Comprehensive Approach to Database Security

Ajoy S. Kumar

asota@hotmail.com

NYOUG
2008

What will I discuss today

- Identify Threats, Vulnerabilities and Risk to Databases
- Analyze the drivers for Database Security
- Identify security solutions for Database
- Analyze use of point solutions to achieve Comprehensive Database Security
- Understand that there are no single solution to achieve complete database security
- Reduce risk to acceptable level by deploying layered defense strategy

Comprehensive Database Security

- Introduction to Security
- Introduction to Databases
- Threat, Vulnerabilities and Risk on Databases
- Threat Trend
- Drivers for Database Security
- Attacks on Databases
- Solutions for Database Security
- Comprehensive Database Security
- Intrusion Detection
- Encryption in Real Life
- Conclusion

Comprehensive Database Security

- **Introduction to Security**
- Introduction to Databases
- Threat, Vulnerabilities and Risk on Databases
- Threat Trend
- Drivers for Database Security
- Attacks on Databases
- Solutions for Database Security
- Comprehensive Database Security
- Intrusion Detection
- Encryption in Real Life
- Conclusion

Introduction to Security

- **Security is based on 3 pillars**
  - Confidentiality
  - Integrity
  - Availability
- **Security Services**
  - Access Control
  - Authentication
  - Authorization
- **Services built around**
  - People
  - Process and
  - Technology

Comprehensive Database Security

- Introduction to Security
- **Introduction to Databases**
- Threat, Vulnerabilities and Risk on Databases
- Threat Trend
- Drivers for Database Security
- Attacks on Databases
- Solutions for Database Security
- Comprehensive Database Security
- Intrusion Detection
- Encryption in Real Life
- Conclusion

Relational Database Management Systems (RDBMS)

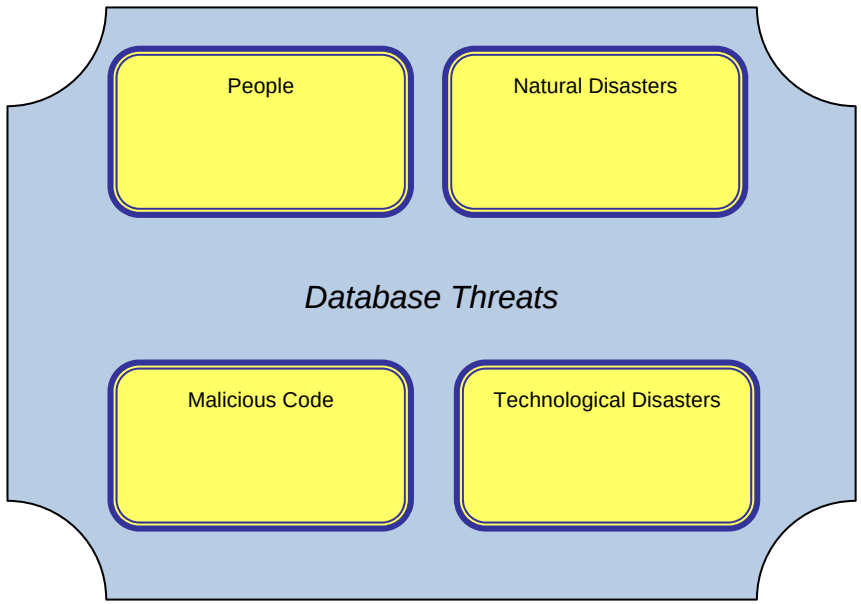
- RDBMS engine interact with clients, servers using operating system files, processes, memory, inter-process communication etc… making a complex system work seamless.
- RDBMS have revolutionized the information usage, they offer:
  - Orderly Storage of data
  - Efficient retrieval of data
  - Offer rich features of Primary key and Foreign key for Integrity
  - Offer Normalization of data
  - SQL, and feature rich APIs hide the complexity of operations
  - Easy Management features for Administrators (performance, storage management, backups for continuity and availability)
  - Offer Security features
  - Offer rich features for Web Integration e.g.: Oracle RDBMS executes Java machine within the database engine
- Internet has brought world wide networks closer, protection boundaries are blurred, Databases are much closer to the internet then perceived

Comprehensive Database Security

- Introduction to Security
- Introduction to Databases
- **Threat, Vulnerabilities and Risk on Databases**
- Threat Trend
- Drivers for Database Security
- Attacks on Databases
- Solutions for Database Security
- Comprehensive Database Security
- Intrusion Detection
- Encryption in Real Life
- Conclusion

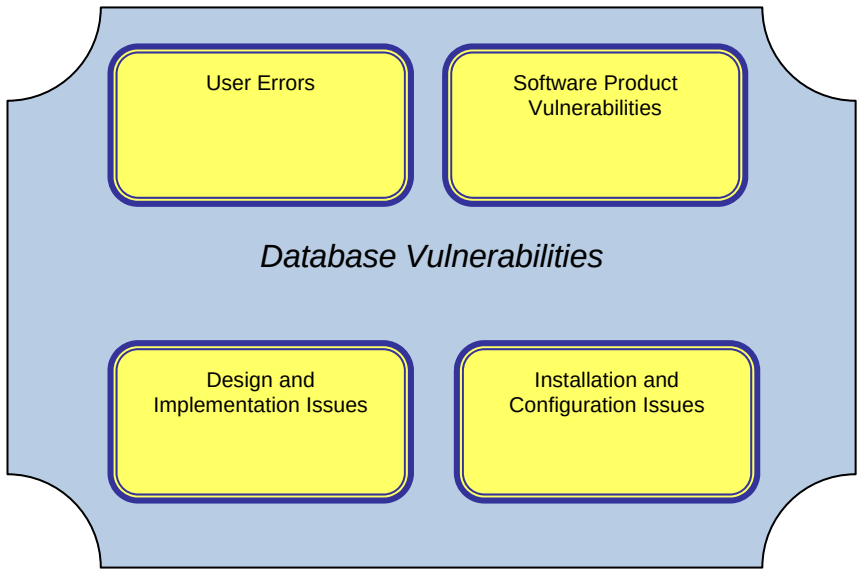
Database Threats

Threat: “A Security violation or attack that can happen any time because of security vulnerability”



