Security with IDS

Rob Jane
IBM

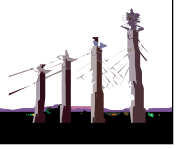
A07
Day, April 29, 2008 • 09:30 a.m. – 10:30 a.m.

2008 IIUG Informix Conference

www.iiug.org

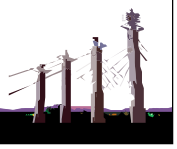
Security with IDS

- Security can be defined as ***ensuring that no unauthorized user is accessing or altering your data***. You can ensure your data security by providing access permissions only to authorized users, auditing the events, and encrypting the data while transmitting over the network. You can establish security checks at different levels starting from login to the table column access



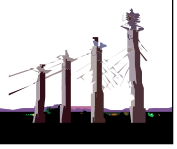
Security with IDS

- Agenda
  - Server Utility and Directory Security
  - Network Data Encryption
  - Backup and Restore
  - Discretionary Access Control
  - CLE, LBAC and Views
  - Auditing
  - Future changes
  - Q&A



Security with IDS

- Agenda
  - Server Utility and Directory Security
  - Network Data Encryption
  - Backup and Restore
  - Discretionary Access Control
  - CLE, LBAC and Views
  - Auditing
  - Future changes
  - Q&A



Security with IDS

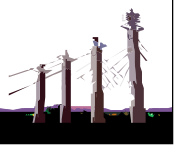
- Server Utility and Directory Security
  - Installation and file permissions
    - User “informix” is the super user within IDS
      - Only a dbsa can start and stop the engine
    - Permissions on $INFORMIXDIR set to 755 and user;group equal to informix:informix
    - Permissions on $ONCONFIG and sqlhosts
    - Filename lengths less than 256

Security with IDS

- Server Utility and Directory Security
  - External modules
    - Use the onconfig DB_LIBRARY_PATH
      - Controls the location of where to get external modules

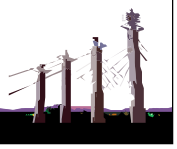
Security with IDS

- Server Utility and Directory Security
  - Authentication
    - Trusted user (hosts.equiv or .rhosts)
    - Pluggable authentication module (PAM)
    - Lightweight Directory Access protocol (LDAP)
    - Password encryption using SPWDCSM
    - $INFORMIXDIR/dbssodir/seccfg to restrict non-listed users from accessing the database server
    - SECURITY_LOCALCONNECTION



Security with IDS

- Server Utility and Directory Security
  - Limiting denial-of-service flood attacks
    - To limit attacks attempting to block threads set the following onconfig settings
      - MAX_INCOMPLETE_CONNECTIONS NNNN (1024)
        - If there are NNNN incomplete connections, deny the service
      - LISTEN_TIMEOUT 10 (seconds)
        - Clean up incomplete connection requests after allotted time

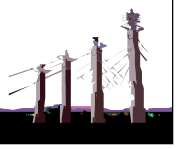


Security with IDS

- Server Utility and Directory Security
  - Network Security
    - Firewalls
      - Enforces security policies such as which user can access which service
      - Another denial-of-service approach
    - ssh
      - provides secured encrypted communication between two un-trusted machines over an unsecured network

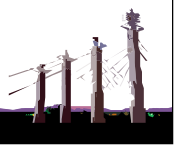
Security with IDS

- Server Utility and Directory Security
  - Connection authentication choices
    - sqlhosts security options and trusted connections
      - S=0 Disables hosts.equiv and .rhosts.
      - S=1 Look at hosts.equiv file
      - S=2 Look at .rhosts file.
      - S=3 Look at hosts.equiv and .rhosts.
      - S=4 PAM
      - S=6 ER & HDR only.
      - S=7 **NEW IDS11.50 FEATURE**



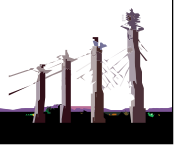
Security with IDS

- Agenda
  - Server Utility and Directory Security
  - Network Data Encryption
  - Backup and Restore
  - Discretionary Access Control
  - CLE, LBAC and Views
  - Auditing
  - Future changes
  - Q&A



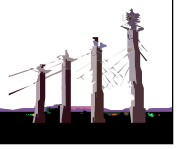
Security with IDS

- Network Data Encryption
  - Communications between servers give an opportunity for hackers to “snoop” the data being transferred
  - Encrypting the data before sending and having the receiving end decrypt the data is a way to avoid this



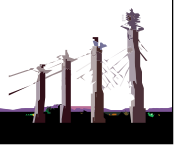
Security with IDS

- Network Data Encryption
  - Apply an algorithm to make data unreadable
  - An encryption key is required to decrypt data
    - Symmetric cryptography – One key for both encryption and decryption
      - IDS uses this technique
    - Public key cryptography – Different keys used for encryption and decryption



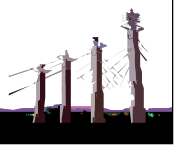
Security with IDS

- Network Data Encryption
  - Encryption technology is integrated with IDS as a pluggable communication supports module (CSM)
  - IDS provides the network encryption communication support module (ENCCSM), which enables you to encrypt complete client-server communication
  - Also, simple password communication support module (SPWDCSM), which enables you to encrypt the user password
  - Built-in functions and libraries are provided



Security with IDS

- Network Data Encryption
  - ER can use encrypted communications
    - ENCRYPT_CDR [012] onconfig parameter
  - HDR can now encrypt communications
    - ENCRYPT_HDR [01] onconfig parameter
    - Shares the existing ER encryption onconfig parameters
  - MACH11 can encrypt communications to the SDS & RSS nodes via SMX (server group multiplexer)
    - ENCRYPT_SMX [012] onconfig parameter

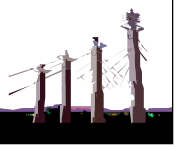


Security with IDS

- Network Data Encryption
  - Onconfig parameters used for encryption
    - ENCRYPT_SWITCH
      - frequency at which ciphers or secret keys should be renegotiated
    - ENCRYPT_CIPHERS
      - Which ciphers to be used
    - ENCRYPT_MAC
      - controls the level of message authentication code generation
    - ENCRYPT_MACFILE
      - the full path names of MAC key files to be used for ER and HDR
    - ENCRYPT_SCHEDULE
      - defines the switch time for the macfiles and the ciphers if there are multiple options defined

