08
PM
PERFORMANCE
MATTERS
Performance Matters!
John Matherson, honors degree, economics.
A research project on sustainable development.
A career in government policy.

Applying Data Encryption To Banner

Presented by: David de Manbey
University of Hartford

April 14 2008

Course ID S-0061

Presentation Objectives

- Summarize the need to encrypt Banner data.
- Describe which types of data need to be encrypted and where to find it within the Banner system.
- Outline basic encryption methods including:
  - add-ons supplied by Oracle
  - third party vendor encryption software
- Provide a Q & A forum for Banner encryption

Presentation Summary

Making A Case For Encryption

Standard Oracle Encryption Tools

Transparent Encryption & Third Party Vendors

Banner Data Needing Encryption

Case Study: University of Hartford Encryption Project

What You Wished Someone Told You Before You Started

08
PM
PERFORMANCE
MATTERS
Performance Matters!
Ron O'Connell, theater professor
Founder, All the World's a Stage,
a showcase for original student work.

Making A Case For Encryption

Do I really have to encrypt my data?

Making A Case For Encryption

What is the cost of identity theft associated with ssn?

In 2007:

- **9.9 million Americans victims of identity theft and SSN Fraud**
- **48 billion worth of costs to us**
- **5 billion in losses to victims, in the USA alone.**

Making A Case For Encryption

Schools Reporting A Breach:

U. of Ca. - Berkley	2005	98,400
Boston College	2005	120,000
Tufts	2005	106,000

Schools in Ct: UConn, State College System, Community Colleges, Yale, Sacred Heart, & Fairfield

USC	2005	270,000
U. of Notre Dame	2006, 2007	unknown
Purdue	2005, 2006(2), 2007(2)	
U. of Ca. – L.A.	2006	800,000

Making A Case For Encryption

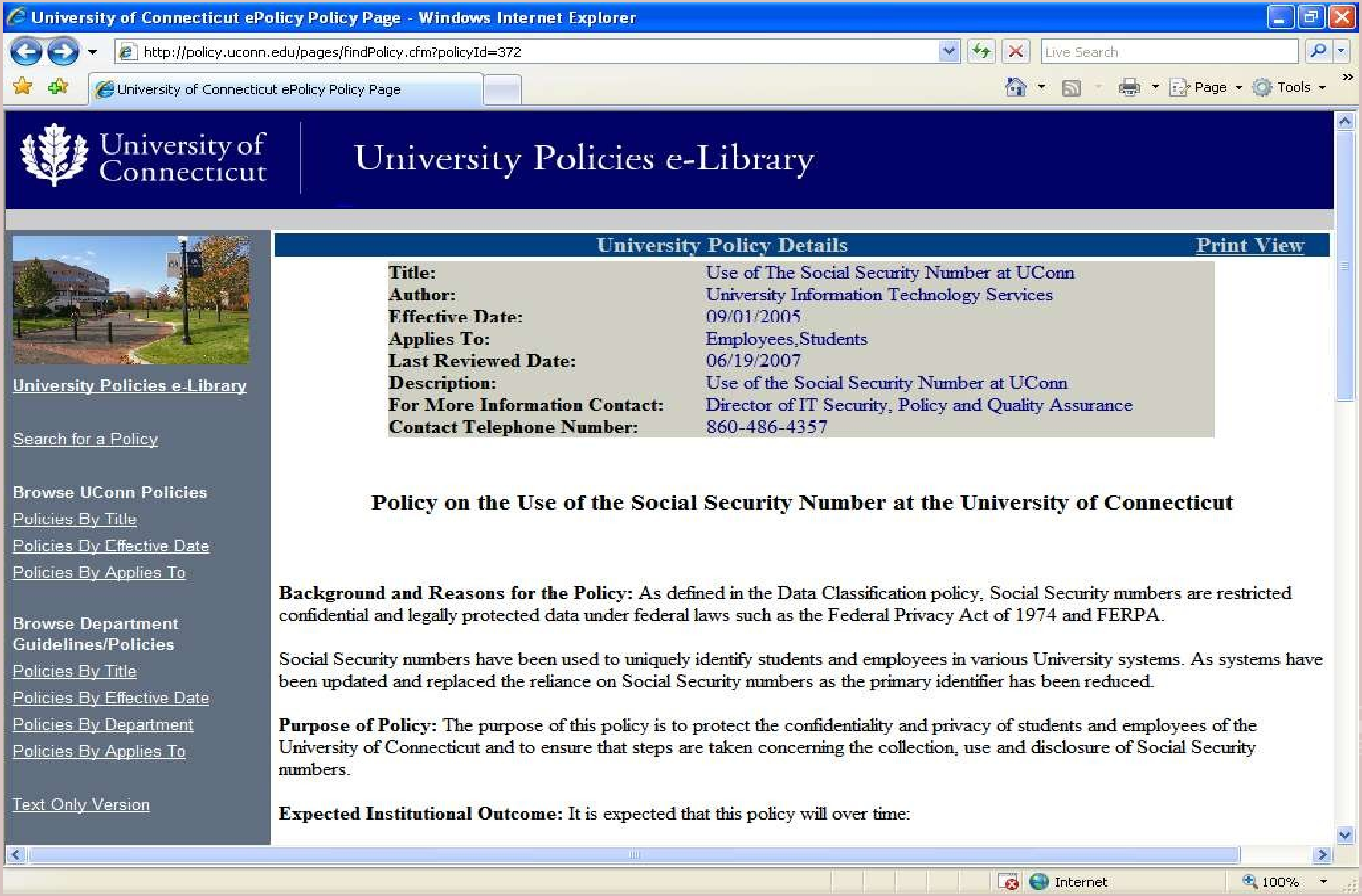
Are Universities concerned with privacy issues concerning ssn?

The first 19 hits returned from Google with the following three keywords: ssn, “primary identifier”, and law were all university sites.

Almost all the University sites had official policies regarding the privacy of ssn.

State laws concerning ssn as an identifier and the privacy of it’s use are as varied as the stars in the sky. Conclusion: All states limit the use of ssn to some degree. Universities are not exempt…

Making A Case For Encryption


University of Connecticut ePolicy Policy Page - Windows Internet Explorer
http://policy.uconn.edu/pages/findPolicy.cfm?policyId=372
Live Search
University of Connecticut ePolicy Policy Page
Page
Tools
Internet
100%

University of Connecticut

University Policies e-Library

University Policies e-Library

Search for a Policy

Browse UConn Policies

Policies By Title

Policies By Effective Date

Policies By Applies To

Browse Department Guidelines/Policies

Policies By Title

Policies By Effective Date

Policies By Department

Policies By Applies To

Text Only Version

University Policy Details Print View

Title:	Use of The Social Security Number at UConn
Author:	University Information Technology Services
Effective Date:	09/01/2005
Applies To:	Employees,Students
Last Reviewed Date:	06/19/2007
Description:	Use of the Social Security Number at UConn
For More Information Contact:	Director of IT Security, Policy and Quality Assurance
Contact Telephone Number:	860-486-4357

Policy on the Use of the Social Security Number at the University of Connecticut

Background and Reasons for the Policy: As defined in the Data Classification policy, Social Security numbers are restricted confidential and legally protected data under federal laws such as the Federal Privacy Act of 1974 and FERPA.

Social Security numbers have been used to uniquely identify students and employees in various University systems. As systems have been updated and replaced the reliance on Social Security numbers as the primary identifier has been reduced.

Purpose of Policy: The purpose of this policy is to protect the confidentiality and privacy of students and employees of the University of Connecticut and to ensure that steps are taken concerning the collection, use and disclosure of Social Security numbers.

Expected Institutional Outcome: It is expected that this policy will over time:

Making A Case For Encryption

Dave's Rules of Ranging for Encryption:

Article I

You should have a policy statement regarding the use of secure information.

This policy should include the display of private information, all electronic communications, and especially the use of such data with laptop computers.

Making A Case For Encryption

People's Bank of Connecticut, UPS & TransUnion

90,000 ssns

A computer tape from a Connecticut bank containing personal data on 90,000 customers was lost in transit recently, the bank reported today. People's Bank, based in Bridgeport, Connecticut, is sending letters to the affected customers, it said in a statement. The tape contains information such as names, addresses, Social Security numbers and checking account numbers. It was bound for the TransUnion LLC credit reporting bureau, based in Woodlyn, Penn., via United Parcel Service of America Inc. (UPS), the bank said.

Making A Case For Encryption

December 12, 2006 **formation Exposed For 800,000 At UCLA**

Apparently it's Identity Theft Tuesday here on Emergent Chaos. CNN reports that a "Hacker attack at UCLA affects 800,000 people", which includes current and former faculty, students and staff. The initial break-in was apparently in October of 2005 and access continued to be available until November 21st of this year. I am

> *concern or inconvenience this incident may cause you. It's a real shame they didn't have more effective security controls and monitoring systems in place. Maybe then this incident wouldn't have happened or been detected and stopped much earlier.*

It's a real shame they didn't have more effective security controls and monitoring systems in place. Maybe then this incident wouldn't have happened or been detected and stopped much earlier.

Making A Case For Encryption

In July, 2003, a California law was implemented requiring "any person or business doing business in California" to report to "data subjects" the incidence of a security breach, defined as, "Unauthorized acquisition of computerized data that compromises the security, confidentiality, of integrity of personal information."

By January of 2007, a total of 33 states will have similar data breach legislation on the books.

