Database Security of E-commerce Systems in Terms of Authorization and Encryption

Hua Ye

SYSC 5703 Integrated Database Systems
Technology Innovation Management
28 March 2007

Outline

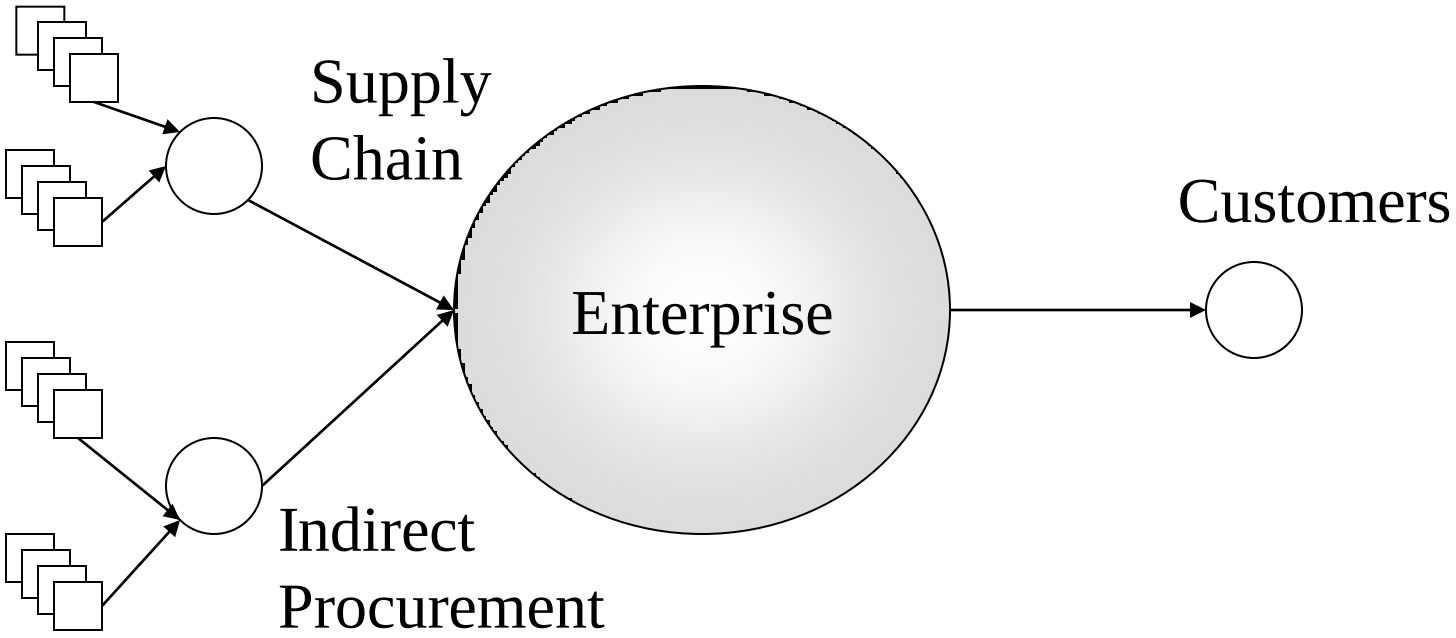
1. Introduction and background
2. Challenges for E-commerce database security
3. Solutions to secure database
   - 3.1 Access control
   - 3.2 Encryption
4. Strategies to protect the databases in E-commerce systems
5. Conclusion

1. Introduction and background

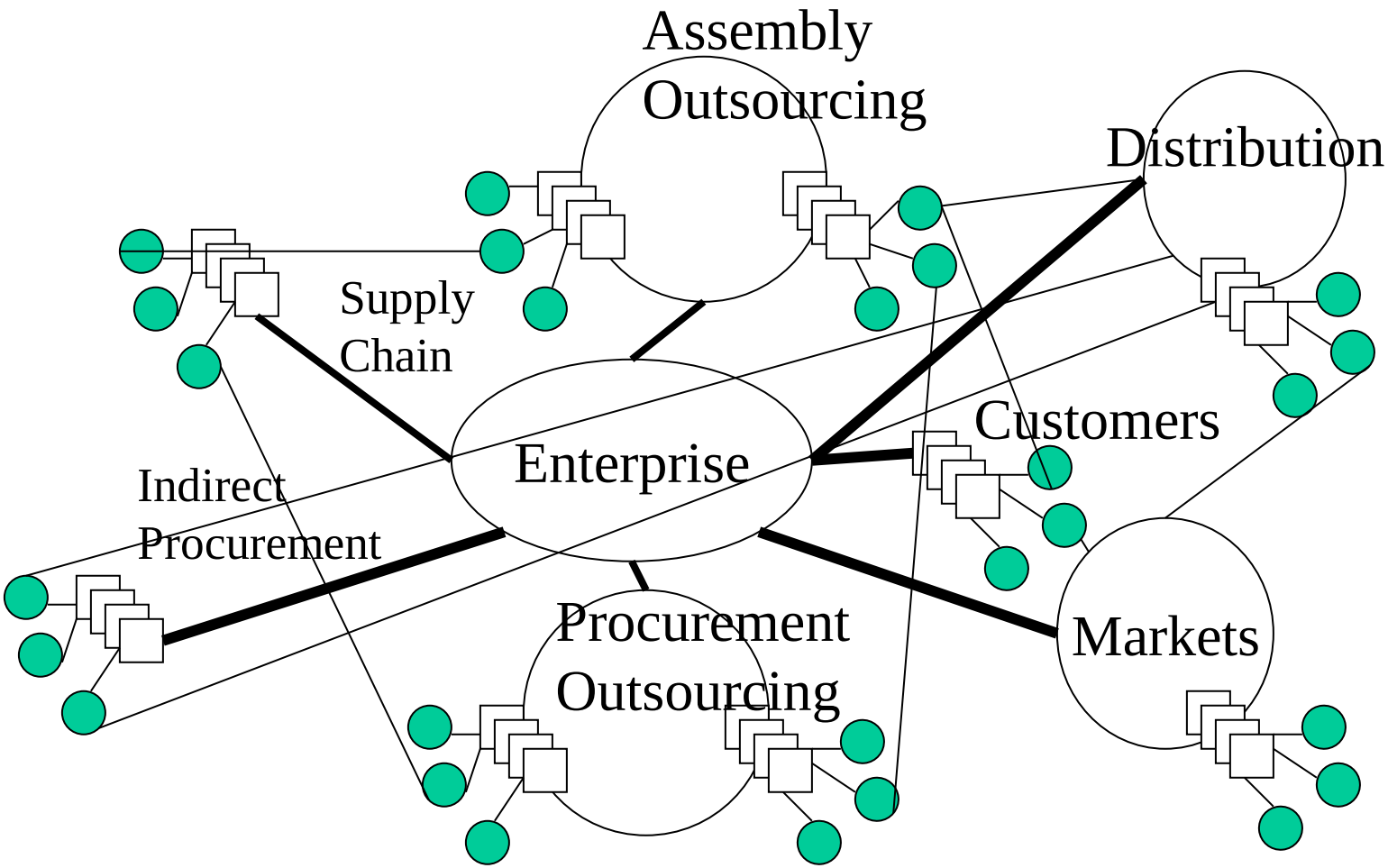
E-commerce introduction

- Electronic commerce (E-commerce)
  - A set of technologies, applications, and business processes
  - Link business, consumers, and communities over electronic system, such as the Internet and other computer networks
  - For buying, selling, and delivering products and services
  - For integrating and optimizing processes within and between participant entities
- Used in different forms and practiced by people of different disciplines
  - B2C, B2B, C2C, G2B, and G2C

