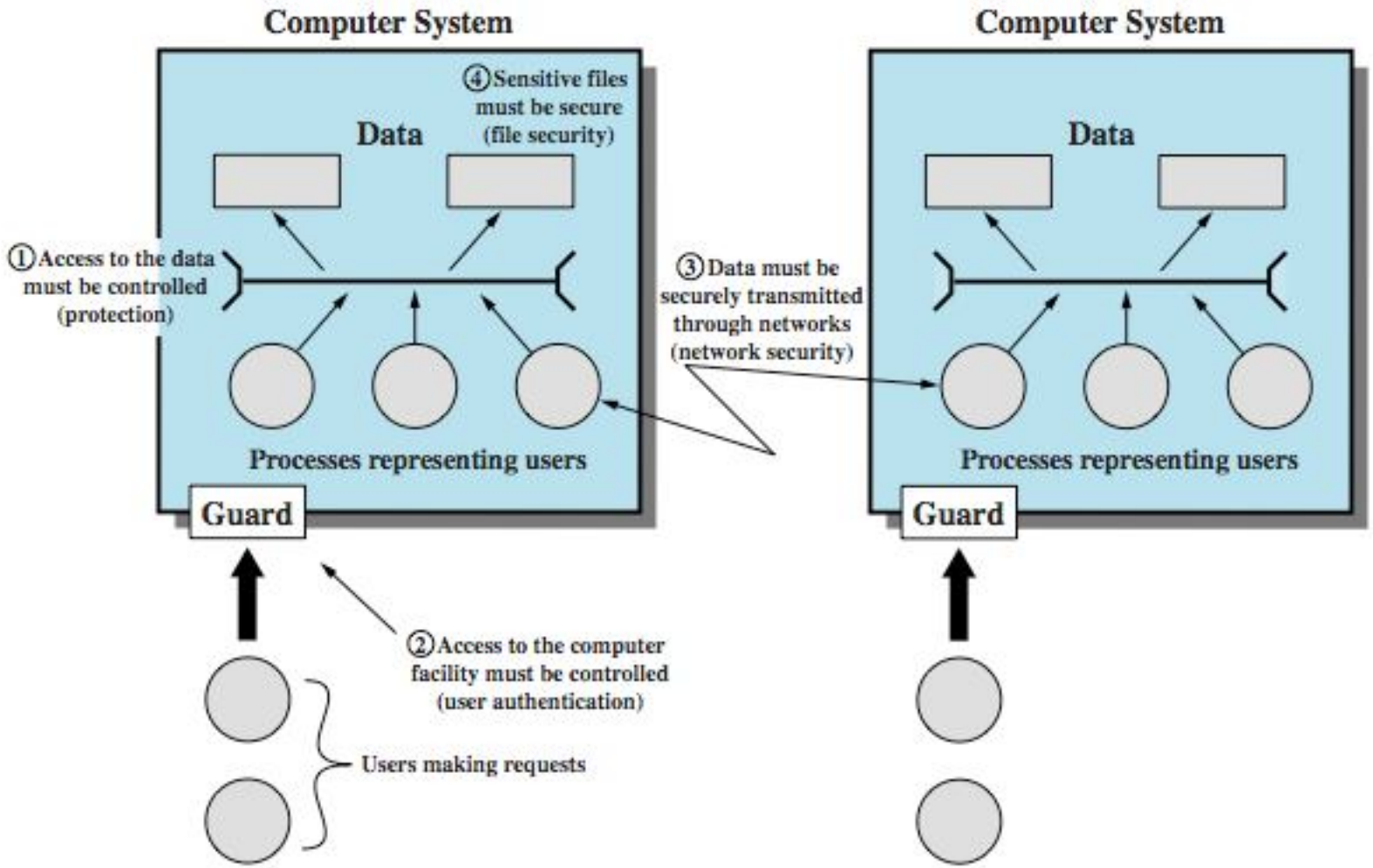
Technical Aspects of Security in Online Banking & Ecommerce

By
Prof. Hoa Tran
New York University &
Chairman of Worldsoft Corp.

Bank Data Structure



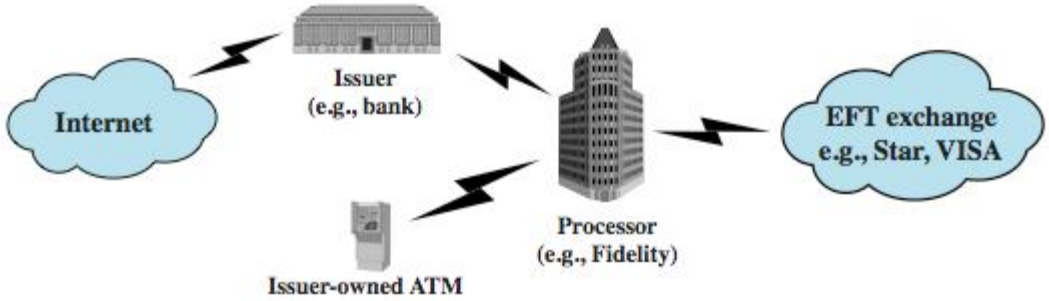
Vulnerabilities and Attacks

- System resource vulnerabilities may
  - be corrupted (loss of integrity)
  - become leaky (loss of confidentiality)
  - become unavailable (loss of availability)
- Attacks are threats carried out and may be
  - passive
  - active
  - insider
  - outsider