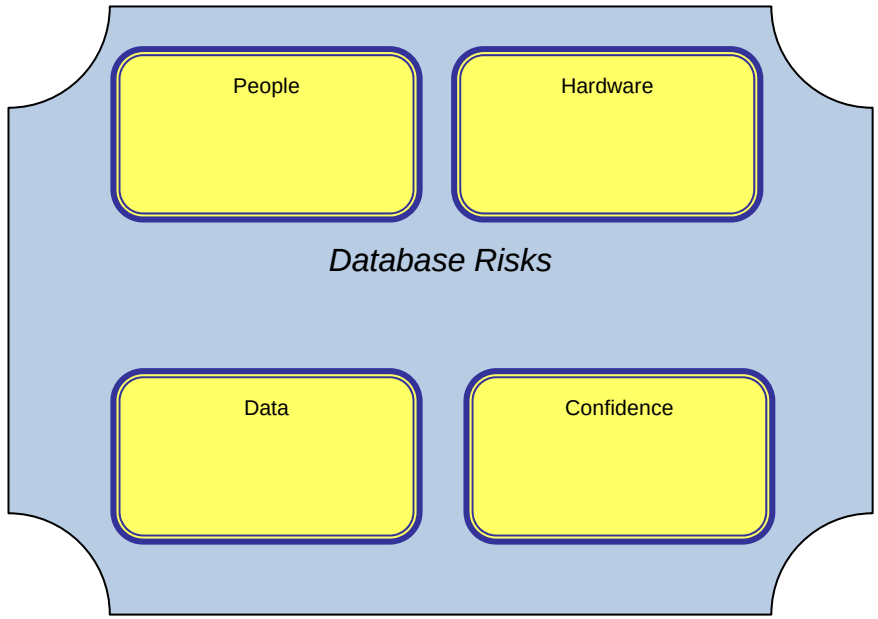
Database Vulnerabilities

Vulnerability: “A weakness in any of the information system components that can be exploited to violate the integrity, confidentiality, or accessibility of the system.”



Database Risks

Risk: “The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.”



Managing Risk

- Risk Management
- Analyze Risk
  - Asset Information (Business Criticality and Sensitivity)
  - Analyze Threat
  - Analyze Controls
  - Analyze vulnerabilities
  - Analyze Likely hood and Impact
  - Cost Benefit Analysis for Controls
- Manage Risk
  - Transfer Risk
  - Mitigate Risk
    - Eliminate Threat
    - Eliminate Vulnerability
  - Terminate Activity
  - Reduce to Acceptable Level

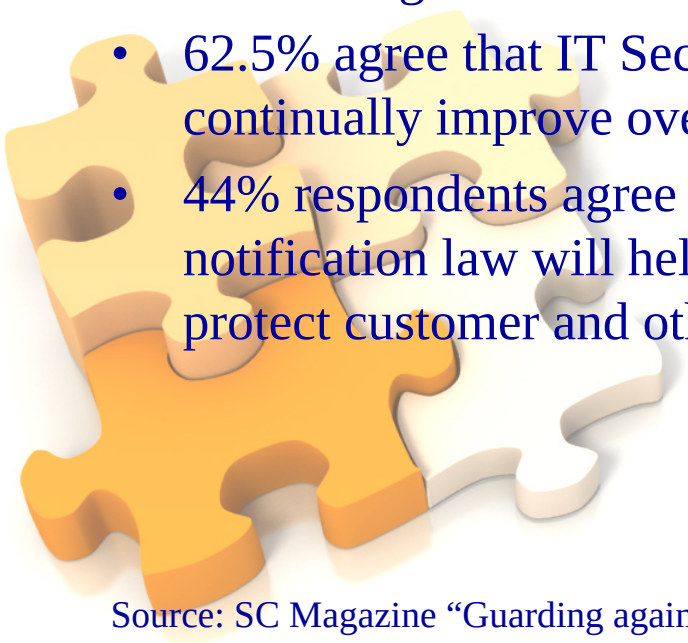
Comprehensive Database Security

- Introduction to Security
- Introduction to Databases
- Threat, Vulnerabilities and Risk on Databases
- **Threat Trend**
- Drivers for Database Security
- Attacks on Databases
- Solutions for Database Security
- Comprehensive Database Security
- Intrusion Detection
- Encryption in Real Life
- Conclusion

Threat Trend for Databases

Industry Facts:

- Over 20% companies acknowledged that they had a suffered a loss, theft or breach of customer data in previous year
- 81% of respondents say that the threat of data breaches is influencing their security initiatives.
- 62.5% agree that IT Security and Executive Leadership will continually improve overall security strategy for safeguarding data
- 44% respondents agree that passage of national data breach notification law will help in their corporate security efforts to protect customer and other data.