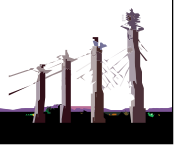
Security with IDS

- Network Data Encryption
  - **IDS 11.50 (Cheetah2) offers an alternative**



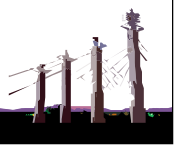
Security with IDS

- Agenda
  - Server Utility and Directory Security
  - Network Data Encryption
  - Backup and Restore
  - Discretionary Access Control
  - CLE, LBAC and Views
  - Auditing
  - Future changes
  - Q&A



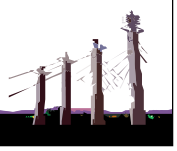
Security with IDS

- Backup and Restore
  - Remote storage facilities also provide hackers the chance to “snoop” data being transmitted
  - Authentication and restrictions are of no use if people can see / obtain the backups you just took
    - You do not want to hand the data on a plate within a nice little parcel



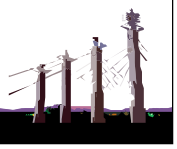
Security with IDS

- Backup and Restore
  - IDS has three main methods
    - Onbar
      - Local or remote disks or tapes
      - Parallel or serial operations
    - Ontape
      - Disk, directory, stdout, tapes & remote devices
      - Serial operation
    - External / Offline.
      - Block server and use 3rd party utilities



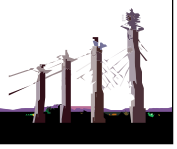
Security with IDS

- Backup and Restore
  - Ensure executables have correct permissions
    - Allow only root or informix (dbsa)
  - If backing up to a file or directory, ensure that these have the correct permissions set
    - Onbar: Depends on storage manager
    - Ontape: IDS has control



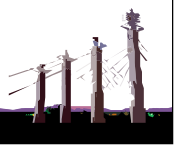
Security with IDS

- Backup and Restore
  - $ ls -al $INFORMIXDIR/bin/onbar*
    - -rwxr-xr-x 1 informix informix 3897 2007-06-19 07:49 /IDS11/bin/onbar
    - -rwsr-sr-x 1 root informix 2240124 2007-06-22 17:21 /IDS11/bin/onbar_d
  - $ ls -al $INFORMIXDIR/bin/ontape
    - -rwsr-sr-x 1 root informix 1873878 2007-06-22 17:20 /IDS11/bin/ontape
  - In Windows, check the properties and see if the user is in Informix-Admin group



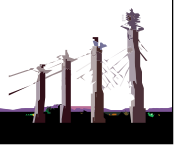
Security with IDS

- Backup and Restore
  - Backups over the network pose a big threat to data being snooped
    - Ontape can use remote shells, remote tapes or pipes
    - Onbar transfers data XBSA communications



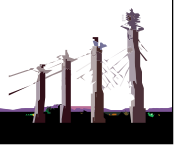
Security with IDS

- Backup and Restore
  - Onbar-ism can compress & encrypt but is basic
    - ISM_ENCRYPTION & ISM_COMPRESSION
  - Storage Vendor offerings
    - Legtao: NSR_COMPRESSION & NSR_ENCRYPTION
    - TSM: ENABLECLIENTCRYPTKEY & ENCRYPTIONTYPE
  - Ontape can also manipulate data if using stdout (named pipes)



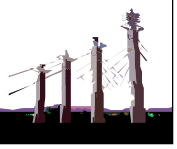
Security with IDS

- Backup and Restore
  - Backup and Restore filters.
  - Capability to “plug in” a program between the server backup utility and the storage target
    - Could be bought 3rd party program
    - In-house coded program
    - OS command. e.g. compress or gzip



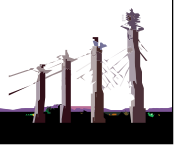
Security with IDS

- Backup and Restore
  - Onconfig parameters
    - BACKUP_FILTER ’/usr/bin/gzip’
    - BACKUP_FILTER 'openssl enc -e -aes-256-cbc -k password -salt'
    - RESTORE_FILTER ’/usr/bin/gunzip’
    - RESTORE_FILTER 'openssl enc -d -aes-256-cbc -k password ‘
  - Cannot chain commands, so use a script



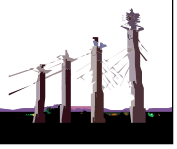
Security with IDS

- Backup and Restore
  - **TEST, TEST & TEST AGAIN**
    - Ensure that the backups do restore



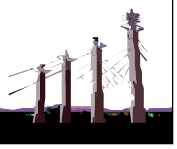
Security with IDS

- Agenda
  - Server Utility and Directory Security
  - Network Data Encryption
  - Backup and Restore
  - Discretionary Access Control
  - CLE, LBAC and Views
  - Auditing
  - Future changes
  - Q&A



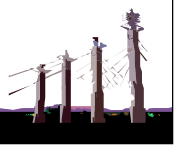
Security with IDS

- Discretionary Access Control (DAC)
  - Primary access control mechanism that enables access to SQL objects using privileges and roles
    - Databases
    - Tables
    - Columns
    - Views
    - Routines
    - Languages



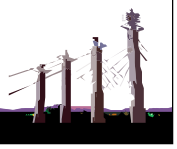
Security with IDS

- Discretionary Access Control (DAC)
  - Security is achieved by granting privileges to the objects
  - When executing an SQL statement, the following is performed in order
    - Check database privileges
    - Check SQL object privileges associated with the query



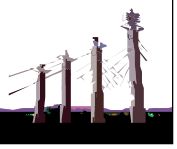
Security with IDS

- Discretionary Access Control (DAC)
  - Database privileges
    - Connect
    - Resource
    - DBA
  - Request is accepted or rejected



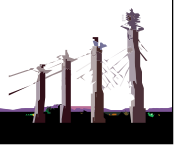
Security with IDS

- Discretionary Access Control (DAC)
  - Next, the object privileges are checked
    - Table (select, update, insert, delete, alter, references, under)
    - View (select, insert, update, delete)
    - Column (select, update, references)
    - Fragment (insert, update, delete)
    - UDT (usage, under)
    - Routine (execute)
    - Language (usage)
    - Sequence (select, alter)