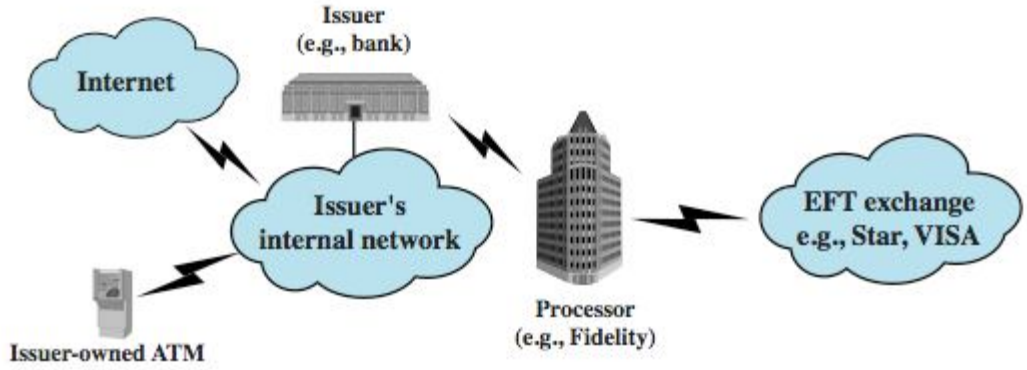
Type of Attacks

- Identification Theft
- System Intrusion
- Malicious Software
- Denial of Service
- Injection Attacks
- Network Security Attacks

ATM Security



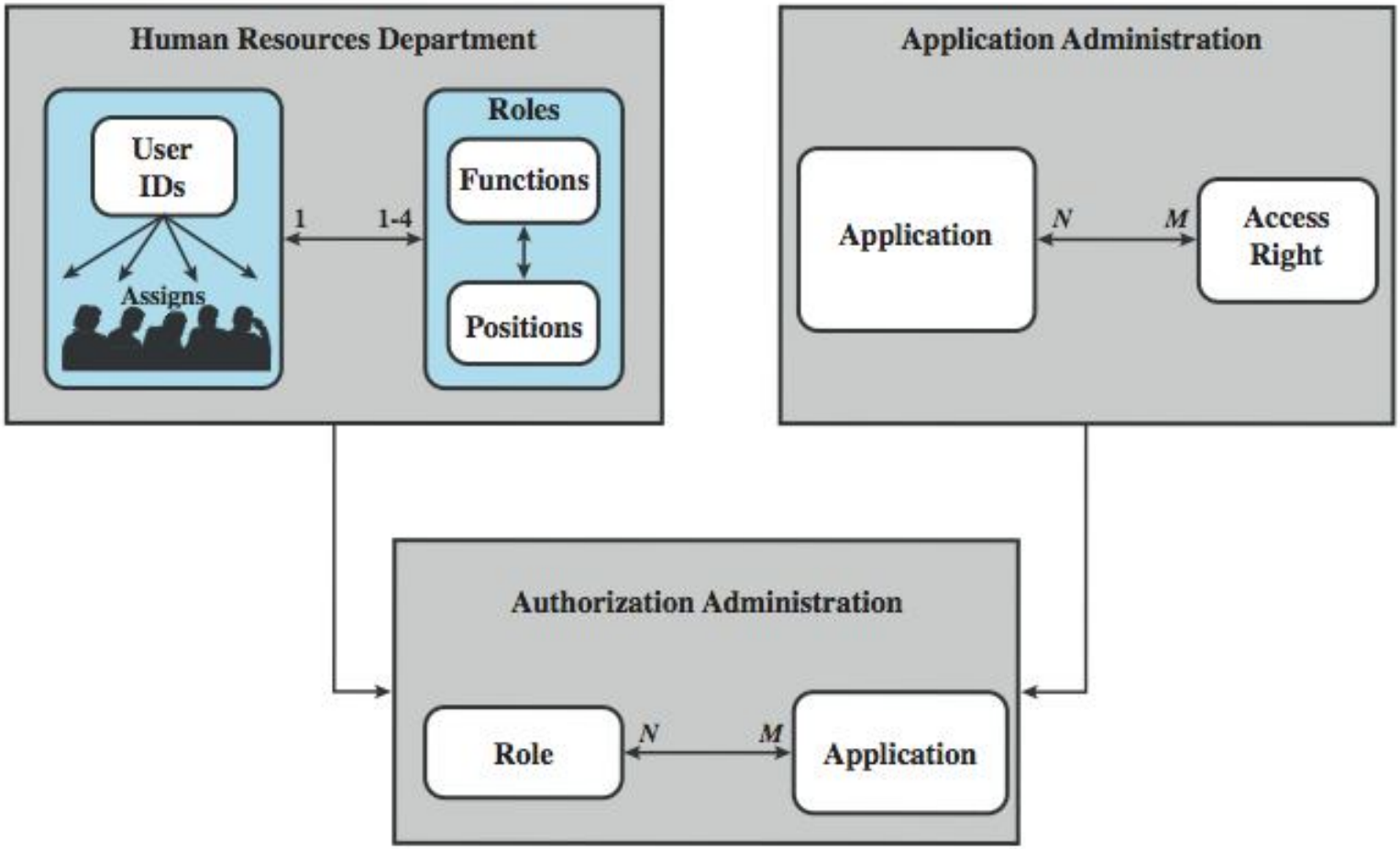
(a) Point-to-point connection to processor