Making A Case For Encryption

Dave's Rules of Ranging for Encryption:

Article II

All sensitive data within an institution needs to be protected through encryption…

All backup tapes need to be encrypted to prevent the loss of such devices in transit or within your own organization.

All sensitive data on laptop computers must be encrypted.

All sensitive data within your data center needs to be encrypted.

08
PM
PERFORMANCE
MATTERS
Performance Matters!
Ron O'Connell, theater professor
Founder, All the World's a Stage,
a showcase for original student work.

Standard Oracle Encryption Tools

DBMS_Obfuscation & DBMS_Crypto

Standard Oracle Encryption Tools

- Standard utility provided for Oracle 9i: DBMS_Obfuscation
- Standard utility provided for Oracle 10G:

  DBMS_Crypto
- Available in both EE and SE releases of Oracle

Standard Oracle Encryption Tools

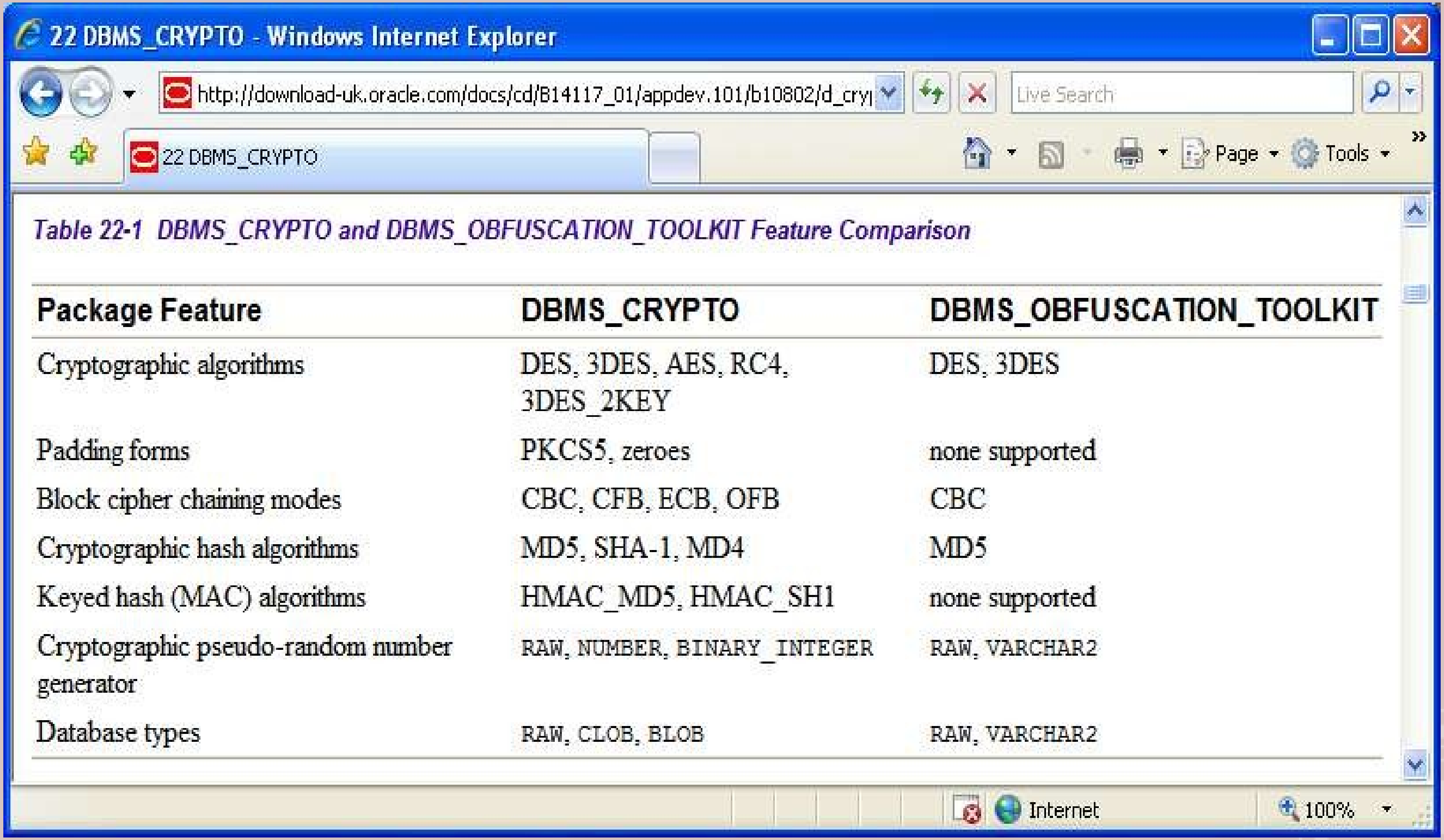

22 DBMS_CRYPTO - Windows Internet Explorer
http://download-uk.oracle.com/docs/cd/B14117_01/appdev.101/b10802/d_cry
Live Search
22 DBMS_CRYPTO
Page
Tools
Internet
100%

Table 22-1 DBMS_CRYPTO and DBMS_OBFUSCATION_TOOLKIT Feature Comparison

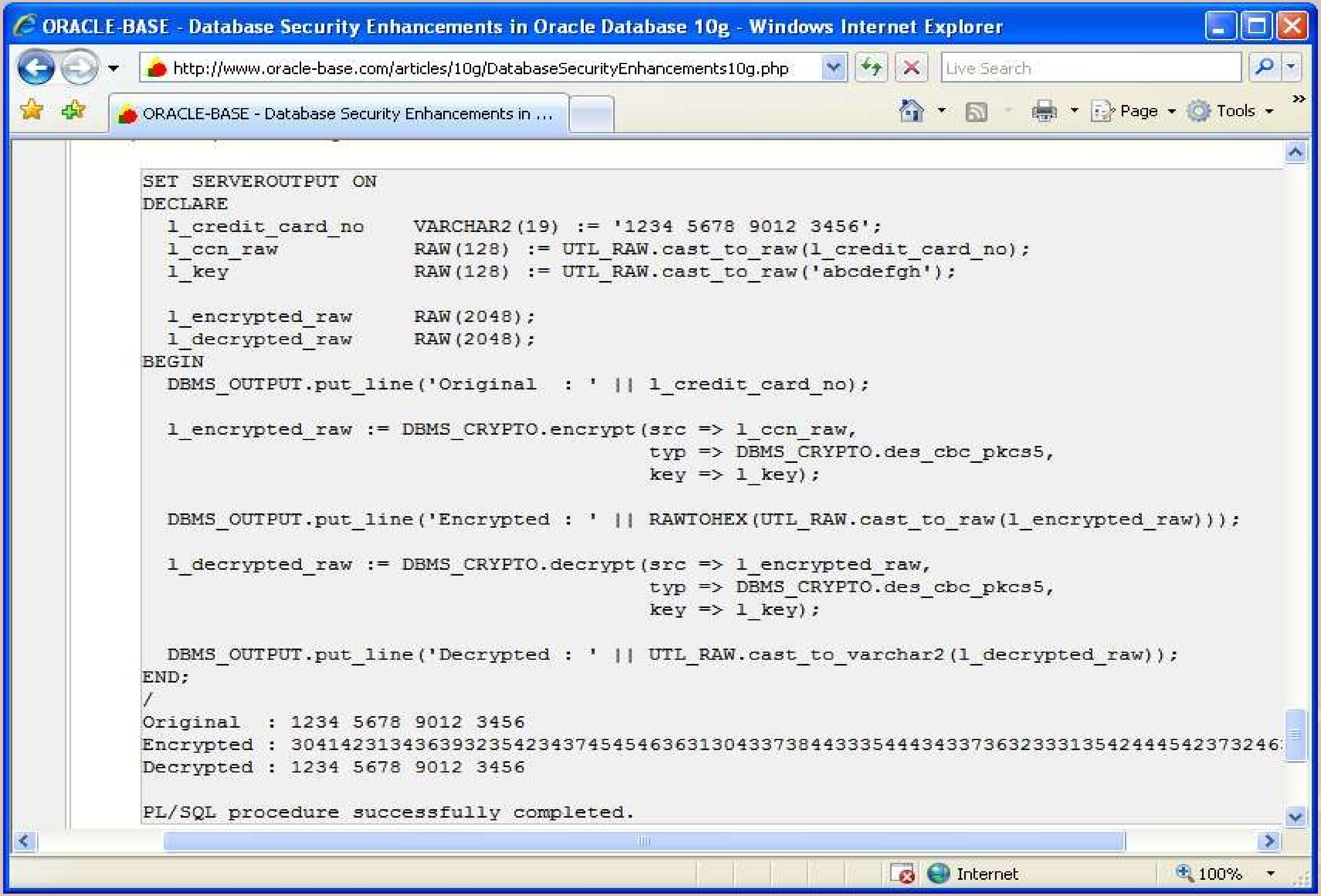
Package Feature	DBMS_CRYPTO	DBMS_OBFUSCATION_TOOLKIT
Cryptographic algorithms	DES, 3DES, AES, RC4, 3DES_2KEY	DES, 3DES
Padding forms	PKCS5, zeroes	none supported
Block cipher chaining modes	CBC, CFB, ECB, OFB	CBC
Cryptographic hash algorithms	MD5, SHA-1, MD4	MD5
Keyed hash (MAC) algorithms	HMAC_MD5, HMAC_SH1	none supported
Cryptographic pseudo-random number generator	`RAW`, `NUMBER`, `BINARY_INTEGER`	`RAW`, `VARCHAR2`
Database types	`RAW`, `CLOB`, `BLOB`	`RAW`, `VARCHAR2`