Source: SC Magazine “Guarding against Data Breach” , I. Armstrong, 2008

Categorizing the Database Security Threat Trend

- SQL Injection is among Top threat
- Database Rootkits
- Denial of Service
  - Spida worm
  - Slammer worm
- Loss of Tapes
- New SQL Injection worm

Comprehensive Database Security

- Introduction to Security
- Introduction to Databases
- Threat, Vulnerabilities and Risk on Databases
- Threat Trend
- **Drivers for Database Security**
- Attacks on Databases
- Solutions for Database Security
- Comprehensive Database Security
- Intrusion Detection
- Encryption in Real Life
- Conclusion

Drivers for Data Security

- Government Regulations
- Corporate Brand and Financial
- Knowledge of Data
- Lack of comprehensive security solutions for databases
- Standards Implementation
- Multi-Tier Complexity
- Patching Problem

Government Regulations

Key Regulations:

GLBA	SOX	FISMA	PATRIOT
PCI	FFIEC	HIPPA	Safe Harbor
Privacy Act 1974	EU	BASEL II	UN

- Payment Card Industry (PCI) requires extensive checks on Database authentication, encryption and separation of duty

ISTPA* research confirms:

- 10 US and EU regulations require organizations to be accountable for - "Organization must be sure to include safeguards to prevent loss, misuse, unauthorized access, disclosure, alteration, and destruction of data."
- 5 US and EU regulations require organizations to be accountable for - "Accountability of Organization for applicable privacy policy"

*ISTPA - International Security Trust and Privacy Alliance

Government Regulations cont…

- 79% respondents of TJX survey confirm regulations is one of the key driver for security
- 39 states have state laws for Privacy Protection
- Legislation for “National Data Law” failed again last year – no doubt it will come back again
- Executives are directly being held accountable for non-compliance with some of these regulations
- There is more pressure on some vertical markets in comparison to others

Corporate Brand and Financial

Reputation Loss:

- TJX Breach incidence resulted in loss of over 90 Million credit cards
- Harvard University lost information of 10,000 applicants and 6,600 student (that could have SSN). The databases were posted to “The Pirate Bay”
- PrivacyRights.org reports – There are to a close to 200 breaches this year*
- PrivacyRights.org reports – Between Jan 2005 and June 15, 2008 - 229,441,775 records containing sensitive personal information were involved in security breaches

Source: http://www.privacyrights.org/ar/ChronDataBreaches.htm#2008

Corporate Brand and Financial cont…

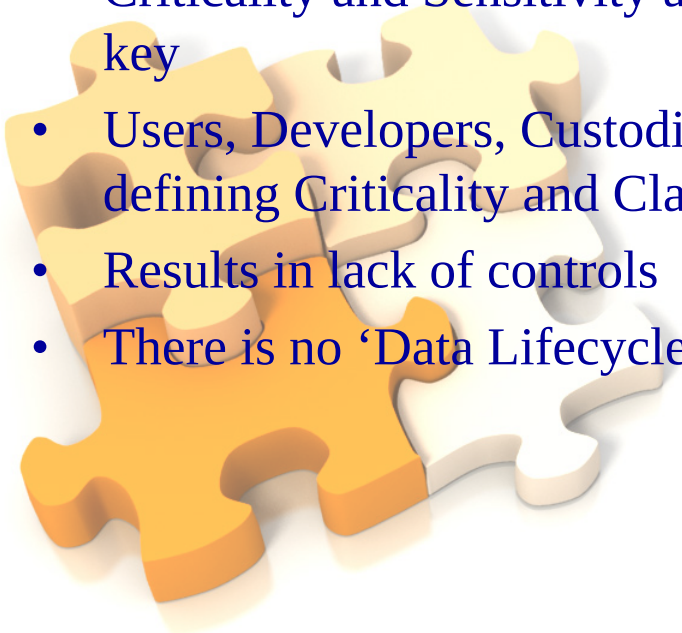
Financial Loss:

- TJX increased pre-tax charges for security compromise to $216 Million from initial estimate of $168M
- 3 States (MA, CT, ME) filed a Class Action lawsuit against TJX to recover costs of damage “totaling tens of millions of dollars”
- 45% respondents of executive board demand compliance*
- 40% respondents say profit loss is the driver for their business*

Source: SC Magazine “Guarding against Data Breach” , I. Armstrong, 2008

Knowledge of Data

- Understanding the business value of information is paramount for:
  - Sensitivity (Classification)of data
  - Business Criticality
- Enterprises continuously create, update, modify and destroy data
- Criticality and Sensitivity at the time of any of above operations is key
- Users, Developers, Custodians and even owners (at times) miss defining Criticality and Classification
- Results in lack of controls
- There is no ‘Data Lifecycles defined in companies’

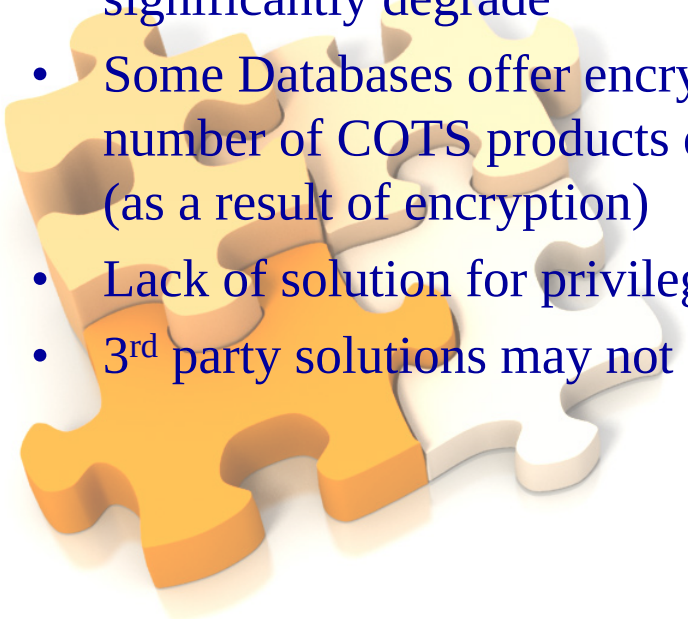


Knowledge of Data cont…

- With the amount of structured and unstructured data created in enterprises – in the absence of “Data Lifecycle” there is limited opportunity for controls
- This is not a Technology issue, controls can be:
  - Administrative
  - Technical or
  - Logical
- Controls must be identified upon data creation or modification