Security Solutions

- User Authentication
- Access Control (Role Base for Bank)
- Database Security
- Intrusion Detection
- VPN
- Firewall
- TSL/SSL
- PKI

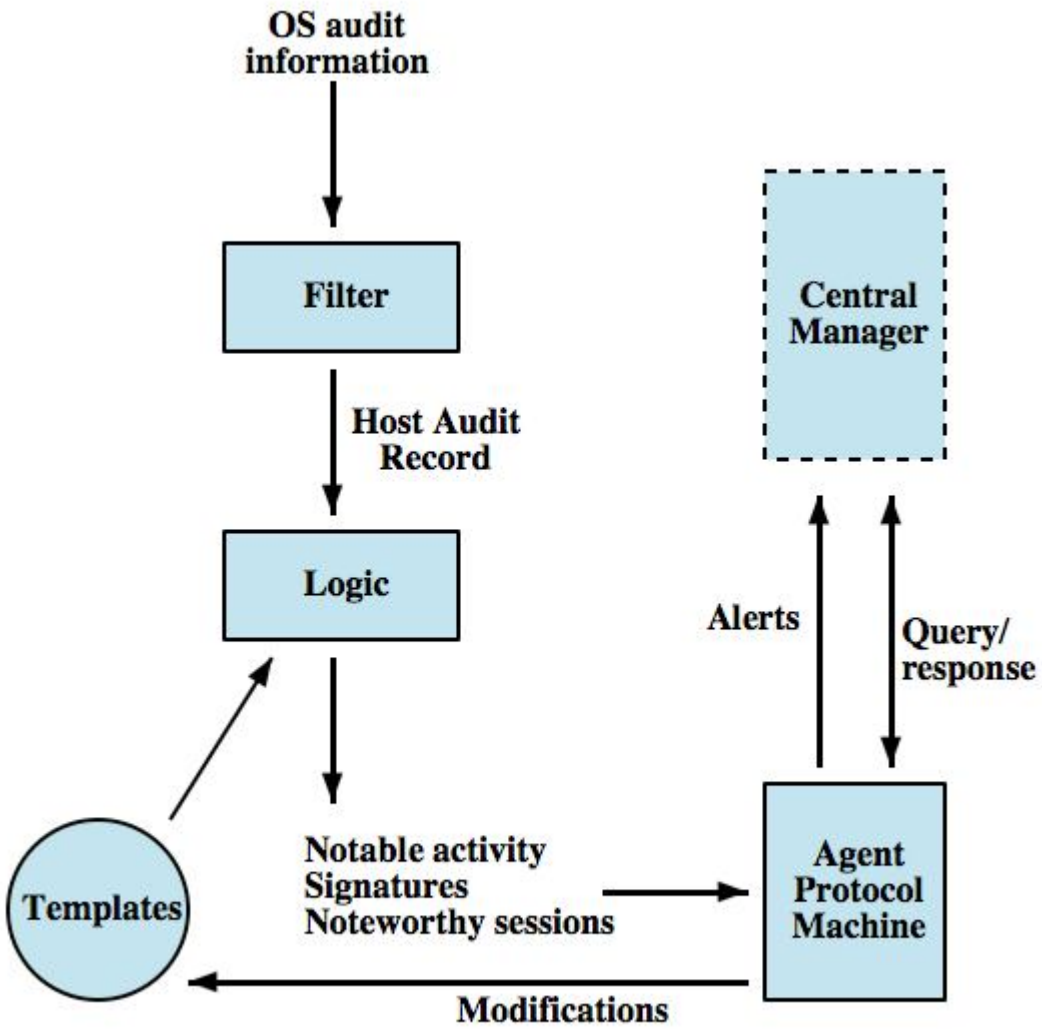
RBAC For a Bank



Intrusion Detection Systems

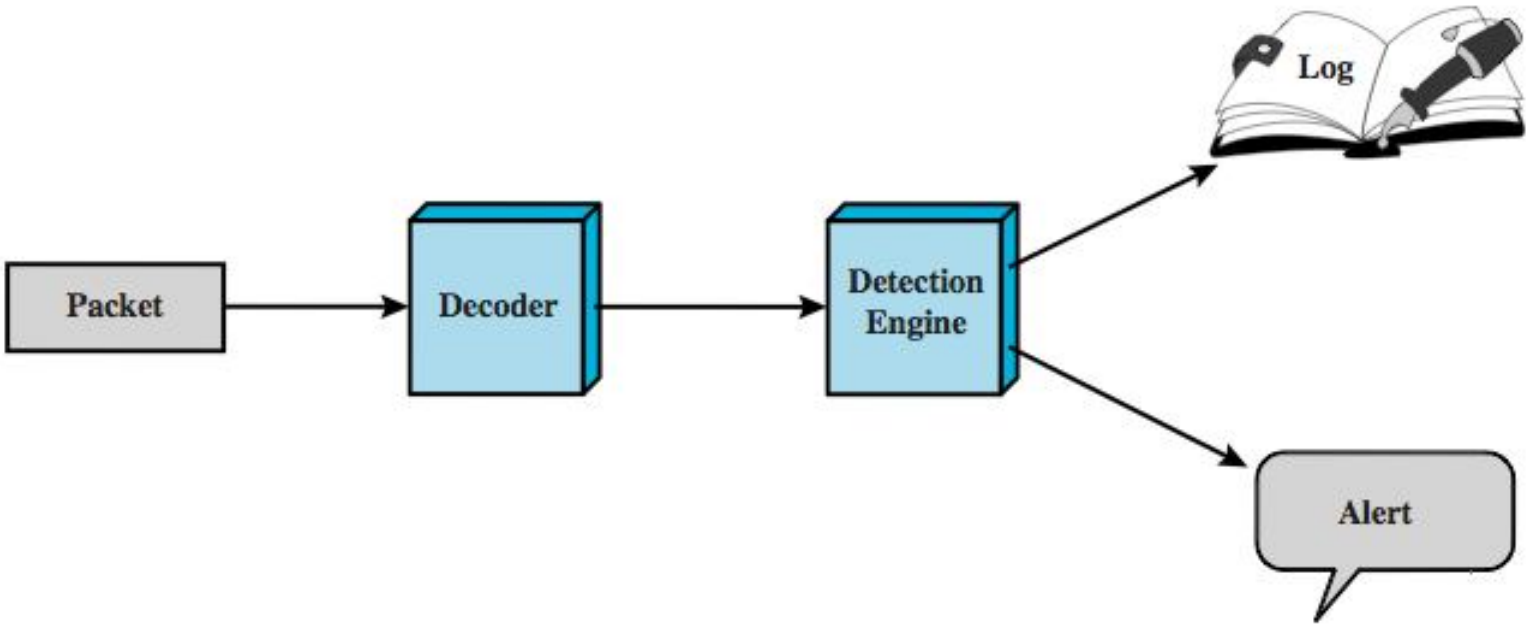
- Classify intrusion detection systems (IDSs) as:
  - Host-based IDS: monitor single host activity
  - Network-based IDS: monitor network traffic
- Logical components:
  - Sensors - collect data
  - Analyzers - determine if intrusion has occurred
  - User interface - manage / direct / view IDS