Traditional enterprise-centric view

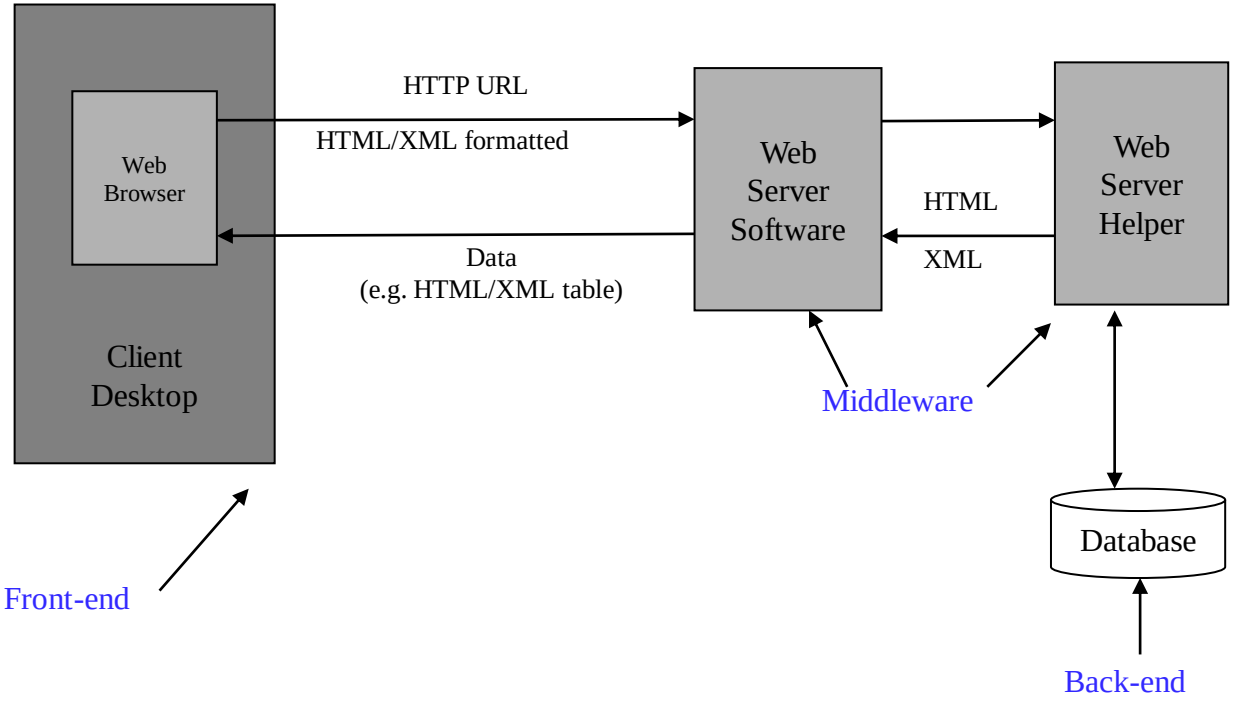


Internet business models and integration requirements



E-commerce system

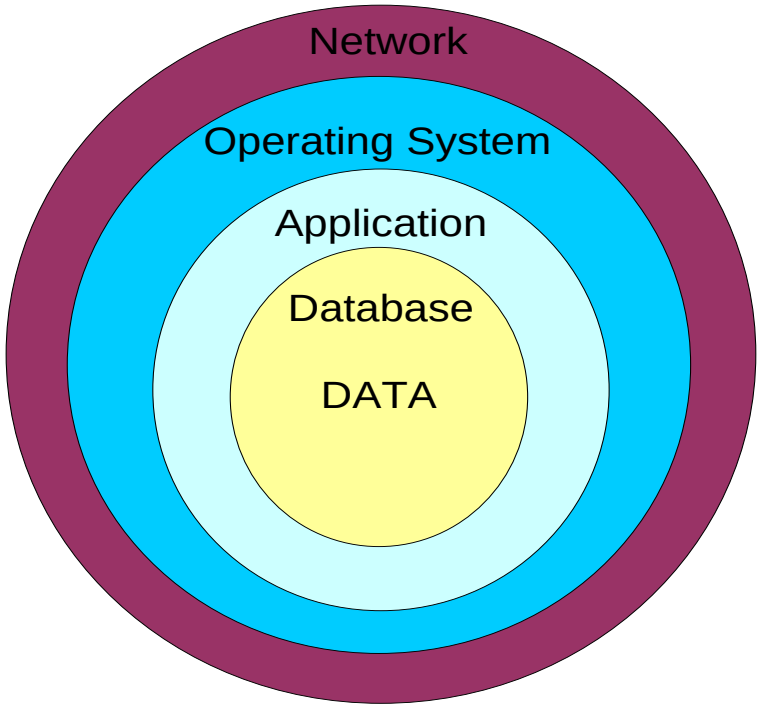
- Early E-commerce system
  - Two areas of concern
    - ✓ Back-end
    - ✓ Front-end
- Current E-commerce system



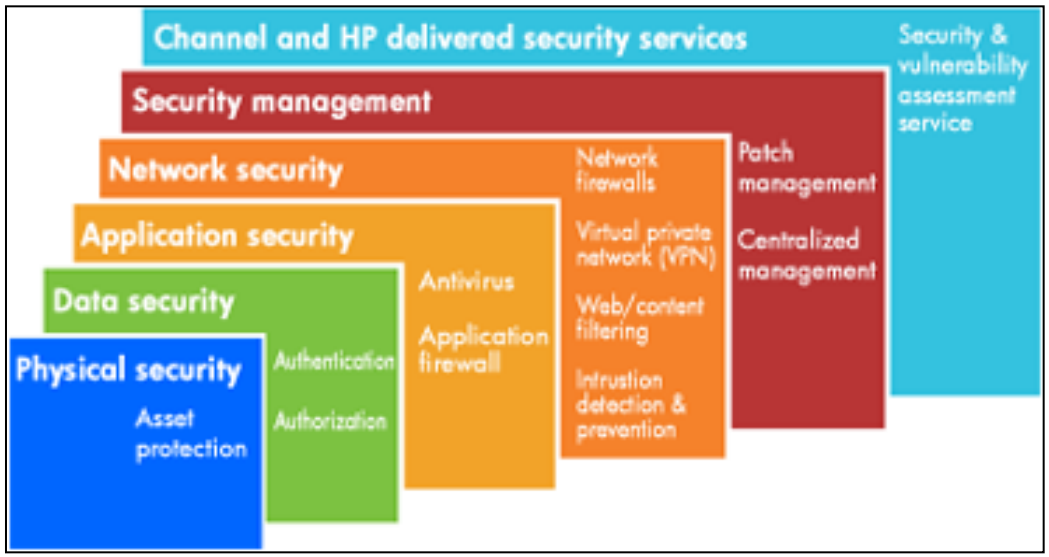
Security layers of E-commerce

- The paradigm of security layers approach
  - Provide broader security management solutions to find and fix vulnerabilities in E-commerce environments

