
Bet on IDS
Paul Watson, Oninit
paul@oninit.com
2008 IIUG Informix Conference
www.iiug.org

# Agenda

- Overview on the Betting Industry
- Technical Demands of the Betting Industry
- Why choose IDS

## What is a Bet ?

- Lotteries
- Games of Chance
- Games of Skill

## Lotteries

- A popular form of gambling which involves the drawing of lots for a prize
- First recorded back in 200 BC
- Often used by government to raise funds. Which has led to be called a regressive tax.
- Lottery comes from the Dutch word *loterij*
- Not legal in ALL countries.

# Games of Chance

- A **game of chance** is a game whose outcome is strongly influenced by some randomizing device.

Examples

- Roulette
- Craps
- Slots

# Games of Skill

- Defined as a game where the skill of the player has a direct effect on the outcome of the game.

Examples

Poker

Blackjack

Football Betting
Horse Racing

The distinction between 'chance' and 'skill' has legal significance in countries where chance games are treated differently than skill games. The legal distinction is often vague and varies widely from one jurisdiction to the next.

## How much are we talking about ?

- Online gambling in  2006 - $12 billion

## Who Gambles ?

Trite Answer: Everyone

Big single demographic: 30-35 Woman from home.
Typically pay $25 for a casual game

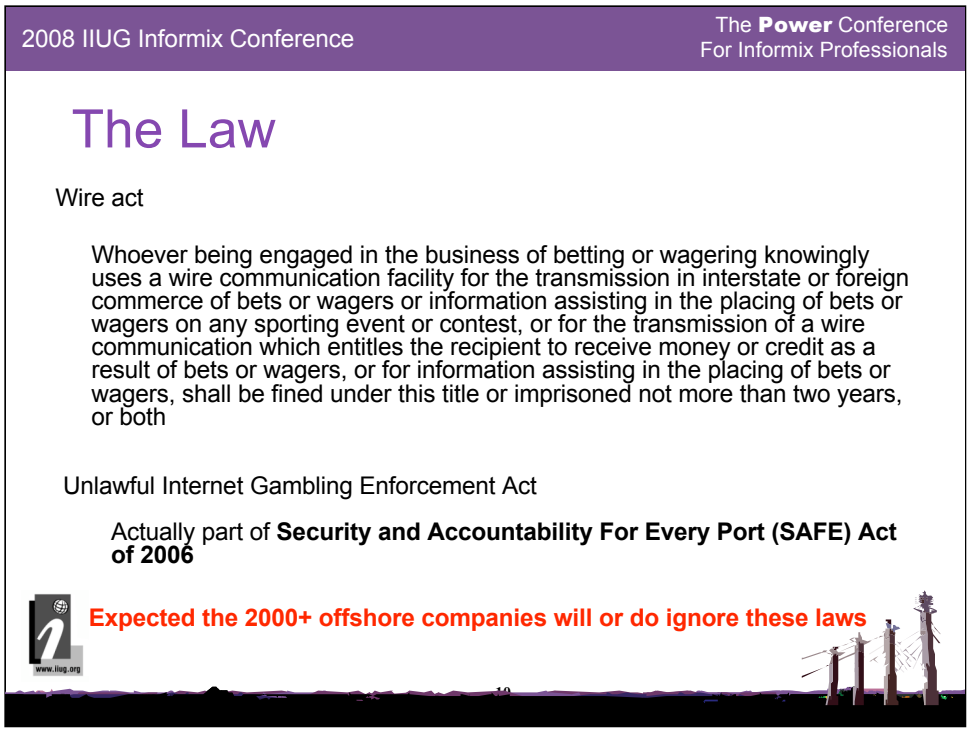
The majority have at least degree level education

The majority are not married

80% lose, 20% break even

## The Problems

- The Law
- Availability
- Security
- Awful Workloads




The law has been interpreted by some, including the Department of Justice, to mean that all online gambling is illegal. However, U.S. Courts have ruled to the contrary. Also, many believe the phrase "in the business of" means only businesses are affected. Some argue that the law only covers sports betting, and not other forms of gambling such as poker.

