

## Controlling the Security Objects Properties for Networks in Windows 2000

Dhuha Basheer Abdullah

Abd- Alnaseer Ahmed

Prof.dhuha\_basheer@uomosul.edu.iq

College of Computer Sciences and Mathematics

University of Mosul, Iraq

Received on: 27/10/2002

Accepted on: 25/01/2003

### ABSTRACT

Information security occupies a wide area in designing network operating systems. Windows 2000 was of the operating systems that offered great interest for network security, so it is recently considered as the most important network operating system because of the high extended capabilities in network security embedded in it. This search is devoted to the study of the network security in windows 2000. A special program for controlling the security properties for the main objects of the Windows 2000 database (Active Directory) has been built. ActiveX Data Object (ADO) is used for searching the Active Directory and ADSI interface for accessing security principal accounts. This software presents the likelihood of accessing the security properties of these objects to the level of flags and bits in the data structure of security properties elements.

**Keywords:** Operating System, Windows2000 system ,Networks Security, Security Objects

السيطرة على صفات الكيانات الأمنية للشبكات في ويندوز 2000

عبد الناصر يونس احمد

ضحى بشير عبد الله

كلية علوم الحاسبات والرياضيات، جامعة الموصل

تاريخ قبول البحث: 2003/01/25

تاريخ استلام البحث: 2002/10/27

### المخلص

تحتل مسألة أمنية المعلومات مساحة كبيرة في بناء نظم تشغيل الشبكات، ولقد كان نظام التشغيل (Windows 2000) من النظم التي أولت أمنية الشبكات أهمية كبيرة، فقد بحق من أهم نظم تشغيل الشبكات في الوقت الحاضر وذلك لما أضيف من إمكانيات في مسائل الأمنية للشبكات في هذا النظام عن نظم التشغيل السابقة. تناول البحث دراسة لأمنية الشبكات في (Windows 2000). ثم دعمت هذه الدراسة ببرنامج في السيطرة على الصفات الأمنية للكيانات الرئيسية في قاعدة بيانات الشبكة (Active Directory). استخدم كيان بيانات (ADO) ActiveX لأغراض البحث في ألد. (Active Directory) واستخدمت واجهة الربط ADSI للتعامل مع الكيانات الأمنية الرئيسية. وقد

أظهر البرنامج إمكانية الوصول في التعامل مع الصفات الأمنية لهذه الكيانات إلى مستوى الأعلام والممثلة ب bits في هياكل البيانات لعناصر الواصفات الأمنية .  
الكلمات المفتاحية: نظام التشغيل، نظام (Windows 2000)، أمنية الشبكات، الكيانات الأمنية.

## مقدمة

لا يمكن لأي فرد أو مؤسسة العيش بشكل منعزل، في هذا العصر الذي أصبح العالم فيه قرية صغيرة بسبب ثورة الاتصالات واستخدام أحدث الأساليب المبتكرة في عالم الاتصالات. وقد أصبح الاعتماد على المعلومات أو ثروة المعلومات والحصول عليها من أهم مقومات النجاح في ظل هذا العصر الذي تشكل فيه المعلومات وحداتها أهم المرتكزات للتقدم والنجاح. إن تبادل هذه المعلومات بشكل سريع لا يتم إلا من خلال شبكات الاتصال وأجهزة الحاسوب إذ يمكن لجهاز الحاسوب التعامل مع هذه البيانات وعرضها بشكل مفهوم.

ويمكن تلخيص الفوائد التي تقدمها الشبكات بما يأتي:

1- مشاركة الموارد والملفات (Sharing resources and files)

2- مشاركة البرمجيات التطبيقية (Sharing Applications)

3- زيادة الإنتاجية (Increase Productivity)

إن استثمار الفوائد أعلاه لا يمكن أن يتم بشكل صحيح إلا من خلال توفير أمنية للمعلومات على الشبكة [1] .

إن أمنية الحاسوب تعريف واسع يشمل منع أي وصول غير مسموح أو غير مرخص لأي جزء من نظام الحاسوب . ويندرج في ذلك المعنى جميع جوانب الأجزاء الصلبة (Hardware) والبرمجيات (Software). إن الصفات الامنية التي تميز بها Windows 2000 عما سبقه من إصدارات Windows هي [5]:

1- جهاز ب Kerberos ممكناً التوقيع المفرد للوصول إلى مصادر الشبكة.

2- دعمه نظام تشفير الملفات (EFS).

3- دعمه الشبكات الخاصة الافتراضية (VPNs) وباستخدام L2TP و PPTP .

4- جهاز بمدير شهادات المفتاح العام Public Key (PK) Certificate manager لغرض إدارة المفتاح.

5- جهاز ب Internet Protocol Security (IPSec) مشفراً جميع المعلومات المتضمنة فوق طبقة النقل (Transport Layer).

6- إمكانية إعداد مراقبة الحوادث الأمنية إلى مستويات تفصيلية، وتسجيل الأحداث لغرض استعراضها فيما بعد.

7- مستوى عالٍ من إعدادات التحكم بالوصول إلى مصادر الشبكة باستخدام المجاميع ، حقوق المستخدم، السماحات ، أو السياسة الأمنية.

### الأمنية الموزعة في نظام التشغيل Windows 2000

إن السمات الرئيسية لنظام الأمنية في (Windows 2000) هي التوثيق (Authentication) والترخيص (Authorization) . وقد استخدم نظام التشغيل (Windows 2000) دليلاً هو Active Directory ليضمن للمديرين إدارة هذه السمات بكفاءة ويسر .

### التوثيق (Authentication)

التوثيق هو عملية التحقق من إن المستخدم الذي يحمل اسماً معيناً هو نفسه الذي يشير إليه ذلك الاسم وبذلك يضمن التوثيق التحقق من هوية المستخدمين الذين يبغون دخول المجال أو الوصول إلى مصادر الشبكة. أن السمة الأساسية للتوثيق في نظام التشغيل Windows 2000 هي دعمه لـ (Single Sign-on) والتي تمكن المستخدم من بلوغ المجال مستخدماً كلمة مرور مرة واحدة ويتوثق بعدها إلى أي حاسوب في المجال.