Lack of Comprehensive Security solutions for databases

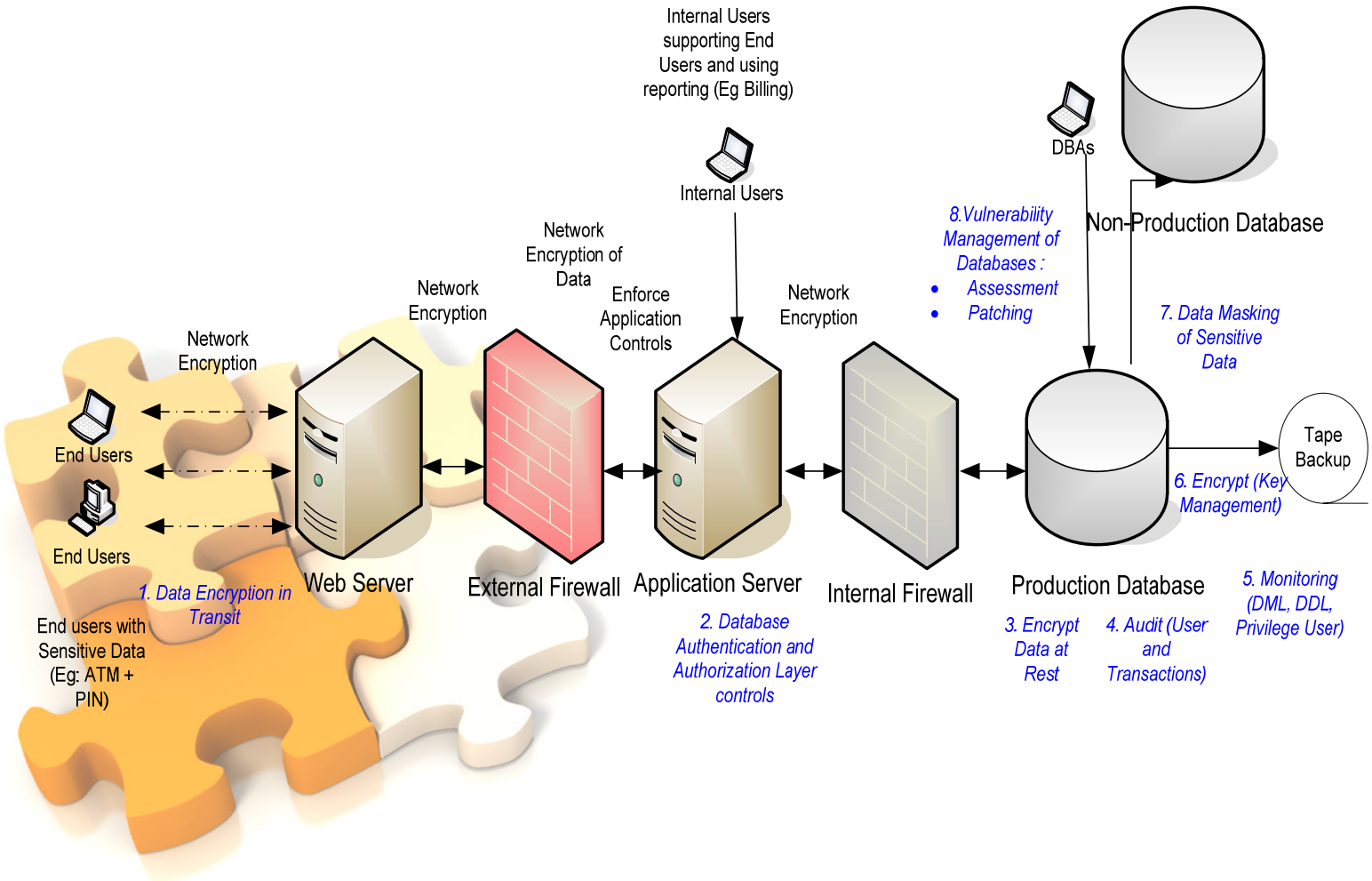
- Database products lack end to end protection solution
- If the solutions are available, other factors prevent the deployment of appropriate controls. E.g. If you want to audit DML (Select, Insert, Update and Delete) – performance of database can significantly degrade
- Some Databases offer encryption for confidentiality, however, number of COTS products do not support the changes to meta data (as a result of encryption)
- Lack of solution for privileged user monitoring
- 3rd party solutions may not support all database technology



Standards Implementation

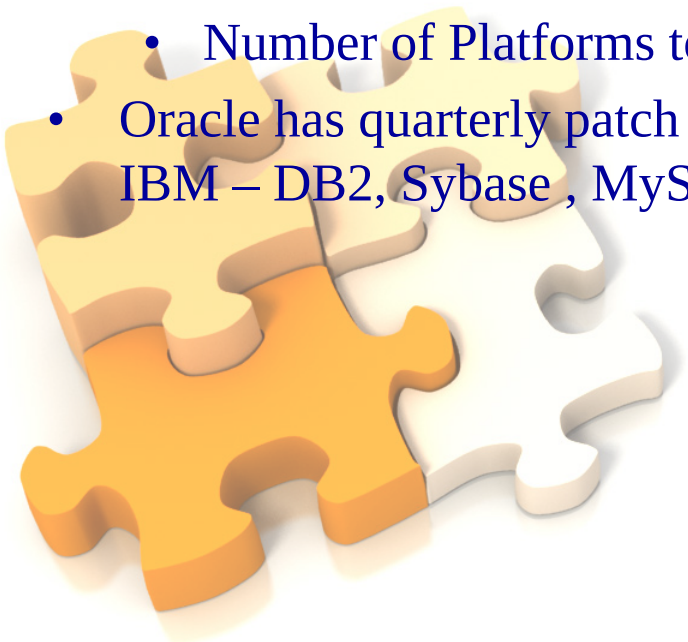
- SQL-92, SQL-99 and SQL-2003 standards are not fully implemented
- No standardized SYNTAX for various features
- This complicates development of 3rd party solutions
- Home grown solutions expensive to maintain
- Databases are getting feature rich, standards needs quicker ratification
  - Hybrid environment gets complex to manage
  - Compliance to standards lags, Securing database gets tougher
  - Issues in interoperability causes issues with Operational Security