Security with IDS

- Discretionary Access Control (DAC)
  - Grant and Revoke
    - Used to setup what users can and cannot perform on the objects
  - Use Roles
    - A role is a classification of tasks

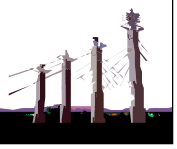


Security with IDS

- Discretionary Access Control (DAC)
  - onconfig DBCREATE_PERMISSION
    - List users permitted to create databases
  - Security for external routine
    - Onconfig IFX_EXTEND_ROLE. If set, users must have extended privileges to register routines

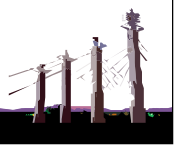
Security with IDS

- Discretionary Access Control (DAC)
  - Spread jobs around
    - Good practice
  - dbsa - Database system administrator
    - maintains and tunes the database
  - dbsso - Database system security officer
    - sets and maintains audit masks
  - aao - Audit analysis officer controls
    - who analyzes audit reports



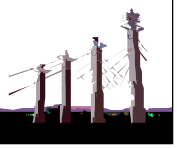
Security with IDS

- Agenda
  - Server Utility and Directory Security
  - Network Data Encryption
  - Discretionary Access Control
  - CLE, LBAC and Views
  - Auditing
  - Future changes
  - Q&A



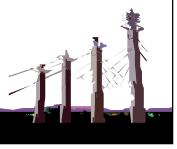
Security with IDS

- CLE, LBAC and Views
  - Restrict data that can been seen
    - Column Level Encryption (CLE)
    - Label Based Access Control (LBAC)
    - Views



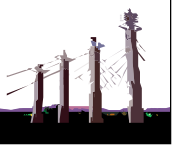
Security with IDS

- CLE, LBAC and Views
  - Used to encrypt specific columns in specific tables. e.g. Salary, bonus or “credit card”
  - This ensures the confidentiality of data
  - A password and cipher is required to see data
  - Hints can be used to remember passwords



Security with IDS

- CLE, LBAC and Views
  - There are two built-in functions to encrypt
    - ENCRYPT_AES() and ENCRYPT_TDES()
  - Secret password can be
    - Globally set
    - Using “set encryption password” SQL statement
    - Within the code at insertion time



Security with IDS

- CLE, LBAC and Views
  - Data types
    - CHAR, VARCHAR, NCHAR, NVARCHAR, LVARCHAR, SMALLINT, INTEGER, INT8, DECIMAL, SMALLFLOAT, FLOAT DATE, DATETIME, INTERVAL, BOOLEAN, BLOB, CLOB
  - There are two built-in functions to decrypt
    - DECRYPT_CHAR() and DECRYPT_BINARY()

Security with IDS

- CLE, LBAC and Views
  - Run a separate VP's named encrypt
  - Password hints can be specified
    - In the encryption function
    - In the "set encryption password" SQL syntax
  - Password retrieval
    - GETHINT() function

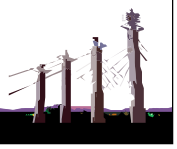
Security with IDS

- CLE, LBAC and Views
  - Sizes

Input Size (bytes)	Triple-DES (no hint)	AES (no hint)	Triple-DES (with hint)	AES (with hint)
1..7	35	43	87	99
8..15	43	43	99	99
16..23	55	67	107	119
24..31	67	67	119	119
32..39	75	87	131	139
40..47	87	87	139	139
100	163	171	215	227
200	299	299	355	355
500	695	707	747	759

Security with IDS

- CLE, LBAC and Views
  - Try to keep the encryption password the same for the column of all rows
  - Do not create an index or a functional index on the encrypted column
  - The encrypted data always requires more space than the unencrypted data

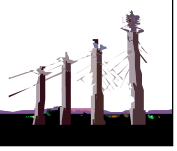


Security with IDS

- CLE, LBAC and Views
  - Security gives peace of mind but comes with a price
    - There will be a performance overhead
      - Encrypting is slower than decrypting
  - If the password is forgotten, the data is lost and support cannot help

Security with IDS

- CLE, LBAC and Views
  - The one area of concern in CLE is the protection of the password
  - Password can be seen within the database as plain text. e.g. In an SPL, so avoid if possible or change on a regular basis
  - Use encrypted communications if possible
  - Set explain will not show the password

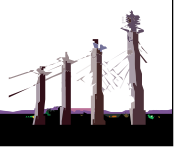


Security with IDS

- CLE, LBAC and Views
  - Label Based Access Control
    - Based on DB2 specifications
  - Works at the column and/or row level
  - Data is not encrypted like CLE
    - (row has a new data type which is encoded)

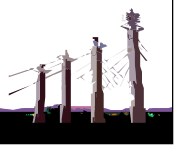
Security with IDS

- CLE, LBAC and Views
  - The aim is allow users to only see data that their level of access permits
  - Avoid data leakage
  - Detailed planning is vital in the setup of LABC and it's best to keep is as simple as possible
  - DBSECADM is king
    - User "informix" is not the admin
    - Creates the building blocks (objects)

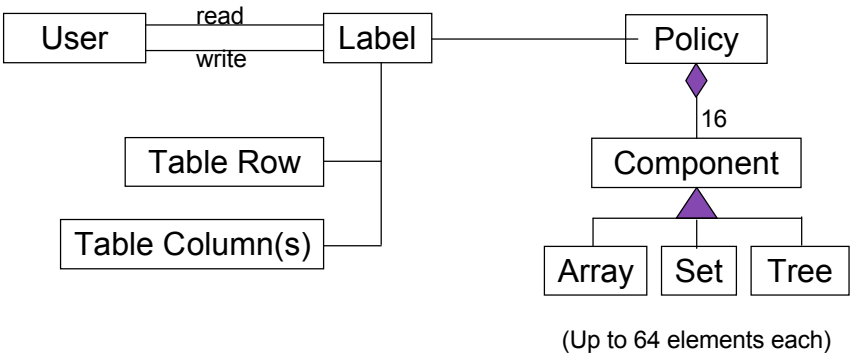


Security with IDS

- CLE, LBAC and Views
  - Main building blocks and steps are
    - Security label components (array, set & tree)
    - Security policies
    - Grant labels to users
    - Configuring tables
    - Using the above building blocks to construct the access for users to the tables
    - Granting exemptions and revoking them