أن عملية التوثيق في Windows 2000 تنفذ بوصفها عملية من جزأين: البلوغ التفاعلي (Interactive Logon) وتوثيق الشبكة (Network Authentication) وان نجاح توثيق المستخدم يعتمد على الجزأين كليهما [10].

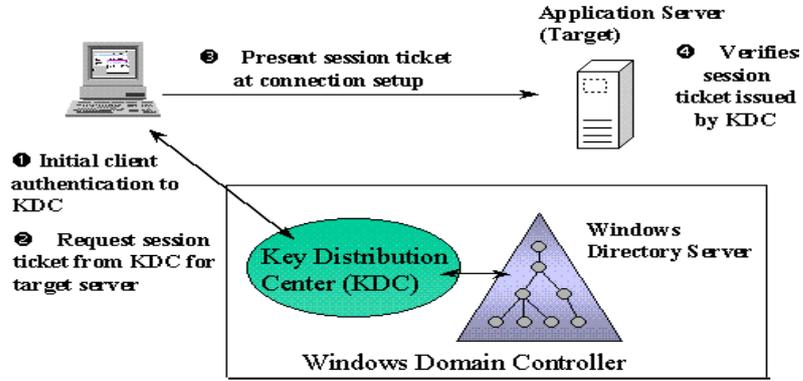
**البلوغ التفاعلي** : البلوغ التفاعلي يؤكد هوية المستخدم إلى الكمبيوتر المحلي (local computer) للمستخدم أو إلى حساب المجال (domain account) .

**توثيق الشبكة** : توثيق الشبكة هوية المستخدم لأي من خدمات الشبكة التي يسعى المستخدم إلى الوصول إليها . ولتوفير هذا النوع من التوثيق فإن النظام الأمني لـ (Windows 2000) يدعم عدداً من ميكانيكيات التوثيق تتضمن Kerberos v5 ، Secure Socket Layer / Transport ، Layer Security (SSL/TLS) ، وكذلك ألد. (Windows NT LAN Manager NTLM) والتي يدعمها لغرض التوافق مع (Windows NT 4.0) [13] [11].

### بروتوكول التوثيق Kerberos

يدعم (Windows 2000) مجموعة بروتوكولات للتحقق من هوية المستخدمين الذين يبغون الحصول على حسابات (Accounts) في النظام، ولكن البروتوكول (Kerberos

Windows 2000 Ver.5 هو المحدد أصلاً (by default) للتوثق الشبكي في أنظمة تشغيل Windows 2000 [4] [5] [10].



الشكل(1):مخطط عام للبروتوكول Kerberos

يلاحظ في الشكل في أعلاه وجود (3) أطراف في البروتوكول Kerberos وهي:

- 1-الزبون الذي يطلب الخدمة.
- 2-الخادم الذي يقدم الخدمة.
- 3-خدمة ال KDC التي توثق الزبون وتعتمد ال Active Directory قاعدة بيانات. تعمل الأطراف في أعلاه مع بعضها متبعة الخطوات الآتية لإنجاز البروتوكول:
  - 1-توثق ابتدائي للزبون إلى ال KDC .
  - 2-طلب الزبون لتذكرة جلسة من ال KDC لتقديمها إلى الخادم.
  - 3-تقديم تذكرة الجلسة إلى الخادم عند تهيئة الاتصال.
  - 4-تحقق الخادم من تذكرة الجلسة الصادرة عن ال KDC.

### الترخيص Authorization

الترخيص هو العملية التي تثبت أن للمستخدم الحقوق الصحيحة والسماحات للوصول إلى مصدر ما في المجال [8]. والتحكم بالوصول ( Access Control ) هو الميكانيكية التي ينفذ من خلالها الترخيص ، فبمجرد أن يتم التوثق من المستخدم ويكون باستطاعته الوصول إلى كيان ما ،

فان نوع الوصول الممنوح يحدد إما عن طريق حقوق الاستخدام المخصصة للمستخدم أو عن طريق السماحات المرتبطة بالكيان نفسه .

### عناصر نموذج التحكم بالوصول

يتكون نموذج التحكم بالوصول من عنصرين رئيسيين:

- 1- شارات الوصول (Access Tokens) والتي تحتوي على معلومات عن المستخدمين الذين قد تم بلوغهم الشبكة (Logged-on Users).
- 2- الواصفات الأمنية (Security Descriptors) والتي تحتوي على معلومات أمنية تحمي الكيان [2] [3] [8].

### شارات الوصول ( Access Tokens )

شارة الوصول هيكل بياني يصف السياق الأمني لمعالجة أو thread . وهي تحتوي على هويات أمنية (SID's) تعرف حساب المستخدم وحسابات المجاميع التي ينتمي إليها المستخدم. كما تحتوي على قائمة بالامتيازات التي يتمتع بها المستخدم أو مجموعته الأمنية.

### الواصفات الأمنية (Security Descriptor)

تحتوي الواصفات الأمنية على معلومات التحكم بالوصول والمتعلقة بكيان ما . والواصف الأمني هو هيكل بيانات ثنائي وبطول متغير (الشكل 2) [9] .

Header
Owner SID
Group SID
DACL
SACL

الشكل (2) الهيكل البياني للواصف الأمني

وعندما يحاول المستخدم القيام بأي فعل من الأفعال الممكنة على الكيان فإن نظام التشغيل يقوم بفحص الواصف الأمني للكيان وذلك لتحديد فيما إذا كان مسموحاً للمستخدم القيام بالفعل الذي يريده .

