السيطرة على صفات الكيانات الأمنية للشبكات في ويندوز ٢٠٠٠

ضحى بشير عبد الله عبد الناصر يونس احمد

كلية علوم الحاسبات والرياضيات

جامعة الموصل

تاريخ استلام البحث:٢٠٠٢/١٠/٢٧ تاريخ قبول البحث:٢٠٠٣/١/٢٥

ABSTRACT

Information security occupies a wide area in designing network operating ystems. 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.

الملخص

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، فعد 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 ActiveX (ADO) لأغراض البحث في ألـ (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 بـ bits في هياكل البيانات لعناصر الواصفات الأمنية .

مقدمة

لا يمكن لأي فرد أو مؤسسة العيش بشكل منعزل،في هذا العصر الذي اصبح العالم فيه قرية صغيرة بسبب ثورة الاتصالات واستخدام احدث الأساليب المبتكرة في عالم الاتصالات. وقد اصبح الاعتماد على المعلومات أو ثروة المعلومات والحصول عليها من أهم مقومات النجاح في ظل هذا العصر الذي تشكل فيه المعلومات وحداثتها 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:

١-مشاركة الموارد والملفات (Sharing resources and files)

٢-مشاركة البرمجيات التطبيقية (Sharing Applications)

٣-زيادة الإنتاجية (Increase Productivity)

إن استثمار الفوائد أعلاه لا يمكن أن يتم بشكل صحيح إلا من خلال توفير أمنية للمعلومات على الشبكة[١] .

إنَ 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).ان الصفات الامنية التي تميز بها Windows 2000 عما سبقه من إصدارات Windows هي[٥]:

١- جهز بـ Kerberos ممكناً التوقيع المفرد للوصول إلى مصادر الشبكة.

٢- دعمه نظام تشفير الملفات (EFS).

٣- دعمه الشبكات الخاصة الافتراضية (VPNs) وباستخدام L2TP وPPTP .

٤- جهز بمدير شهادات المفتاح العام Public Key (PK) Certificate managerلغرض إدارة المفتاح.

٥- جهز بـ Internet Protocol Security (IPSec)مشفراً جميع المعلومات المتضمنة فوق طبقة النقل (Transport Layer).

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

٧- 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 التوثق (Authentication) والترخيص (Authorization) . وقد استخدم نظام التشغيل (Windows 2000) دليلا هو ألـ Active Directory ليضمن للمديرين إدارة هذه السمات بكفاءة ويسر.

التوثق(Authentication)

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

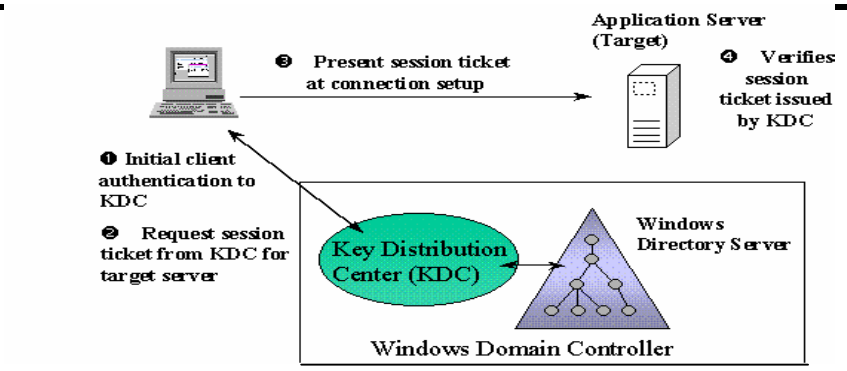
أن عملية التوثق في Windows 2000 تنفذ بوصفها عملية من جزأين: البلوغ التفاعلي (Interactive Logon) وتوثق الشبكة (Network Authentication) وان نجاح توثق المستخدم يعتمد على الجزأين كليهما [10].