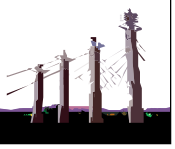
Security with IDS



(Up to 64 elements each)

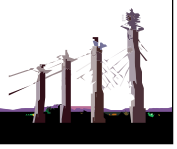
Security with IDS

- CLE, LBAC and Views
  - Security label components
    - There are three different types
      - Array
      - Set
      - Tree
    - Describe different ways to look at the data in conjunction with the business setup or model yiu which to emulate



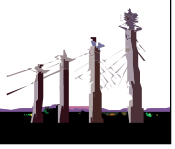
Security with IDS

- CLE, LBAC and Views
  - Security label components
    - ARRAY
      - An ordered set of elements where the importance decreases
      - CREATE SECURITY LABEL COMPONENT classification **ARRAY** ['VP', 'Manager', 'Team Lead', 'Staff'];
      - Maximum of 64 elements



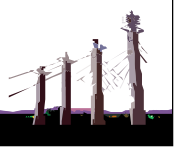
Security with IDS

- CLE, LBAC and Views
  - Security label components
    - SET
      - An unordered set of elements which are of equal importance (groupings)
      - CREATE SECURITY LABEL COMPONENT department **SET** {'Marketing', 'Sales', 'Engineering', 'Finance', 'HR'};
      - Maximum of 64 elements



Security with IDS

- CLE, LBAC and Views
  - Security label components
    - TREE
      - An ordered set of elements which reflects organizational charts
      - CREATE SECURITY LABEL COMPONENT region **TREE** ('HeadQuarters' ROOT,
        'East' UNDER 'HeadQuarters',',
        'West' UNDER 'HeadQuarters',
        'Georgia' UNDER 'East',
        'Florida' UNDER 'East',
        'Atlanta' UNDER 'Georgia');
      - Maximum of 64 elements

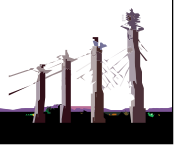


Security with IDS

- CLE, LBAC and Views
  - Security policy
    - Consists of one or more “Security Label Components”
    - Can have up to 16 per policy
    - Databases can have many different policies

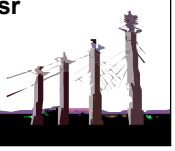
Security with IDS

- CLE, LBAC and Views
  - Security policy
    - CREATE SECURITY POLICY company_policy COMPONENTS region, department, classification;
    - CREATE SECURITY POLICY company_sales COMPONENTS classification, region;



Security with IDS

- CLE, LBAC and Views
  - Security Label
    - Is derived from a “Security Policy”
    - They are assigned to “users”
      - CREATE SECURITY LABEL company_sales.**sales_vp** COMPONENT organization 'VP', COMPONENT region 'HeadQuarters';
      - CREATE SECURITY LABEL company_sales.**sales_rep_wa** COMPONENT organization ‘'Staff”, COMPONENT region ‘Atlanta';
      - CREATE SECURITY LABEL company_policy.**hr_usr** COMPONENT department ‘'HR”;



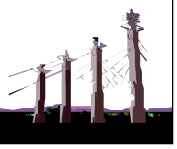
Security with IDS

- CLE, LBAC and Views
  - Granting
    - Assign the “security lables” to actual users
      - GRANT SECURITY LABEL sales_plcy.sales_vp TO "usr1";
      - GRANT SECURITY LABEL sales_plcy.sales_rep TO "usr3" FOR WRITE ACCESS;
      - GRANT SECURITY LABEL sales_plcy.sales_rep_mgr TO "usr3" FOR READ ACCESS;

IDSLBACREADARRAY

Security with IDS

- CLE, LBAC and Views
  - Granting
    - GRANT SECURITY LABEL sales_plcy.sales_rep_mgr TO "usr3" **FOR READ ACCESS**;
    - Available options
      - IDSLBACREADARRAY, IDSLBACREDSET, IDSLBACREADTREE
      - IDSLBACWRITEARRAY [WRITEUP|WRITEDOWN], IDSLBACWRITESET, IDSLBACWRITETREE
      - ALL



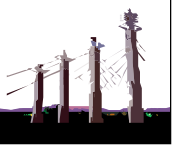
IDSLBACREADARRAY

Security with IDS

- CLE, LBAC and Views
  - Revoke
    - At any time, a “security label” can be revoked
      - REVOKE SECURITY LABEL company_sales.sales_vp FROM "usr1";
  - Exemptions
    - Give a user different credentials for a temporary period
  - SETSESSIONAUTH privilege
    - Allows users to acquire LABC privileges of other users as long as DBSECADM has granted them

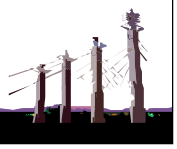
Security with IDS

- CLE, LBAC and Views
  - Protecting Tables
    - The final piece to fit is the link to the table
    - The table can be protected in two ways
      - Columns
        - and/or
      - Rows
    - The table has be associated with a “Security Policy”



Security with IDS

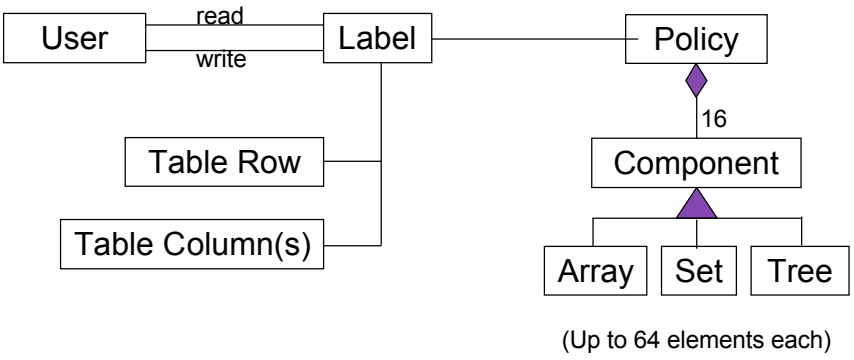
- CLE, LBAC and Views
  - Protecting Tables - Row Protection
    - A new special column of type IDSSECURITYLABEL is required in the tables schema
    - CREATE TABLE sales_data (
      ulabel IDSSECURITYLABEL,
      product CHAR(128) NOT NULL,
      sale_total FLOAT NOT NULL
) **SECURITY POLICY** company_sales;