- إن المكونات الرئيسية للواصف الأمني هي :
- **Header** : ويحتوي على رقم التنقيح (revision number) ومجموعة من أعلام السيطرة التي تصف الميزات الخاصة بالواصف الأمني .
  - **Owner** : ويحتوي هذا الحقل على الـ SID لمالك الكيان .
  - **Primary Group** : ويحتوي هذا الحقل على الـ SID للمجموعة الأولية للمالك .
  - **Access Control Lists** : قائمة التحكم بالوصول (ACL) هي قائمة مرتبة من مداخل التحكم بالوصول (Access Control Entries ACE's) التي تحدد الحماية المستخدمة لكيان ما ولخصائصه .
- ويمكن للواصف الأمني أن يحتوي على نوعين من الـ ACL :-
- 1- قائمة التحكم بالوصول الاستثنائي (Discretionary Access Control List DACL) التي تحدد المستخدمين والمجموعات المسموح لها والممنوعة من الوصول.
  - 2- قائمة النظام للتحكم بالوصول (System Access Control List SACL) التي تبين الكيفية التي يتم بها تسجيل عملية الوصول . والشكل (3) يوضح الهيكل البياني لقائمة التحكم بالوصول.

ACL Size	ACL Revision
ACL Count	
ACE [ 1 ]	
ACE [ ... ]	
ACE [ n ]	

الشكل ( 3 ) قائمة التحكم بالوصول

#### مداخل التحكم بالوصول ( Access Control Entries ACEs )

- إن جميع مداخل التحكم بالوصول (ACEs) تحتوي على معلومات التحكم بالوصول الآتية :-
- SID يعرف هوية مستخدم أو مجموعة.
  - (access mask) يعين حقوق الوصول .
  - مجموعة من الأعلام (bit flags) تحدد إمكانية وراثه كيانات الابن للـ ACE وعلم يشير إلى نوع الـ ACE .

يدعم (Windows 2000) ستة أنواع من مداخل التحكم بالوصول . ثلاثة منها من نوع مدخل التحكم بالوصول العام ، التي يمكن أن تظهر في قوائم التحكم بالوصول الملحقة بجميع الكيانات القابلة للحماية (securable objects) ، أما الثلاثة الأخرى الباقية فهي من النوع الخاص بكيانات خاصة (object-specific) التي يمكن أن توجد فقط في قوائم التحكم بالوصول لكيانات الـ (Active Directory) [9] .  
والشكلان (4) و (5) يوضحان نوعي مداخل التحكم بالوصول.

ACE Size	ACE Type
Inheritance and Audit Flags	
Access Mask	
SID	

الشكل (4) مدخل التحكم بالوصول العام

ACE Size	ACE Type
Inheritance and Audit Flags	
Access Mask	
Object Type	Inherited Object Type
Inheritance and Audit Flags	

الشكل (5) مدخل التحكم بالوصول الخاص بالكيانات

### الدليل النشط Active Directory

أد (Active Directory) وهو خدمة دليل لـ (Windows 2000 Server) يخزن معلومات حول كيانات موجودة على الشبكة ويسهل على المدراء والمستخدمين إيجادها واستخدامها . تتكامل الأمنية مع أد (Active Directory) خلال توثق البلوغ والتحكم بالوصول إلى كيانات الدليل ، إذ يستطيع المدراء إدارة وتنظيم بيانات الدليل في الشبكة عن طريق بلوغ أحادي للشبكة ، كما يمكن لمستخدمي الشبكة المرخصين الوصول إلى المصادر حيثما كانت على الشبكة [6].

### خواص أد (Active Directory) وفوائده

يتضمن أد (Active Directory) الخواص والفوائد الآتية :

- التحكم بالوصول نزولا إلى مستوى الصفات للحسابات.

- الإدارة المرتكزة على السياسة ( Policy – Based Demonstration )
- يخزن ألد (Active Directory) السياسات التي تدعى كيانات ( Group Policy ) والتي تخصص كل منها لسياق معين .
- قابلية التوسع.
- قابلية العمل البيئي مع خدمات دليل أخرى.
- الدعم لصيغ الاسم القياسي لضمان سهولة النقل من نظام إلى آخر وسهولة الاستخدام.
- توفر مجموعة غنية من ألد (Application Programming Interfaces APIs).
- إدارة بديهية وبسيطة من خلال هيكل مجال هرمي بسيط.
- بحث سريع من خلال (Global Catalog) .
- تحديث سريع ومتوافق من خلال توحيد النسخ متعدد الأسياذ .
- توافقية خلفية مع الإصدارات السابقة من نظام تشغيل (Windows NT) .
- دليل موحد حيث يدمج مفهوم الإنترنت في فضاء التسمية (Namespace) مع خدمات الدليل لنظام التشغيل.
- الإدارة المركزية لجميع المصادر .
- توفر ألد ( Active Directory Service Interface ( ADSI ) لتسهيل البرمجة والتعامل مع ألد (Active Directory) وأداء مهام إدارية شائعة كإضافة مستخدمين جدد ، إدارة الطابعات وتحديد مواقع المصادر في البيئة الموزعة [7] [12] [15] .

### أنواع الكيانات الرئيسية لأمنية الشبكة في الـ Active Directory

- إن الأنواع الرئيسية لكيانات ألد (Active Directory) التي تعمل ككيانات أمنية رئيسية هي: [14]
- حسابات User** : إن كل مستخدم ينبغي بلوغ الشبكة يجب عليه امتلاك حساب User وكلمة مرور خاصة به .
  - حسابات Computer** : وهي حسابات تحدد أي الحواسيب الزبائن هي أعضاء في المجالات المعنية.
  - حسابات Groups** : هنالك نوعان رئيسان من المجموعات (Groups) : مجموعات Security ومجموعات Distribution وكلا النوعين من المجموعات يمكن أن يحتوي على حسابات User .

