Database Security

Slides by Rayford Vaughn, Modifications by Rogers and Brown

Data Sensitivity

- Sensitive Data is data that should not be made public
- Three cases
  - Data is either sensitive or not
  - Sensitivity varies from element to element
  - Sensitivity varies from user to user
- Sensitive (Attribute within a record or entire record) when
  - Inherently sensitive
  - Declared sensitive
  - Source is sensitive
  - Only sensitive with respect to previously disclosed data

Traditional Security Concerns

- Confidentiality
- Integrity
- Availability
- Accountability

Availability

- Data is accessible all the time
- Management of multiple requests for the same data

Accountability

- Log access to database
- Helps with non-repudiation
  - Reconstruction of events
- Example where auditing helps
  - Query P → R //No
  - Query A + Query B + Query C → R //Yes

Integrity

- DB integrity types
  - Physical database integrity
    - Data in the database is safe
    - Data can be reconstructed
  - Logical database integrity
    - Structure of the database is preserved
    - No inconsistency
  - Element integrity
    - Correctness/accuracy of the data is maintained

Integrity Goals

- Database integrity production must achieve:
  - Internal consistency : Database entries must obey prescribed rules
  - External consistency : Database entries are correct
    - Combine checking data entered with auditing to check consistent state

Integrity Rules

- Most rules are application specific, but two rules inherent to relational model
  - Entity integrity rule :
    - No component of the primary key can accept null values
  - Referential integrity rule :
    - Database must not contain unmatched foreign key values

Application Specific Integrity Checks

- Field checks
  - Check that entries are valid elements of domain
- Consistency checks
  - Check that entries in different relations do not conflict
- Scope checks
  - Checks that query results are not computed for too small a sample (for specialized DB)
- Change logs
  - Check that all changes are recorded with original and modified entry values

Confidentiality

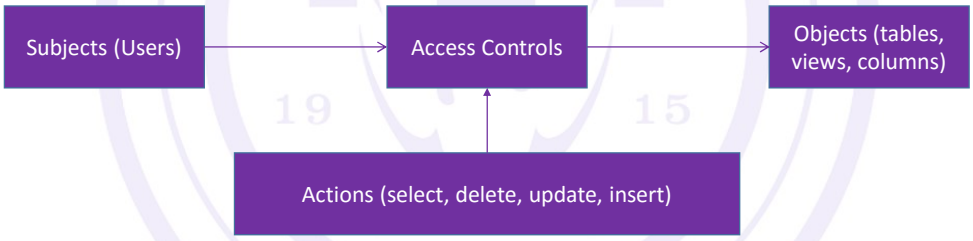
- More complex than OS
  - Deals with information (data with semantic/context)
- Uses access control for maintaining confidentiality

Access Control Goals

- Database access control must achieve :
  - Completeness : all database entries must be protected
  - Consistent : access control rules must not conflict
  - Example:
    - List employees with maximum salary //No
    - List employees for salary > average (salary) //Yes
  - Security policy is consistent if no elements in database for which access in two ways gives different access control decisions

SQL Model Security

- Basic SQL security model implements Discretionary Access Control (DAC)
  - Owner of an object defines controls for other users' access to the object



Security Controls in SQL

- SQL provides ability to protect
  - Data : Tables, records, columns, domains, vies
  - Transactions
- SQL provides controlled access to six DBMS functions
  - Creating, modifying, seeing, deleting, referencing, using
- SQL security based on privileges and views

Privileges

- When object is created, a user is designated as “owner” of the object
- Users other than owner have to be granted privileges in order to access an object
- The basic components of privilege are
  - Grantor
  - Grantee
  - Object
  - Action
  - Grantable

Granting / Revoking Privileges

- Privileges can be granted/revoked to entities in base relations
- In SQL, privileges are managed
  - Using GRANT and REVOKE operations
    - Apply to particular actions
    - Can be restricted to certain attributes of a table

Granting Privileges to Users

- GRANT privilege-list ON object TO user-list [WITH GRANT OPTION]

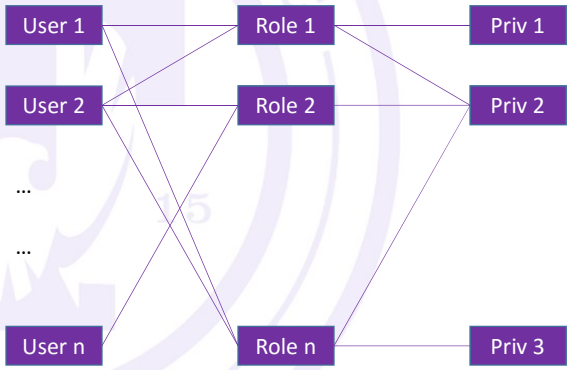
```
Grant Select, Update (Salary)
on table Employee
to Joe, Shelby

Grant Update(Salary)
on table Employee
to Mary with grant option
```

