### Some objectives

- High availability
  - Expanding expectations, approaching 24x7
  - Redundancy/replication, security, human factors
- Protect confidential information
- Limit services to legitimate users or customers
- Conduct secure commercial transactions

### Availability

- Application up and running correctly
- Some types of downtime:
  - Off-line upgrade and maintenance
  - Software crashes
  - Equipment failure
  - Successful denial-of-service attack

### Availability costs!

- On-line upgrade and maintenance
- More application testing, more rapid bug reports and fixes
- Equipment or application redundancy
- Data replication
- Operational vigilance

### Question

- What availability would you like to see in:
  - Consumer stock trading system?
  - Currency trading system?
  - Train control system?
  - Bank ATM?
  - Social application like email?
  - Telephone system?

### Different security environments

- Intranet and extranet
  - All users may be trusted
- Organization-to-organization
  - Users in other organizations are less trusted, have less access
- Citizenry
  - Determined adversaries must be assumed
Access control

- First line of defense is to limit information and services to authorized users
- Requires:
  - Authorization policies
  - Databases with authorizations
  - Confidentiality of information and communication
  - Authentication of users who do gain access

Non-repudiation

- The second line of defense is to maintain a provable audit of commitments
- Requires non-repudiation: neither sender nor recipient can deny message
- Non-repudiation requires message integrity

Core technology

- Encryption
  - Depends on the existence of hard (not impossible) problems that are thought to be uncomputable by the fastest computers in reasonable time
  - “Size” of problem can be adjusted to future and anticipated computing technology
  - Symmetric and asymmetric versions