The U.S. Fifth Circuit Court of Appeals has ruled that the Wire Act applies only to sports betting and not other types of online gambling.[2] The Supreme Court has not ruled on the meaning of the Federal Wire Act as it pertains to online gambling.

This title (found at 31 U.S.C. § 5361-5367) prohibits the transfer of funds from a financial institution to an Internet gambling site, with the notable exceptions of "fantasy" sports, online lotteries, and horse/harness racing.

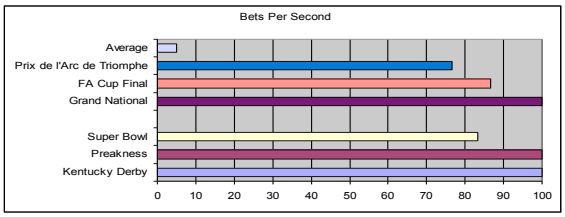
## Availability

- Five Nine availability is the norm for the larger companies, that is 315 seconds per year
- Downtime measure in excess of $50K per hour

## Workloads

- For example  The worlds largest betting exchange

5 million transactions per day.
Peaking at 300 bets per second
1,200,000,000 bets in 2005
200,000 web pages per minute
99.5% of ALL bets are processed in under 250ms




Sporting Bet

Equivalent of 13 games of poker per second (pro forma 2004: 8 games per second)

Average daily Paradise Poker rake up 88.8% to $283,824 (2004: $150,277)

## So Why Do They Use IDS

- The Trite Answer ????

**They have no choice**
**NOTHING else will do what they need**

# Uptime

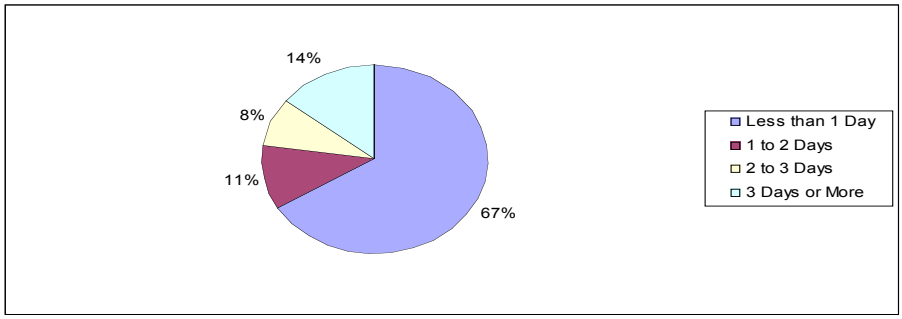
| Informix Version | Average / Days Since Installation |
|---|---|
| 7.x | 201 |
| 9.x | 264 |
| 10.x | 154 |

Note: V10 had only be GA one year

Source: Oninit.com

# TCO

Average DBA Days / Year
25% report no DBA time at all
An Average of 7 minutes per user week




Source: Oninit.com

# User Comments

"Can't remember ever having an IDS related outage"

"Our last outage due to Informix was at least 5 years ago"

"This database has never been down except for server OS upgrades"

"Informix IDS has been approved as a very solid DBMS"

" Can't remember the last outage…over 5 years ago "

"The last unplanned outage was in 2004 when we had a massive power failure"

"I have worked here for almost 4 years and we have never had an outage"


Source: Oninit.com

# What is Label-Based Access Control?

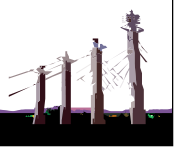
- LBAC aka Advanced Access Control
  - based on the design in DB2
  - Essentially the same
- Provides Mandatory Access Control (MAC)
  - Orange Book (B1) style label-based security
    - But different from MLS – multi-level security – in some aspects
  - Analogous to Oracle's Label Security
  - Intended for certification versus Common Criteria
    - At EAL4, against LSPP (Labelled-Security Protection Profile)
- Based on the Bell-LaPadula model
  - Bell, LaPadula, 'Secure Computer System: Unified Exposition and Multics Interpretation', ESD-TR-75-306, Mitre Corporation, 1976.