Privilege
- ✓ SELECT
- ✓ DELETE
- ✓ INSERT [column name]
- ✓ UPDATE [column name]
- ✓ REFERENCES
- ✓ USAGE

- ✓ Object
  - ✓ [TABLE] table-name
- ✓ User-list
  - ✓ Login-id | PUBLIC
- ✓ WITH GRANT OPTION
  - ✓ Provides right to delegate

Role Based Privilege

- SQL 99 allows role based privileges
  - CREATE role teller
  - GRANT select ON account TO teller
  - GRANT teller TO john



Cascading of Revocation

- As right to grant privileges can be granted (using grantable privilege component) requires special consideration while revocating
  - Do we take away right of the user in question ONLY
  - Do we take away right of the user in question ALONG WITH all other rights granted by the user

Revoking Privilege

- REVOKE [GRANT OPTION FOR] privilege-list ON object FROM user-list [RESTRICT|CASCADE]
- GRANT OPTION FOR
  - Revokes grant option for specified privileges
- CASCADE
  - Revokes privilege of grantee and any one else who have been granted privilege by grantee
- RESTRICT
  - Revokes privilege of grantee
- REVOKE GRANT OPTION FOR UPDATE ON Retail_Price FROM Sales_Manager;
  REVOKE SELECT ON customer FROM John;
  REVOKE UPDATE ON Retail_Price FROM Sales_Manager CASCADE;

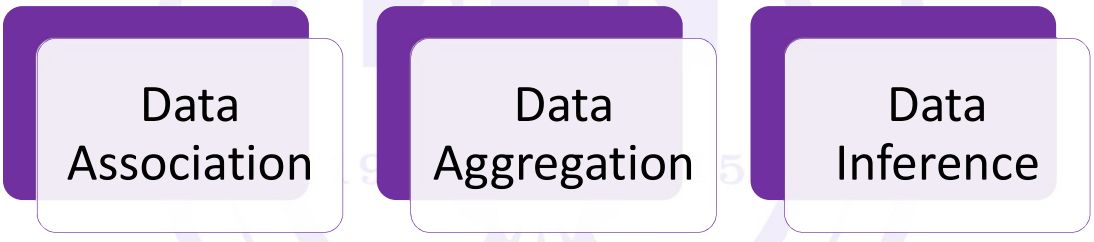
Access Control Through Views

- Many security policies are better expressed by granting privileges to views derived from base relations
  - Views are flexible
  - Views allow access control to be defined at a description level appropriate to the application

Views Based Access Control - Example

- Create a view containing only information about the employee
  - CREATE VIEW My_Info AS
    SELECT *
    FROM employee
    WHERE employee_name = Current_User( )
- Create a view containing only the employee's peers information
  - CREATE VIEW My_Peers AS
    SELECT *
    FROM employee
    WHERE rank = (SELECT rank
    FROM employee
    WHERE employee_name = Current_User ( ))

Special Security Concerns for DB



Data Association

- Occurs when two items are not sensitive, but their association is
- Example :
  - Longitude + Latitude
  - Plane + Cargo

Example Relation employee

SSN	employee_name	birth_date	gender	salary	criminal_conviction	department
123456789	Adam	1/12/58	M	40k	0	AC1
246813579	Ruth	7/4/76	F	30k	1	AC2
987654321	Collin	3/3/67	M	66k	0	AC2
357951264	Diane	8/7/66	F	100k	0	AC3
456789123	Ellis	1/25/73	M	85k	0	AC2
654978321	Jane	11/10/65	F	86k	0	AC1

Data Aggregation

- Occurs when a combination of allowed queries results in disclosure of sensitive information
- Examples
  - SELECT name FROM employee WHERE salary = MAX (salary)
  - SELECT MAX (salary) AS H FROM employee GROUP BY salary
  - SELECT MIN (salary) AS L FROM employee GROUP BY salary
  - SELECT name FROM employee WHERE salary BETWEEN 2L AND H
  - SELECT name FROM employee WHERE salary BETWEEN 3L AND H

Data Inference

- Attacker combines information from outside the database with database responses to infer something about information that is not authorized for disclosure
- Example :
  - Knows:
    - Diane works in the AC3 department
  - Conducts queries (Aggregation):
    - SELECT MAX (salary) AS H FROM employee GROUP BY salary
    - SELECT MIN (salary) AS L FROM employee GROUP BY salary
    - SELECT COUNT (*), department FROM employee WHERE salary BETWEEN 2L AND H GROUP BY department
    - SELECT COUNT (*), department FROM employee WHERE salary BETWEEN 2L AND H GROUP BY department
  - Infers:
    - Diane's Salary