Multi-Tier Complexity



Patching Problem

- Patching Problem-
  - Weakness in SDLC
  - New Features (goodness, but lack of controls makes it bad)
  - New Security Fixes
  - Time to test
  - Number of Platforms to patch
- Oracle has quarterly patch release, Microsoft has Patch Tuesday, IBM – DB2, Sybase , MySQL release patches at specific frequency



Comprehensive Database Security

- Introduction to Security
- Introduction to Databases
- Threat, Vulnerabilities and Risk on Databases
- Threat Trend
- Drivers for Database Security
- **Attacks on Databases**
- Solutions for Database Security
- Comprehensive Database Security
- Intrusion Detection
- Encryption in Real Life
- Conclusion

Popular attacks on Databases

- SQL Injection
  - Input validation (lack) attack
    - Top List of OWASP – categorized as “Injection Flaw”
    - Top list of WASC – categorized as “Command Execution”
  - Used for:
    - Authorization bypass
    - Information Stealing
    - Denial of Service
    - Attacking the integrity of information

Popular attacks on Databases cont…

- DB Rootkits
- Rootkits are hard to discover, DB rootkits are extremely hard to discover
- Research conducted by Alexander Kornburst
- Hacker presence is stealth
- Trojans are hidden in the database by manipulating Database ‘internals’
- Best discovered accidently
- All database technologies are prone to this powerful attack

Comprehensive Database Security

- Introduction to Security
- Introduction to Databases
- Threat, Vulnerabilities and Risk on Databases
- Threat Trend
- Drivers for Database Security
- Attacks on Databases
- **Solutions for Database Security**
- Comprehensive Database Security
- Intrusion Detection
- Encryption in Real Life
- Conclusion

Solutions for Database Security

- Identity
- Authentication
- Access Control
- Audits
- Masking
- Compliance to Baseline settings
- Event monitoring
- Case for Privilege User monitoring
- Encryption for Data Protection

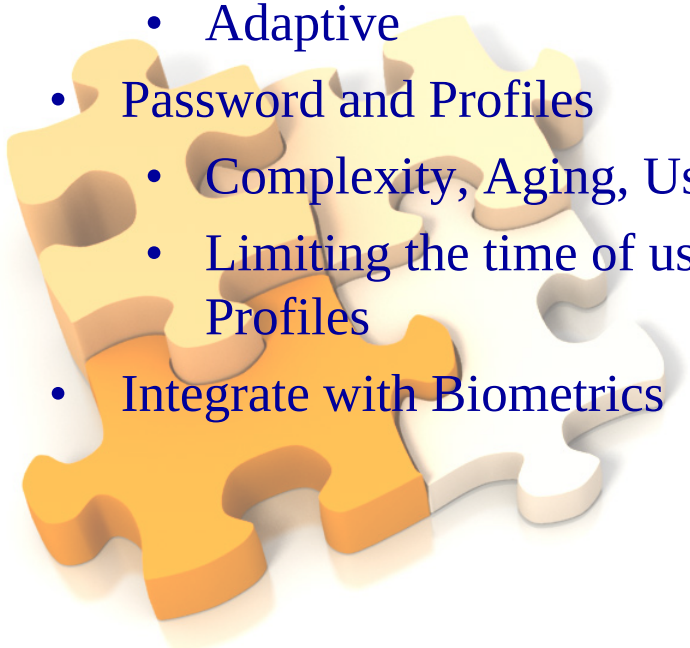
Solutions for Database Security

Identity

Authentication

- Native
- Integration with OS
- Adaptive

- Password and Profiles
  - Complexity, Aging, Usage managed from inside database
  - Limiting the time of using, usage of resources enforced by Profiles
- Integrate with Biometrics