## تكوين البرنامج

اعتماداً على الدراسة التي اظهرت أن قاعدة البيانات (Active Directory) هي العنصر الأهم في مسائل إدارة الشبكة والتي من ضمنها مسألة أمنية الشبكة تم في هذا البحث بناء برنامج يوفر وصولاً إلى حسابات الكيانات الأمنية الرئيسية في خدمة الدليل (Active Directory). وقد تم استخدام كيان بيانات ActiveX (ADO) حيثما تطلب الأمر لاستعراض الكيانات من صنف معين والكائنة على ألد (Active Directory) ، واستخدمت واجهات الربط مع خدمة الدليل ADSI للوصول إلى صفات ودوال الكيان المعين لغرض معالجتها . يتكون البرنامج من خمس واجهات. وظفت احداها لاستعراض الكيانات وحسب محددات معينة . اما الواجهات الأخرى فقد احتوت الواجهة الأولى منها على أطر تعرض صفات عامة للكيان ، وعلى مدخل إلى واجهة الواصف الأمني للكيان . اما الواجهات الثلاث الأخرى فهي واجهات تعكس من خلال العناصر التي تحتويها ومن خلال ارتباطها مع بعضها معمارية الواصف الأمني وفيما يأتي وصف للواجهات المكونة للبرنامج.

## واجهة استعراض الكيانات (الشكل 5 )

يتم الوصول إلى كيانات ألد. (Active Directory) من خلال استخدام ألد. AdsPath أو ألد. GUID في عملية الربط إلى الكيان في واجهات اتصال ADSI. تحتوي واجهة اتصال استعراض الكيانات على عناصر عديدة . ففيما يتعلق بصنف الكيان فإن واجهة الاتصال تحتوي على أزرار اختيار تمثل الكيانات الأمنية الرئيسية الثلاث : المستخدم (User) ، الحاسوب (Computer) والمجموعة (Group) . وأما فيما يتعلق بمستوى البحث فقد وفرت واجهة الاتصال ثلاثة مستويات للبحث : القاعدة (Base) ، مستوى واحد (One Level) والشجرة الثانوية (Sub tree) . إن تمثيل وظيفة استعراض الكيانات قد تم من خلال استخدام كيان بيانات ActiveX (ADO) وعلى وفق الخطوات الآتية :-

## 1- تكوين كيان ADOConnection

- تخصيص قيمة لصفة Connection::Provider: هو هي ADSDS Object في حالة ألد.

. Active Directory

- تأسيس ربط فيزيائي إلى مصدر البيانات ويتم ذلك من خلال استخدام Connection::Open method. وأسم مصدر البيانات في حالة ألد Active Directory هو "Active Directory Provider".

## 2- تكوين كيان Connection ::Command

يعرف كيان Command بأنه أمر معين في النية استخدامه في التنفيذ على مصدر البيانات، وهو يستخدم للاستعلام في قاعدة البيانات وإعادة السجلات (records) في كيان recordset، لغرض تنفيذ عملية رئيسية أو لمعالجة هيكل قاعدة بيانات.

3- قراءة ألد AdsPath للمجال الذي سيتم البحث فيه.

## 4- بناء عنصر Commandtext

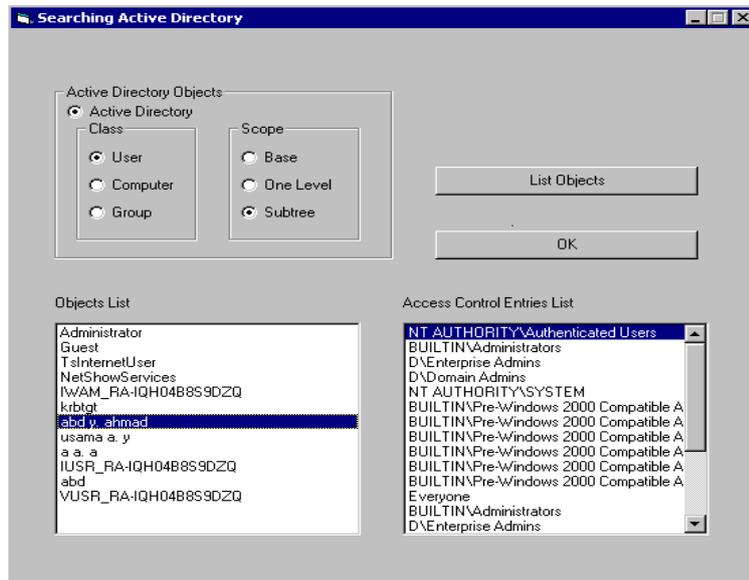
استحصال صفة ADsPath كصفة من صفات المجال وإضافتها كعنصر في ألد Commandtext

بناء عنصر المرشح من ألد Commandtext.

بناء عنصر الصفات المعادة من ألد Commandtext.

بناء عنصر عمق البحث من ألد Commandtext.

تنفيذ عملية الاستعلام باستخدام Command::Execute.



الشكل (5) واجهة استعراض الكيانات

## واجهة الصفات العامة للكيان Main Properties (الشكل 6)

إن عناصر هذه الواجهة هي :

- أطر الصفات العامة :
- تعرض في هذه الاطر صفات عامة للكيانات التي يتم اختيارها من خلال واجهة استعراض الكيانات . وقد خصص لكل صنف من الكيانات اطار لعرض صفاته .
- الأمر **Browse** : ويتم من خلاله الانتقال الى واجهة استعراض الكيانات .
- الأمر **OK** : ويتم من خلاله قبول الكيان الذي تم اختياره .
- الأمر **Discretionary ACL** : ويتم من خلاله الانتقال الى واجهة التحكم بالوصول الاستثنائي .
- الأمر **Security Descriptor** : ويتم من خلاله الانتقال الى واجهة الواصف الامني .

The screenshot shows a Windows-style dialog box titled "Main Properties" with a sub-title "Object Properties". The dialog is organized into several sections. At the top, there is an "Object Name" text box, a "Security Descriptor" button, an "OK" button, a "Browse" button, and a "Discretionary ACL" button. Below this, there are three columns of fields: "User" (with fields for Description, Full Name, Last Login, and checkboxes for Account Disabled and Password Required), "Computer" (with fields for Computer ID, Model, Operating System, and Processor), and "Group" (with fields for Description and Count). An "Exit" button is located at the bottom right of the dialog.