# What is Label-Based Access Control?

- Data is labelled
  - By columns,
  - Or by rows
  - Or both
- Users are granted labels
- Access to data is controlled
  - Based on user's label
  - And data's label
  - Read permissions different from write permissions
    - If required


# Why would you use LBAC?

- LBAC controls prevent unauthorized access
  - By system administrators
  - As well as by users

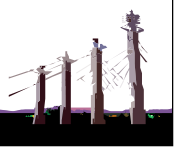


# LBAC Demonstration

User Label – Public

| Security Label | Name | Rank | Task |
|---|---|---|---|
| Public | John Smith | CEO | Run Company |
| Public | James Talbot | CFO | Run Accounts |
| Public | Malcolm Knight | CIO | Run IT |

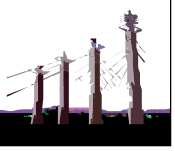
SELECT * FROM People



# LBAC Demonstration

User Label – Confidential

| Security Label | Name | Rank | Task |
|---|---|---|---|
| Public | John Smith | CEO | Run Company |
| Confidential | Heinrich Messier | Accountant | SEC Relations |
| Public | James Talbot | CFO | Run Accounts |
| Confidential | Jessica McHenry | IT Specialist | Networks |
| Confidential | Melissa Williams | IT Specialist | Databases |
| Public | Malcolm Knight | CIO | Run IT |

# LBAC Demonstration

| Security Label | Name | Rank | Task |
|---|---|---|---|
| Secret | Verity Dolittle | M & A | Buy Google |
| Public | John Smith | CEO | Run Company |
| Confidential | Heinrich Messier | Accountant | SEC Relations |
| Secret | Alex Grimwald | M & A | Buy Yahoo! |
| Public | James Talbot | CFO | Run Accounts |
| Confidential | Jessica McHenry | IT Specialist | Networks |
| Secret | Jane Ferguson | M & A | Buy Microsoft |
| Confidential | Melissa Williams | IT Specialist | Databases |
| Secret | Kate Ball | M & A | Buy Oracle |
| Public | Malcolm Knight | CIO | Run IT |


# Why would you use LBAC?

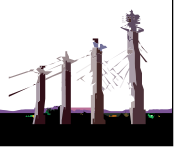
- LBAC provides extra control over who can see what
  - Labels can be applied to columns
    - To prevent unauthorized users from reading those columns.
  - Labels can be applied to rows
    - Unauthorized users will not see rows with too sensitive labels
- Access can be controlled declaratively
  - By granting or revoking labels
  - By granting or revoking exemptions
- Provides extra protection for the most sensitive data
  - Credit card numbers
  - Social security numbers


# Mechanics of LBAC

- LBAC can be frightening
  - Don't be scared
  - Don't use it if you don't need it
- LBAC has
  - Security policies
  - Security label components
  - Security labels
- Designing policies
  - Work out the types of protection needed
    - Create the security label components
    - Create the security policy
    - Create the security labels
  - Remember the KISS Principle

# Creating a Security Policy

- Security Policy
  - Database object that can be applied to tables
  - Composed of one or more security label components
  - Created after label components
- Security Label Component
  - Components can be Array, Set, or Tree types
  - Controls which rules apply to access

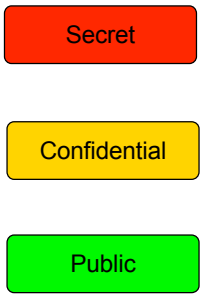
# Creating a Security Policy

- Security Label
  - Always associated with a specific security policy
  - Includes one value for each component in the policy
    - A value is zero or more of the elements of the component
  - Created after security policy
  - Labels apply to users
    - Subject labels
  - Labels apply to data
    - Object labels

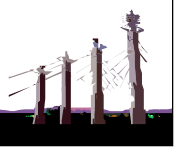
# Array Component

- Ordered list of elements
  - Up to 64 elements
  - First one is the highest
- Only one element allowed in a label for a component
- Read data that is less than or equal to your level
  - No read up
- Write data equal to your level.
- **`CREATE SECURITY LABEL COMPONENT level ARRAY ['Secret', 'Confidential', 'Public'];`**