Security with IDS

- CLE, LBAC and Views
  - Protecting Tables - Column Protection
    - Append “COULMN SECURED WITH” syntax
    - CREATE TABLE hr_data (
      name CHAR(32),
      title CHAR(32),
      salary FLOAT
      COLUMN SECURED WITH hr_usr
) **SECURITY POLICY** company_policy;

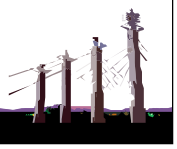
Security with IDS



(Up to 64 elements each)

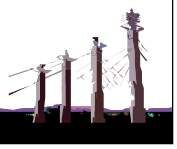
Security with IDS

- CLE, LBAC and Views
  - Built-in Functions
    - Using these functions, users are able to insert data labels in tables that are not equivalent to their WRITE labels
      - seclabel_by_comp()
      - seclabel_by_name()
      - seclabel_to_char()
        - Decrypts the value to readable form



Security with IDS

- CLE, LBAC and Views
  - Example
    - CREATE SECURITY LABEL COMPONENT classification ARRAY [‘VP', ‘Manager’, ‘Team Lead', ‘Staff'];
    - select * from tab;
      - Which is row level protected
    - The “VP” will see all the rows
    - The “Staff” will only see what their level permits
    - There is no indication to the “Staff” that there were less rows returned – it’s transparent

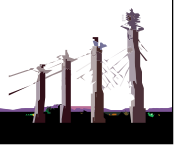


Security with IDS

- CLE, LBAC and Views
  - Can achieve something similar to LBAC in presenting data to users but is not as comprehensive
  - Have to code applications so that users see the correct views

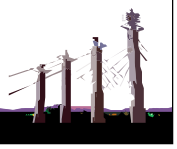
Security with IDS

- Agenda
  - Server Utility and Directory Security
  - Network Data Encryption
  - Backup and Restore
  - Discretionary Access Control
  - CLE, LBAC and Views
  - Auditing
  - Future changes
  - Q&A



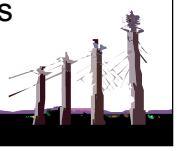
Security with IDS

- Auditing.
  - Attempts can be made to circumnavigate the restrictions implemented
  - Switch on and use IDS auditing. Although this is an “after the event” tool, it can be used to analyze the audit trials to see if there have been attempted breaches



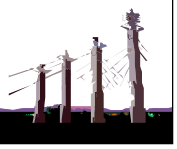
Security with IDS

- Auditing.
  - Configuration
    - $INFORMIXDIR/aaodir/adtcfg
      - ADTMODE 1
      - ADTPATH /work/aaodir
      - ADTSIZE 5000000
      - ADTERR 0
    - Values take affect on start-up of engine
    - The onaudit utility allows dynamic changes



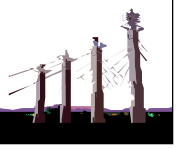
Security with IDS

- Auditing.
  - Each required database operation has an associated four or five letter event
    - CRTB = create table (successful or not)
    - SCRTB = successful create table
    - FCRTB = failed create table
  - Choose the ones to be enabled by using “audit masks” and different masks can be applied to different users



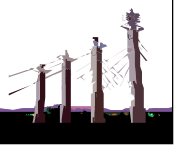
Security with IDS

- Auditing.
  - Choose the events to be audited by enabling "audit masks"
  - Different masks can be applied to different users. These are
    - Template, user, default, require, & exclude
  - Masks make admin for the dbsso easier



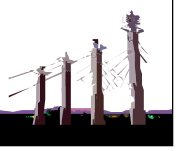
Security with IDS

- Auditing.
  - To ensure no abuse of the auditing, you should have an aao and dbsso where the
    - aao uses onaudit to setup the configuration
    - dbsso uses onaudit to set up the masks
    - dbsa runs the server and should not be involved in the auditing



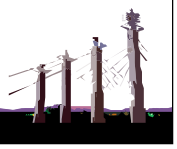
Security with IDS

- Auditing.
  - What information can be seen ?
    - Instance tag
    - Time stamp
    - Host name
    - Process ID
    - Server name
    - User name
    - Event specific information



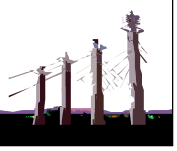
Security with IDS

- Auditing.
  - onshowaudit can be used to see details within the log
    - -l : read all audit log files identified by ADTPATH
    - -f : read a specific log file
    - -u : only show details for a specific user
    - -s : specific a server



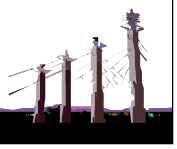
Security with IDS

- Auditing.
  - The output is pipe delimited and so can be easily loaded into a table if required
    - CREATE TABLE aud_tab (
      - instance CHAR(5),
      - timestamp DATETIME YEAR TO FRACTION(3),
      - host CHAR(32),
      - pid INT,
      - server CHAR(32),
      - username CHAR(32),
      - errno INT,
      - event_code CHAR(5),
      - database CHAR(128),
      - eventinfo CHAR(2048)
      -);



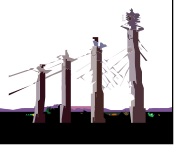
Security with IDS

- Auditing.
  - There are a few considerations to take on board and these are governed by how much you want to audit
    - Disk space
    - System performance
    - Administration overhead
    - Avoid some events like RDRW



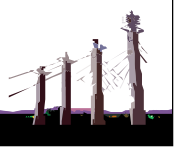
Security with IDS

- Auditing.
  - sysdbopen and sysdbclose
    - Built-in procedures that can execute an SPL
    - Could be used as a simple identifier
      - Store in a table users connecting an exiting



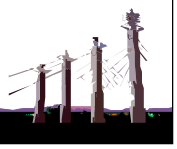
Security with IDS

- Agenda
  - Server Utility and Directory Security
  - Network Data Encryption
  - Discretionary Access Control
  - Column level encryption and LBAC
  - Auditing
  - Future changes
  - Q&A



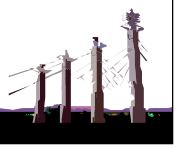
Security with IDS

- Future changes
  - Secure Socket Layer (SSL)
  - Single Sign On (SSO)
  - Password Management



