95 z serwerem Windows NT.

LITERATURA

[1] Microsoft Windows 95 Resource Kit. Microsoft Press, 1995.
[2] Windows 95 User's Guide, Microsoft Corporation 1995.
[3] Silberschatz A., Peterson J., Galvin P.: Podstawy systemów operacyjnych. WNT, Warszawa 1993.
[4] Microsoft Developer Network. Volume July 95. Redmont 1995.
[5] Microsoft TechNet. Volume 3, Issue 7, July 95. Redmont 1995.
[6] Windows NT System Guide. Microsoft Corporation 1995.

Recenzent: Dr hab. inż. Adam Mrózek

Wpłynęło do Redakcji 18 grudnia 1995 r.

Abstract

This article, which is divided into four parts, discusses security in Windows95-based network and remote management.

The first discusses resource sharing services in Windows 95 — Microsoft File and Printer Sharing for NetWare Networks and File and Printer Sharing for Microsoft Networks. When a computer is running Windows 95 with File and Printer Sharing services, other users can connect to shared printers, volumes, directories, and CD-ROM drives on that computer.

The second part describes the techniques used for resource protection – user-level and share-level security. With user-level security, a user's request to access a shared resource is passed through to a security provider, which can be either Windows NT or NetWare server, that grants or denies the access. With shared-level security, users assign passwords to their shared resources, and any user who knows correct password can access the shared resource.

The third section discusses how user profiles can help users to maintain their own preferences including desktop, network and application settings when logging on to a workstation. This section also describes how system policies could be used to control what users can and cannot do on the desktop and on the network. These features can help managing numerous computers by allowing to change configurations remotely from one workstation.

These built-in capabilities for remote administration are described in the last section.