# Security Label Component – Array

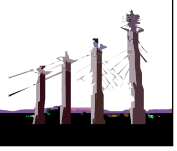



- If your read label is Secret
  - You can read anything
  - Your write label must be Secret
- If your read label is Confidential
  - You can read Confidential or Public data
  - Your write label must be Confidential
- If your read label is Public
  - You can only read Public
  - Your write label must be Public
- Closest to the Bell-LaPadula model

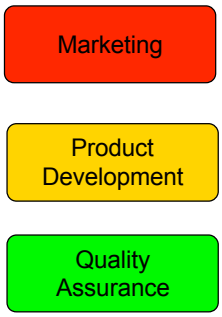



# Set Component

- Non-ordered set of elements
  - Up to 64 elements
- One or more elements in a label for a component
- You can read or write data if your label contains **all** the elements in the data label
- `CREATE SECURITY LABEL COMPONENT department SET {'Marketing', 'Product Development', 'Quality Assurance'};`

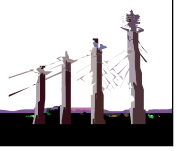
# Security Label Component – Set



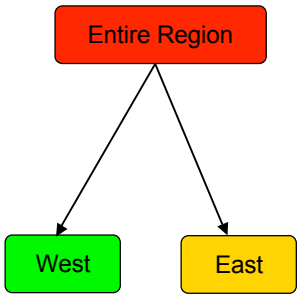

- If your read label has { Marketing }
  - You can read anything that is marked just Marketing
  - Or has an empty Department label component
  - But not anything marked Marketing and Product Development
- If your read label is { Product Development, Quality Assurance }
  - You can read items marked Product Development
  - You can read items marked Quality Assurance
  - Or both
  - Or with an empty label component

# Tree Component

- Hierarchical set of elements
  - Up to 64 elements
- You can have one or more elements in a label
- You can read or write data if your label contains **any** of the elements in the data label, or the ancestor of one such element.
- **`CREATE SECURITY LABEL COMPONENT region TREE ('Entire Region' ROOT, 'East' UNDER 'Entire Region', 'West' UNDER 'Entire Region');`**

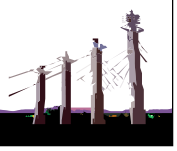
# Security Label Component – Tree




- If your read label is Entire Region
  - You can read anything
- If your read label is West
  - You can only read West or empty
- If your read label is (West,East)
  - You can only read East or West
  - You cannot read items labelled Entire Region

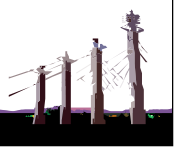
# Read Access Rules

- Read Access Rules are applied when data is read.
  - Data is read on SELECT, UPDATE and DELETE.
  - **IDSLBACREADARRAY**
    - Each array component of the user security label must be greater than or equal to the array component of the data security label
    - The user can only read data at or below his/her level.
  - **IDSLBACREADSET**
    - Each set component of the user security label must include the all the set components of the data security label.
  - **IDSLBACREADTREE**
    - Each tree component of the user security label must include at least one of the elements in the tree component of the data security label (or the ancestor of one such element).

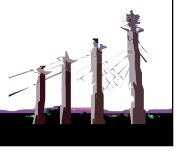
# Write Access Rules

- Write access rules are applied when data is written.
  - Data is written on INSERT, UPDATE and DELETE.
  - **IDSLBACWRITEARRAY**
    - Each array component of the user security label must be equal to the array component of the data security label
    - That is, the user can write data only at his/her level.
    - No write-down.
  - **IDSLBACWRITESET**
    - Each set component of the user security label must include the set component of the data security label.
  - **IDSLBACWRITETREE**
    - Each tree component of the user security label must include at least one of the elements in the tree component of the data security label (or the ancestor of one such element).