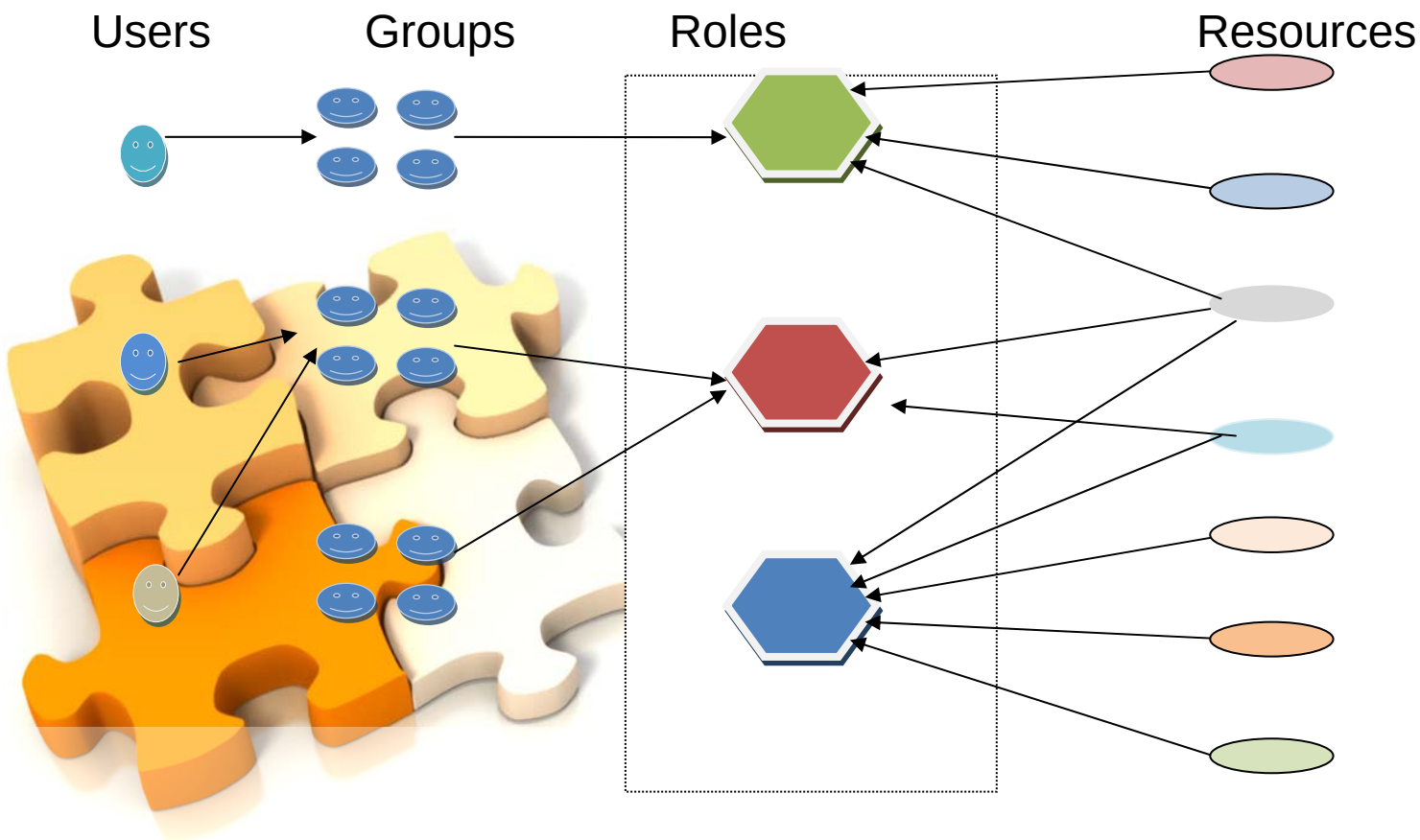
Solutions for Database Security cont…

Access Control

- Mandatory Access Control
  - DB2 (Multi Level Security)
  - Oracle (Trusted Oracle)
- Discretionary Access Control
  - All Technologies
- Role Based Access Control
- Offers flexibility of DAC, and some features of MAC
  - Most popular model for enforcing
    - Principle of Least Privilege and
    - Separation of Duty

Solutions for Database Security

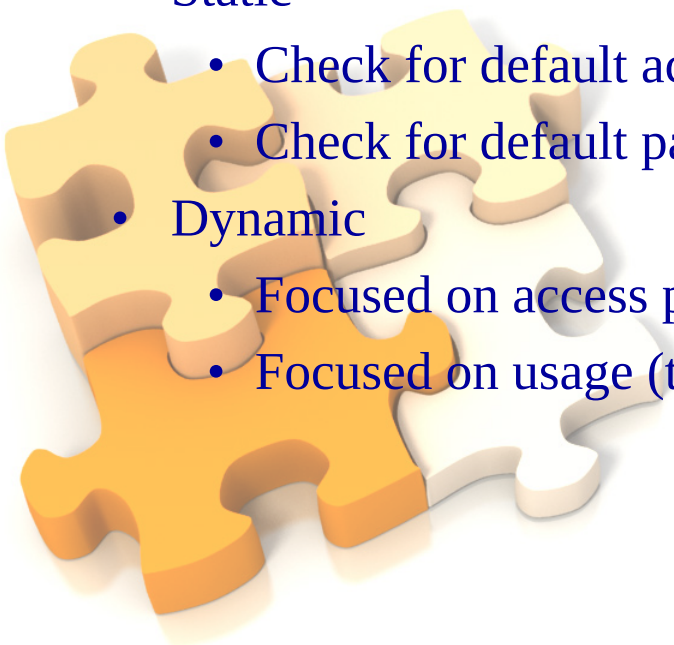
Role Based Access Control



Security Audit and Audit Trails

Security Audit

- Penetration Test
- Gaps in Configuration settings
  - Static
    - Check for default accounts
    - Check for default passwords
  - Dynamic
    - Focused on access patterns
    - Focused on usage (timings, frequency)



Security Audit and Audit Trails cont…

Audit Trail

- Audit actions carried out on the databases
- Required by HIPPA, PCI, CAL, BASEL II

Key Categories for auditing:

- Logon/Logoff
- Audit DDL
- Audit DML (for sensitive data)
- Audit Database Errors
- Audit Stored Procedures
- Audit changes to privileges, user/logins

Masking

Data Masking

- Home grown
- Industry solutions
- Focus on strengthening the process

Database Monitoring – Baseline and Compliance

Asset Inventory

- Risk Model
  - Data Classification
  - Business Criticality
  - Location in enterprise infrastructure (plays a role)