الشكل (6) واجهة الصفات العامة للكيان

### واجهة الواصف الأمني Security Descriptor (الشكل 7)

بعد الارتباط إلى أحد كيانات IADs فإنه يمكن قراءة صفة "ntSecurityDescriptor" له. ان صفة "ntSecurityDescriptor" ترتبط بمتغير من صنف كيان "IADsSecurity Descriptor" والذي بدوره يتكون من مجموعة من الصفات والدوال.

وتتكون واجهة الواصف الأمني من العناصر الآتية :

- صندوق النص **Revision** : ويحتوي على قيمة Revision للواصف الأمني . وهذه القيمة من الصنف Long (32 bit) .
- صندوق النص **Owner** : ويمثل النص فيه اسم المالك (Owner) للكيان .

الشكل(7): واجهة الواصف الامني

- صندوق النص **Group** : ويمثل النص فيه أسم المجموعة ( Group ) التي تنتمي إليها الهوية الأمنية (Security ID) للمالك . وهذه الصفة من صنف بيانات String .
- الإطار **Control Information** : ويحتوي على مجموعة من ألد Check boxes ذات دلالات تتعلق بالواصف الأمني نفسه . تم الحصول على قيم ألد Check boxes من خلال تحليل القيمة المستحصلة من الصفة IADsSecurityDescriptor::Control، وهي قيمة من صنف

البيانات Long التي يحمل كل bit فيها دلالة معينة ، إن أ. bits ودلالاتها معرفة في (Win  
(Win Security \_ Descriptor \_ Control) 32 وهو من صنف بيانات structure .  
الإطار **Copy Security Descriptor** : إذ يمكن من خلال التعامل مع عناصر هذا الإطار  
تحديد واصف أمني لكيان معين ومن ثم نسخه إلى الكيان قيد المعالجة .  
- الأمر **Discretionary ACL** : ينقل هذا الأمر التنفيذ إلى واجهة قائمة ضبط الوصول  
الاستثنائي ليتم من خلالها عرض محتويات قائمة الوصول وأداء وظائف معينة تتعلق بهذه القائمة

تتم هذه العملية من خلال الخطوات الآتية :

- الربط إلى الكيان المراد نسخ واصفه الأمني .
- قراءة صفة ntSecurityDescriptor إلى كيان IADsSecurityDescriptor من خلال  
دالة القراءة IADs::Get .
- استخدام الدالة IADsSecurityDescriptor::CopySecurityDescriptor لنسخ هذه  
الصفة إلى كيان من نوع IADsSecurityDescriptor .
- إحلال الكيان الجديد في صفة ntSecurityDescriptor للكيان قيد المعالجة باستخدام دالة  
الكتابة IADs::put .
- تثبيت التغيير الحاصل إلى أ. Active Directory باستخدام الدالة IADs::Set Info .

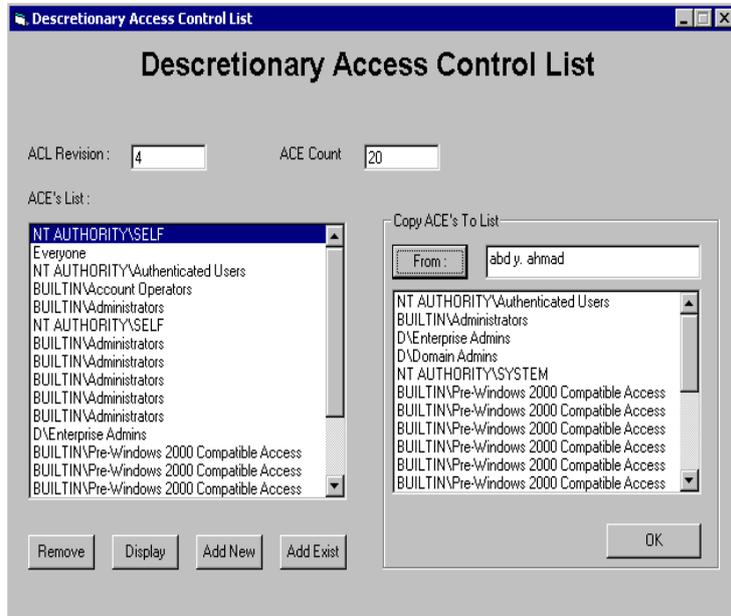
### واجهة قائمة التحكم بالوصول الاختياري (الشكل 8) Discretionary Access Control List

إن جميع الصفات والدوال التي استخدمت في الوصول إلى ومعالجة بيانات قائمة التحكم  
بالوصول الاختياري هي صفات ودوال لواجهة الربط الأمنية IADsAccessControlList . إن  
الإجراء العام الذي تم لإدارة سيطرة الوصول على كيان IADs تطلب الخطوات الآتية :

- 1- استحصال الواصف الأمني للكيان المقصود .
- 2- استحصال قائمة الوصول الاختياري من الواصف الأمني .
- 3- معالجة مداخل التحكم بالوصول في قائمة الوصول الاختياري .