Security – A Persistent Problem

- Why?
  - Financial Motivation
  - Religious / Political Motivation
  - Personal Grudge
  - Boredom
- How?
  - Physical Access
  - Exploit lack of awareness and training
  - Exploit weak security policies and procedures
  - Exploit vulnerabilities in applications and security mechanisms

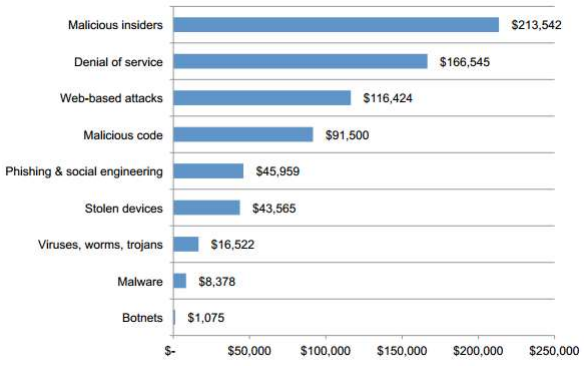
Security – A Persistent Problem

- Victim?
  - Financial Institutions
  - Educational Institutions
  - Government Agencies
  - E-Commerce Web Sites
  - ANYONE

Some Statistics

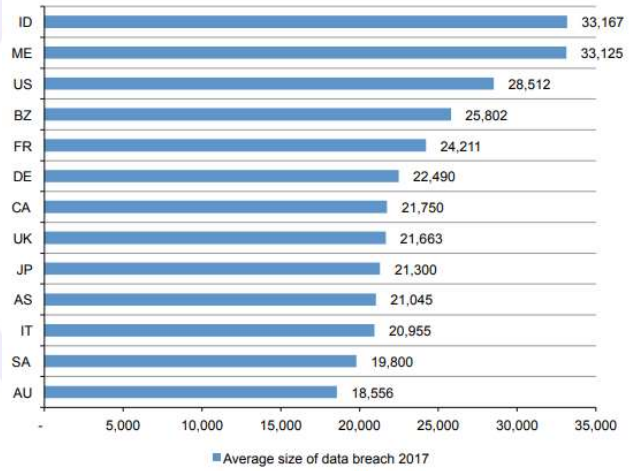
- Probability of a data breach involving a minimum of 10,000 records
  - US – 22.9%
  - Highest – Brazil 37.2%, Lowest – Germany 15.6%
- Average cost of a data breach
  - US – $6.69 Million
  - Highest – US, Lowest – India $1.53 Million
    - Strange correlation – the US spends the most to notify about data breaches, India spends the least

Biggest Costs in US Cyber Crime

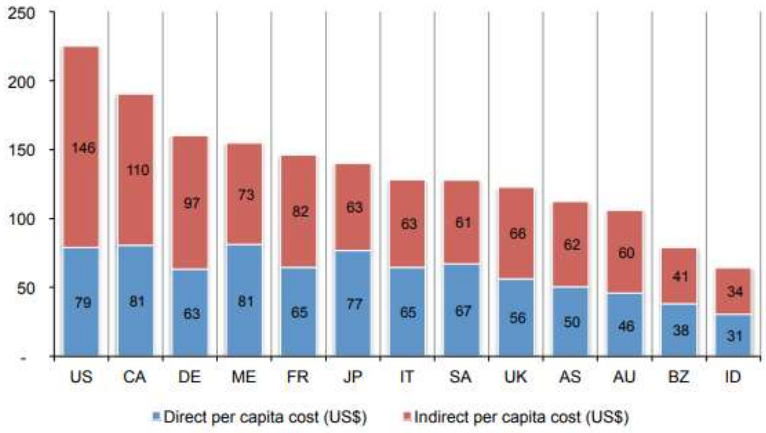


Data on slides 30 - 33 from 2017 Ponemon Institute report

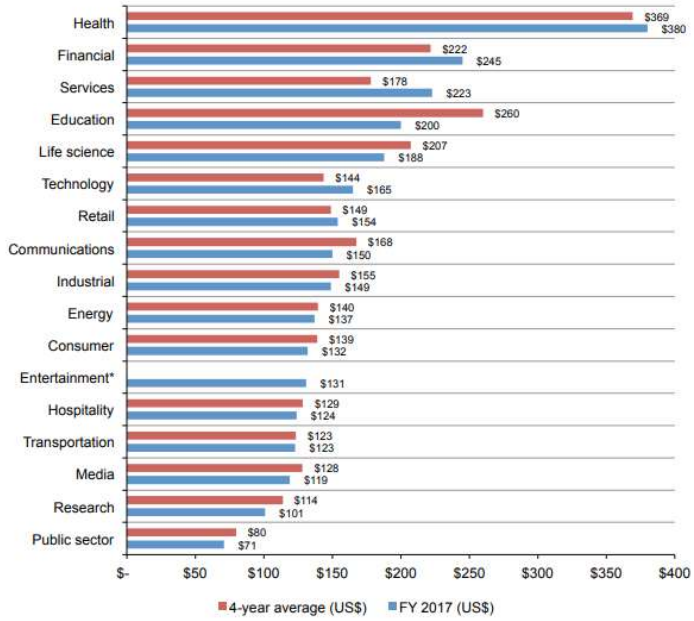
Average Number of Breached Records by Country or Region