Define Baseline

- Security Audits
- Best Practices enforcement

Monitor the Compliance

- Continuous monitoring process
- Address gaps

Real Time Monitoring

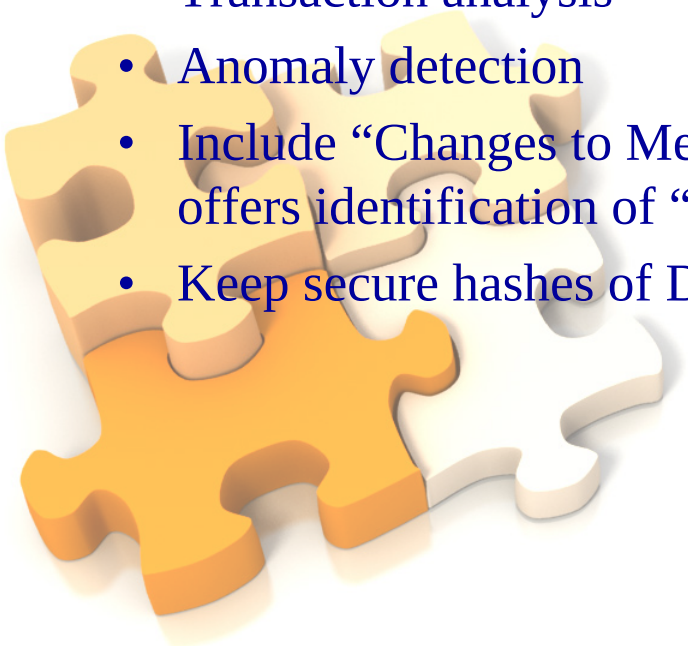
- Information on who, when, where (to and from) and what

- Collection of events from
  - Databases
  - Servers
  - Network
  - Applications
  - Storage

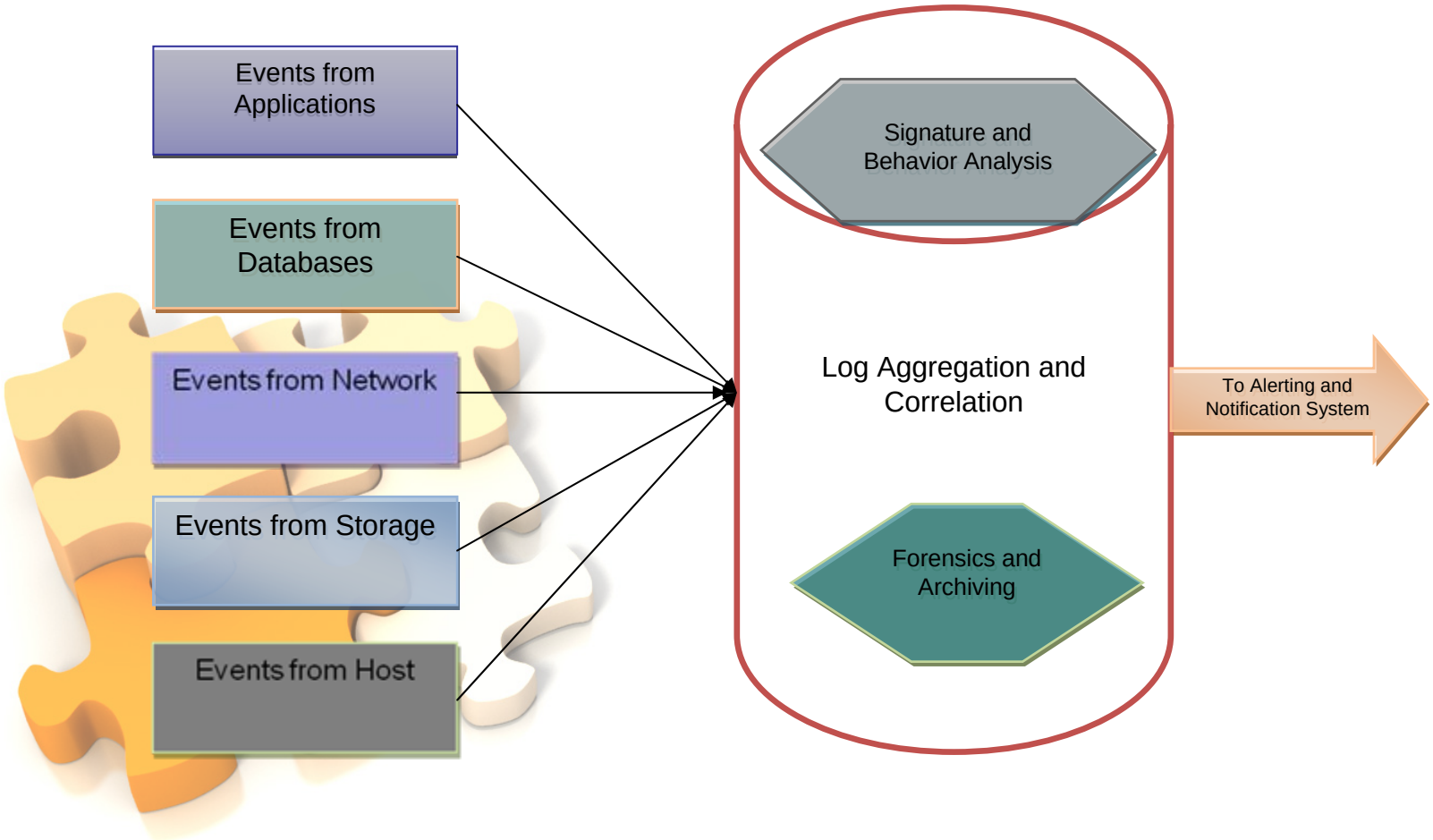
Intrusion Detection

"Many trees move. He is approaching. Birds rise up. He is concealing himself" – Sun Tzu

- Aggregate and Correlate events
  - Behavior analysis
  - Transaction analysis
  - Anomaly detection
  - Include "Changes to Meta Data" in monitoring program – offers identification of "rootkits"
  - Keep secure hashes of Database engine and Operating System



Database Monitoring – Event Monitoring (Intrusion Detection)

