Auditing Encryption in Oracle Databases

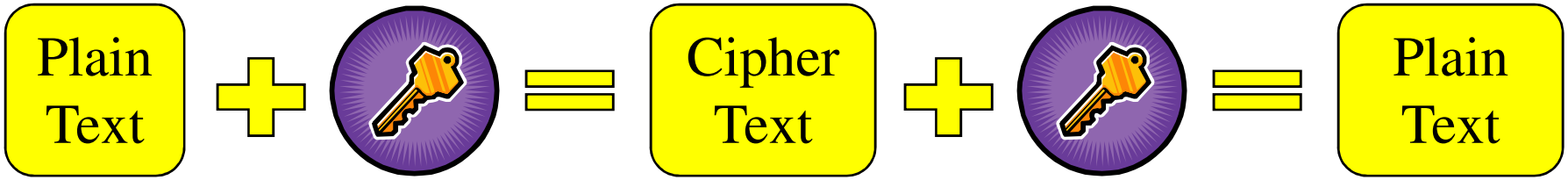
Prepared and presented by: Tanya Baccam
SANS Institute – Senior Certified Instructor
CPA, CITP, CISSP, CISA, CISM, GSEC, GPPA, GCIH, OCP DBA
Baccam Consulting LLC
www.securityaudits.org

Objectives

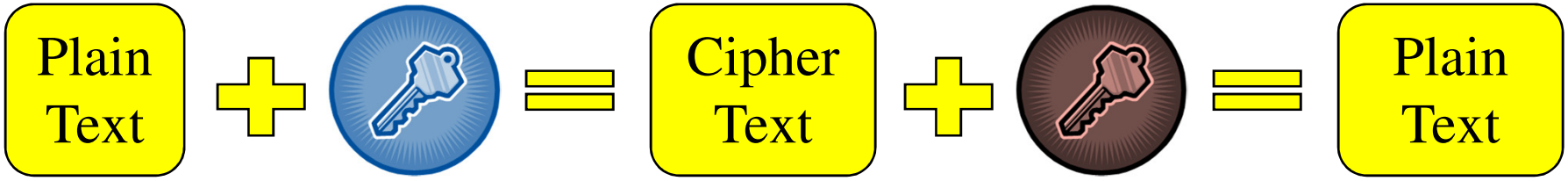
- Encryption 101
- Common Reasons Encryption is Used
- Options for encryption
- Questions auditors should ask

Crypto Algorithms

- Symmetric
  - A single key for encryption and decryption



- Asymmetric
  - A different key for encryption and decryption



- Hashing
  - "One-way" cryptosystems

Symmetric Algorithms

- Secret key, single key, one key
- Advantage
  - Faster
- Disadvantage
  - Key management
- Examples
  - DES
  - AES

Asymmetric Algorithms

- Public key crypto
- Susceptible to "man-in-the-middle" attacks
- Common uses
  - Digital signatures
  - Protect the symmetric key
- Example
  - RSA
  - El Gamal

Hashing Algorithms

- "One way" encryption
- Message digest
- Common uses
  - Password hashes
  - Improve efficiencies of digital signatures
  - Ensure data integrity
- Examples
  - SHA
  - MD5

Encrypting Data in Different States

- Consider whether controls should exist for data in transit
  - Across the network
- Consider whether controls should exist for data at rest
  - Database
  - Backups

Common Reasons to Encrypt

- Protect the data from _____
- Compliance/Legislative Requirements
- Additional "security"

Common Reasons Not to Encrypt

- Performance impacts
- Alternative encryption options
- Key Management
- Data availability

Data to Encrypt

- Financial data
  - Credit card account numbers and tracking data, bank account numbers, credit-related data
- Personal health data
  - Insurance-related data, actual medical information
  - Personal data about patients - social security numbers, addresses, and other sensitive information
- Private individual data
  - Username, password, Social security numbers, tax ID, email address, employer, spouse's name, phone number, bank account info addresses and phone numbers, and other personally-identifiable data
- Military and government data
  - Data specific to government programs - military departments and operations
- Confidential/sensitive business data
  - Data that has to be kept secret including trade secrets, research and business intelligence data, management reports, customer information, sales data, etc.