إن عناصر واجهة قائمة الوصول الاختياري هي :

- صندوق النص **ACL Revision**: تمت قراءة قيمة Revision لقائمة الوصول الاختياري من خلال دالة الصفة `IADsAccessControlList::AclRevision`. إن صنف البيانات لهذه القيمة هو Long . وتمثل هذه القيمة مستوى أcl Revision لقائمة الوصول.
  - صندوق النص **ACEsCount** : تمت قراءة قيمة ACEsCount من خلال صفة `IADsAccessControlList::AclCount`. إن صنف البيانات لهذه القيمة هو Long . وتمثل هذه القيمة عدد مداخل التحكم بالوصول في قائمة التحكم بالوصول .
  - صندوق القائمة **ACEs List** : وهي قائمة تحتوي على قيم صفة trustee لمداخل التحكم بالوصول في قائمة التحكم بالوصول .
  - الإطار **Copy ACEs To List** : يتم من خلال هذا الإطار اختيار كيان معين ونسخ مداخل التحكم بالوصول له إلى قائمة التحكم بالوصول للكيان قيد المعالجة .
  - الأمر **Remove** : يتم من خلال هذا الأمر إزالة مدخل ضبط وصول مؤشر في صندوق قائمة مداخل التحكم بالوصول ACEs List للكيان قيد المعالجة وتتم العملية من خلال إزالة مدخل التحكم بالوصول من خلال استخدام الدالة `IADsAccessControlList::RemoveAce`.
  - الأمر **Display** : يتم من خلال هذا الأمر فتح واجهة خاصة ببيانات ووظائف مدخل التحكم بالوصول المؤشر في صندوق قائمة ACEs List .
  - الأمر **Add Exist**: يتم من خلال هذا الأمر إضافة مدخل تحكم بالوصول يعود إلى كيان موجود في الـ Active Directory إلى قائمة التحكم بالوصول للكيان قيد المعالجة .
- `IADsAccessControl List::Add Ace`.



الشكل (8) : قائمة التحكم بالوصول الاختياري

### واجهة مدخل التحكم بالوصول Access Control Entry (الشكل 9)

إن صفات مدخل التحكم بالوصول يمكن الوصول إليها ومعالجتها من خلال دوال الصفات لواجهة الربط الأمنية IADsAccessControlEntry . وتحوي واجهة مدخل ضبط الوصول على العناصر الآتية :

#### - صندوق النص Trustee

تمت قراءة قيمة Trustee من خلال دالة الصفة IADsAccessControlEntry::Trustee وهي قيمة من صنف بيانات String وتمثل أسم الكيان الممنوح سماعات الوصول المثبتة في مدخل التحكم بالوصول .

#### - صندوق النص Object Type

القيمة فيه تشير إلى صنف كيان ADSI . إن القيمة هي أ GUID للصفة أو الكيان بصيغة String . وإن قراءة هذه الصفة قد تمت من خلال استخدام دالة الصفة IADsAccessControlEntry :: Object Type

#### - صندوق النص Inherited Object Type

وتشير القيمة فيه إلى نوع كيان الأب لكيان ADSI . والقيمة هي GUID للكيان وبصيغة String إن قراءة هذه الصفة تمت من خلال استخدام دالة الصفة IADsAccessControlEntry :: InheritedObjectType .

#### - صندوق النص Flags

والقيمة فيه تشير إلى فيما إذا كان مدخل التحكم بالوصول يمتلك صنف كيان أم صنف كيان موروث . إن القيم الشرعية لهذه الصفة معرفة في ADS\_FLAG\_TYPE\_ENUM وكالاتي :

ADS\_FLAG\_OBGECT\_TYPE\_PRESENT = 0x1

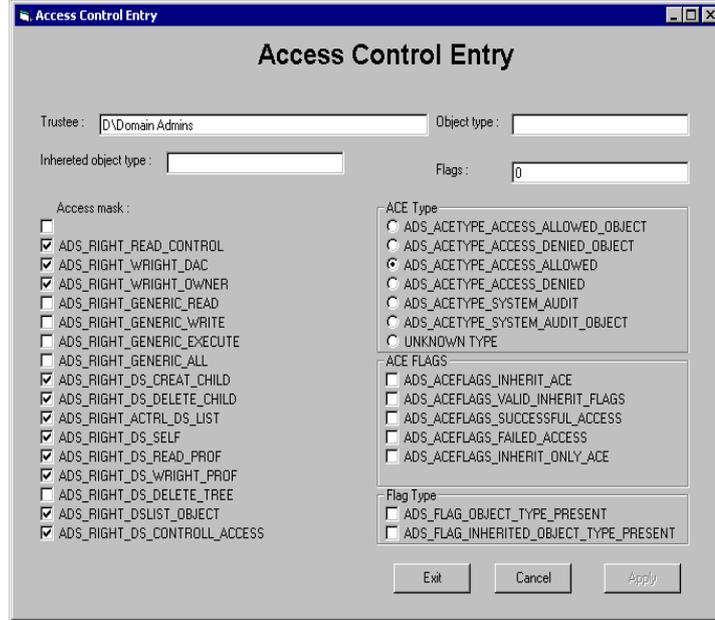
وتشير إلى وجود حقل ObjectType في مدخل ضبط الوصول

ADS\_FLAG\_INHERITED\_OBGECT\_TYPE\_PRESENT = 0x2

وتشير إلى وجود حقل InheritedObjectType في مدخل ضبط الوصول

#### - الإطار Access Mask

ويحتوي على مجموعة من أُل check boxes التي تترجم قناع الوصول إلى سماعات للوصول. إن صنف البيانات لهذه الصفة هو Long (32bit) . تمت قراءة قيمة قناع الوصول من خلال استخدام دالة الصفة IADsAccessControlEntry::Access Mask . وقد تم تحليل هذه القيمة إلى bits مفردة لكل منها دلالاتها الخاصة .



الشكل (9) : واجهة مدخل التحكم بالوصول

إن مواقع وتسميات أُل bits هي :

حق إلغاء الكيان : **ADS\_RIGHT\_DELETE= 0x10000**

حق قراءة المعلومات من الواصف الأمني **ADS\_RIGHT\_READ\_CONTROL= 0x20000**

الكيان ولا يشمل ذلك المعلومات في أُل SACL.

حق تغيير قائمة التحكم بالوصول الاختياري في

الواصف الأمني للكيان .

حق اكتساب ملكية الكيان . **ADS\_RIGHT\_WRITE\_OWNER= 0x80000**

حق القراءة من أو تغيير أُل **ADS\_RIGHT\_ACCESS\_SYSTEM\_SECURITY= 0x1000000**

في SACL الواصف الأمني للكيان .