# Creating a Security Policy

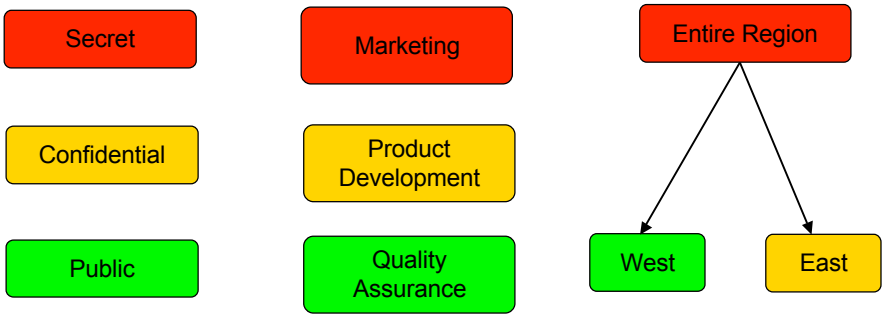
- A Security Policy is created from Security Label Components
  - Up to 16 components
  - But think in terms of using 1 to at most 3
- **`CREATE SECURITY POLICY company COMPONENTS level, department, region;`**
  - This policy has three components.
  - Labels for this policy have a value for each component
    - Zero or more elements for the tree and set components
      - Department
      - Region
    - Precisely one element for the array component
      - Level

# Creating a Security Policy

- Additional optional clause
  - WITH IDSLBACRULES [[OVERRIDE | RESTRICT] NOT AUTHORIZED WRITE SECURITY LABEL]
- Controls what happens when users specifies label
  - On INSERT or UPDATE
- No label supplied
  - Data is written with the user's WRITE security label
- If the explicitly label supplied is not authorized
  - RESTRICT – Prohibit the operation
- Alternatively, even if label is not authorized
  - OVERRIDE – Use the user WRITE label
- No alternative to IDSLBACRULES at the moment

# Multi-Component Security Policy




Each label will have one of Secret, Confidential, Public
Each label will have zero or more of Marketing, Product Development, Quality Assurance
Each label will have zero of mode of Entire Region, East, West

# Creating Security Labels

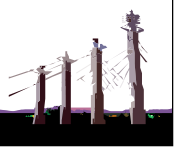
- A Security Label specifies the value for each component in a Security Policy
- **CREATE SECURITY LABEL company.director**

```
COMPONENT level 'Secret',
COMPONENT department 'Product Development', 'Quality
  Assurance',
COMPONENT region 'Entire Region';
```

  - Single element in label for components level and region
  - Multiple elements in label for component department


# Applying a Security Policy

- Protecting rows
  - Row level protection granularity
  - Attach security policy to table
  - Add security label column of new type:
    - IDSSECURITYLABEL
- Protecting columns
  - Column level protection granularity
  - Attach security policy to table
  - Attach security label to one or more columns
- Protecting rows and columns
  - Attach security policy to table
  - Apply label to one or more columns
  - Add security label column

# Protecting a Table

- CREATE TABLE T1
  ( C1 IDSSECURITYLABEL, { Always NOT NULL }
    C2 INTEGER NOT NULL,
    C3 CHAR(10) NOT NULL
       COLUMN SECURED WITH director
  ) SECURITY POLICY company;
- ALTER TABLE T2
    ADD(C1 IDSSECURITYLABEL),
    MODIFY(C2 INTEGER NOT NULL
              COLUMN SECURED WITH manager),
    ADD SECURITY POLICY company;

Only a DBSECADM with either RESOURCE or DBA privileges can create or modify a protected table.

# Granting Security Labels

- Security labels can be GRANTED to users.
  - The same label can be granted to many users.
  - Each user can be granted 0, 1 or 2 labels for a policy
    - One READ label
    - One WRITE label
  - If the labels are different,
    - The READ label must dominate the WRITE label.
    - i.e. You have to be able to read what you write.
  - Labels may not be granted to roles.
- **`GRANT SECURITY LABEL company.director TO mr_ceo FOR ALL ACCESS;`**
  - i.e. mr_ceo cannot read Marketing information

# Granting Exemptions

- The read-write rules are quite stringent
  - No read up (within an array or tree)
  - No write down (within an array or tree)
- Sometimes, data needs to be reclassified.
- EXEMPTIONS allow you to control that.
  - A user can be granted an exemption to bypass one or more access rules for a component type in a security policy
- Only someone with DBSECADM authority can grant exemptions
  - DBSECADM cannot grant themselves labels or exemptions

