Definitions

- an entity of importance
- a set of actions taken to prevent or minimize adverse consequences to assets
- a weakness in the security system
- to compensate, partially or fully, for vulnerabilities
- someone who intentionally attempts to violate security

More Definitions

- an attempt to exploit vulnerabilities
- an attack has succeeded (causes the security system to fail)
- potential for a breach
- probability of a breach in conjunction with the cost of the resultant damage
- the method, medium mode of delivery for an attack
Authentication

Authentication is a process for verifying identity (and possibly ownership). To authenticate requires something more than the object being authenticated.

authentication factors

2-factor authentication

Authentication is often followed by ______________.
Complexity
yet another hacker advantage

__________________ are ever more complex.
__________________ are ever more complex.
__________________ are ever more complex.
__________________ are ever more complex.

Common Threats/Attacks
What are they?
  malware
  virus/worm
  spoofing
  shoulder surfing
  packet sniffing
  replay
  denial of service (DoS)
More Threats/Attacks

What are they?
- backdoor
- bot / DDoS
- logic bomb
- cracking (password or encryption)
- social engineering
- session hijacking
- spyware & keylogging
- physical theft or vandalism

The Goals of Mitigation
Threat Mitigation Methods

Physical
- authentication device (locks, card readers, biometric scanners, etc.)
- surveillance system

Network
- firewall
- intrusion detection system (IDS)
- security protocol
- honeypot
Threat Mitigation Methods

Software
  - firewall
  - intrusion detection system (IDS)
  - encryption (including digital signature)
  - authorization system
  - anti-virus software
  - backup system
  - audit/logging
  - SPAM filter
  - software upgrade/patch