Example 1



Example 2

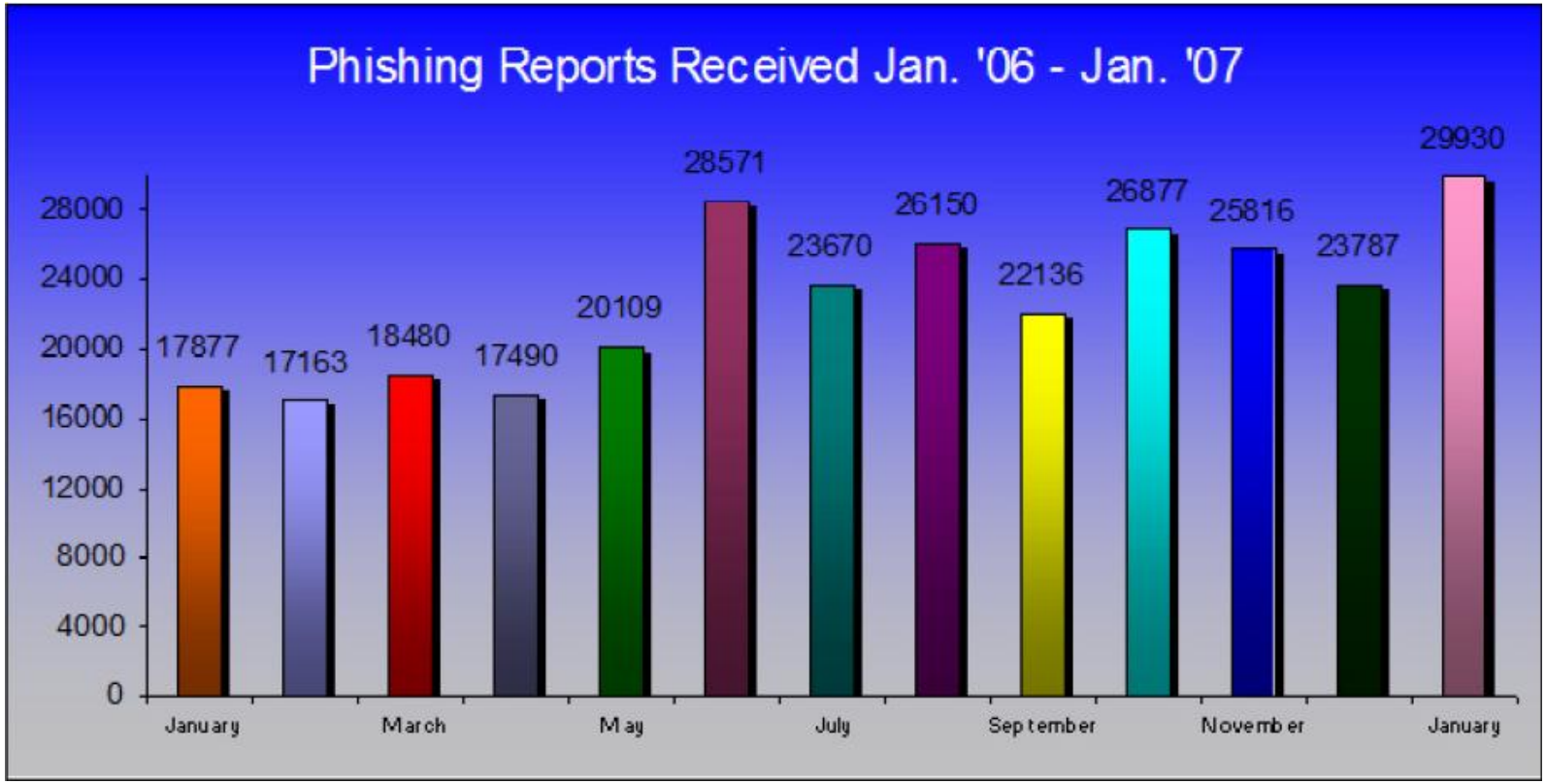


2. Challenges for E-commerce database security

Challenges for E-commerce database security (1)

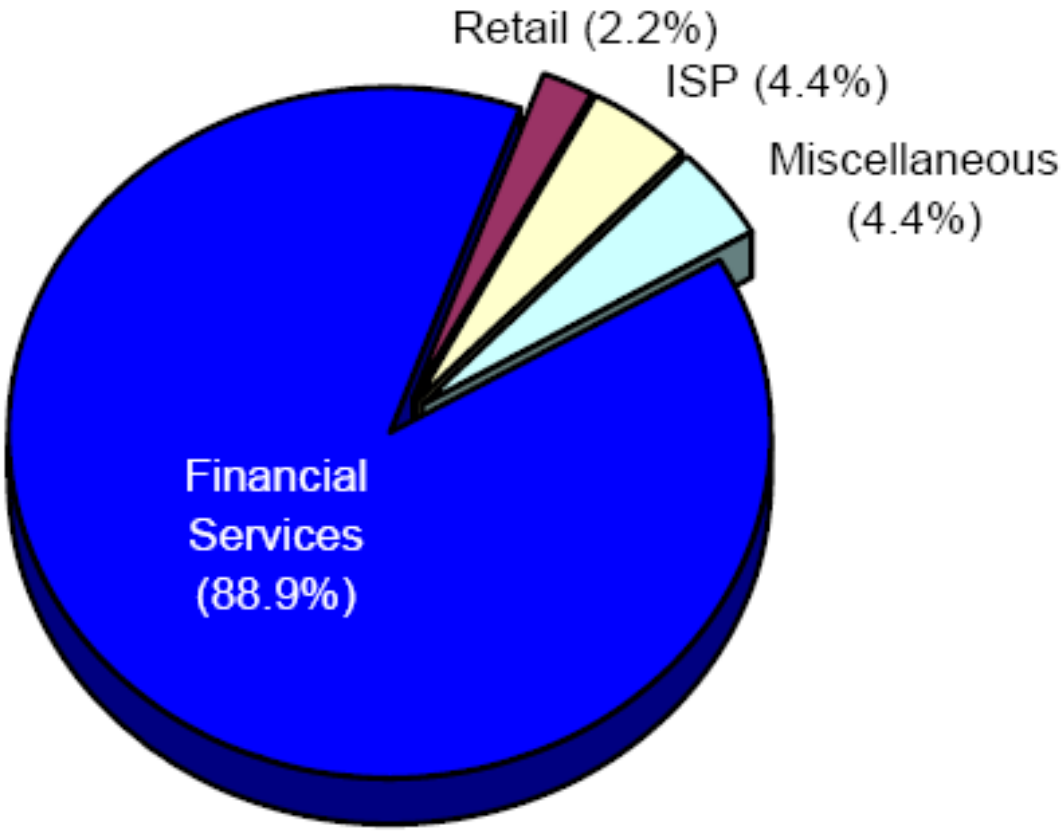
- Shift from the traditional infrastructure to the Internet for E-commerce
  - Problems with privacy, authenticity or accountability
- Recent rapid proliferation of Web-based applications
  - Increase the risk exposure of databases
  - More crucial for data protection

Challenges for E-commerce database security (2)



The total number of unique phishing reports submitted to APWG in January 2007 reached an all time high of 29,930, an increase of more than 25 percent from December 2006 and nearly 5 percent from the previous high in last June. In contrast, the number of unique phishing attacks reported in January 2004 was just 176.
http://www.antiphishing.org/reports/apwg_report_january_2007.pdf
http://www.antiphishing.org/reports/APWG.Phishing.Attack.Report.Jan2004.pdf

Challenges for E-commerce database security (3)



Financial services continue to be the most targeted industry sector at 88.9% of all attacks in the month of January 2007.
http://www.antiphishing.org/reports/apwg_report_january_2007.pdf

Major vulnerabilities

- Major vulnerabilities relevant to database
  - **Crosstalk**
    - ✓ Garble data
    - ✓ Theft of valuable confidential information
  - **Files**
    - ✓ Theft
    - ✓ Copying
    - ✓ Unauthorized access
  - **User, operator, or programmer**
    - ✓ Identification
    - ✓ Authentication
    - ✓ Subtle software modification

Security issues

- Most prevalent security issues relevant to the vulnerabilities
  - **Unauthorized or anomalous activities**
    - ✓ Hackers
    - ✓ Viruses
    - ✓ IM phishing attacks
  - **Authorization and encryption on a basic level**
    - ✓ e.g., some databases do not ensure password robustness and they are even stored as plain ASCII text
  - **Combination of some independent roles**
    - ✓ e.g., database administrators usually perform both database operation and administration duties
  - **Inactive auditing procedures**
    - ✓ Auditing procedures are often inactivated to avoid decreasing the performance of the system
  - **Insider threats**
    - ✓ 80% of data loss is caused by insiders