Distributed Host-Based IDS



SNORT

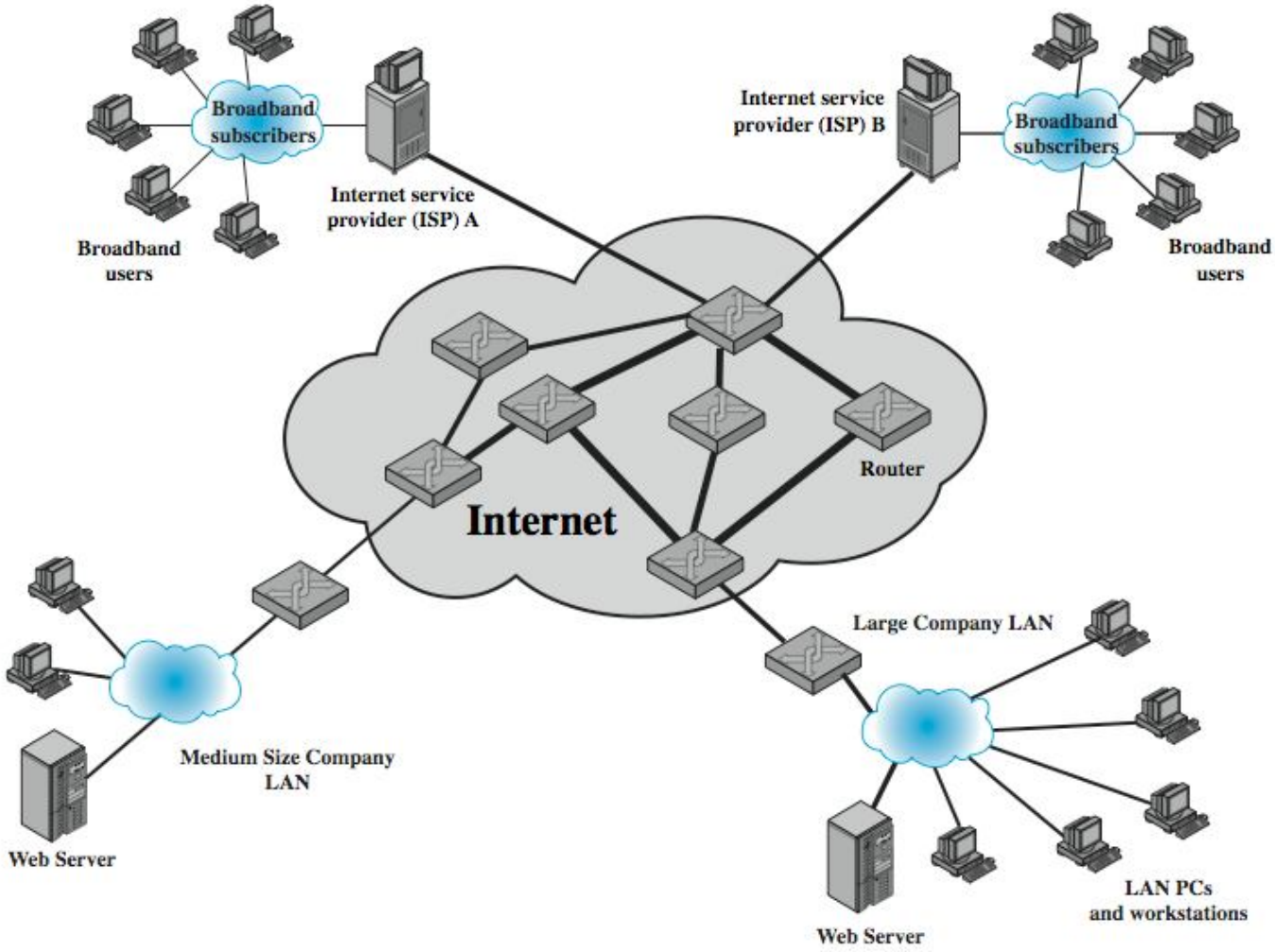
- **Lightweight IDS**
  - Real-time packet capture and rule analysis
  - Passive or inline



Denial of Service Attacks

- Can use simple flooding ping
- From higher capacity link to lower
- Causing loss of traffic
- Source of flood traffic easily identified

Denial of Service Attacks



Attack Prevention

- Block spoofed source addresses
  - on routers as close to source as possible
  - still far too rarely implemented
- Rate controls in upstream distribution nets
  - on specific packets types
  - e.g. some ICMP, some UDP, TCP/SYN
- Use modified TCP connection handling
  - use SYN cookies when table full
  - or selective or random drop when table full