Standard Oracle Encryption Tools

Few advantages of DBMS_Crypto over DBMS_Obfuscation:

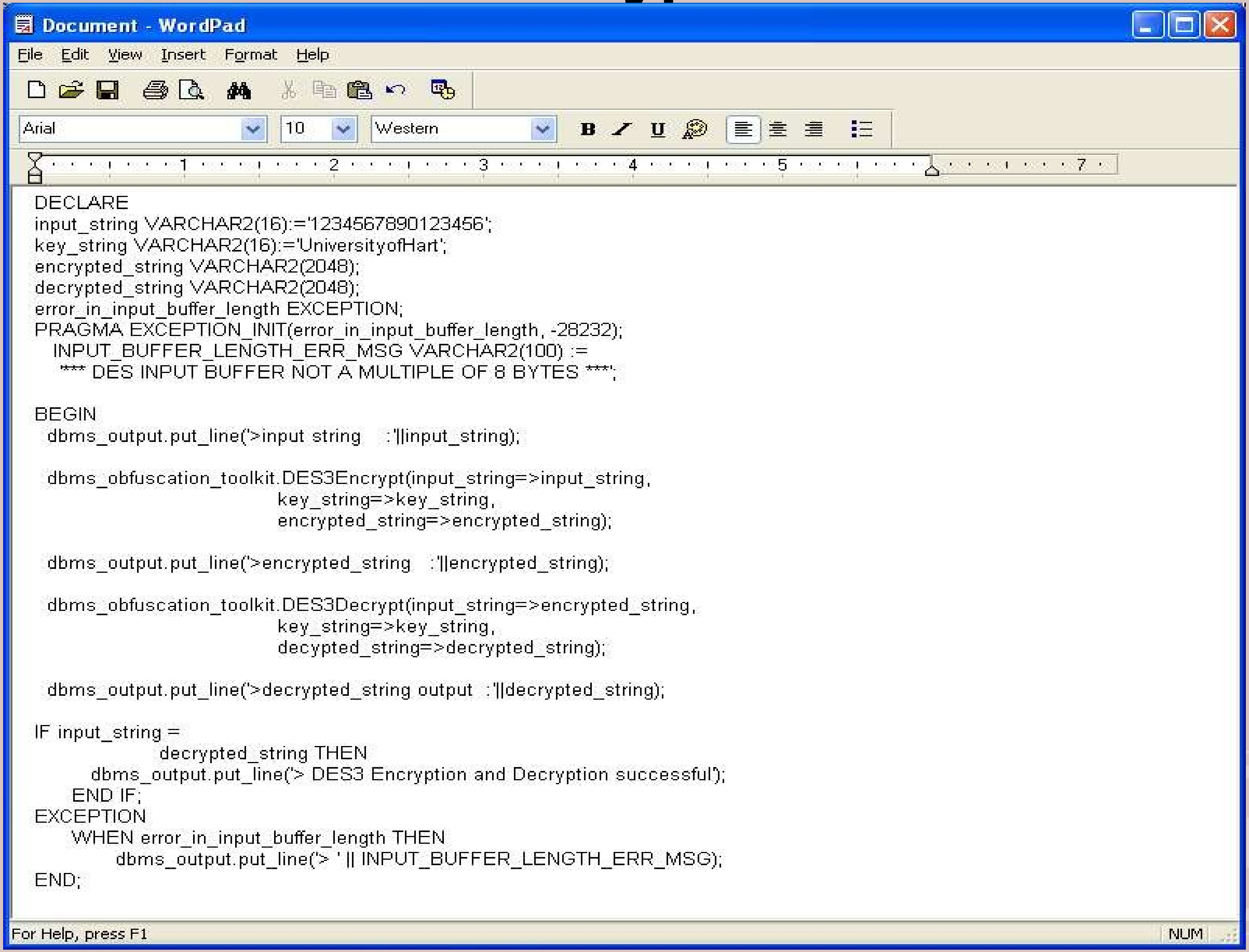
- Speed
- Extra encryption methods
- Support for blob and clob
- ???? Easier to use ????

Standard Oracle Encryption Tools


ORACLE-BASE - Database Security Enhancements in Oracle Database 10g - Windows Internet Explorer
http://www.oracle-base.com/articles/10g/DatabaseSecurityEnhancements10g.php
Live Search
ORACLE-BASE - Database Security Enhancements in ...
Page
Tools
Internet
100%

```
SET SERVEROUTPUT ON
DECLARE
  l_credit_card_no    VARCHAR2(19) := '1234 5678 9012 3456';
  l_ccn_raw           RAW(128)  := UTL_RAW.cast_to_raw(l_credit_card_no);
  l_key               RAW(128)  := UTL_RAW.cast_to_raw('abcdefgh');

  l_encrypted_raw     RAW(2048);
  l_decrypted_raw     RAW(2048);
BEGIN
  DBMS_OUTPUT.put_line('Original  : ' || l_credit_card_no);

  l_encrypted_raw := DBMS_CRYPTO.encrypt(src => l_ccn_raw,
                                         typ => DBMS_CRYPTO.des_cbc_pkcs5,
                                         key => l_key);

  DBMS_OUTPUT.put_line('Encrypted : ' || RAWTOHEX(UTL_RAW.cast_to_raw(l_encrypted_raw)));

  l_decrypted_raw := DBMS_CRYPTO.decrypt(src => l_encrypted_raw,
                                         typ => DBMS_CRYPTO.des_cbc_pkcs5,
                                         key => l_key);

  DBMS_OUTPUT.put_line('Decrypted : ' || UTL_RAW.cast_to_varchar2(l_decrypted_raw));
END;
/
Original  : 1234 5678 9012 3456
Encrypted : 30414231343639323542343745454636313043373844333544434337363233313542444542373246
Decrypted : 1234 5678 9012 3456

PL/SQL procedure successfully completed.
```

Standard Oracle Encryption Tools



```
DECLARE
input_string VARCHAR2(16):='1234567890123456';
key_string VARCHAR2(16):='UniversityofHart';
encrypted_string VARCHAR2(2048);
decrypted_string VARCHAR2(2048);
error_in_input_buffer_length EXCEPTION;
PRAGMA EXCEPTION_INIT(error_in_input_buffer_length, -28232);
   INPUT_BUFFER_LENGTH_ERR_MSG VARCHAR2(100) :=
    '*** DES INPUT BUFFER NOT A MULTIPLE OF 8 BYTES ***';

BEGIN
  dbms_output.put_line('>input string    :'||input_string);

  dbms_obfuscation_toolkit.DES3Encrypt(input_string=>input_string,
                                       key_string=>key_string,
                                       encrypted_string=>encrypted_string);

  dbms_output.put_line('>encrypted_string   :'||encrypted_string);

  dbms_obfuscation_toolkit.DES3Decrypt(input_string=>encrypted_string,
                                       key_string=>key_string,
                                       decypted_string=>decrypted_string);

  dbms_output.put_line('>decrypted_string output  :'||decrypted_string);

IF input_string =
                    decrypted_string THEN
         dbms_output.put_line('> DES3 Encryption and Decryption successful');
      END IF;
EXCEPTION
      WHEN error_in_input_buffer_length THEN
             dbms_output.put_line('> ' || INPUT_BUFFER_LENGTH_ERR_MSG);
END;
```

Standard Oracle Encryption Rules

Dave’s Rules of Ranging for Encryption:

Article III

2. Encypting Data is simple
3. Decrypting data is simple
4. Decrypting data transparently is “NOT SO SIMPLE”

Performance Matters!
Ron O'Connell, theater professor
Founder, All the World's a Stage,
a showcase for original student work.

SUNGARD HIGHER EDUCATION

SUMMIT 2008

Transparent Encryption & Third Party Vendors

Evaluation of TDE, DBEncrypt, and Encryption Wizard

Transparent Encryption & Third Party Vendors

Evaluated the three following products:

- Transparent Data Encryption (TDE) from Oracle
- DBEncrypt Inc. from Application Security
- Encryption Wizard from Relational Database Consultants Inc.

Note: *Twelve page evaluation report on these products will be made available for viewing or download.*

Transparent Encryption & Third Party Vendors

Summary for DBEncrypt:

Installation	D
Ease of Use	A
Transparent Encryption	A
Performance	D
Cost	B
Support	F
Overall	C-

Disclaimer: *These are the personal views of an evaluation done January 22, 2007 by the University of Hartford. Your personal experience with the product may differ.*

Transparent Encryption & Third Party Vendors

DBEncrypt:

- **Installation**: Had to alter sql*net to run 32 bit instead of 64 bit. Incorrect binaries loaded into Oracle directories that had to be moved manually into correct directories.

- **Ease of Use**: Gui made encrypting and decrypting values very simple.

- **Transparent Encryption**: Worked as advertised. However, all triggers and indexes on encrypted data had to be dropped before encrypting data.

Disclaimer: *These are the personal views of an evaluation done January 22, 2007 by the University of Hartford. Your personal experience with the product may differ.*

Transparent Encryption & Third Party Vendors

DBEncrypt:

- **Performance**: Decrypting single values instantaneous. Inserts did suffer a slight performance hit. Any use of an encrypted column in a “Where” clause caused the product to decrypt the entire table first, resulting in what appeared to be a hung machine. Breaking out of the hung situation resulted in “runaway” processess on the system that consumed excessive cpu.

- **Cost:** The cost is 15k per instance before any discounts. There was never any indications that we would receive a discount from the baseline price.