Key Options for Data

- Different key for each record
  - Key is calculated
- Same key for all records
  - User
  - File system
  - Database

Oracle Encryption Options

- dbms_obfuscation_toolkit
  - Oracle 8i/9i
  - DES and 3DES
- dbms_crypto
  - Oracle 10g
  - DES, 3DES, AES, RC4
- Oracle Advanced Security
  - Transparent Data Encryption
    - Oracle 10g, R2 and later
- Enterprise Edition
  - Network Encryption
- Of course, third party solutions and other alternatives exist too
  - Tokenization
  - Application encryption
  - File/Disk encryption

dbms_crypto versus dbms_obfuscation_tookit

Functionality	dbms_crypto	dbms_obfuscation
Cryptographic algorithms	DES, 3DES, AES, RC4, 3DES_2KEY	DES, 3DES
Block cipher chaining modes	CBC, CFB, ECB, OFB	CBC
Cryptographic hash algorithms	MD5, SHA-1, MD4	MD5
Key hash (MAC) algorithms	HMAC_MD5, HMAC_SH1	None
Cryptographic pseudo-random number	RAW, NUMBER, BINARY_INTEGER	RAW, VARCHAR2
Database types	RAW, CLOB, BLOB	RAW, VARCHAR2

dbms_obfuscation Example (1)

```
create or replace function encrypt (lv_data in
   varchar2,lv_key in varchar2)
return varchar2
is
   encrypt_str long;
begin
   encrypt_str:=dbms_obfuscation_toolkit.desencrypt(inp
   ut_string => lv_data,
       key_string => lv_key);
   return encrypt_str;
end;
/
```

dbms_obfuscation Example (2)

```
create or replace function decrypt (lv_data in
   varchar2,lv_key in varchar2)
return varchar2
is
   decrypt_str long;
begin
   decrypt_str:=dbms_obfuscation_toolkit.desdecrypt(inp
   ut_string => lv_data,
       key_string => lv_key);
   return decrypt_str;
end;
/
```