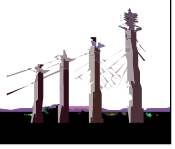
Security with IDS

- Future changes
  - Secure Socket Layer (SSL)
  - Single Sign On (SSO)
  - Password Management



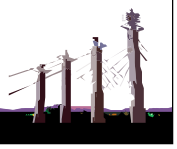
Security with IDS

- Secure Socket Layer (SSL)
  - Encrypted communications is currently only possible with CSM (ENCCSM)
  - SSL will provide end-to-end secure communication for SQLI and DRDA clients
    - (Only possible way for DRDA)
  - The aim is to have a communication protocol that provides privacy and integrity for data communication over the network



Security with IDS

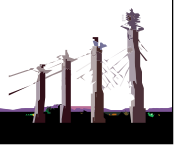
- Secure Socket Layer (SSL)
  - Uses digital certificates
    - Electronic ID cards issued by trusted parties known as a Certificate Authority (CA)
  - This feature uses digital certificates to
    - Exchange keys for encryption
    - Server authentication
    - Client authentication (optional)



VeriSign.

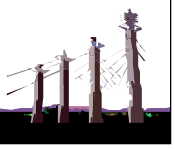
Security with IDS

- Secure Socket Layer (SSL)
  - There are two types of keys
    - Public key
      - Known to everyone
    - Private (secret) key
      - Known only to the recipient



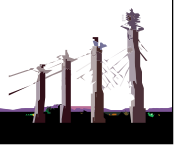
Security with IDS

- Secure Socket Layer (SSL)
  - What's supported
    - DRDA clients
      - JCC (SQLJ & DB2 JDBC) and DB2 CLI
    - SQLI clients
      - CSDK (ESQLC & JDBC)
    - IDS utilities
      - dbaccess, dbexport, dbimport, dbschema & dbload
    - ER, HDR, SDS & RSS, I-Star



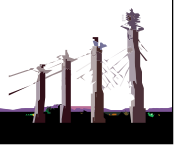
Security with IDS

- Secure Socket Layer (SSL)
  - Unsupported
    - oncheck, onspaces, HPL & MaxConnect
  - Caveats
    - PAM and SSO can be configured
    - CSM will be disabled for all other communications as SSL is an alternative



Security with IDS

- Secure Socket Layer (SSL)
  - Data going back and forth between a client and server is encrypted using a symmetric key (secret/private) algorithm
  - An asymmetric key (public) algorithm is used for the exchange of secret keys in the symmetric algorithm and for digital signatures
  - The asymmetric key algorithm uses the public key in the servers digital certificate
  - With the server's digital certificate, the client can also verify the server's identity

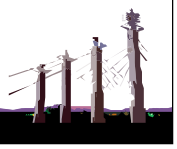


Security with IDS

- Secure Socket Layer (SSL)
  - The Public key is used to encrypt information
  - The Private key is used to decrypt information
  - If the client and server handshaking is successful, a unique key is established and the two sides can communicate securely

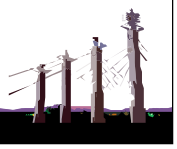
Security with IDS

- Secure Socket Layer (SSL)
  - Digital certificates are stored in a key database (also known as a keystore)
  - The keystore is protected by a password
  - The sever side needs to know the password to retrieve a digital certificate
  - The password is encrypted within a file located by a new onconfig parameter



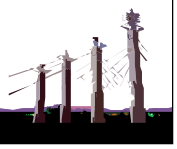
Security with IDS

- Secure Socket Layer (SSL)
  - IBM's Global Security Kit bundled with the IDS server and client provides an iKeyman utility that can be used to create keystores and manage digital certificates



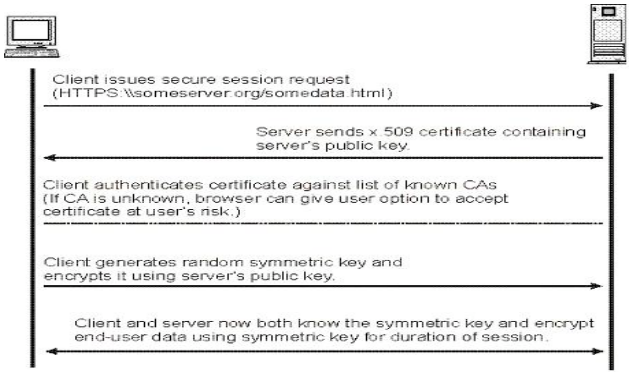
Security with IDS

- Secure Socket Layer (SSL)
  - Both client and server must have a keystore for housing digital certificates
  - Server side keystore will store digital certificate issued (or signed) by Certificate Authority
  - Client side keystore will store digital certificate of Certificate Authority (also called root certificate) that issued the server digital certificate



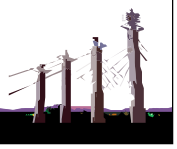
Security with IDS

- Secure Socket Layer (SSL)



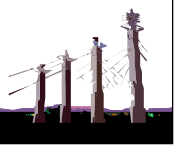
Security with IDS

- Secure Socket Layer (SSL)
  - Server side
    - New parameter
      - SSL_KEYSTORE_LABEL
        - Default is ids_label if not set
    - Changes to existing parameters
      - NETTYPE
        - (allow ssl protocol)



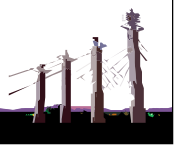
Security with IDS

- Secure Socket Layer (SSL)
  - Server side
    - New files
      - keystore file ($INFORMIXDIR/ssl/<svr_name>.kdb
      - keystore stash file ($INFORMIXDIR/ssl/<svr_name>.sth
    - These filenames and locations are fixed
    - The ownership/permissions of above files must be informix:informix and 600



Security with IDS

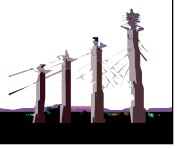
- Secure Socket Layer (SSL)
  - Client side
    - New files
      - Keystore file & Keystore stash file
    - Location is not fixed
      - Uses $INFORMIXDIR/etc/conssl.cfg and contains
        - SSL_KEYSTORE_FILE
        - SSL_KEYSTORE_STH
      - If not set, defaults are
        - $INFORMIXDIR/etc/client.kd and client.sth