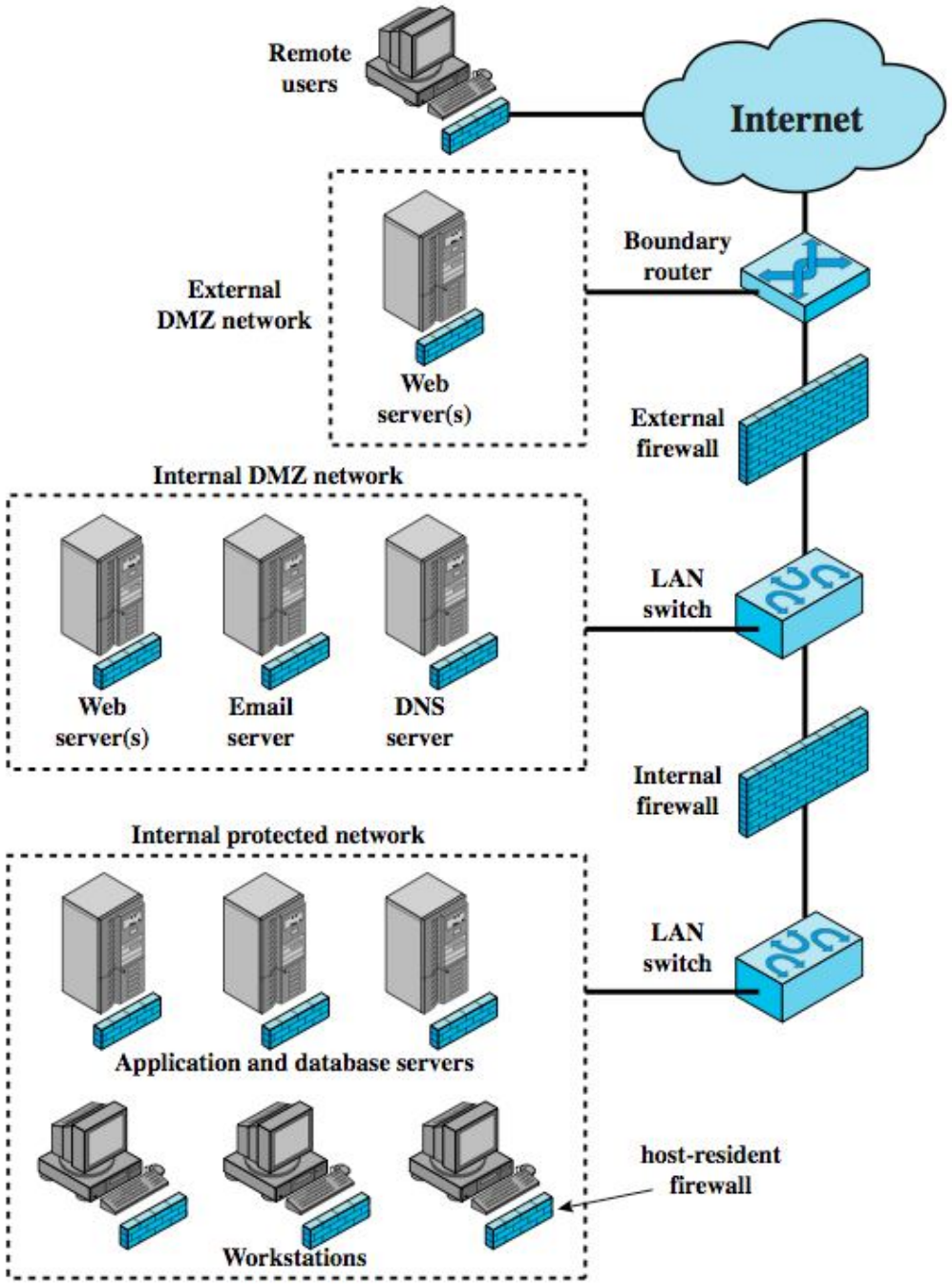
Attack Prevention

- Block IP directed broadcasts
- Block suspicious services & combinations
- Manage application attacks with “puzzles” to distinguish legitimate human requests
- Good general system security practices
- Use mirrored and replicated servers when high-performance and reliability required

Firewall

- Packet Filtering
- Stateful Inspection
- Application Level Gateway
- Bastion Host
- Individual host-based
- Personal

Distributed Firewalls



Buffer Overflow

- **Caused by programming error**
- **Allows more data to be stored than capacity**
- **Available in a fixed sized buffer**
  - Buffer can be on stack, heap, global data
- **Overwriting adjacent memory locations**
  - Corruption of program data
  - Unexpected transfer of control
  - Memory access violation
  - Execution of code chosen by attacker