3. Solutions to secure database

Basic requirements

- Three basic requirements
  - **Confidentiality or secrecy**
    - ✓ Users should not be able to see things which they are not supposed to
    - ✓ Implemented primarily through encryption techniques
  - **Integrity**
    - ✓ Users should not be able to modify things they are not supposed to
    - ✓ Related to a specific form of encryption or digital signature
  - **Availability**
    - ✓ Users should be able to see and modify things they are allowed to

Access control

- Security policy
  - Specify who is authorized to do what
- Two major mechanisms are adopted at the DBMS level for *relational databases*
  - Discretionary access control
  - Mandatory access control

Discretionary access control (1)

- Discretionary access control
  - Based on the concept of access rights or privileges for objects and mechanisms for giving users privileges or revoking privileges
  - Most commercial DBMSs only provide discretionary security policy

Authorization administrations policy	Centralized administration; Ownership administration; Joint administration
Authorization identities	Users; Roles
Database objects	Tables (columns); Views; Procedures; Application programs
Access operations	SELECT; UPDATE; INSERT; REFERENCES
Privileges	– GRANT privileges ON object TO users [WITH GRANT OPTION] – REVOKE [GRANT OPTION FOR] privileges ON object FROM users
SQL specifications	– CREATE USER, DROP USER, ALTER USER – CREATE ROLE, DROP ROLE, GRANT ROLE – SET ROLE, REVOKE ROLE – GRANT PRIVILEGE, REVOKE PRIVILEGE
Models	– The system R authorization model – Content-based access control – Fine-grained access control – Role Based Access Control (RBAC) Model

Discretionary access control (2)

- Example 1
  - GRANT INSERT, SELECT ON Customers TO Mike
  - GRANT DELETE ON Customers TO Mike WITH GRANT OPTION
  - GRANT UPDATE (address) ON Customers TO Mike
  - REVOKE SELECT ON Customers FROM Mike
  - SET ROLE marketing_assistant
- Example 2
  - GRANT SELECT ON Canada Customers TO Mike
    - ✓ Only enables Mike to find the customers from Canada, but not the other customers
- Together with GRANT/REVOKE commands, views are a very powerful access control tool

Discretionary access control (3)

- Vulnerable to malicious attacks
- Trojan Horses problem
  - Mike creates a table *Horse* and gives INSERT privileges to Peter
  - Mike modifies the code of an application program used by Peter to additionally write some secret data to the table *Horse*
  - Now, Mike can see the secret information of Peter
  - ➢ Modification of the code
    - ✓ Beyond the control of DBMSs
    - ✓ Sophisticated Trojan Horses may leak information by means of covert channels enabling illegal access to data

Note:
A covert channel is any component or feature of a system that is misused to encode or represent information for unauthorized transmission, without violating the stated access control policy.

Mandatory access control (1)

- Why Mandatory Access Control (MAC) ?
  - Try to address such problems through access control based on information classification
    - ✓ These classifications are based on a partially ordered set of access classes, which are associated with every subject and object
  - A subject is granted access to a given object if and only if some order relationship, depending on the access mode, is satisfied by the access classes of the object and the subject

Mandatory access control (3)

Fundamentals	Based on system-wide policies that cannot be changed by individual users – Each database object or subject is assigned a security class – Each subject (user or user program) is assigned a clearance for a security class – Rules based on security classes and clearances govern who can read/write which objects – MAC has also been applied to commercial relational DBMSs, such as Oracle9i
Database subjects	Users; User programs
Database objects	Tables; Views; Tuples
Security classes	– A security level: Top secret (***TS***), secret (***S***), confidential (***C***), unclassified (***U***): ***TS*** > ***S*** > ***C*** > ***U*** – A set of categories: finer grained security classifications of subjects and objects than the classification provided by the security level, and are the basis for enforcing need-to-know restrictions
Principles	– No read-up: subject S can read object O only if class(S) >= class(O) – No write-down: subject S can write object O only if class(S) <= class(O) – * In some implementations of the multilevel relational model, write operations at higher access classes are not allowed for integrity reasons. Such a restriction is usually known as a no write-up restriction

Mandatory access control (4)

- Prevent information in a sensitive object from flowing with the enforcement of the two principles
  - No read-up
  - No write-down
  - ➢ For example, a table about Memory Stick

ID	Name	Memory capacity	Class
100	Sandisk	2G	***S***
101	Platinum	1G	***C***

✓ If a user with ***C*** wants to insert "100, Sony, 2G, C" into the table, the mandatory access control will disallow the insertion and tell the user that there is another object with Id 100 that has a class > ***C***

Note:

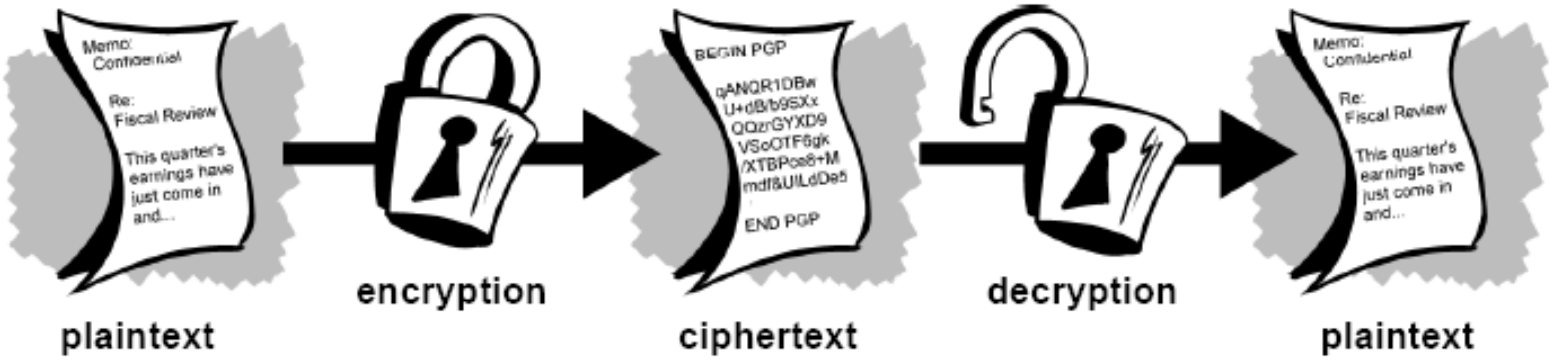
Users with ***S*** and ***TS*** clearance will see both rows, users with ***C*** will only see the 2nd row, and users with ***U*** will see no rows.