Security with IDS

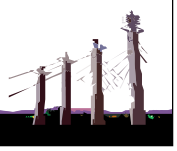
- Secure Socket Layer (SSL)
  - New connection protocol
    - drsocssl protocol for supporting SSL communication with DRDA clients
    - onsocssl/olsocssl protocol for supporting SSL communication with SQLI clients

```
lenexa_on     onsoctccp   server  lenexa_serv
menlo_on      onsocssl    server  menlo_serv
portland_on   drsocssl    server  portland_serv
```



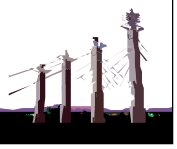
Security with IDS

- Secure Socket Layer (SSL)
  - IBM's Global Security Kit bundled with the IDS server and client provides an iKeyman utility
  - The iKeyman utility that can be used to create keystores and manage digital certificates needed for SSL communication
  - More information on iKeyman is available at
    - w3-03.ibm.com/software/sales/saletool.nsf/resources/GSKITiKeyman/$file/GSK7c_SSL_Ikm_Guide.pdf



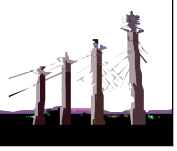
Security with IDS

- Secure Socket Layer (SSL)
  - Prerequisites for iKeyman utility
    - IBM JDK/JRE 1.3.1, 1.4.1 or higher with JCE PKS Security packages
  - Environment for iKeyman utility
    - export JAVA_HOME=<JDK/JRE installation>
    - export PATH=$JAVA_HOME/jre/bin:$PATH
    - export CLASSPATH=<GSKit installation>/classes/cfwk.zip:<GSKitinstallation>/classes/gsk7cls.jar:$JAVA_HOME/jre/lib/ext/ibmpkcs11.jar



Security with IDS

- Secure Socket Layer (SSL)
  - Sample commands for creating keystore and self-signed test certificates using iKeyman command line utility:
  - Server Keystore
    - gsk7cmd -keydb -create -db menlo_on.kdb -pw snoopy -type cms -stash
    - gsk7cmd -cert -create -db menlo_on.kdb -pw snoopy -label ids_label -dn "CN=menlo.ibm.com,O=ibm,C=US" -size 1024 -default_cert yes
    - gsk7cmd -cert -extract -db menlo_on.kdb -format ascii -label ids_label -pw snoopy -target ids_label.cert
      - where DBSERVERNAME is menlo_on
      - SSL_KEYSTORE_LABEL is ids_label



Security with IDS

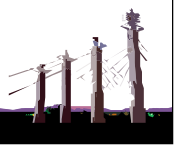
- Secure Socket Layer (SSL)
  - Sample commands for creating keystore and self-signed test certificates using iKeyman command line utility
  - Client Keystore
    - gsk7cmd -keydb -create -db client.kdb -pw snoopy -type cms -stash
    - gsk7cmd -cert -add -db client.kdb -pw snoopy -label ids_label -file ids_label.cert -format ascii

Security with IDS

- Future changes
  - Secure Socket Layer (SSL)
  - Single Sign On (SSO)
  - Password Management

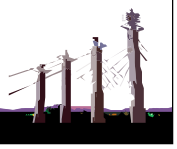
Security with IDS

- Single Sign On (SSO)
  - Currently
    - Users log on to a system with a user name and password
    - The user has to provide the user name and password to authenticate to other applications
    - password management and administration can be consuming



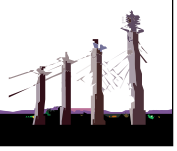
Security with IDS

- Single Sign On (SSO)
  - IDS has two authentication methods
    - Traditional use of OS facilities
    - PAM/LDAP
  - We now have a third alternative !



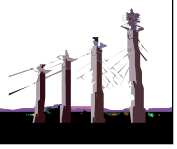
Security with IDS

- Single Sign On (SSO)
  - This is an authentication mechanism which allows users to enter the password once …
    - (the authentication part)
  - … to gain access to other resources
    - (computers & software systems)
  - Easy administration because you have one central location where all user names and passwords are maintained



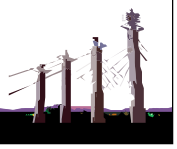
Security with IDS

- Single Sign On (SSO)
  - IDS uses Kerberos for SSO support
    - Kerberos is one of many SSO solutions in the market place
  - It is based on an open standard
  - It is essentially a secure network authentication protocol



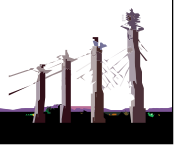
Security with IDS

- Single Sign On (SSO)
  - Uses shared security keys
  - Passwords are never flown on the wire
  - The server and client can authenticate one another (mutual authentication)
  - Requires a trusted third entity
    - Key Distribution Centre (KDC)
      - This contains all the keys



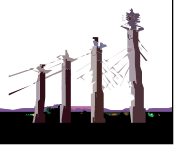
Security with IDS

- Single Sign On (SSO)
  - Kerberos also provides
    - Single point of failure
    - Denial of service attacks (DOS)
    - Dictionary attacks of weak passwords
    - And many more …
  - SSO can be used with web applications



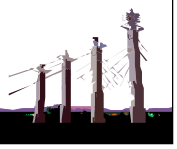
Security with IDS

- Single Sign On (SSO)
  - How does it work
    - A user logging on to the client machine using a domain account, authenticates to the Kerberos key distribution centre (KDC)
    - The KDC issues a ticket-granting ticket (TGT) to the client with a limited lifetime (typically 8-12 hours)



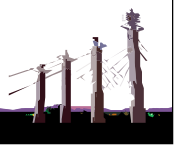
Security with IDS

- Single Sign On (SSO)
  - How does it work - continued
    - During the first phase of the connection, the server sends the target principal name, which is the service account name for the IDS server service, to the client
    - Using the server's target principal name and the target-granting ticket, the client requests a service ticket from the ticket-granting service (TGS) which also resides at the domain controller (KDC)



Security with IDS

- Single Sign On (SSO)
  - How does it work - continued
    - If both the client's ticket-granting ticket and the server's target principal name are valid, the TGS issues a service ticket to the client
    - The principal name recorded in the database directory may now be specified as name/instance@REALM