Disclaimer: *These are the personal views of an evaluation done January 22, 2007 by the University of Hartford. Your personal experience with the product may* differ.

Transparent Encryption & Third Party Vendors

DBEncrypt:

- **Support:** No one seemed interested in selling us the product. The support line did not understand their own product. Questions/problems reported were either ignored or never followed through to conclusion.

- **Overall:** For small applications this product may be fine but not for encrypting the entire Banner system. Poor performance, required custom code, and horrible support make this product a poor choice.

Disclaimer: *These are the personal views of an evaluation done January 22, 2007 by the University of Hartford. Your personal experience with the product may* differ.

Transparent Encryption & Third Party Vendors

Summary for TDE:

Installation	??
Ease of Use	??
Transparent Encryption	A
Performance	D
Cost	F
Support	D
Overall	B

Disclaimer: *These are the personal views of an evaluation done January 22, 2007 by the University of Hartford. Your personal experience with the product may differ.*

Transparent Encryption & Third Party Vendors

TDE:

- **Installation**: Looks to be neither simple or difficult.
- **Ease of Use**: Appears to be easy to setup.
- **Transparent Encryption**: Should work as advertised.

Disclaimer: *These are the personal views of an evaluation done January 22, 2007 by the University of Hartford. Your personal experience with the product may differ.*

Transparent Encryption & Third Party Vendors

TDE:

- **Performance**: Based on listserv reactions and Oracle documentation this product should perfrom normally under most circumstances. However, I do believe that range scans could cause significant performance issues. Oracle documentation does warn against possible significant performance issues.
- **Cost:** The cost is 15k per cpu before discount. Large boxes (12 cpu+) make this product cost prohibitive. Typical cost for a production box would be 4 cpu's with a 40% discount or 36k. Licenses on a test box push this number higher.

Disclaimer: *These are the personal views of an evaluation done January 22, 2007 by the University of Hartford. Your personal experience with the product may* differ.

Transparent Encryption & Third Party Vendors

TDE:

- **Support:** All tar’s went unanswered after two weeks! Either Oracle did not know the answer to my questions or was reluctant to answer some very pointed questions.

- **Overall:** Probably adequate**.** High cost, possible performance issues, and 10G requirement does not make this product attractive to all.

Disclaimer: *These are the personal views of an evaluation done January 22, 2007 by the University of Hartford. Your personal experience with the product may* differ.

Transparent Encryption & Third Party Vendors

Summary for Encryption Wizard:

Installation	A
Ease of Use	A
Transparent Encryption	A
Performance	A
Cost	A
Support	A
Overall	A

Disclaimer: *These are the personal views of an evaluation done January 22, 2007 by the University of Hartford. Your personal experience with the product may differ.*

Transparent Encryption & Third Party Vendors

Encryption Wizard:

- **Installation**: A snap to install.
- **Ease of Use**: So easy a caveman can use it.
- **Transparent Encryption**: Worked as advertised.

Disclaimer: *These are the personal views of an evaluation done January 22, 2007 by the University of Hartford. Your personal experience with the product may differ.*

Transparent Encryption & Third Party Vendors

Encryption Wizard:

- **Performance**: Unique use of functional (bit-mapped) indexes on encrypted columns increased performance over existing b-tree indexes. Also performed very well with range scans. Functional indexes have trouble using RBO and do not recommend implementing this product for tables requiring functional indexes utilizing RBO.

- **Cost:** Only 5k per Oracle license.

Disclaimer: *These are the personal views of an evaluation done January 22, 2007 by the University of Hartford. Your personal experience with the product may* differ.

Transparent Encryption & Third Party Vendors

Encryption Wizard:

- **Support:** Better than excellent**.** Direct line into developers of product that answer all questions and are willing to make adjustments to their product.

- **Overall:** Transparent encryption, good performance, and low cost make this a winner. Company is not your typical fortune 500, but its' customers do include IBM, Disney, and Fidelity.

Disclaimer: *These are the personal views of an evaluation done January 22, 2007 by the University of Hartford. Your personal experience with the product may* differ.

Transparent Encryption & Third Party Vendors

Summary for All Vendors:

	DBEncrypt	TDE	Enc. Wizard
Installation	D	??	A
Ease of Use	A	??	A
Transparent Encryption	A	A	A
Performance	D	D	A
Cost	B	F	A
Support	F	D	A
Overall	C-	B	A

Disclaimer: *These are the personal views of an evaluation done January 22, 2007 by the University of Hartford. Your personal experience with the product may differ.*

Standard Oracle Encryption Rules

Dave's Rules of Ranging for Encryption:

Article IV

Never underestimate the importance of performance in performance in any data encryption strategy or implementation

Making A Case For Encryption

Dave's Rules of Ranging for Encryption:

Article V

Remember to encrypt **<u>all</u>** environments, including development and test, and remember to factor in the costs of encrypting all environments.

08
PM
PERFORMANCE MATTERS
Performance Matters!
Ron O'Connell, theater professor
Founder, All the World's a Stage,
a showcase for original student work.

Banner Data Needing Encryption

I thought all I needed to encrypt was ssn in the spbpers table?

Banner Data Needing Encryption

Where to find ssn within Banner:

- Search for table columns with the letters “ssn” embedded in them.
- Search for table columns with a format of varchar2(9).
- Ask developers and power users where they know ssn is used.
- View attributes of ssn data from within Banner forms.

Note: The University of Hartford has done analysis on where ssn is used throughout Banner, but we are certain we have not found all occurrences.

Banner Data Needing Encryption

Finding all tables that have “ssn” embedded within a column name:

```
select owner,
              table_name,
              column_name
    from dba_tab_columns
    where column_name like '%SSN%'
    order by 1,2;
```

Note: *University of Hartford found 530 values. Actual count will vary by Institution.*

Banner Data Needing Encryption

Finding all tables that contain a column with varchar2(9).

```
Select owner,
              table_name,
                        column_name
    from dba_tab_columns
    where data_length=9
    and data_type ='VARCHAR2';
```

Note: *University of Hartford found 1,722 values. Actual count will vary by Institution.*

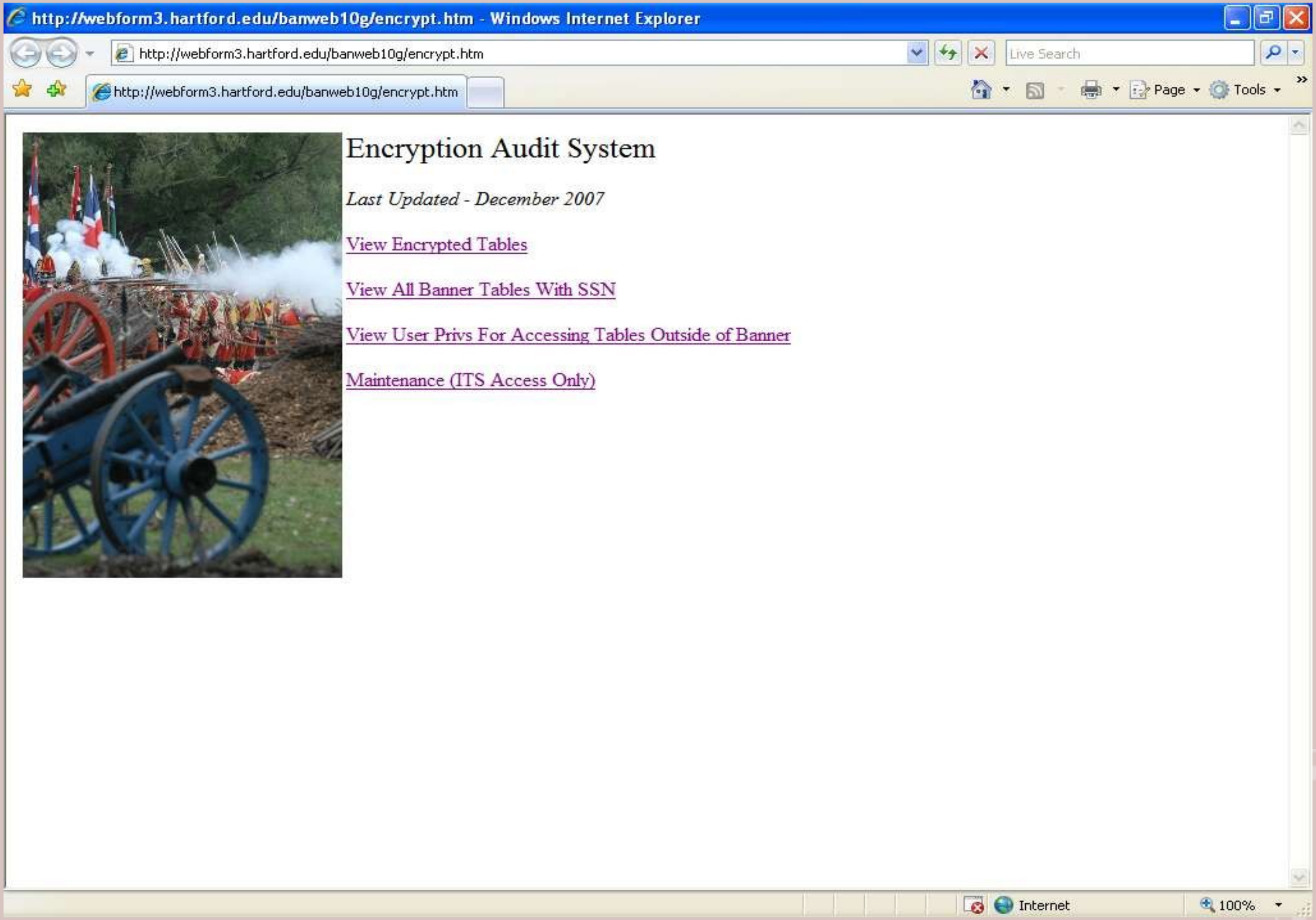
Banner Data Needing Encryption

Dave’s Rules of Ranging for Encryption:

Article VI

Whenever possible, delete sensitive data from your database rather than encrypting it.