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

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

بروتوكول التوثق Kerberos

يدعم (Windows 2000) مجموعة بروتوكولات للتحقق من هوية المستخدمين الذين يبغون الحصول على حسابات (Accounts) في النظام ،ولكن البروتوكول (Kerberos Ver.5)هو المحدد أصلاً (by default) للتوثق الشبكي في أنظمة تشغيل Windows 2000 [4] [5] [10].



الشكل(١):مخطط عام للبروتوكول Kerberos

يلاحظ في الشكل في أعلاه وجود (٣) أطراف في البروتوكول Kerberos وهي:

١-الزبون الذي يطلب الخدمة.

٢-الخادم الذي يقدم الخدمة.

٣-خدمة أل KDC التي توثق الزبون وتعتمد أل Active Directory قاعدة بيانات.

تعمل الأطراف في أعلاه مع بعضها متبعة الخطوات الآتية لإنجاز البروتوكول:

١-توثق ابتدائي للزبون إلى الـــ KDC .

٢-طلب الزبون لتذكرة جلسة من الـــ KDC لتقديمها إلى الخادم.

٣-تقديم تذكرة الجلسة إلى الخادم عند تهيئة الاتصال.

٤-تحقق الخادم من تذكرة الجلسة الصادرة عن الـــ KDC.

الترخيص Authorization

الترخيص هو العملية التي تثبت أن للمستخدم الحقوق الصحيحة والسماحات للوصـــول إلى مصدر ما في المجال [8]. والتحكم بالوصول (Access Control) هو الميكانيكية التـــي 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:

١- شارات الوصول (Access Tokens) والتي تحتوي على معلومات عن المستخدمين الذين قد تم بلوغهم الشبكة (Logged-on Users).

٢- 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 ٢) [9] .

Header
Owner SID
Group SID
DACL
SACL

الشكل (٢) 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 الـــ SID لمالك الكيان .

- **Primary Group** : ويحتوي هذا الحقل على ألـــ SID للمجموعة الأولية للمالك .

- **Access Control Lists** : قائمة التحكم بالوصول (ACL) هي قائمة مرتبة من مـــداخل التحكم بالوصول (ACE's Access Control Entries) التي تحدد الحمايـــة المـــستخدمة لكيان ما ولخصائصه .

ويمكن للواصف الأمني أن يحتوي على نوعين من ألـــ ACL :-

١- قائمة التحكم بالوصول الاستنـــسابي (DACL Discretionary Access Control List) التي تحدد المستخدمين والمجموعات المسموح لها والممنوعة من الوصول.

٢- قائمة النظام للتحكم بالوصول (SACL System Access Control List) التـــي تبـــين الكيفية التي يتم بها تسجيل عملية الوصول . والشكل (٣) يوضح الهيكل البياني لقائمة الـــتحكم بالوصول.

ACL Size	ACL Revision
ACL Count	
ACE [1]	
ACE […]	
ACE [*n*]	

الشكل (٣) قائمة التحكم بالوصول

مداخل التحكم بالوصول (Access Control Entries ACEs)

إن جميع مداخل التحكم بالوصول (ACEs) تحتوي على معلومات التحكم بالوصول الأتية :-

- SID يعرف هوية مستخدم أو مجموعة.

- (access mask) يعين حقوق الوصول .

- مجموعة من الأعلام (bit flags) تحدد إمكانية وراثة كيانات الابن للـــ ACE وعلم يشير إلى نوع ألـــ ACE .

يدعم (Windows 2000) ستة أنواع من مداخل التحكم بالوصول . ثلاثة منها مـــن نوع مدخل التحكم بالوصول العام ، التي يمكن أن تظهر في قوائم التحكم بالوصـــول الملحقـــة 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 الـــ (Active Directory) [9] .
والشكلان (٤) و (٥) يوضحان نوعي مداخل التحكم بالوصول.