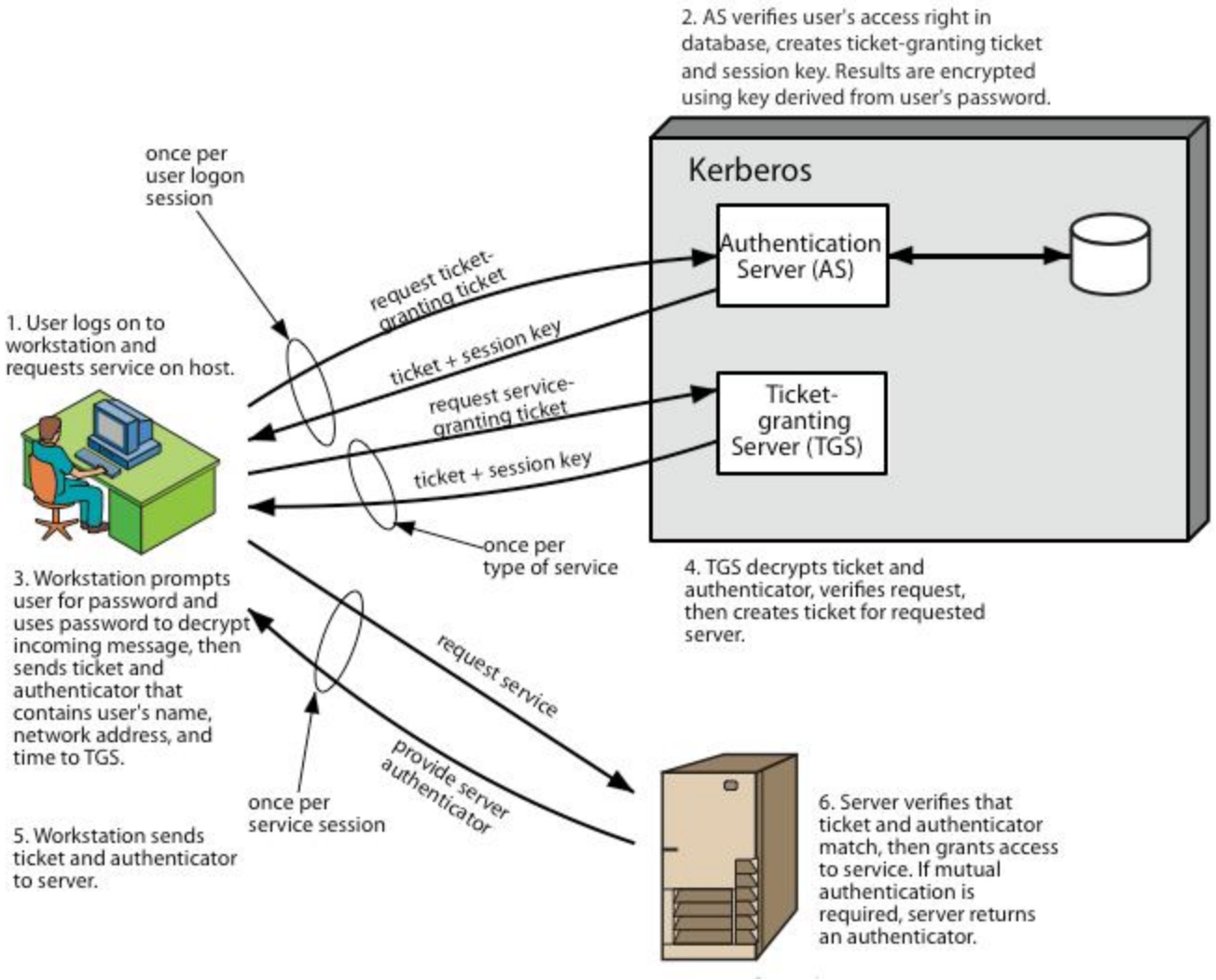
Buffer Overflow Defenses

- Buffer overflows are widely exploited
- Large amount of vulnerable code in use
  - despite cause and countermeasures known
- Two broad defense approaches
  - compile-time - harden new programs
  - run-time - handle attacks on existing programs