Banner Data Needing Encryption



http://webform3.hartford.edu/banweb10g/encrypt.htm - Windows Internet Explorer
http://webform3.hartford.edu/banweb10g/encrypt.htm
Live Search
http://webform3.hartford.edu/banweb10g/encrypt.htm
Page
Tools
Internet
100%

Encryption Audit System

Last Updated - December 2007

View Encrypted Tables

View All Banner Tables With SSN

View User Privs For Accessing Tables Outside of Banner

Maintenance (ITS Access Only)

Banner Data Needing Encryption

Dave's Rules of Ranging for Encryption:

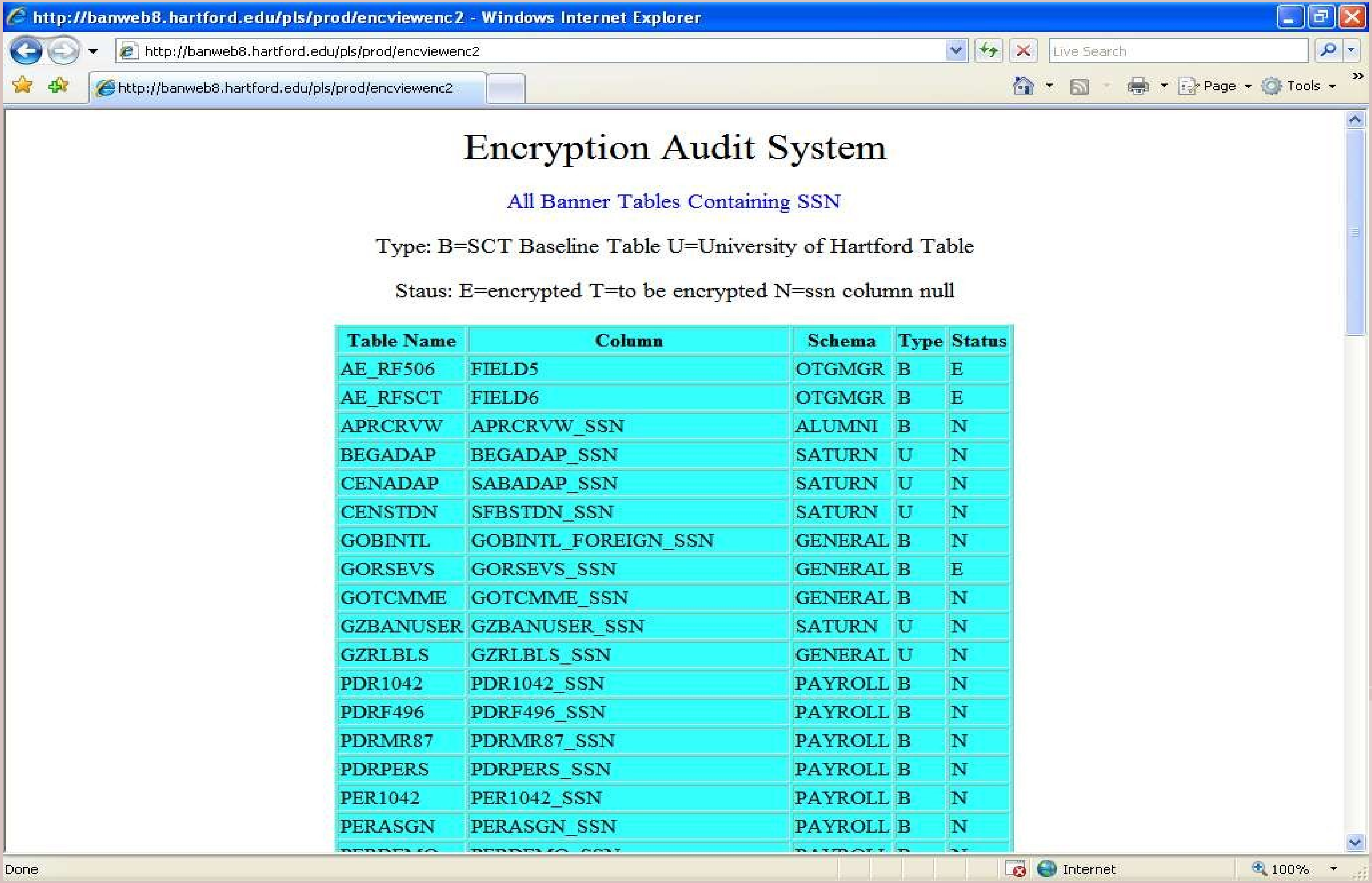
Article VII

Choose a tool that also provides APIs or SQL functions for system maintenance.

Doing security through GUI in even a small institution will require thousands of individual entries. APIs in conjunction with dynamic sql can create thousands of sql statements in seconds.

APIs will also let you write interfaces to allow users and developers to do system functions.

Banner Data Needing Encryption



http://banweb8.hartford.edu/pls/prod/encviewenc2 - Windows Internet Explorer
http://banweb8.hartford.edu/pls/prod/encviewenc2
Live Search
http://banweb8.hartford.edu/pls/prod/encviewenc2
Page
Tools
Done
Internet
100%

Encryption Audit System

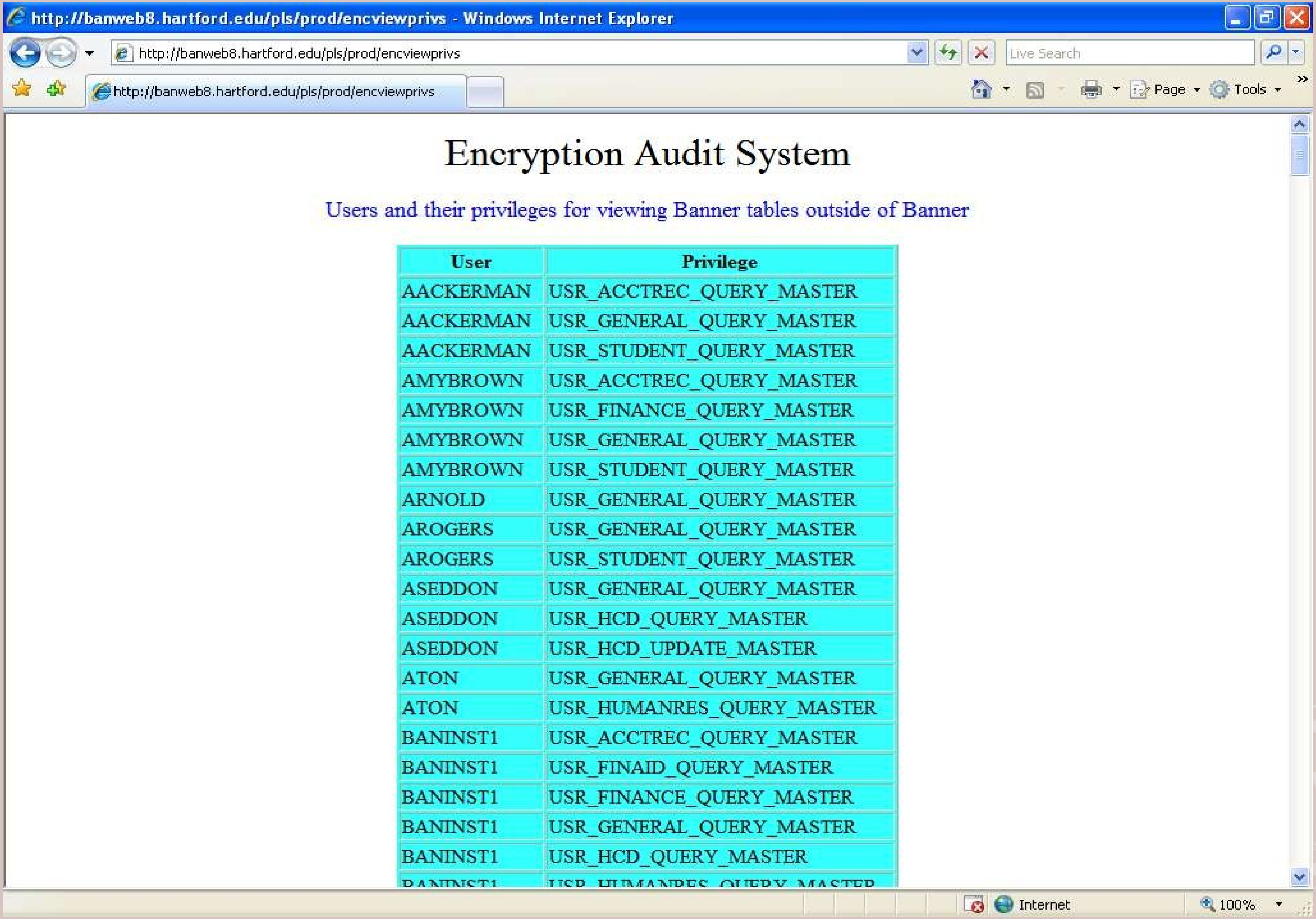
All Banner Tables Containing SSN

Type: B=SCT Baseline Table U=University of Hartford Table

Staus: E=encrypted T=to be encrypted N=ssn column null

Table Name	Column	Schema	Type	Status
AE_RF506	FIELD5	OTGMGR	B	E
AE_RFSCT	FIELD6	OTGMGR	B	E
APRCRVW	APRCRVW_SSN	ALUMNI	B	N
BEGADAP	BEGADAP_SSN	SATURN	U	N
CENADAP	SABADAP_SSN	SATURN	U	N
CENSTDN	SFBSTDN_SSN	SATURN	U	N
GOBINTL	GOBINTL_FOREIGN_SSN	GENERAL	B	N
GORSEVS	GORSEVS_SSN	GENERAL	B	E
GOTCMME	GOTCMME_SSN	GENERAL	B	N
GZBANUSER	GZBANUSER_SSN	SATURN	U	N
GZRLBLS	GZRLBLS_SSN	GENERAL	U	N
PDR1042	PDR1042_SSN	PAYROLL	B	N
PDRF496	PDRF496_SSN	PAYROLL	B	N
PDRMR87	PDRMR87_SSN	PAYROLL	B	N
PDRPERS	PDRPERS_SSN	PAYROLL	B	N
PER1042	PER1042_SSN	PAYROLL	B	N
PERASGN	PERASGN_SSN	PAYROLL	B	N
PERDEMO	PERDEMO_SSN	PAYROLL	B	N