- . ADS\_RIGHT\_GENERIC\_READ= 0x80000000 : حق القراءة من الواصف الأمني للكيان .  
تفحص الكيان وأبنائه وقراءة جميع الصفات .
- ADS\_RIGHT\_GENERIC\_WRITE= 0x40000000 : حق كتابة جميع الصفات والكتابة على  
أد ACL .
- ADS\_RIGHT\_GENERIC\_EXECUTE= 0x20000000 : حق استعراض الأبناء لهذا الكيان .
- ADS\_RIGHT\_GENERIC\_ALL= 0x10000000 : حق تكوين الأبناء أو إلغائها ، إلغاء الشجرة  
الثانوية ، قراءة الصفات وكتابتها، تفحص الأبناء والكيان نفسه، وإضافة الكيان الى الدليل أو إزالته  
منه والقراءة والكتابة بحق موسع .
- ADS\_RIGHT\_DS\_CREATE\_CHILD= 0x1 : حق تكوين أبناء من الكيان .
- ADS\_RIGHT\_DS\_DELETE\_CHILD= 0x2 : حق إلغاء أبناء الكيان.
- ADS\_RIGHT\_ACTRL\_DS\_LIST= 0x4 : حق استعراض أبناء الكيان.
- ADS\_RIGHT\_DS\_SELF= 0x8 : حق أداء عملية مسيطر عليها من قبل حق وصول كتابة  
مشروع .
- ADS\_RIGHT\_DS\_READ\_PROP= 0x10 : حق قراءة صفات الكيان .
- ADS\_RIGHT\_DS\_WRITE\_PROP= 0x20 : حق كتابة صفات الكيان .
- ADS\_RIGHT\_DS\_DELETE\_TREE= 0x40 : حق إلغاء جميع أبناء هذا الكيان . بغض  
النظر عن طبيعة السماحات على الأبناء .
- ADS\_RIGHT\_DS\_LIST\_OBJECT= 0x80 : حق استعراض كيان معين .
- ADS\_RIGHT\_DS\_CONTROL\_ACCESS= 0x100 : حق القيام بعملية مسيطر عليها من  
قبل حق وصول موسع .

### الإطار ACE Type

وتشير القيمة فيه إلى صنف مدخل التحكم بالوصول . إن القيمة هي من صنف بيانات  
Long (32bit) . وقد تمت قراءة هذه القيمة من خلال استخدام  
الدالة IADsAccessControlEntry::AceType، وقد تم تحليل هذه القيمة إلى bits مفردة لكل  
منها دلالاتها الخاصة . إن قيم هذه الصفة معرفة في ADS \_ ACE TYPE \_ ENUM وكالاتي  
:

ADS\_ACE\_TYPE\_ACCESS\_ALLOWED= 0x0 : مدخل التحكم بالوصول هو من صنف ACCESS\_ALLOWED القياسي .

ADS\_ACE\_TYPE\_ACCESS\_DENIED= 0x1 : مدخل ضبط الوصول هو من صنف SYSTEM\_DENIED القياسي .

ADS\_ACE\_TYPE\_SYSTEM\_AUDIT= 0x2 : مدخل ضبط الوصول هو من صنف AUDIT القياسي .

ADS\_ACE\_TYPE\_ACCESS\_ALLOWED\_OBJECT= 0x5 : نظام Windows 2000 وما بعده : يمنح مدخل التحكم بالوصول وصولاً إلى كيان ، أو كيان ثانوي من الكيان كمجموعة صفات أو صفة .

ADS\_ACE\_TYPE\_ACCESS\_DENIED\_OBJECT= 0x6 : نظام Windows 2000 وما بعده : يمنع مدخل التحكم بالوصول وصولاً إلى كيان ، أو كيان ثانوي من الكيان كمجموعة صفات أو صفة .

ADS\_ACE\_TYPE\_SYSTEM\_AUDIT\_OBJECT= 0x7 : نظام Windows 2000 وما بعده : يسجل مدخل التحكم بالوصول ، الوصول إلى كيان أو كيان ثانوي من الكيان مثل مجموعة صفات أو صفة .

### الإطار Ace Flag

ويحتوي على مجموعة من ألد check boxes التي تشير قيمها إلى فيما إذا كانت الكيانات والحاويات الأخرى تستطيع وراثة مدخل التحكم بالوصول من مالك قائمة التحكم بالوصول . تم الحصول على قيم ألد check boxes من تحليل القيمة المقروءة من خلال استخدام الدالة IADsAccessControlEntry::Ace Flag . إن قيمة هذه الصفة هي من صنف بيانات Long (32bit) . وإن هذه القيمة تحتوي على bits لها دلالاتها الخاصة وهي معرفة في ADS \_ ACE\_TYPE\_ENUM وكالاتي :

ADS\_ACE\_FLAG\_INHERIT\_ACE= 0x2 : كيانات الابن سترث مدخل التحكم بالوصول هذا ويكون مدخل التحكم بالوصول الموروث قابلاً للوراثة ما لم يكن علماً .

ADS\_ACE\_FLAG\_NO\_PROPOGATE\_INHERIT\_ACE= 0x4 : النظام سوف يجعل قيمة العلم ADS\_ACE\_FLAG\_INHERIT\_ACE صفراً لمداخل التحكم بالوصول الموروثة لكيانات الابن .

ADS\_ACE\_FLAG\_INHERIT\_ONLY\_ACE= 0x8 : يشير إلى أن مدخل التحكم بالوصول هو لغرض الوراثة فقط ولا يمارس تحكماً في الوصول على الكيان الملحق به.

ADS\_ACE\_FLAG\_INHERITED\_ACE= 0x10 : يشير إلى فيما إذا كان مدخل التحكم بالوصول موروثاً أم لا .

ADS\_ACE\_FLAG\_VALID\_INHERIT\_FLAGS= 0x1F : يشير إلى فيما إذا كانت الأعلام شرعية والنظام هو الذي ينصب هذا bit .