ACE Size	ACE Type
Inheritance and Audit Flags	
Access Mask	
SID	

الشكل (٤) مدخل التحكم بالوصول العام

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

الشكل (٥) مدخل التحكم بالوصول الخاص بالكيانات

الدليل النشط Active Directory

ألـــ (Active Directory) وهو خدمة دليل لـــ (Windows 2000 Server) يخزن معلومات حول كيانات موجودة على الشبكة ويـــسهل علـــى المـــدراء والمـــستخدمين إيجادهـــا واستخدامها . تتكامل الأمنية مع ألـــ (Active Directory) خـــلال توثـــق البلـــوغ والـــتحكم بالوصول إلى كيانات الدليل ، إذ يستطيع المدراء إدارة وتنظيم بيانات الدليل في الـــشبكة عـــن طريق بلوغ أحادي للشبكة ، كما يمكن لمستخدمي الشبكة المرخصين الوصول الـــى المـــصادر حيثما كانت على الشبكة [6].

خواص ألـــ (Active Directory) وفوائده

يتضمن ألـــ (Active Directory) الخواص والفوائد الأتية :

- التحكم بالوصول نزولا الى مستوى الصفات للحسابات.
- الإدارة المرتكزة على السياسة (Policy – Based Demonstration)

- يخزن ألــ (Active Directory) السياسات التي تدعى كيانات (Group Policy) والتي تخصص كل منها لسياق معين .
- قابلية التوسع.
- قابلية العمل البيني مع خدمات دليل أخرى.
- الدعم لصيغ الاسم القياسي لضمان سهولة النقل من نظام إلى آخر وسهولة الاستخدام.
- توفر مجموعة غنية من ألــ (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 الأسياد .
- 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 ألــ (ADSI) Active Directory Service Interface لتسهيل البرمجة والتعامل مع ألــ (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 الــ Active Directory

إن الأنواع الرئيسية لكيانات ألــ (Active Directory) التي تعمل ككيانات أمنية رئيسية هي :[14]

حسابات User : إن كل مستخدم يبغي بلوغ الشبكة يجب عليه امتلاك حساب User وكلمة مرور خاصة به .

حسابات Computer : وهي حسابات تحدد أي الحواسيب الزبائن هي أعضاء في المجالات المعينة.

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 ألـ (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 الاربع الاخرى 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 ٥)

يتم الوصول إلى كيانات ألـ (Active Directory) من خلال استخدام ألـ AdsPath أو ألـ 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 الأتية :-

١- تكوين كيان ADOConnection

- تخصيص قيمة لصفة Connection::Provider:و هي ADsDS Object في حالة ألـ Active Directory .

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

٢ - 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 .

٣ - قراءة ألـ AdsPath للمجال الذي سيتم البحث فيه.

٤ - بناء عنصر Commandtext

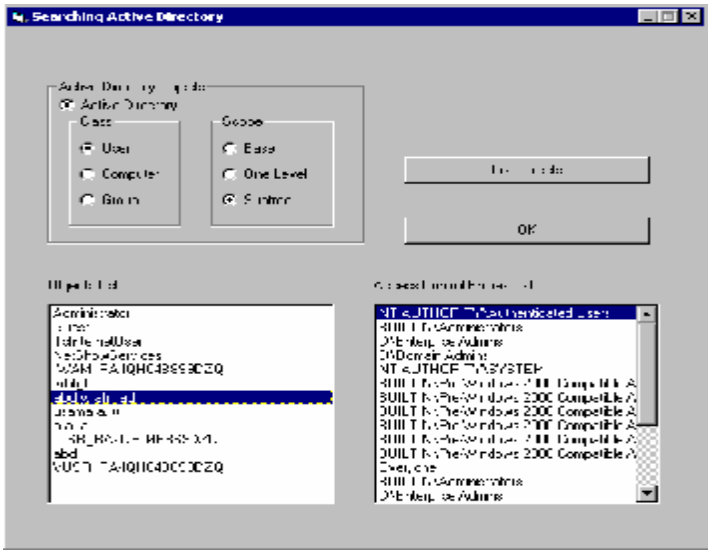
استحصال صفة ADsPath كصفة من صفات المجال وإضافتها كعنصر في ألـ Commandtext

بناء عنصر المرشح من ألـ Commandtext.