Banner Data Needing Encryption

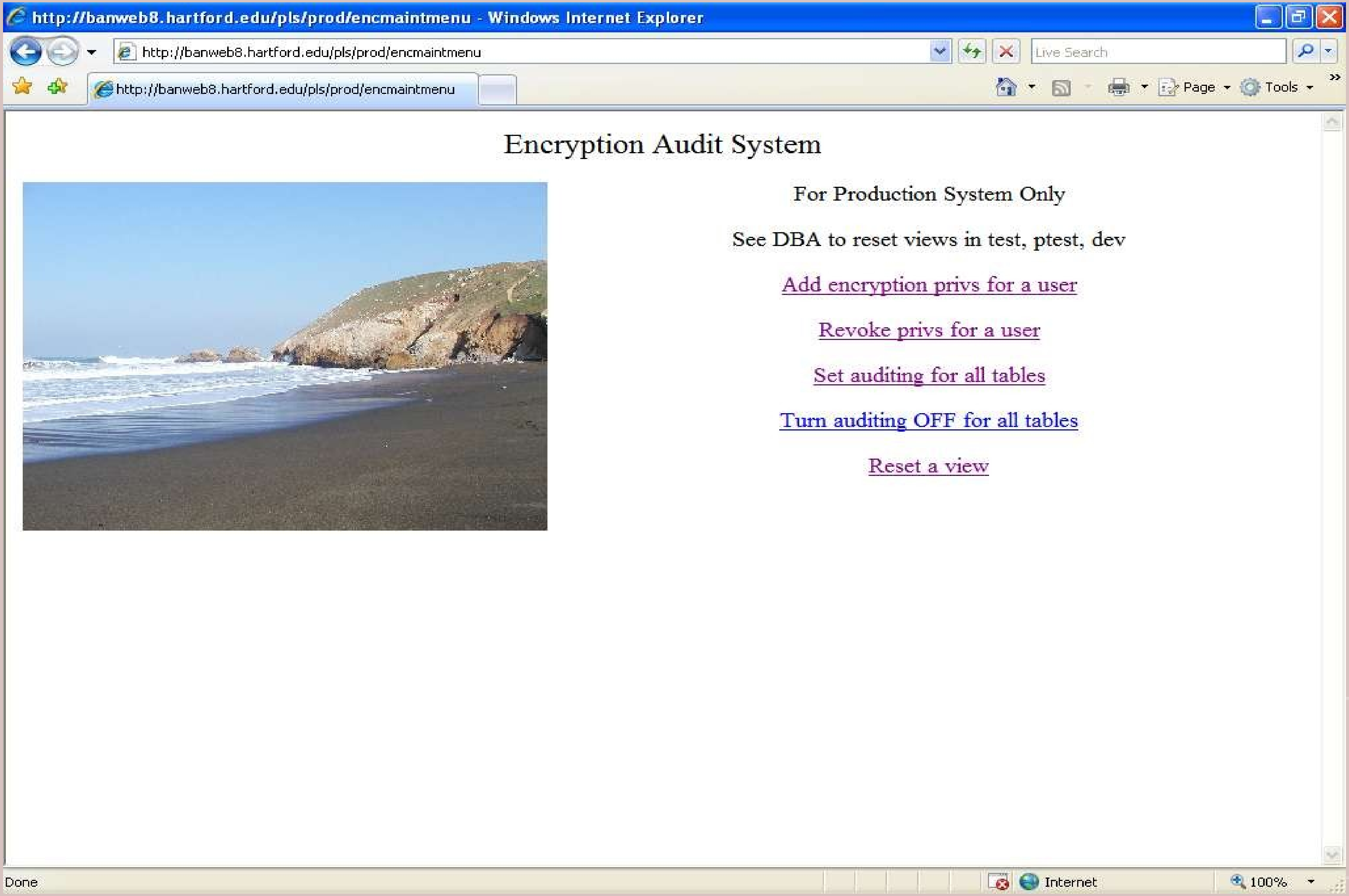

http://banweb8.hartford.edu/pls/prod/encviewprivs - Windows Internet Explorer
http://banweb8.hartford.edu/pls/prod/encviewprivs
Live Search
http://banweb8.hartford.edu/pls/prod/encviewprivs
Page
Tools
Internet
100%

Encryption Audit System

Users and their privileges for viewing Banner tables outside of Banner

User	Privilege
AACKERMAN	USR_ACCTREC_QUERY_MASTER
AACKERMAN	USR_GENERAL_QUERY_MASTER
AACKERMAN	USR_STUDENT_QUERY_MASTER
AMYBROWN	USR_ACCTREC_QUERY_MASTER
AMYBROWN	USR_FINANCE_QUERY_MASTER
AMYBROWN	USR_GENERAL_QUERY_MASTER
AMYBROWN	USR_STUDENT_QUERY_MASTER
ARNOLD	USR_GENERAL_QUERY_MASTER
AROGERS	USR_GENERAL_QUERY_MASTER
AROGERS	USR_STUDENT_QUERY_MASTER
ASEDDON	USR_GENERAL_QUERY_MASTER
ASEDDON	USR_HCD_QUERY_MASTER
ASEDDON	USR_HCD_UPDATE_MASTER
ATON	USR_GENERAL_QUERY_MASTER
ATON	USR_HUMANRES_QUERY_MASTER
BANINST1	USR_ACCTREC_QUERY_MASTER
BANINST1	USR_FINAID_QUERY_MASTER
BANINST1	USR_FINANCE_QUERY_MASTER
BANINST1	USR_GENERAL_QUERY_MASTER
BANINST1	USR_HCD_QUERY_MASTER
BANINST1	USR_HUMANRES_QUERY_MASTER

Banner Data Needing Encryption



http://banweb8.hartford.edu/pls/prod/encmaintmenu - Windows Internet Explorer
http://banweb8.hartford.edu/pls/prod/encmaintmenu
Live Search
http://banweb8.hartford.edu/pls/prod/encmaintmenu
Page
Tools
Done
Internet
100%