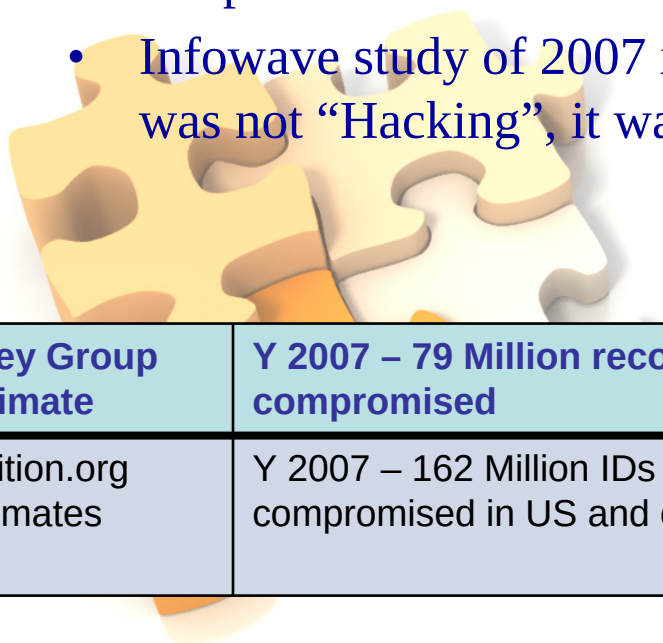


Case for Privilege User monitoring

- Database does not have features to protect data from DBAs
- Category of users with legitimate access to “Sensitive” data
  - Database Administrators (DBA)
  - System Administrators (including Tape Operators)
- Capability to browse, alter, create sensitive data, while hiding the tracks (stop auditing, delete audit trails)
- Capability to restore “Sensitive” data tapes to “Test” environments – have full range of access
- Complex problem
  - Process - Separation of duty (Role of Security Administrator)
  - Technology offers some help (encryption)
  - IBM has designed a Label Based Access Control (LBAC) for protecting rows and columns from DBAs

Encryption for Information Protection

- Sensitive information is formed by combination of data elements. These elements include:
  - Name, Social Security number, Credit card number, Date of Birth, Medical records, Intellectual Property, elements of personnel information, Trade Secrets etc.
- Infowave study of 2007 identifies - prime reason for compromise was not “Hacking”, it was lack of Internal controls



Foley Group Estimate	Y 2007 – 79 Million records (ID) compromised	Y 2006 – 20 Million records (ID) compromised
Attrition.org Estimates	Y 2007 – 162 Million IDs compromised in US and overseas	Y 2006 – 45 Million IDs compromised

Encryption for Information Protection

- It is a business problem
  - Business: Loose competitive advantage with loss of sensitive data.
    - Veterans Department – Loss of unencrypted tapes
    - Citibank, BONY-Mellon (April 2008) – loss of tape – Enterprise wide Encryption initiative
  - Regulations: Certain regulations explicitly specify need to protect sensitive information
    - PCI requires sensitive fields encrypted
  - Need to Follow Data: Data gets created, altered, improved, backed up tapes, restored on Test Systems, replicated.
    - Encrypt at source of creation, alteration may offer some control

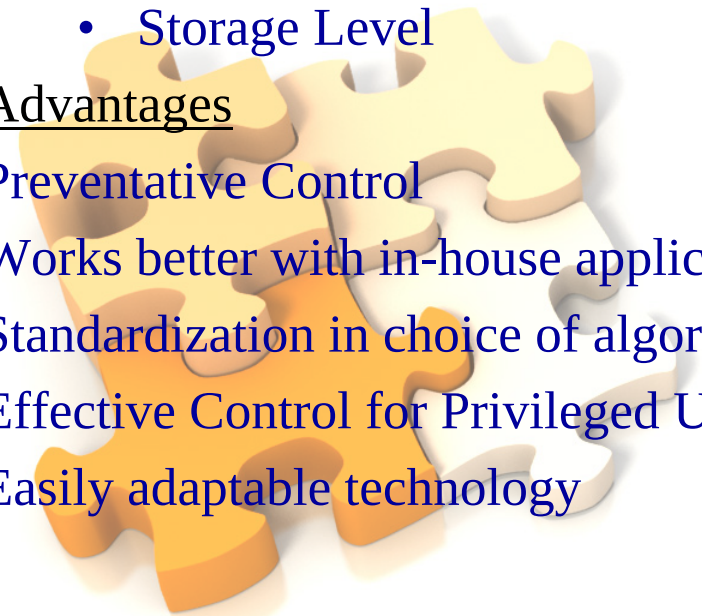
Encryption for Information Protection

Protect the confidentiality

Data at Rest — Data in Transit

Database technology vendors offer native encryption

- Solutions offered for
  - Table Level Protection — Column Level Protection
  - Storage Level



Advantages	Disadvantages
Preventative Control	COTS product support issue
Works better with in-house applications	Performance implications
Standardization in choice of algorithms	Extra Storage requirements
Effective Control for Privileged User	KEY MANAGEMENT
Easily adaptable technology	Issues with Recoverability

- Not a Golden bullet, implement with appropriate process

Conclusion and Future Direction

- Database Security is a business problem
- Database Security can only be achieved with layered defenses
- Data Security is not a one time problem, it is constant journey
- Database and 3rd party vendors offer point solutions
- Use of point solutions helps institute key controls
- Data Governance program will help areas of focus
- Government is regulating, however, it is insufficient, enactment of "National Data Law" has failed in congress, but with rise in breaches, momentum is shifting
- Standards development and enforcement will help solve the problem in long
- This study was more focused on Technology solution for Information Protection, there is a great need to research and develop "Information Management Lifecycle" that includes security as one of the key driver
- Solutions must integrate People, Process and Technology