# Granting Exemptions

- **GRANT EXEMPTION ON RULE**
  **IDSLBACWRITEARRAY WRITEDOWN**
  **FOR company TO mr_ceo;**
  - User 'mr_ceo' can now breach the array rule
  - He can write a row with level 'public' or 'confidential'.
  - Must still keep to the rules for department and region
- Exemptions should only be granted temporarily
  - Otherwise, why bother with LBAC at all!
- **REVOKE EXEMPTION ON RULE**
  **IDSLBACWRITEARRAY WRITEDOWN**
  **FOR company FROM mr_ceo;**

IDSLBACREADARRAY, IDSLBACREADSET, IDSLBACREADTREE do not need qualifiers

IDSLBACWRITESET and IDSLBACWRITETREE do not need qualifiers.

# SQL Function: SECLABEL_BY_COMP

- **SECLABEL_BY_COMP**
  - Security label value based on policy and components
  - A built-in function
  - Used in insert and update operations
  - Returns the row security label of a data row
    - Specified by its individual components
  - INSERT INTO T1 VALUES (SECLABEL_BY_COMP('company', 'Director:Marketing:West'), 1, 'xyz')

# SQL Functions

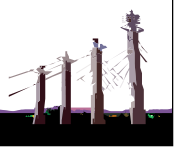
- **SECLABEL_BY_NAME**
  - Security label value based on policy and label name
  - A built-in function
  - Used in insert and update operations
  - Returns the row security label of a data row
    - Specified by label name
  - UPDATE T1 SET C1 = SECLABEL_BY_NAME(‘company', ‘manager')

# SQL Functions

- **SECLABEL_TO_CHAR**
  - Convert security label value to component string
  - A built-in function used in select operations
  - To retrieve the row security label column
  - And returns it as a string
  - SELECT SECLABEL_TO_CHAR('company', C1), C2, C3 FROM T1

# DBSECADM

- Database security administrator
- Server level role
- Can be granted by DBSA only
- Responsibilities
  - Create, drop, alter and rename security label components
  - Create, drop and rename security policies
  - Create, drop and rename security labels
  - Attach, detach policies to/from tables
  - Grant and revoke security labels
  - Grant and revoke policy exemptions
  - Grant and revoke setsessionauth privilege

# SETESSIONAUTH privilege

- SET SESSION AUTHORIZATION statement
  - Allows DBA to assume identity of another user
    - Without any authentication step
  - DBA can see other users' data in protected table
- New privilege SETSESSIONAUTH
  - To prevent unauthorized access
  - Allows DBSECADM to control who can use
    - SET SESSION AUTHORIZATION
  - Not automatically granted to DBA

# SETESSIONAUTH privilege

- Only DBSECADM can grant SETSESSIONAUTH
- Only users with SETSESSIONAUTH privilege
  - Can use the SET SESSION STATEMENT
- During conversion from older server to 11.10
  - SETSESSIONAUTH privilege is granted to DBA
  - For backward compatibility.


# Utilities

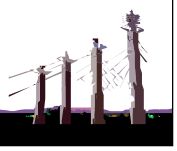
- dbschema, dbexport, dbimport
  - User must be granted DBSECADM role if database contains LBAC objects
  - User must have necessary labels or exemptions if all rows in protected tables are to be exported/imported
- onload, onunload
  - User must possess all exemptions to bypass the security policy

# Utilities

- HPL (Express mode)
  - User must possess all exemptions to bypass the security policy
- All other load/unload utilities
  - User must have necessary labels or exemptions if all rows in protected tables are to be loaded/unloaded

# Restrictions

- Tables that cannot be protected
  - VTI tables
  - Tables with VII indexes
  - Temp tables
  - Typed tables
  - Hierarchical tables
- Security label column cannot have
  - Referential constraints
  - Check constraints
  - Primary Key or Unique constraints
    - If security label column is the only column in constraint
  - Column protection
  - Encryption

# Is that all?

- No.
- There are lots of other operations
  - ALTER, RENAME, DROP operations
- There are other issues to discuss
  - ER, HDR
- Performance
  - SELECT * FROM RowProtectedTable
    - LBAC has a cost
    - Dependent on your usage

# Questions ???

Session: C
Bet on IDS

# Paul Watson