بناء عنصر الصفات المعادة من ألـ Commandtext.

بناء عنصر عمق البحث من ألـ Commandtext.

تنفيذ عملية الاستعلام باستخدام Command::Execute .



الشكل(٥)واجهة استعراض الكيانات

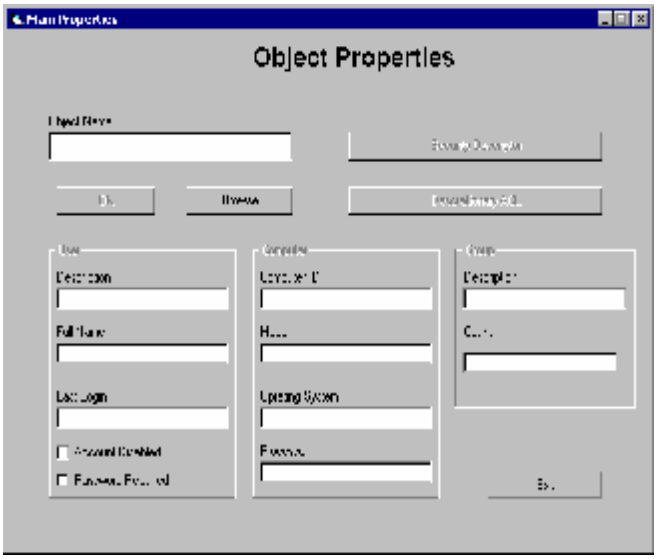
واجهة الصفات العامة للكيان Main Properties (الشكل ٦)

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 اطارُ 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 الاستنسابي .
- **الأمر Security Descriptor** : ويتم من خلاله الانتقال الى واجهة الواصف الامني .



الشكل (٦) واجهة الصفات العامة للكيان

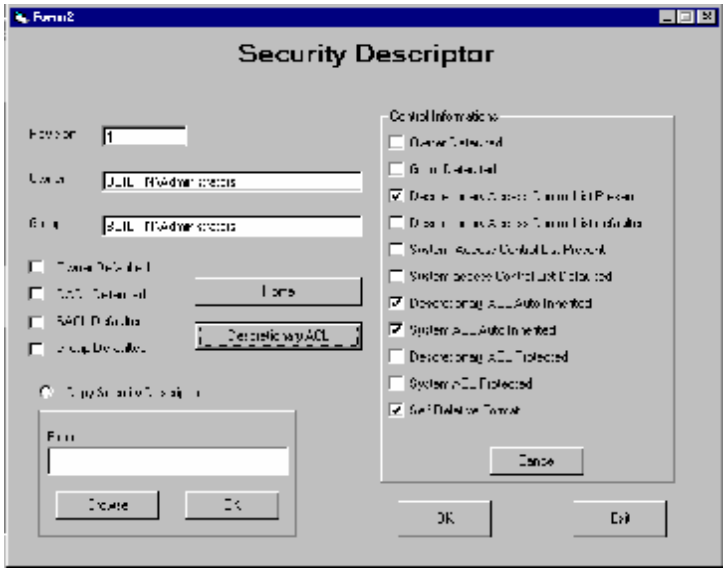
واجهة الواصف الأمني Security Descriptor (الشكل٧)

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 الاتية :

- **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(٧): 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 ألـ Check boxes ذات دلالات تتعلق بالواصف الأمني نفسه . تم الحصول على قيم ألـ 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 ألـ bits ودلالاتها معرفة في (Win 32 Security _ Descriptor _ Control) 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 الاستنسابي ليتم من خلالها عرض محتويات قائمة الوصول وأداء وظائف معينة تتعلق بهذه القائمة .

تتم هذه العملية من خلال الخطوات آلاتية :

- 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 التغير الحاصل إلى ألـ Active Directory باستخدام الدالة IADs::Set Info .