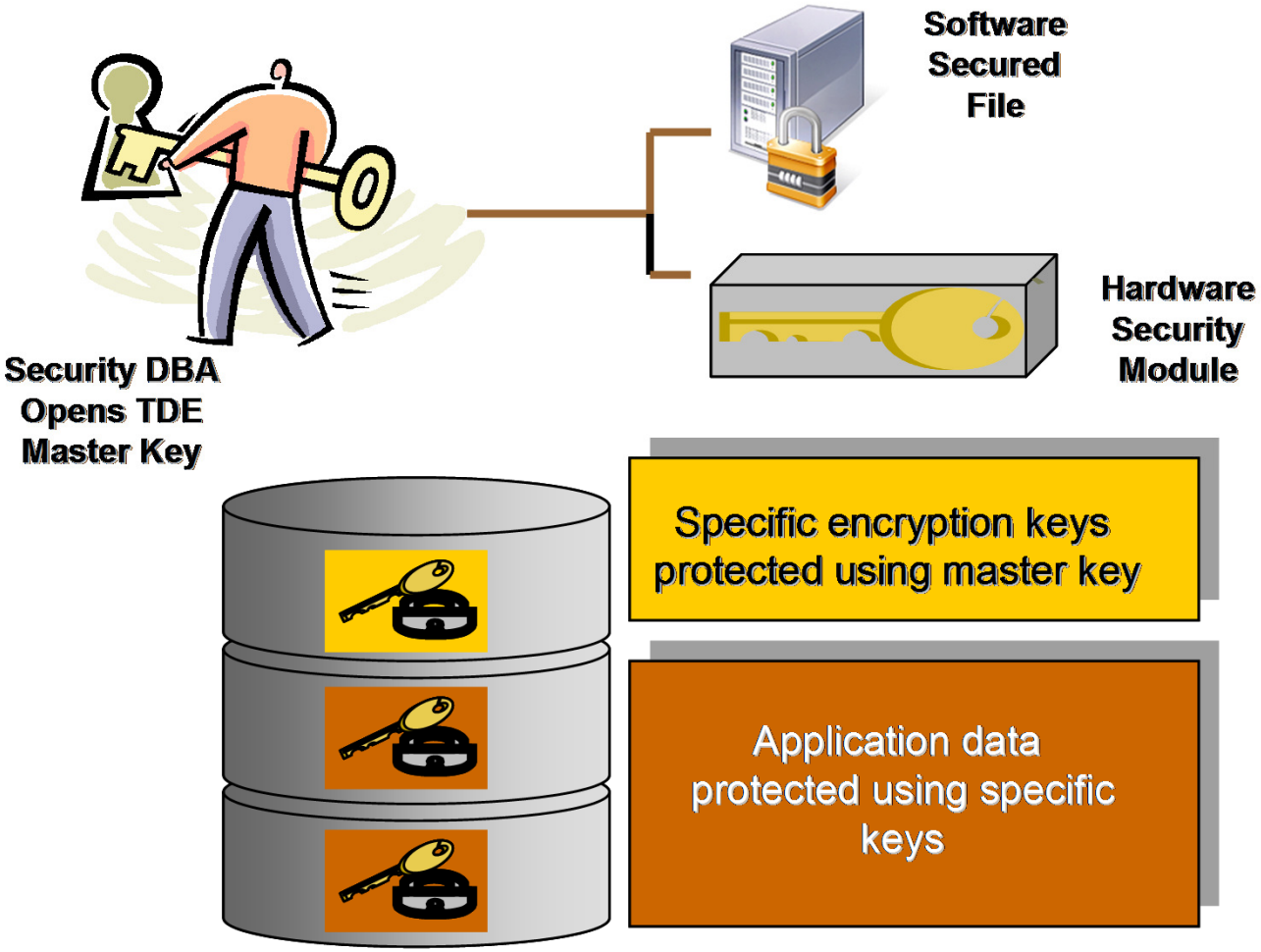
Transparent Data Encryption

- Part of Oracle Advanced Security
  - Available in 10gR2 and later
  - 11gR1 supports tablespace encryption
- Encrypts data transparently
  - No writing code is necessary
- Key Management done by the Oracle DB
- Backups can also be encrypted
  - Data Pump automatically decrypts before storing
  - Data Pump can store the data encrypted
- TDE master key can be stored externally on a hardware security module (HSM)
- Verification
  - V$ENCRYPTED_TABLESPACES
    - What tablespaces are encrypted
  - DBA_ENCRYPTED_COLUMNS
    - Algorithms used to encrypt columns

TDE Column Encryption Process

- Define a column to be encrypted
  - TDE uses salts by default
  - Can optionally disable the salt
- Oracle creates a cryptographically secure encryption key for the table containing the column
- Oracle encrypts the clear text data in that column
- Table key is encrypted with a master key
- Master key is stored in a wallet
  - Wallet is protected with a password
- Encrypted table keys are placed in the data dictionary

TDE Example


Software
Secured
File
Hardware
Security
Module
Security DBA
Opens TDE
Master Key
Specific encryption keys
protected using master key
Application data
protected using specific
keys

Tablespace versus Column Encryption

- When to use Tablespace Encryption
  - Difficult to identify all sensitive data
  - Encrypting a lot of data
  - Need to transport tablespaces
  - Available as of 11g
- When to use Column Level Encryption
  - Only encrypting a few columns
  - Limited amount of sensitive data
- Consider how to re-keying the table and/or master keys

Tcpdump

- /usr/sbin/tcpdump -i eth0 -s 0 host 10.10.10.15 and not port 23 -w testXX.dmp
- /usr/sbin/tcpdump -r testXX.dmp -X -n | grep -B 10 -A 10 ALTER

```
00:57:11.244003 IP 10.10.10.15.1061 > 10.10.10.10.1521: P 5825:6021(196) ack 624
1 win 17149
        ox0000:  4500 00ec 2e03 4000 8006 a3dc 0a0a 0a0f  E.....@.........
        0x0010:  0a0a 0a0a 0425 05f1 aec2 0339 4bb7 b04a  .....%.....9K..J
        0x0020:  5018 42fd c189 0000 00c4 0000 0600 0000  P.B.............
        0x0030:  0000 035e 1b21 8000 0000 0000 00f0 3053  ...^.!........0S
        0x0040:  0626 0000 004c 3651 060d 0000 0000 0000  .&...L6Q........
        0x0050:  0080 3651 0600 0000 0001 0000 0000 0000  ..6Q............
        0x0060:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x0070:  0000 0000 0000 0000 0082 3651 0684 3d53  ..........6Q..=S
        0x0080:  0600 0000 0000 0000 0000 0000 0090 3651  ..............6Q
        0x0090:  0626 414c 5445 5220 5553 4552 2074 6573  .&ALTER.USER.tes
        0x00a0:  7430 3120 4944 454e 5449 4649 4544 2042  t01.IDENTIFIED.B
        0x00b0:  5920 7465 7374 3031 0100 0000 0100 0000  Y.test01........
        0x00c0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x00d0:  0000 0000 0700 0000 0000 0000 0000 0000  ................
        0x00e0:  0000 0000 0000 0000 0000 0000            ............
00:57:11.283424 IP 10.10.10.10.1521 > 10.10.10.15.1061: . ack 6021 win 16060
        0x0000:  4500 0028 ec17 4000 4006 268c 0a0a 0a0a  E..(..@.@.&.....
        0x0010:  0a0a 0a0f 05f1 0425 4bb7 b04a aec2 03fd  .......%K..J....
        0x0020:  5010 3ebc 9014 0000                      P.>.....
00:57:11.542444 IP 10.10.10.10.1521 > 10.10.10.15.1061: P 6241:6352(111) ack 602
1 win 16060
```