Advanced databases

- Access control for *object-based databases*
  - Not suitable with the access control models for relational DBMSs
  - Take into account all semantic modeling constructs commonly found in *object-oriented data models*
    - ✓ Composite objects
    - ✓ Versions
    - ✓ Inheritance hierarchies
    - ✓ etc.
  - ➢ The Orion authorization model is the first and most comprehensive discretionary access control model
  - ➢ MAC models can be classified in two main categories, i.e., single-level models and multilevel models
- Access control for XML
  - A standard access control model: XACML

Encryption

- Security is necessary when communicating over different media in E-commerce environments
  - Use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data



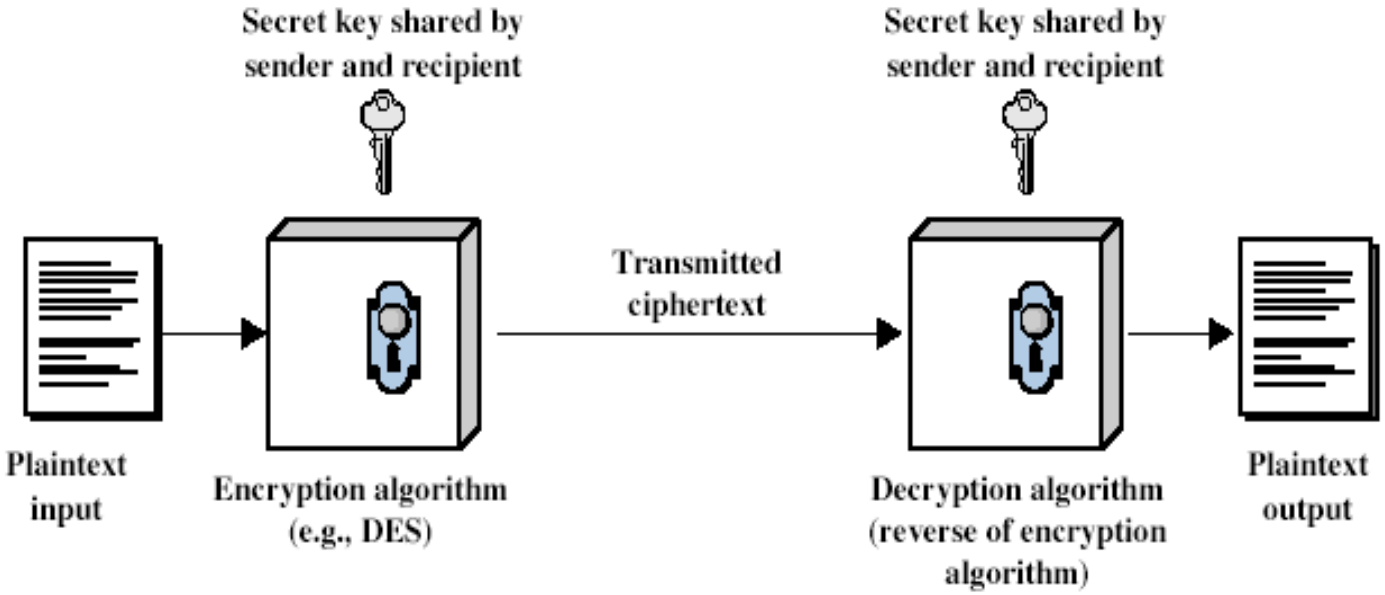
Introduction of encryption

- The encryption algorithms can be either *strong* or *weak*
  - A good algorithm (strong cryptography) can only be broken by discovering the key

- Broadly categorize cryptographic systems by the following criteria
  - Operations used
    - ✓ Substitution, transposition, etc.
    - ✓ For example, the two basic techniques in symmetric ciphers are substitution and transposition
  - Symmetric vs. public-key
    - ✓ Whether the two parties use the same key or not
  - Block vs. stream cipher
    - ✓ Whether the plaintext is processed a block or a character at a time

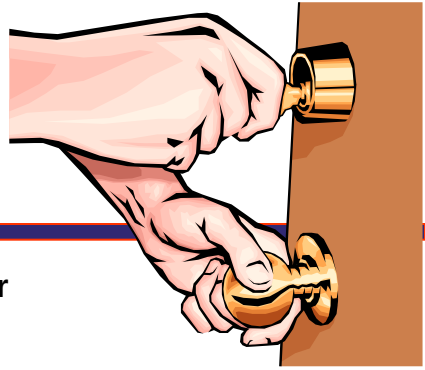
Symmetric encryption

- Symmetric encryption
  - Use one key for both encryption and decryption



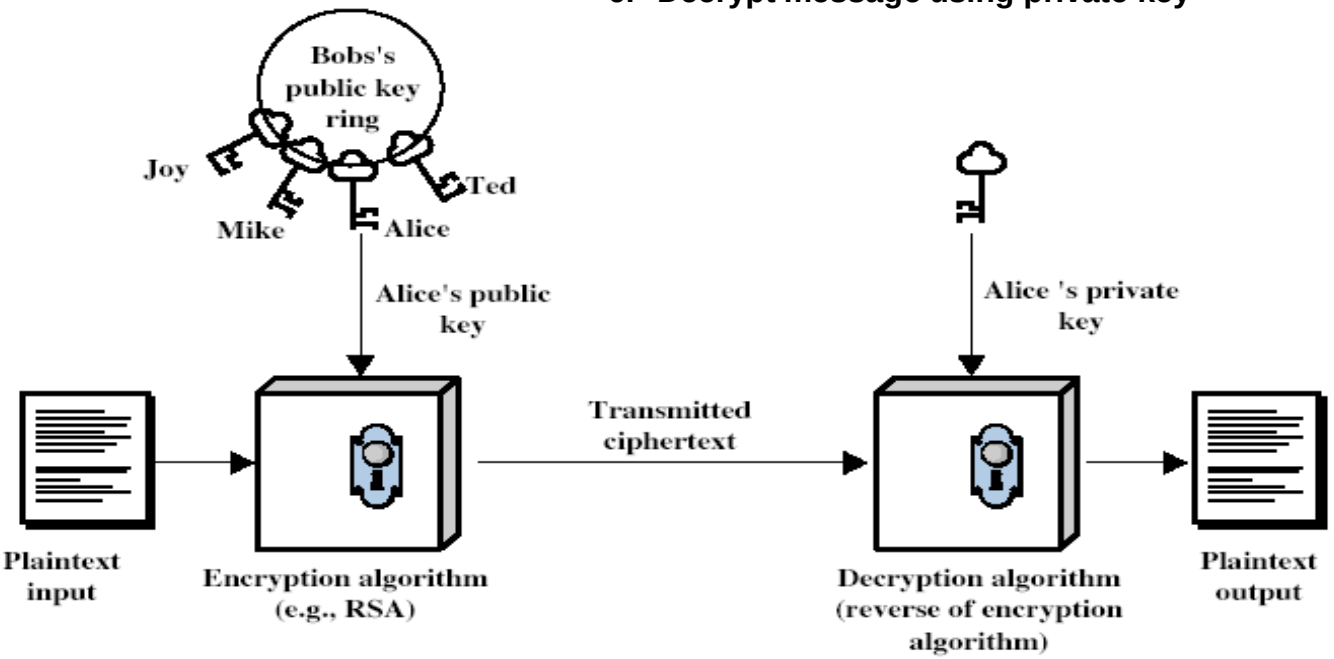
For a sender and recipient to communicate securely using conventional encryption, they must agree upon a key and keep it secret between themselves.

Asymmetric encryption



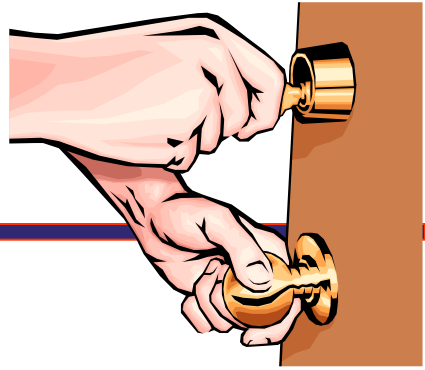
- Asymmetric encryption
  - A public key
  - A private-key

1. **Generate public and private key pair**
2. **Publish public key to repository**
3. **Retrieve public key from repository**
4. **Encrypt message using public key**
5. **Send encrypted message over non-secure channels**
6. **Decrypt message using private key**



The scheme is asymmetric because those who encrypt messages or verify signatures cannot decrypt messages or create signatures.

Why public-key cryptography?