واجهة قائمة التحكم بالوصول الاختياري (الشكل ٨) 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 الأتية :

١- استحصال الواصف الأمني للكيان المقصود .

٢- استحصال قائمة الوصول الأختياري من الواصف الأمني .

٣- معالجة مداخل التحكم بالوصول في قائمة الوصول الأختياري .

إن عناصر واجهة قائمة الوصول الأختياري هي :

- **صندوق النص ACL Revision**: تمت قراءة قيمة Revision لقائمة الوصول الأختياري من خلال دالة الصفة IADsAccessControlList::AclRevision .إن صنف البيانات لهذه القيمة هو Long . وتمثل هذه القيمة مستوى ألـ 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 .

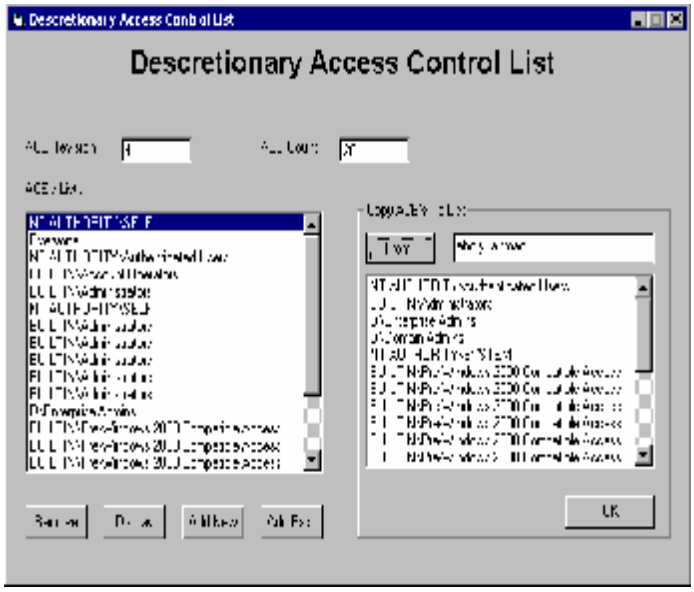
- **الإطار Copy ACEs To List** : يتم من خلال هذا الإطار اختيار كيان معين ونسخ مداخل التحكم بالوصول له إلى قائمة التحكم بالوصول للكيان قيد المعالجة .

- **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 (٨) : قائمة التحكم بالوصول الاختياري

واجهة مدخل التحكم بالوصول Access Control Entry (الشكل ٩)

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

- صندوق النص Trustee

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

- صندوق النص Object Type

القيمة فيه تشير إلى صنف كيان ADSI . إن القيمة هي ألـ 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 وكالأتي :

ADS_FLAG_OBGECT_TYPE_PRESENT = 0x1

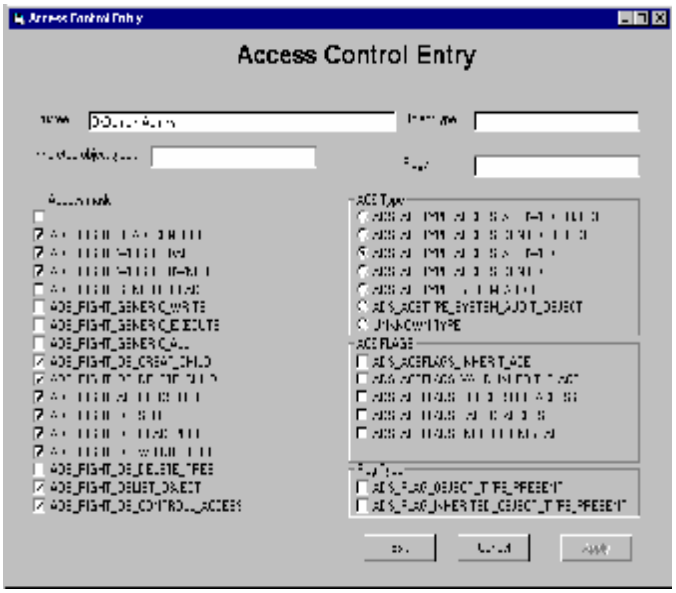
وتشير إلى وجود حقل ObjectType في مدخل ضبط الوصول