Network Encryption

- Can force encryption for communication with the database
- Must be configured on the client and server side

	Rejected	Accepted	Requested	Required
Rejected	OFF	OFF	OFF	ORA-12660
Accepted	OFF	OFF	ON	ON
Requested	OFF	ON	ON	ON
Required	ORA-12660	ON	ON	ON

- Options such as SSH, OpenSSL could also be used

Alternatives to Encryption for Data at Rest

- Tokenization
  - Representation of the data
- Obfuscation
  - Only store a portion of the data
- Redaction

Oracle Data Redaction

- Selective, on-the-fly redaction of data in SQL results
- Conducted in the database so the app doesn't need extensive changes
- Policies are created
- Example
  - Change SS# to ***-**-1234 or 999-99-1234

Encryption Audit Questions

- How is encryption used? Are third-party solutions used?
- When is the data being encrypted? When is the data not being encrypted?
- What data is being encrypted? What data is not being encrypted?
- What are the classification policies and requirements for encryption?
- What are the database development standards related to encryption?
- What algorithms are being used?
- What is the key length?
- How is the key being protected? How is the key being monitored?

Audit Procedures (1)

- Review the organization's information security policy to determine whether it provides sufficient guidance in information classification and application of encryption.
- Review and test the encryption software to assess whether it adequately supports the information security policy and information classification.
- Review and test key management procedures to assess their adequacy in supporting the information security policy.
- Review the points of decryption and assess whether data custodians and owners are aware of the need for compensating controls.
- Review user procedures and interview selected users to determine whether encryption is effectively applied.

Source: http://www.isaca.org/Journal/archives/2004/Volume-3/Pages/What-Auditors-Should-Know-About-Encryption.aspx

Audit Procedures (2)

- Review contracts with certificate authorities and other service organizations to assess whether responsibilities and obligations are clearly understood.
- Where applicable, review the external control assurance report on CAs and other service organizations.
- Review the extent of deployment of encryption in relation to statutory requirements and expectations.
- Review procedures and infrastructure controls for wireless networks to assess whether encryption provides comparable security wired networks.
- Review procedures and infrastructure controls for mobile devices to assess whether encryption provides comparable security to workstations.

Source: http://www.isaca.org/Journal/archives/2004/Volume-3/Pages/What-Auditors-Should-Know-About-Encryption.aspx

Encrypting

- Look at business needs and requirements
- Consider what encryption may not provide
  - Does not solve access control issues
  - Can not prevent DBA access
  - Not an "automatic" security solution
- Verify where and how encryption is being used

Summary

- Understanding encryption is critical to protecting data
- Use encryption based on business requirements
- Multiple options for encryption exist
- There are key questions an auditor should ask
- Don’t forget there are many more components to Oracle database security!

Courses

- Auditing Active Directory/Windows in Dallas, TX
  - October 12-14, 2015
  - http://www.securityaudits.org/adw102015.html
- Auditing Network Security in Dallas, TX
  - November 2-4, 2015
  - http://www.securityaudits.org/network112015.html
- CISSP
  - Beginning of 2016
  - http://www.securityaudits.org/events.html
- Additional courses
  - www.securityaudits.org/events.html
  - https://www.sans.org/instructors/tanya-baccam

Thank you!

Prepared and presented by: Tanya Baccam
SANS Institute – Senior Certified Instructor
CPA, CITP, CISSP, CISA, CISM, GSEC, GPPA, GCIH, OCP DBA
Baccam Consulting LLC
www.securityaudits.org