- Developed to address two key issues
  - Key distribution
    - ✓ How to secure communications in general without having to trust a Key Distribution Centre (KDC) with your key
  - Digital signatures
    - ✓ How to verify a message comes intact from the claimed sender

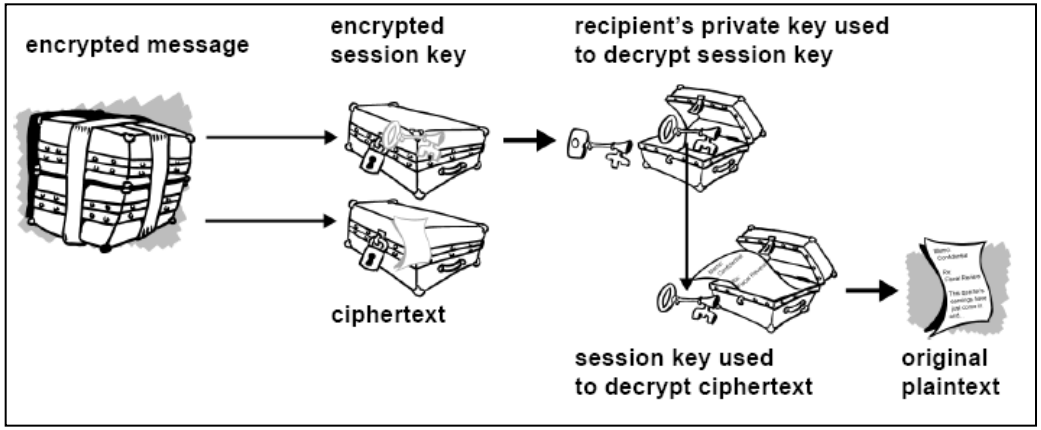
PGP (1)

- Respective advantages in the algorithms
  - Symmetric encryption
    - ✓ Faster
  - Asymmetric encryption
    - ✓ Provide a better solution to key distribution and data transmission issues

- **PGP** (Pretty Good Privacy)
  - Combine some of the best features of both symmetric encryption and asymmetric encryption
  - A hybrid cryptosystem

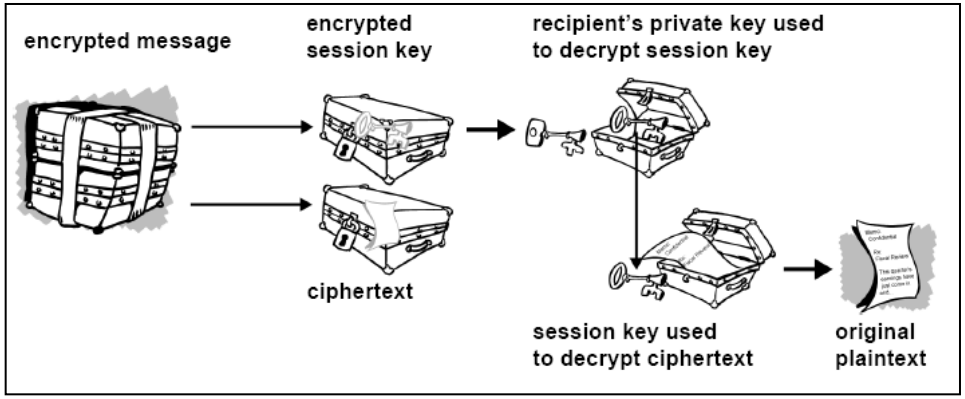
PGP (2)

- Session key
  - A one-time-only secret key
    - ✓ A random number generated from the random movements of your mouse and the keystrokes you type



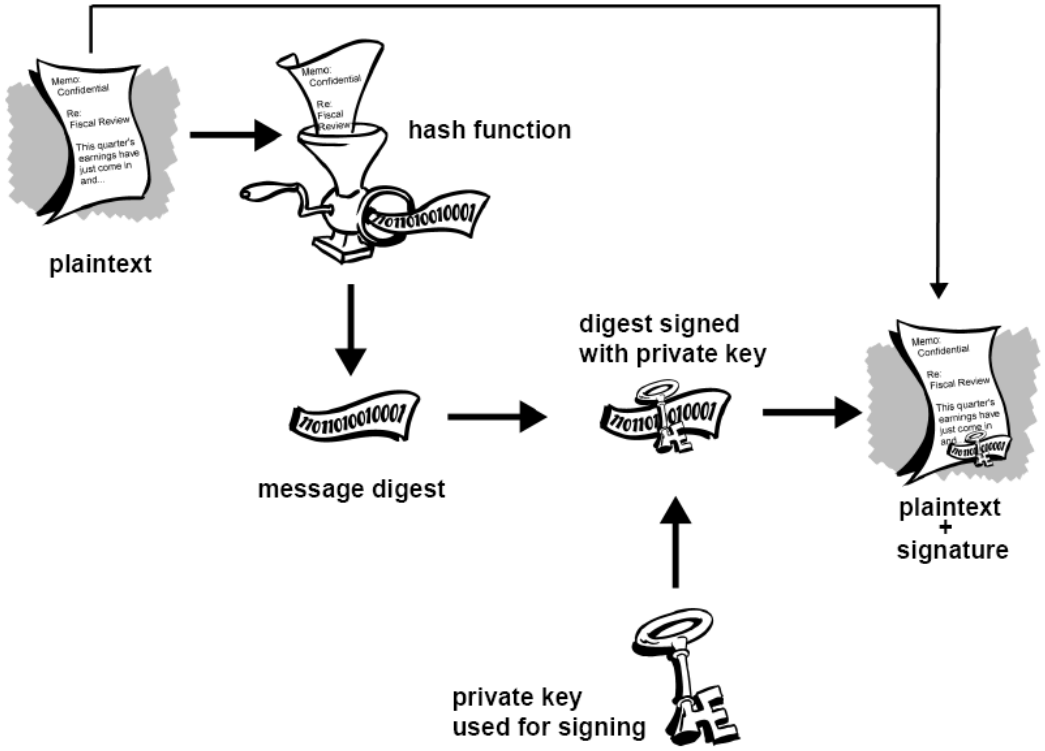
How PGP encryption works

How PGP decryption works



PGP (3)

- Use a cryptographically strong hash function on the plaintext the user is signing
  - Generate a fixed-length data item known as a message digest
- Use the digest and the private key to create the "signature", and transmits it with the plaintext together