ADS_FLAG_INHERITED_OBGECT_TYPE_PRESENT = 0x2

وتشير إلى وجود حقل InheritedObjectType في مدخل ضبط الوصول

- الإطار Access Mask

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



الشكل(٩) : واجهة مدخل التحكم بالوصول

إن مواقع وتسميات ألـــ bits هي :

ADS_RIGHT_DELETE= 0x10000 : حق إلغاء الكيان .

ADS_RIGHT_READ_CONTROL= 0x20000 : حق قراءة المعلومات من الواصف الأمني للكيان و لا يشمل ذلك المعلومات في ألـــ SACL.

ADS_RIGHT_WRITE_DAC= 0x40000 : حق تغيير قائمة التحكم بالوصول الأختياري فـــي الواصف الأمني للكيان .

ADS_RIGHT_WRITE_OWNER= 0x80000 : حق اكتساب ملكية الكيان .

ADS_RIGHT_ACCESS_SYSTEM_SECURITY= 0x1000000 : حق القراءة من أو تغيير ألـــ SACL في 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 ألـ DACL .

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 .

<u>الإطار ACE Type</u>

وتشير القيمة فيه إلى صنف مدخل التحكم بالوصول . إن القيمة هي من صنف بيانات Long (32bit) . وقد تمت قراءة هذه القيمة من خلال استخدام الدالةIADsAccessControlEntry::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= 0x 0 : مدخل التحكم بالوصول هو من صنف القياسي ACCESS ALLOWED .

ADS_ACE TYPE_ACCESS_DENIED= 0x1 : مدخل ضبط الوصول هو من صنف القياسي SYSTEM DENIED .

ADS_ACE TYPE_SYSTEM_AUDIT= 0x2 : مدخل ضبط الوصول هو من صنف القياسيAUDIT .

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 .

<u>الإطار Ace Flag</u>

ويحتوي على مجموعة من ألـ 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 ألـ 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 وكالأتي :

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 ألـ 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 ألـ Active Directory تمثل العمود الفقري للعمليات التي تنفذ في سياق هذين المحورين الرئيسين،ولأهمية البيانات في ألـ Active Directory فقد خصص لكل حساب واصفاً أمنياً (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 ألـ 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 الـ Active Directory،وبذلك يحقق البرنامج سيطرة على جانب من أمنية الشبكات لنظام التشغيل Windows 2000.

ويمكن الأنطلاق من هذا البرنامج بوصفه عملاً مستقبلياً ليكون نواةً في:

١ - تصميم تطبيقات خدمية أمنية خاصة قد تظهر حاجة مدير المجال إليها.

٢ - توسيع ألـــ Schema للـــ Active Directory إما بإضافة كيانات جديدة أو بإضافة صفات جديدة – ذات صفة أمنية – لكيانات موجودة أصلاً .

٣ - توسيع نطاق التعامل مع الكيانات ليتجاوز ألـــ Active Directory إلى نظام الملفات وإلى ألـــ Computer registry .

٤ - اقتراح عدد من الحقوق الموسعة الممكنة على الكيانـــات الموجـــودة فـــي ألـــــ 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 متغييراً يمكن فهمه من قبل المستخدم العادي .

المصـــــــادر

(١) شلباية، مراد و فاروق،علي، ٢٠٠٠ ،**مقدمة الـــى الـــشبكات**، *دار المـــسيرة للنـــشر والتوزيع*،ط١،٢٠٠٠م.

[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**" , *VBPJ* , February 1999 . *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*

[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*

[13] Otel F.,2000 , "**Some Security Aspects of Link Layer Protocol**", *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

[15] Wildermuth S. , 2000 , "**Active Directory Doesn't Manage Network Resources , It Can Manage Your Data Too**" , *MICROSOFT SYSTEM JOURNAL* , January 2000.