

What's covered here?

- Security issues
- Encryption
- Authentication and Authorization
- Audits

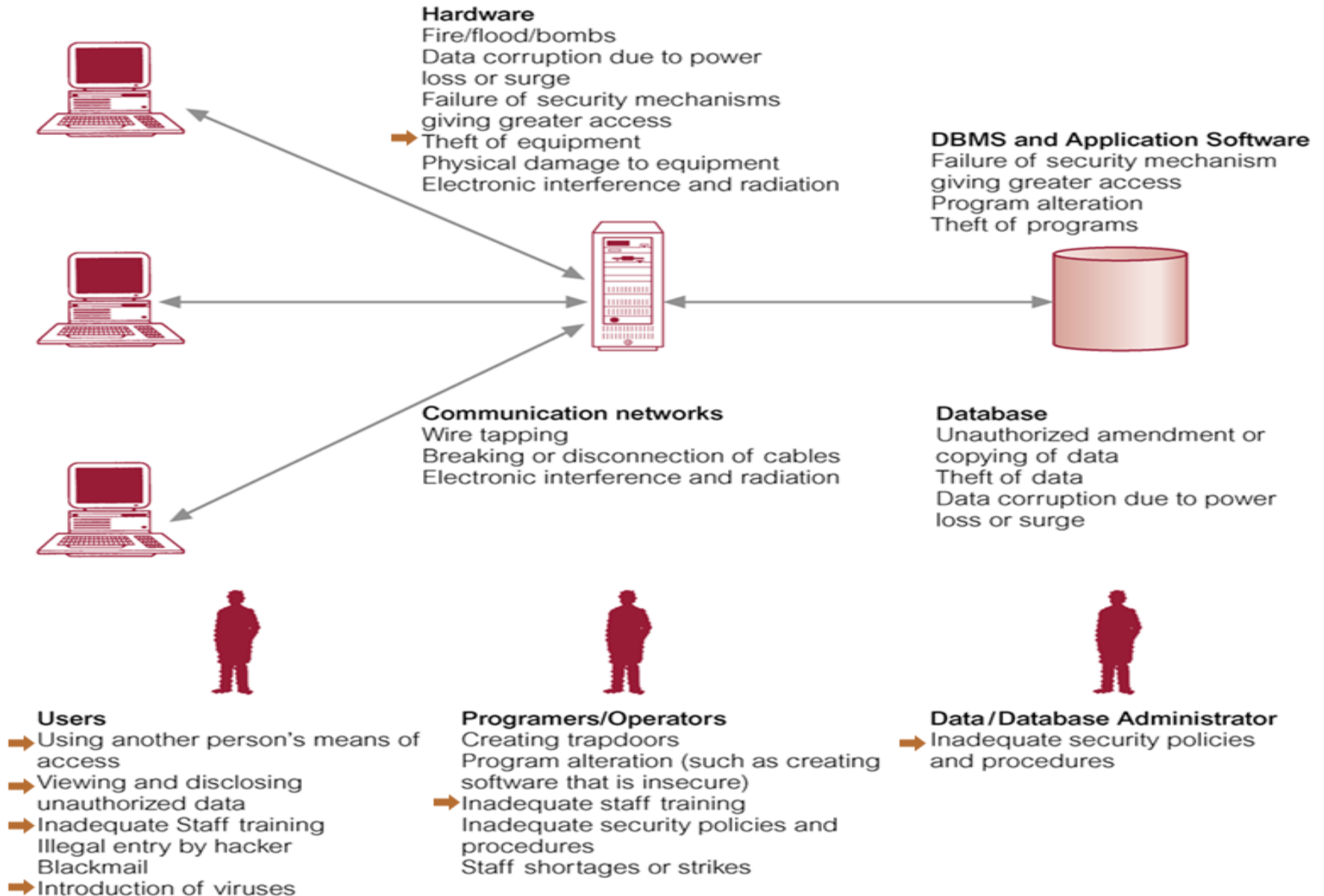
Why should we protect data?

- Data is a valuable resource and could be of strategic importance
- Legal, ethical, and policy issues
- System reliability
- Intentional and unintentional threats

Control Approaches

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)

Summary of Threats to Computer Systems



Encryption

- Secure data in an insecure environment
- Encryption algorithm
- encryption key, decryption key

Data Encryption Standard (DES)

- Developed by the U.S. government and used worldwide
- Uses bit manipulation
 - substitution and permutation
 - Encrypted as blocks of 64 bits.