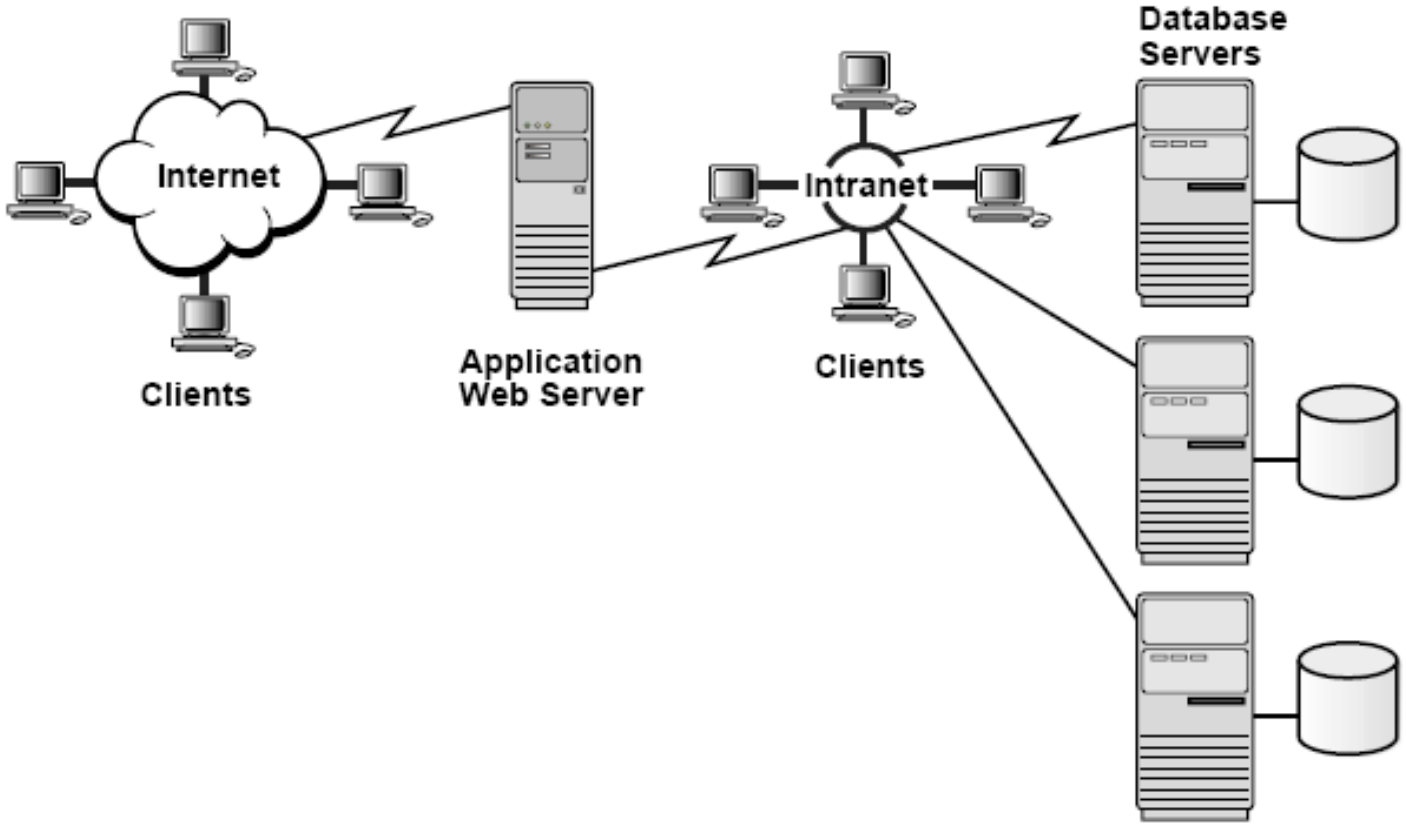
Encryption algorithms

Symmetric encryption	DEA, Triple-DES, FEAL, SKIPJACK, Blowfish …
Asymmetric encryption	Elgamal, RSA, Diffie-Hellman, DSA …
Hash Algorithms	MD2, MD4, MD5, RIPEMD, SHA1, Snefru, Tiger ...

4. Strategies to protect the databases in E-commerce systems

An overview of E-commerce systems

- An overview of the complex computing environment
  - Data security plan must encompass



Four dimensions

- Data security issues should be addressed in four dimensions
  - Physical
  - Personnel
  - Procedural
  - Technical

Physical / Personnel

- 1st dimension - Physical
  - The first defence approach: initiate a firewall machanism on the interface between the Internet and the Intranet
    - ✓ According to the position of database servers mainly at the back-end in the E-commerce system architecture
- 2nd dimension - Personnel
  - The people responsible for system administration and data security must be reliable
  - A good practice is to separate tasks by roles
    - ✓ Commonly known as segregation of duties

Procedural (1)

- 3rd dimension – Procedural
  - At first, address the security requirements and the scope of current threats to the data
  - Prepare the basis for risk evaluation, treatment and acceptance
  - Build an intelligent auditing strategy to highlight security problems while maintaining database performance
    - ✓ Three broad severity classes for vulnerabilities
      - High
      - Medium
      - Low
    - ✓ Auditing methods: Field Level Auditing, Record Level Auditing, Database Level Auditing
    - ✓ Typically categorize security breaches as unauthorized data observation, incorrect data modification, and data unavailability
    - ✓ Require detailed audit information about who is accessing what data, when and how according to auditors
    - ✓ Use trigger to monitor changes in databases

Procedural (2)

– Trigger example

```
CREATE OR REPLACE TRIGGER audit_emp
AFTER INSERT OR UPDATE OF sal ON emp
WHEN (sal > 10000)
FOR EACH ROW
BEGIN
  INSERT INTO sal_audit VALUES
  (:new.empno, :new.ename, :new.job,
   :new.mgr, :new.sal, :new.deptno);
END;
```

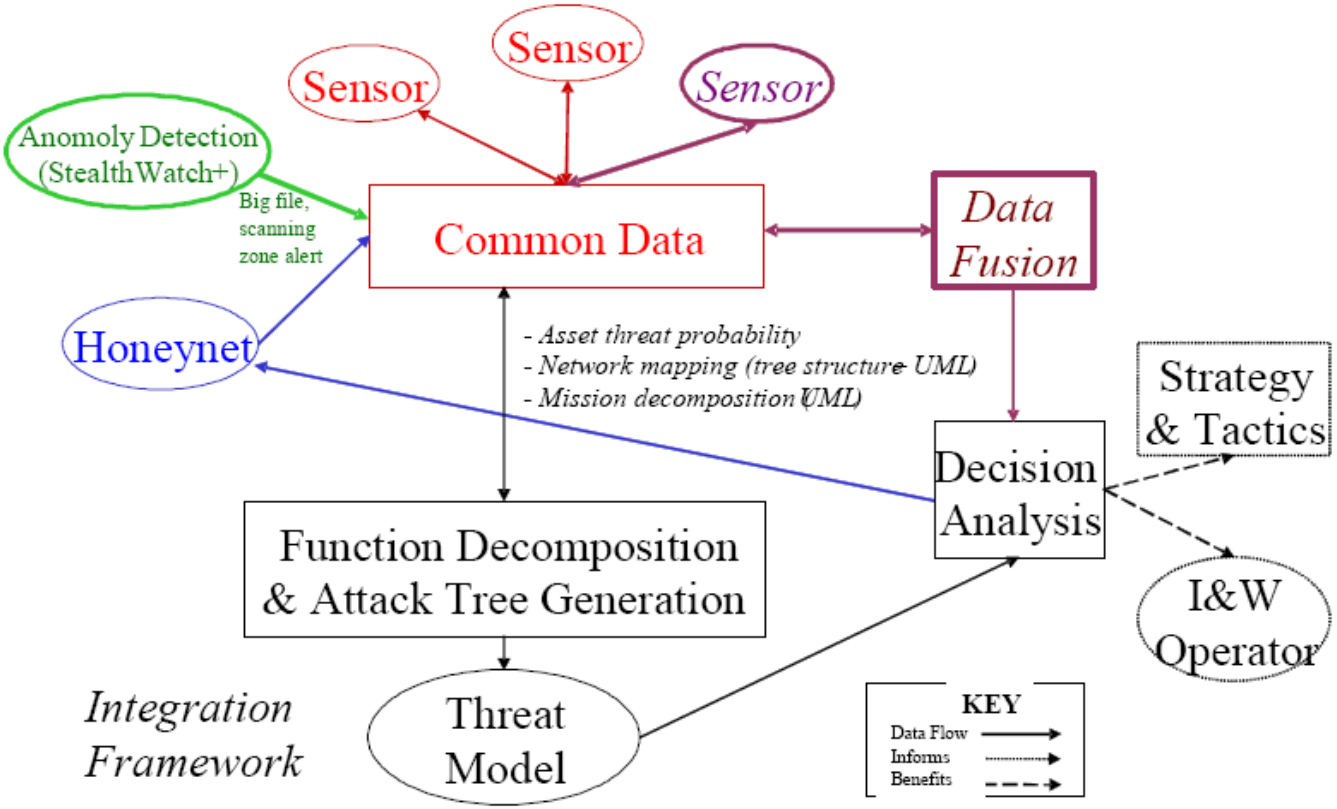
* Trigger Event
* Trigger Restriction
* Trigger Action