Encryption Audit System

For Production System Only

See DBA to reset views in test, ptest, dev

Add encryption privs for a user

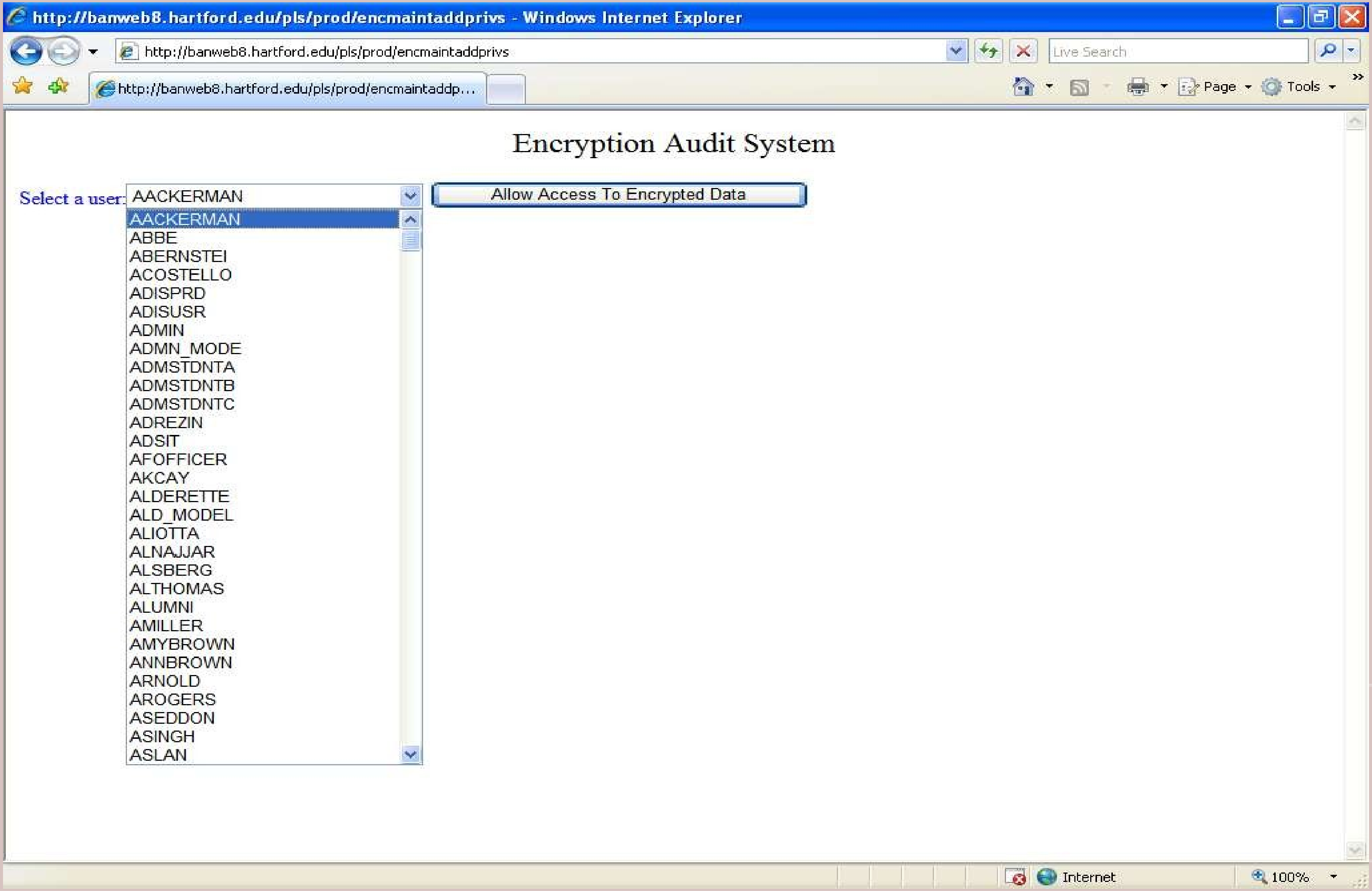
Revoke privs for a user

Set auditing for all tables

Turn auditing OFF for all tables

Reset a view

Banner Data Needing Encryption



http://banweb8.hartford.edu/pls/prod/encmaintaddprivs - Windows Internet Explorer
http://banweb8.hartford.edu/pls/prod/encmaintaddprivs
Live Search
http://banweb8.hartford.edu/pls/prod/encmaintaddp...
Page
Tools
Internet
100%

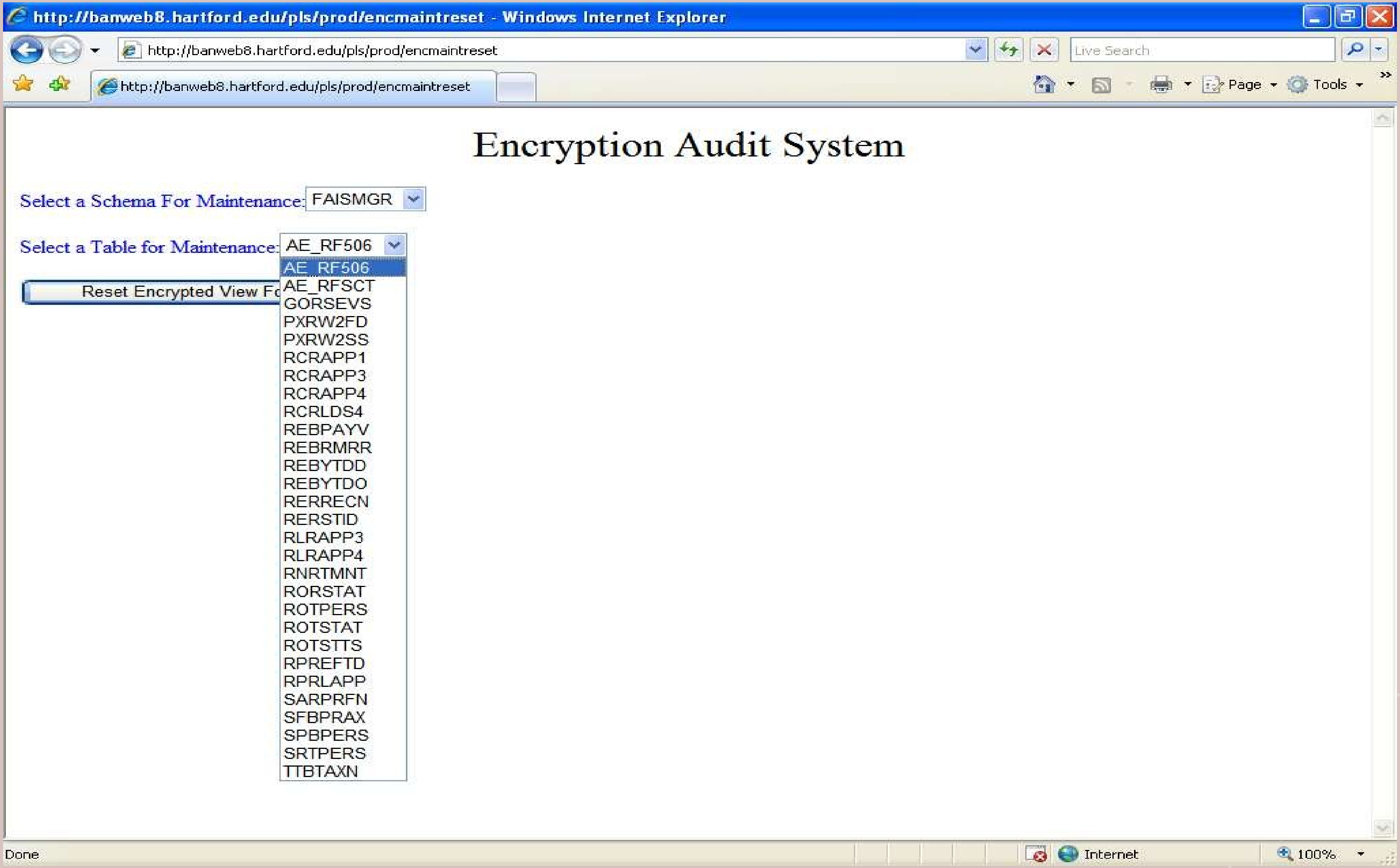
Encryption Audit System

Select a user: AACKERMAN

Allow Access To Encrypted Data

AACKERMAN
ABBE
ABERNSTEI
ACOSTELLO
ADISPRD
ADISUSR
ADMIN
ADMN_MODE
ADMSTDNTA
ADMSTDNTB
ADMSTDNTC
ADREZIN
ADSIT
AFOFFICER
AKCAY
ALDERETTE
ALD_MODEL
ALIOTTA
ALNAJJAR
ALSBERG
ALTHOMAS
ALUMNI
AMILLER
AMYBROWN
ANNBROWN
ARNOLD
AROGERS
ASEDDON
ASINGH
ASLAN

Banner Data Needing Encryption



http://banweb8.hartford.edu/pls/prod/encmaintreset - Windows Internet Explorer
http://banweb8.hartford.edu/pls/prod/encmaintreset
Live Search
Page
Tools
Done
Internet
100%

Encryption Audit System

Select a Schema For Maintenance: FAISMGR

Select a Table for Maintenance: AE_RF506

Reset Encrypted View Fo

AE_RF506
AE_RFSCT
GORSEVS
PXRW2FD
PXRW2SS
RCRAPP1
RCRAPP3
RCRAPP4
RCRLDS4
REBPAYV
REBRMRR
REBYTDD
REBYTDO
RERRECN
RERSTID
RLRAPP3
RLRAPP4
RNRTMNT
RORSTAT
ROTPERS
ROTSTAT
ROTSTTS
RPREFTD
RPRLAPP
SARPRFN
SFBPRAX
SPBPERS
SRTPERS
TTBTAXN

Performance Matters!
Ron O'Connell, theater professor
Founder, All the World's a Stage,
a showcase for original student work.

SUNGARD HIGHER EDUCATION

SUMMIT 2008

Case Study: University of Hartford Encryption Project

All the steps from A-Z

Case Study: University of Hartford Encryption Project

<u>First Order Of Business:</u>

Scrubbed Banner data:

Determined what types of sensitive data we would be storing in the database – ssn, creditcard, drivers license, account numbers.

If storing data such as creditcard, be sure you are in compliance with Federal and State regulations as well as vendor regulations such as PCI.

Searched for all occurrences of data within Banner (SunGard), third party tools (such as imaging), and any other applications.

Nulled all fields for data we decided not to store **<u>and</u>** nulled all fields for data that we had decided to keep but not for this particular table. Included both baseline SunGard tables and in house created tables.

Case Study: University of Hartford Encryption Project

Second Order Of Business:

Choose toolset:

Investigated use of Oracle available tools, TDE, and third party vendors.

Chose transparent encryption as an architecture.

Evaluated third party products.

Case Study: University of Hartford Encryption Project

Phase I:

Completed Phase I – March 29, 2007

Encrypted tables that were small and needed no special alterations.

Encrypted tables for the General, Payroll, and HR schemas.

Case Study: University of Hartford Encryption Project

Phase II:

Completed Phase II – May 23, 2007

Seventeen Financial Aid tables encrypting millions of rows.

Remaining tables to be encrypted required functional indexes which required CBO with Oracle 10G.

Case Study: University of Hartford Encryption Project

Phase III:

Completed Phase III – December 28, 2007

Financial Aid, Document Imaging, Student, and AR tables encrypting millions of rows.

Columns implemented with functional indexes.