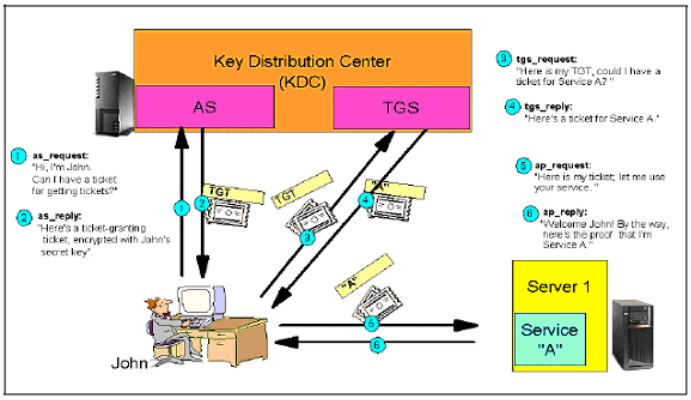


Security with IDS

- Single Sign On (SSO)
  - How does it work - continued
    - The client sends this service ticket to the server
    - The server validates the client's server ticket
    - If the client's service ticket is valid, then the authentication is completed

Security with IDS

- Single Sign On (SSO)

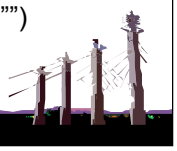


Security with IDS

- Single Sign On (SSO)
  - Configuration – IDS
    - Setup alias in $INFORMIXDIR/etc/$ONCONFIG
    - sqlhosts option field (column five) set to “s=7” along with GSSCSM as the csm module
    - Configure $INFORMIXDIR/etc/oncsm.cfg file

Security with IDS

- Single Sign On (SSO)
  - Configuration – IDS
    - $INFORMIXDIR/etc/$ONCONFIG
      - DBSERVERNAME on_demo
      - DBSERVERALIAS on_sso
    - $INFORMIXDIR/etc/sqlhosts
      - on_demo onscotcp svr on_demo_serv
      - on_sso onsoctcp svr sso_serv s=7, csm=(GSSCSM)
    - $INFORMIXDIR/etc/concsm.cfg
      - GSSCSM(“/usr/informix/lib/csm/igss11a.so”,””,””)



Security with IDS

- Single Sign On (SSO)
  - Configuration – Unix
    - Server
      - $INFORMIXDIR/lib/csm/igsss11a.so
      - $INFORMIXDIR/lib/csm/libixgss.so
    - Client
      - $INFORMIXDIR/lib/csm/client/igsss11a.so
        $INFORMIXDIR/lib/csm/libixgss.so

Security with IDS

- Single Sign On (SSO)
  - Configuration – Windows
    - Server
      - $INFORMIXDIR/bin/igsss11a.dll
        $INFORMIXDIR/bin/libixgss.dll
    - Client
      - $INFORMIXDIR/lib/client/csm/igsss11a.dll
      - $INFORMIXDIR/lib/client/csm/libixgss.dll

Security with IDS

- Single Sign On (SSO)
  - Configuration – Kerberos
    - Some requirements
      - Clients and server machines must belong to same realm (or trusted)
      - Creation of a server keytab if appropriate
      - All machine clocks to be synchronized
        - 5 minute skew permitted
      - Refer to the Kerberos documentation for full details

Security with IDS

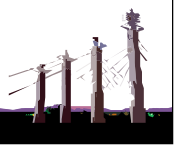
- Single Sign On (SSO)
  - The Generic Security Services Application Programming Interface (GSSAPI) is a generic API RFC 2743 for client server communication specifically used for authentication
  - Kerberos is an Internet Engineering Task Force (IETF) standard RFC 1510 that defines a typical key exchange mechanism
  - Applications can use the Kerberos service to authenticate their users and exchange cryptographic keys with them
  - Included with most major Kerberos 5 distributions is a GSSAPI implementation. Thus, if a particular application or protocol says that it supports the GSSAPI, then that means that it supports Kerberos

Security with IDS

- Future changes
  - Secure Socket Layer (SSL)
  - Single Sign On (SSO)
  - Password Management

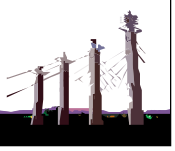
Security with IDS

- Password Management
  - An encrypted password file is required for the running of the “connection manager” (CM)
    - CM is used in MACH11 and consists of SLA’s to route a client to an appropriate server
      - Primary, Secondary, SDS or RSS
  - Users can connect easily to multiple nodes without the need to be trusted
  - Can also be used with CDR



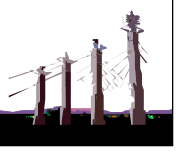
Security with IDS

- Password Management
  - onpassword program
    - Only the user “informix” can run this command
    - Used to encrypt a plain text password file into an encrypted password file
    - Details stored in $INFORMIXDIR/etc/passwdfile
    - Can be used to decrypt the file to create a plain text file again



Security with IDS

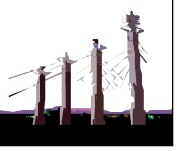
- Password Management
  - onpassword -k *access_key*
    - [-e *plaintext_file* | -d *output_filename*]
  - access_key can be up to 24 characters long
    - If lost or forgotten, then decrypting the file will not be possible
    - If you want to amend the details, a new plain text file will be needed



Security with IDS

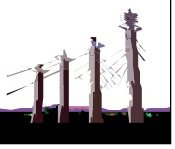
- Password Management
  - The plain input file is an ASCII text file with the following structure

```
ServerName_1   AlternateServer_1   UserName_1   Password_1
ServerName_2   AlternateServer_2   UserName_2   Password_2
```



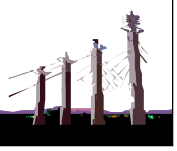
Security with IDS

- Password Management
  - AlternateServer specifies the name of an alternate server to connect with in case the connection cannot be made to ServerName
  - AlternateServer name is used when ServerName is a located on a secure port (e.g. using the s=6 option in the sqlhosts file)



Security with IDS

- Agenda
  - Server Utility and Directory Security
  - Network Data Encryption
  - Discretionary Access Control
  - Column level encryption and LBAC
  - Auditing
  - Future changes
  - Q&A



Security with IDS

Session A07
Security with IDS

Rob Jane
IBM
robert.jane@uk.ibm.com