Technical (1)

- 4rd dimension – Technical
  - Combine the advantages of authorization and encryption
  - Choose to implement security protocols at many different levels within the seven layer Open Systems Interconnect (OSI) reference model for distributed communications architectures according to the architectors of E-commerce
  - Issues real-time security alerts or blocks suspicious activities before they occur

Technical (2)

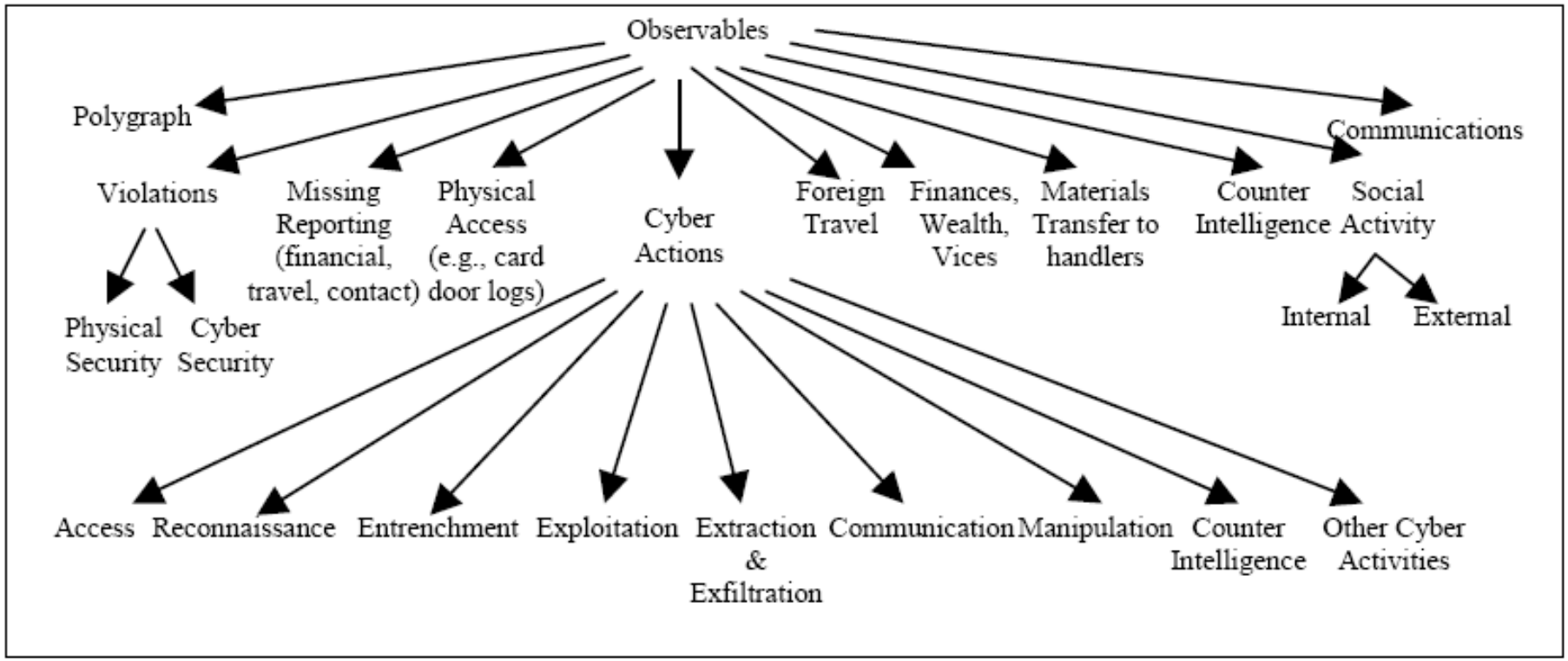
- Example: an early indication architecture



- A central Common Data system collecting, then correlating data, from multiple sources
- Once fused and analyzed, correlated data can indicate anomalous activities

Technical (3)

– Catch the insider threat



- No single observable will always indicate an insider threat
- Multiple observables can be used as input for early indications and warning
- The category of Cyber Actions broken down into smaller sub-groups

5. Conclusion

Conclusion

- The adequate protection of databases is not an option any longer because of these increased risks in E-commerce.

- Basic strategies to protect the database of E-commerce systems
  - Combine the advantages of authorization and encryption
  - Address data security issues from four dimensions
    - ✓ Physical
    - ✓ Personnel
    - ✓ Procedural
    - ✓ Technical

Reference (1)

- Anti-Phishing Working Group. 2004. **Phasing Attack Trends Report January**, 2004. Available at: http://www.antiphishing.org/reports/APWG.Phishing.Attack.Report.Jan2004.pdf.
- Anti-Phishing Working Group. 2007. **Report for the Month of January**, 2007. Available at: http://www.antiphishing.org/reports/apwg_report_january_2007.pdf.
- Anton A., & Earp J. 2000. **A Multidisciplinary Electronic Commerce Project Studio for Secure Systems**. http://www4.ncsu.edu/~jbearp/ncisse2000.pdf.
- Bener, A. 2003. **E-commerce Architecture**. Available at: http://www.cmpe.boun.edu.tr/courses/cmpe472/spring2005/cmpe472archit-2003.ppt.
- Bener, A. 2005. **Information Systems Security and Control**. Available at: http://www.cmpe.boun.edu.tr/courses/cmpe472/spring2005/IS_Security_Control.ppt.
- Kinicki, B., & Finkel, D., & Mikhailov, M., & Sommers, J. 2003. **Electronic Commerce Performance Study**. Available at: http://www.cs.wisc.edu/~jsommers/pubs/euromedia.pdf.
- Bertino, E., & Sandhu, R. 2005. **Database Security-Concepts, Approaches, and Challenges**. IEEE Transactions on Dependable and Secure Computing, 02(1): 2-19.
- Luo, Q., & Krishnamurthy S., & Mohand, C., & Piraheshd, H., & Wooq H., & Lindsayd, B., & Naughton, J. 2002. **Middle-Tier Database Caching for e-Business. Proceedings of the 2002 ACM SIGMOD international conference on Management of data**. Available at: http://portal.acm.org/citation.cfm?coll=GUIDE&dl=GUIDE&id=564763.
- Trinanes J. **Database Security in High Risk Environments**, http://www.governmentsecurity.org/articles/DatabaseSecurityinHighRiskEnvironments.php.
- Martinez, S. 2000. **Introduction to Cryptography**. Available at: http://www.encryptsolutions.com/english/info/doc/bugs_intro_main.html.
- MasterCard International Incorporated, 2003. **Electronic Commerce Security Architecture Best Practices**. Available at: http://www.powerpay.biz/docs/risk/MC_best_practices_online.pdf.
- Network Associates, Inc. 1999. **An Introduction to Cryptography**. Available at: http://technology.ohio.edu/email/files/IntroToCrypto.pdf.

Reference (2)

- Oracle. 2003. Oracle Security Overview. Available at: http://download-east.oracle.com/docs/cd/B14117_01/network.101/b10777.pdf.
- Chen, Q., & Yao, J., & Xing, R. 2006. **Middleware Components for E-commerce Infrastructure: An Analytical Review**. Issues in Informing Science and Information Technology, Volume 3.
- **Security protection - protection at every layer**. Available at: http://www.hp.com/sbso/security/layers.html.
- Spitzner, L. 2003. **Honeypots: Catching the Insider Threat**. Available at:
- http://www.acsa-admin.org/2003/papers/spitzner.pdf.
- Wokosin, L. 2002. Components of E-Commerce. Available at: http://www.stc.org/confproceed/2002/PDFs/STC49-00007.pdf.