Case Study: University of Hartford Encryption Project

Phase IV:

Phase IV – in progress

Complete elimination of ssn used as a primary key identifier in certain circumstances in Admissions.

Cleanup ssn in applications such as document imaging where ssn was used as a primary key indicator at one time.

Alter security to narrow the number of users allowed to view ssn.

Case Study: University of Hartford Encryption Project

Summary:

Very few problems encountered.

Millions upon millions of rows encrypted and removed from nearly 100 tables.

Initial cost, ongoing maintenance, and total resources necessary to implement were all reasonable.

Still battling cultural issues regarding the continued use of ssn.

Performance Matters!
Ron O'Connell, theater professor
Founder, All the World's a Stage,
a showcase for original student work.

SUNGARD HIGHER EDUCATION

SUMMIT 2008

What You wished Someone Told You Before You Started

Potpori of Hints and What To Watch for

What You Wished Someone Told You Before You Started

When scrubbing Banner data, remember to delete any ssn values that once existed as a primary id:

Check spriden_id for any former ssn values prior to conversion from ssn to student id.

Check any third party tools that may still have ssn’s in the id field.

Document Imaging tracks documents by id, not pidm. Any ssn values in spriden as the student id will populate MANY imaging tables with ssn.

What You Wished Someone Told You Before You Started

If creating bitmap indexes beware Oracle ORA-28604:

ora-28604: table too fragmented to build bitmap index

Many solutions suggested including unload/reload of table and indexes to rebuild all components

See Oracle note: 119674 for dealing with problem

The following solution found in an Oracle listserv seems to work best and is the easiest to implement:

Alter table XXX minimize records_per_block;

What You Wished Someone Told You Before You Started

ORA-22816 and ORA-06512:

Many encryption packages have as their underlying architecture an updateable view that contains the unencrypted values.

If these views are updateable using an “instead of” trigger; ora-22816 and ora-06512 errors will occur within Banner api’s.

This condition is noted as Oracle bugs 1589656 and 155654.1. Oracle does not plan to provide a patch, but instead provides work arounds.

What You Wished Someone Told You Before You Started

ORA-22816 and ORA-06512:

Results when using an “instead of” trigger for updateable views.

Known Banner API’s that have to be modified:

dml_rerstid	(rekd_rerstid1.sql)
dml_pxrw2fd	(pxkd_pxrw2fd1.sql)
dml_spbpers	(gokd_spbpers1.sql)
dml_rebpayv1.sql	(rekd_rebpayv1.sql)

Must replace all existing “returning” clauses.

What You Wished Someone Told You Before You Started

ORA-22816 and ORA-06512:

Example of altered returning clause:

Before:

```
Begin
  insert into pxrw2fd
   values p_rec
 returning rowid
    into p_rowid_out;
 end p_insert;
```

After:

```
insert into pxrw2fd
values p_rec;
select a.rowid
into p_rowid_out
from pxrw2fd a
where p_rec.pxrw2fd_year = a.pxrw2fd_year
and p.rec.pxrw2fd_quarter = a.pxrw2fd_quarter
and p_rec.pwxrw2fd_empr_code = a.pxrw2fd_empr_code
and p_rec.pxrw2fd_pidm = a.pxrw2fd_pidm
and p_rec.pxrw2fd_seq_no = a.pxrw2fd_seq_no;
End p_insert
```

What You Wished Someone Told You Before You Started

Possible issues with triggers and insert statements:

Triggers: Whether using Oracle standard tools (dbms_crypto) or third party products for TDE, data items may need to be decrypted before database triggers fire. If encrypted values are not primary key identifiers, this issue should probably never become an issue.

Insert statements: Those products that create updateable views and create an extra column in the view for encryption/decryption will cause insert statements like the following to fail:

```
insert into tableA select * from tableB;
```

What You Wished Someone Told You Before You Started

Failure to use an index for an encrypted table can have disastrous results with performance.

All functions such as “like” and “substr” under the rule based optimizer turn off indexes.

Rule hints under CBO have the same problems with Oracle functions.

What You Wished Someone Told You Before You Started

Modifications for encryption:

For bug with returning clause altered the following API's:

pxkd_pxrw2fd1.sql	(dml_pxrw2fd)
rekd_rerstid1.sql	(dml_rerstid)
gokd_spbpers1.sql	(dml_spbpers)
rekd_rebpayv1.sql	(dml_rebpayv)

What You Wished Someone Told You Before You Started

Modifications for encryption:

For Performance:

Altered package for form Goamtch for spbpers:

gokcmpk1.sql gokcmpk

What You Wished Someone Told You Before You Started

Modifications for encryption:

For Document Imaging:

Nulled field6 for table ae_rfsct that caused indexing to abend. Appears Document Imaging does not recognize synonyms for tables and instead uses fully qualified names – resulting in retrieval of encrypted data and abends.

Altered euaerfsct.sql and nulled out update of ssn.

Altered eiaerfsct.sql and nulled out update of ssn.

What You Wished Someone Told You Before You Started

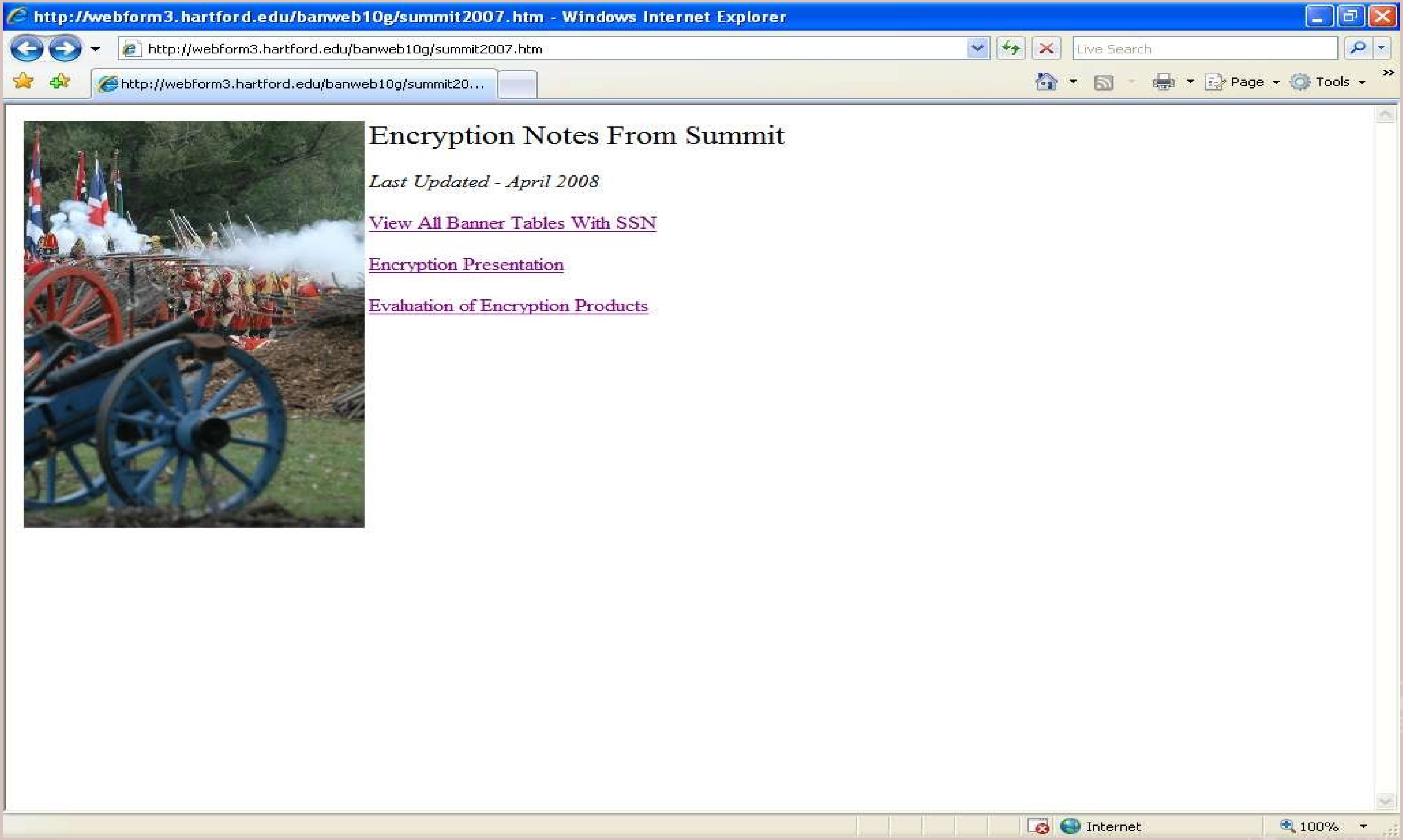
Modifications for encryption:

For University of Hartford reports and systems:

For those tables that were encrypted and were fully qualified by schema owner, had to be recoded to just use tablename to pickup view for encrypted table.

The Only URL You Want To Remember

- http://webform3.hartford.edu/banweb10g/summit2007


http://webform3.hartford.edu/banweb10g/summit2007.htm - Windows Internet Explorer
http://webform3.hartford.edu/banweb10g/summit2007.htm
Live Search
http://webform3.hartford.edu/banweb10g/summit20...
Page
Tools
Internet
100%

Encryption Notes From Summit

Last Updated - April 2008

View All Banner Tables With SSN

Encryption Presentation

Evaluation of Encryption Products

Thanks!

David de Manbey

University of Hartford

Email: demanbey@hartford.edu

Please complete the online class evaluation

Course ID S-0061