ADS\_ACE\_FLAG\_SUCCESSFUL\_ACCESS= 0x40 : يكون رسائل تسجيل لمحاولات الوصول الناجحة .

ADS\_ACE\_FLAG\_FAILED\_ACCESS= 0x80 : يولد رسائل تسجيل لمحاولات الوصول الفاشلة .

#### الاستنتاجات والتوصيات

تبين من خلال الدراسة التي تمت في هذا البحث إن هناك محورين رئيسيين للأمنية في الشبكات في نظام التشغيل Windows 2000 : التوثق (Authentication) والترخيص (Authorization) وتم التوصل إلى أن هناك خدمات دليل وقاعدة بيانات هي ألد Active Directory تمثل العمود الفقري للعمليات التي تنفذ في سياق هذين المحورين الرئيسيين، ولأهمية البيانات في ألد Active Directory فقد خصص لكل حساب واصفٍ أمني (Security Descriptor) لا يحدد فقط من يمكنه الوصول إلى هذا الحساب ولكن يذهب إلى أبعد من ذلك في تحديد الصفات المسموح بالوصول إليها ونوع حق الوصول.

وفي ضوء المعطيات المذكورة أنفاً تم التوجه إلى بناء برنامج للسيطرة على حسابات الكيانات الأمنية الرئيسية (User ,Computer ,Group) في ألد Active Directory . إن البرنامج هو برنامج للتعامل مع الواصفات الأمنية ومن المستوى الأدنى إذ يذهب في تعامله إلى حد معالجة الأعلام الممثلة بـ bits وكل على حدة ، ليؤدي وظائف التعديل والإضافة والإزالة لبعض البيانات ذات الأهمية الأمنية للكيانات الرئيسية في ألد Active Directory، وبذلك يحقق البرنامج سيطرة على جانب من أمنية الشبكات لنظام التشغيل Windows 2000.

- ويمكن الانطلاق من هذا البرنامج بوصفه عملاً مستقبلياً ليكون نواةً في:
- 1- تصميم تطبيقات خدمية أمنية خاصة قد تظهر حاجة مدير المجال إليها.
  - 2- توسيع ألد Schema لـ Active Directory إما بإضافة كيانات جديدة أو بإضافة صفات جديدة - ذات صفة أمنية - لكيانات موجودة أصلاً .
  - 3- توسيع نطاق التعامل مع الكيانات ليتجاوز ألد Active Directory إلى نظام الملفات وإلى ألد Computer registry .
  - 4- اقتراح عدد من الحقوق الموسعة الممكنة على الكيانات الموجودة في ألد Active Directory .
- تطوير البرنامج ليفيد في دراسة الموضوع من خلال توسيع واجهات البرنامج بإضافة عناصر اتصال تعكس التغيير الذي يحدث على البنية التحتية للواصف الأمني بوصفه متغيراً يمكن فهمه من قبل المستخدم العادي .

المصادر

- (1) شلباية، مراد و فاروق، علي، 2000، مقدمة الى الشبكات، دار المسيرة للنشر والتوزيع، ط2000، ام.
- [2] “Active Directory Architecture” , Microsoft , 2001  
<http://windows.about.com/cs/activedirectory/>
- [3] Brown K., 2000 , “Exploring Handle Security In Windows” , msdn magazine , March 2000 .
- [4] Brown K. , 2000 , “Understanding Kerberos Credential Delegation in Windows 2000 Using the TktView Utility” , msdn magazine , May 2000.
- [5] Chapil D., 2000 , “Exploring Kerberos , The Protocol for Distributed Security in Windows 2000” , MICROSOFT SYSTEM JOURNAL ,vol. 4, no. 1, pp40-52.
- [6] Esposito D. , 1999 , “With further ADO : Coding Active Directory Data Objects 2.0 with Visual Studio 6.0” , MICROSOFT SYSTEMS JOURNAL , February 1999 .
- [7] Fox D. , 1999 , “Directory-Enable Apps With ADSI” , VBPI , February 1999 .  
[www.devx.com/premier/mgznarch/vbpj/1999/02feb99/fox099.pdf](http://www.devx.com/premier/mgznarch/vbpj/1999/02feb99/fox099.pdf)
- [8] Grant J. R. , 1999 , “Operating System Security” , April 1997.  
<http://people.msoe.edu/~sebern/courses/cs384/papers97/grant.pdf>
- [9] Johansson J. M. , “Windows 2000 Security – An Overview and Analysis.” [www.foo.be/docs/adsi-ldap/Windows2000Security-Aduserpasswordproperties.pdf](http://www.foo.be/docs/adsi-ldap/Windows2000Security-Aduserpasswordproperties.pdf)
- [10] “Kerberos in Win2K” , Windows NT magazine , October 1999.
- [11] Kling J. , 1999 , Working with Objects in Active Directory , Exploring Windows NT , December 1999.
- [12] Mrozowski P. , 2001, “Taking Advantage of ADSI” , CoDe magazine , Winter 2001.  
[www.kirtlandsys.com/misc/Taking%20Advantage%20of%20ADSI.pdf](http://www.kirtlandsys.com/misc/Taking%20Advantage%20of%20ADSI.pdf)
- [13] Otel F.,2000 , “Some Security Aspects of Link Layer Protocol”,  
[www.ce.chalmers.se](http://www.ce.chalmers.se)

- [14] Waddell J. L. , 2001 , “**Basic Security Issues of Active Directory**” , *SANS Institute* , June 2001 .  
[www.set.usn.edu/SBlesse/ref/docs/MICROSOFT-Basic%20Security%20Issues%20of%20Active%20Directory.pdf](http://www.set.usn.edu/SBlesse/ref/docs/MICROSOFT-Basic%20Security%20Issues%20of%20Active%20Directory.pdf)
- [15] Wildermuth S. , 2000 , “**Active Directory Doesn’t Manage Network Resources , It Can Manage Your Data Too**” , *MICROSOFT SYSTEM JOURNAL* , January 2000.