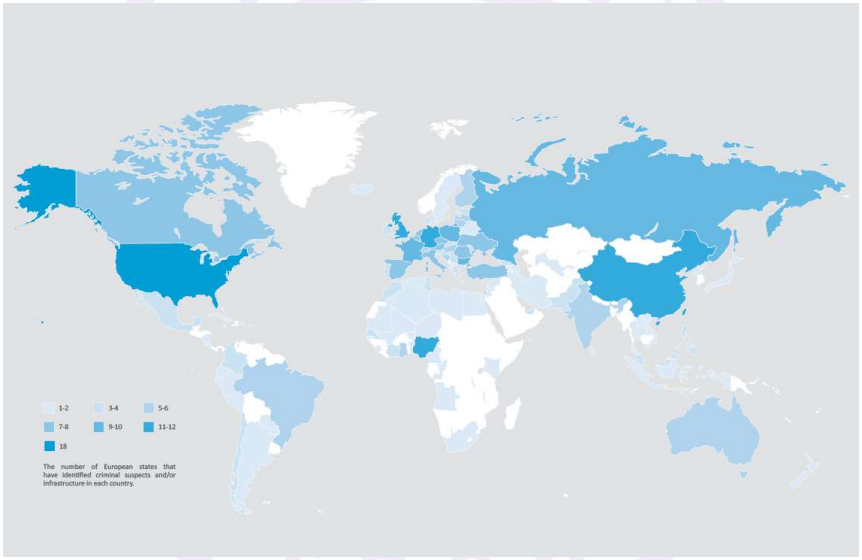
Direct and Indirect Per Capita Data Breach Costs



Per Capita Cost by Industry



Cyber Crime Heatmap



Data from EuroPol IOCTA 2016

Security Job Demand

- Bureau of Labor and Statistics, US Dept of Labor
  - Number of Jobs in 2016 : 100,000
  - 2016 Median Pay : $92,600 per year
  - 2016-2026 Job Outlook : 28% growth – much faster than the average of all occupations
    - Demand expected to be very high
    - Means we are looking at needing an additional 28,000 professionals every year for the next 8 years

Problems With Security

- Most do not understand or know about it
- Those who do understand have a tendency to underestimate it
- Those who do understand and do not underestimate it, address it insufficiently

Two Sides in Security

- Offensive
  - Threats and Attacks using Vulnerabilities to cause Harm or Loss
- Defensive
  - Goals include Integrity, Confidentiality and Available through the use of a security perimeter to avoid loss and maintain control

Terms

- Threat
  - Potential to inflict harm to an asset or cause security violations
- Attach
  - Infliction of harm to an asset or causing security violations
- Vulnerability
  - A weakness in security procedures or system design, implementation or operation that can be used to cause security policy violations

General Classes of Threats

- Disclosure
- Deception
- Disruption
- Usurpation

Specific Types of Attacks

- Snooping / Sniffing
- Spoofing
- Modification
- Repudiation of Origin
- Delay
- Denial of Receipt
- Denial of Service

CIA Model of Information Assurance

- Confidentiality
  - Keeping data and resources hidden
- Integrity (Data and Origin)
  - Keeping data (and data sources) and resources uncorrupted
- Availability
  - Keeping data and resources usable
- Accountability (a.k.a. Non-repudiation)
  - Holding one accountable for actions

Goals of Security – Defense in Depth

- Prevent
  - Securing an environment to avoid penetration
- Deter
  - Applying protection mechanisms to hurdle intruder efforts and thus causing delays in achieving a malicious gain
- Detect
  - Ensuring visibility of suspicious activities
- Response
  - Reacting to security incidents by notification, eradication, interdiction, prosecution
  - Continuing to survive to some extent
- Recover
  - Assessing and repairing damage
  - Improving

Security Policy

- An organizational security policy applies to all systems and its users and sets out what should and should not be allowed
- Types
  - Military
    - Readers may not access documents above his/her privilege level
  - Commercial
    - Customer may not change the price of the product

Venues for Security Controls

- Hardware
- Software
- Data
  - In processing
  - In transit
  - In storage
- People

End of Database Security