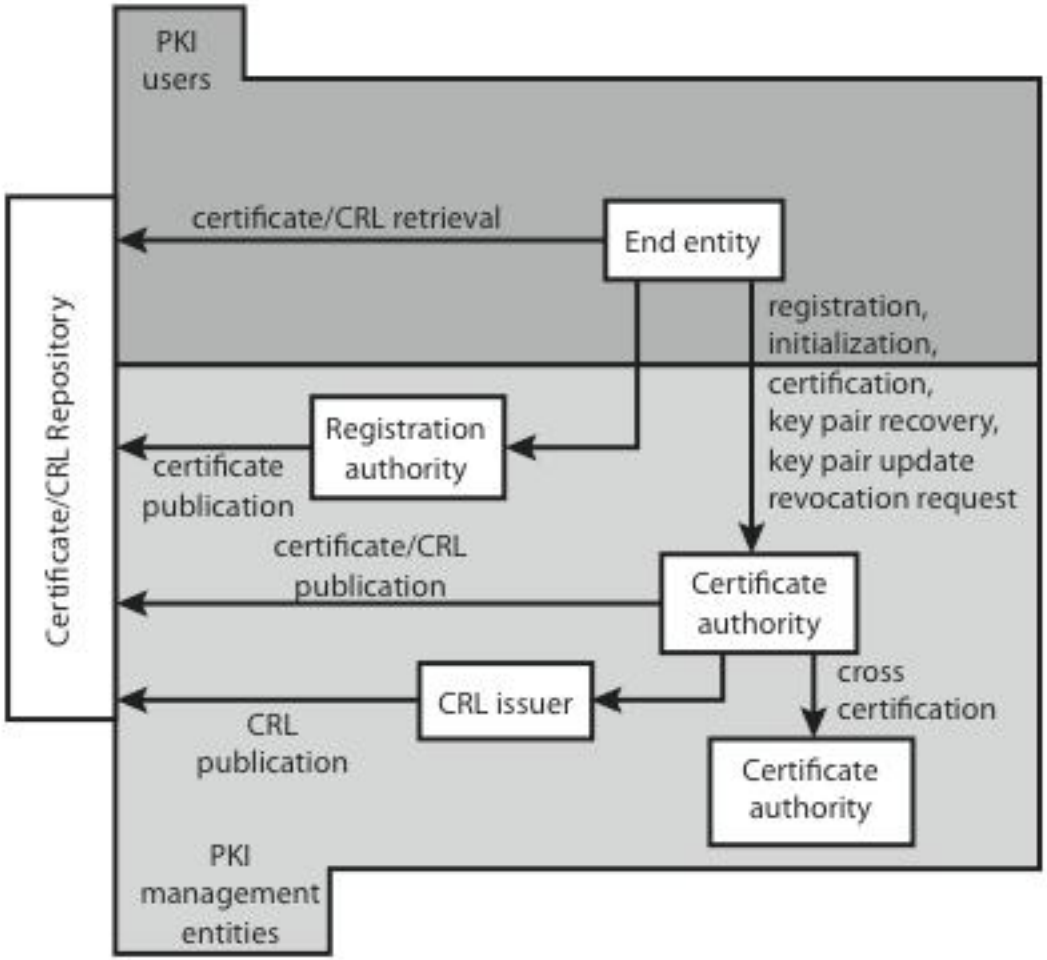
Ecommerce Security

- Authentication functions
- Developed to support application-level authentication & digital signatures
- Kerberos private-key authentication service
- TSL/SSL
- Public-key infrastructure (PKI)
- Federated identity management

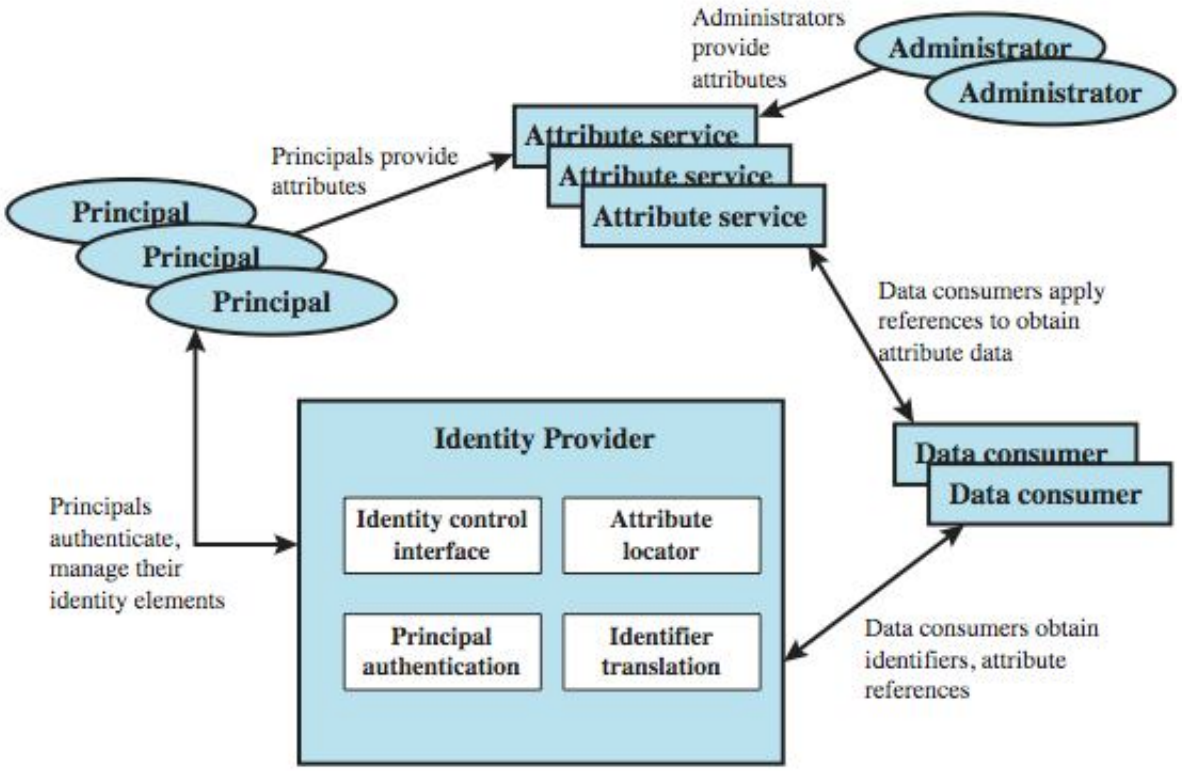
Kerberos Overview



Public Key Infrastructure



Identity Management



Products

- 2FA
- VASCO
- RSA
- Entrust

2FA (Two Factor Authentication)

- User provides second means of identification to obtain access
- Integrate with VASCO’s authentication token solution
- Integrate with Data Security System Solution’s token management