Advanced Encryption Standards (AES)

- National Institute of Standards (NIST) introduced the Advanced Encryption Standards (AES)
- Uses block size of 128/192/256 bits and thus takes longer to crack

Public Key Encryption

- Introduced by Diffie and Hellman in 1976
- Based on **mathematical functions**
- They also involve the use of **two separate keys**

Public Key Encryption

- **Public** key is made for public and **private** key is known only by owner

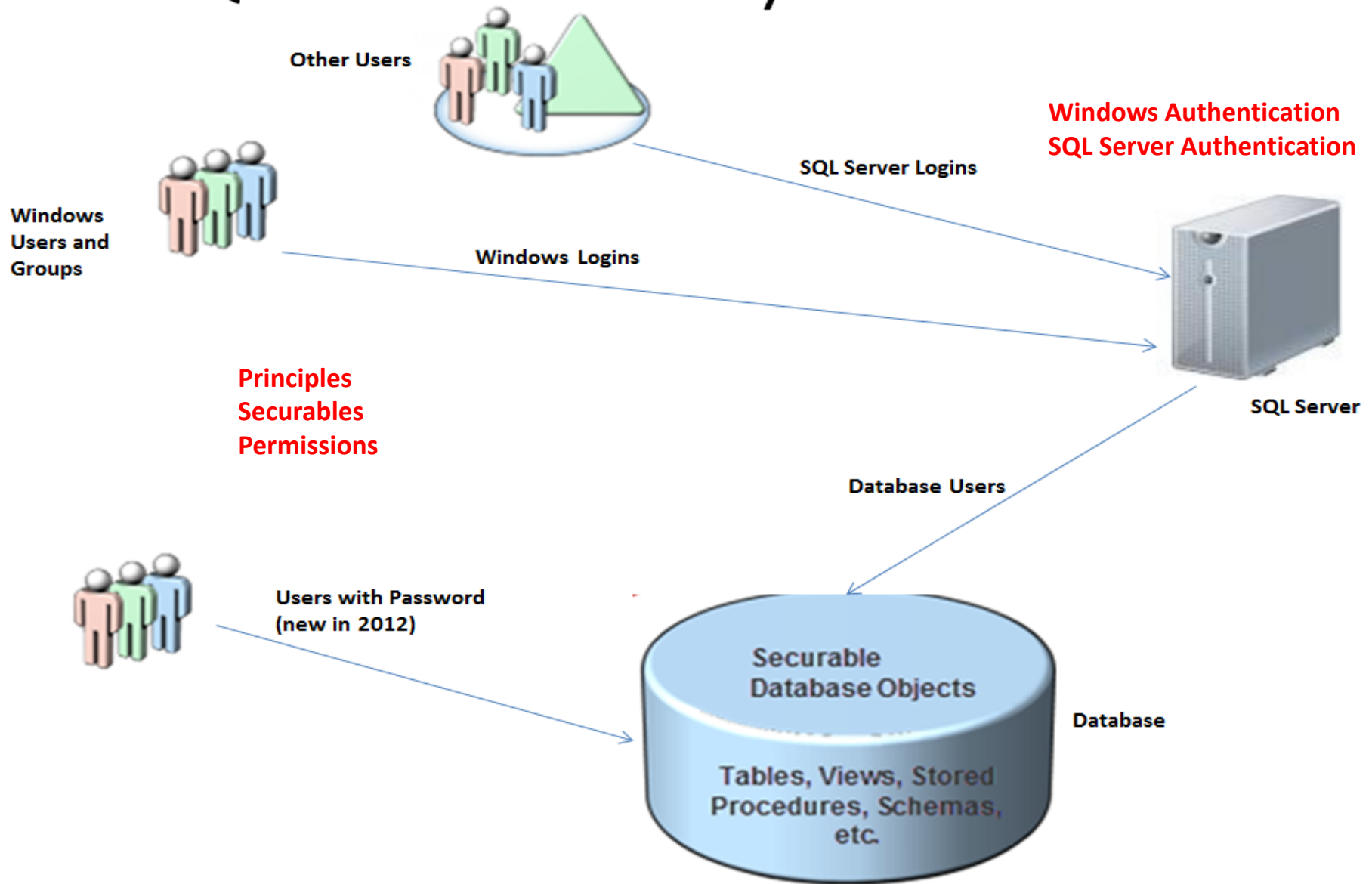
RSA Public Key Encryption

- One of the first public key schemes
- Introduced in 1978 by Ron Rivest (R), Adi Shamir (S), and Len Adleman (A) at MIT

Digital Signatures

- Means of **associating a mark unique to an individual with a body of text**
- Digital signature consists of a string of symbols.
- **Signature must be different for each use**
- Digital signatures are based on Public Key techniques

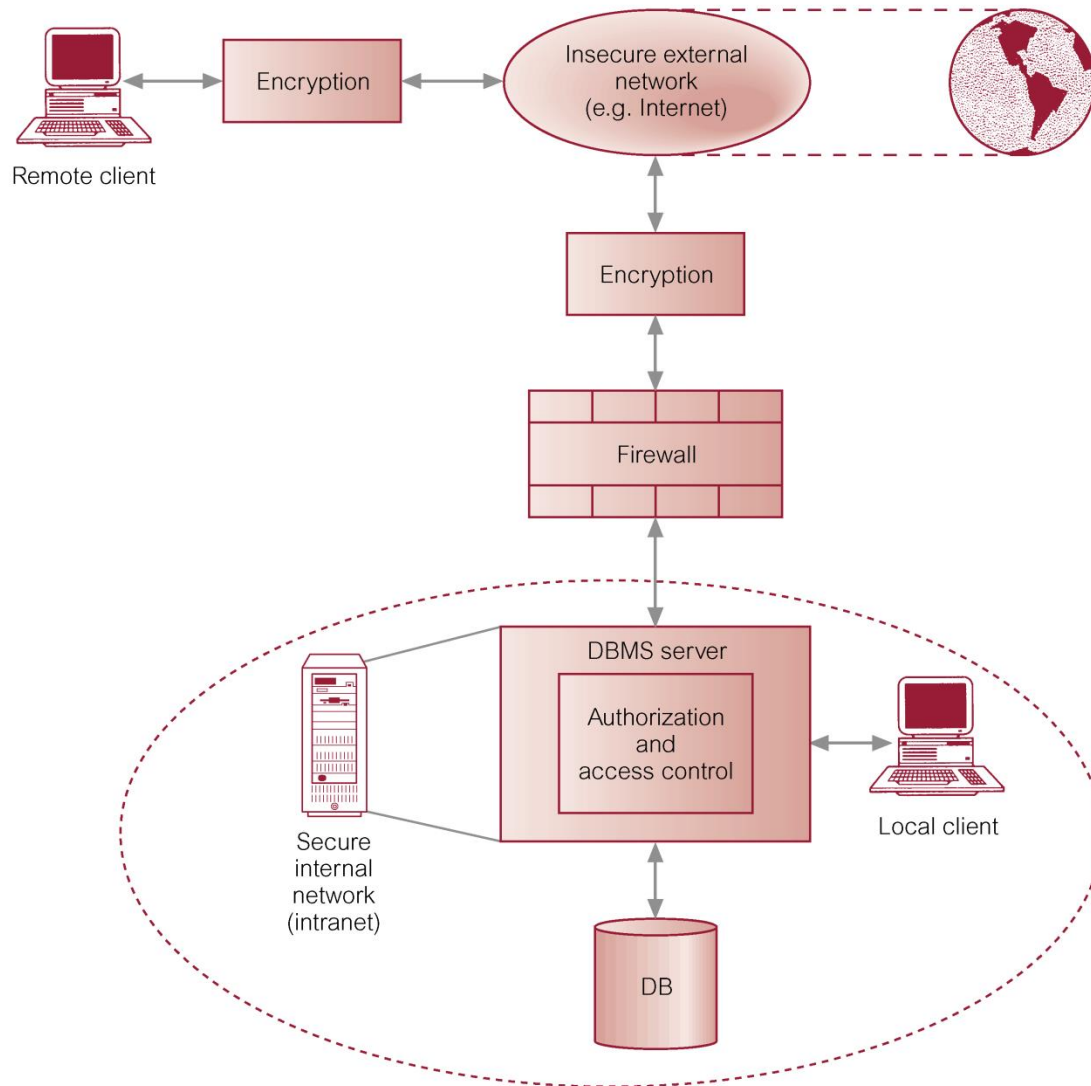
SQL Server Security Overview



Role-Based Access Control

- Role hierarchy in RBAC is a natural way of organizing roles to reflect the organization's lines of authority and responsibility

Modern Computer Environment



Audits

- Database audit consists of reviewing the log
- Database log that is used mainly for security purposes is sometimes called audit trail