Security

Jonathan Geisler

April 26, 2006

Security

Security is the assurance that system resources are being used as intended. This incorporates:

- Physical access
- Human psychology
- Network access
- OS protections

Authentication vs. Authorization

- *Authentication* is determining **who** the agent trying to act is via:
  - What the agent has
  - What the agent knows
  - What is inherent to the agent
- *Authorization* is determining **whether** the agent is allowed to act in a specified manner

Passwords

- Vulnerabilities
  - Easily guessable
  - Observable
  - Human nature
- Alternatives
  - One-time passwords

Passwords

- Vulnerabilities
  - Easily guessable
  - Observable
  - Human nature
- Alternatives
  - One-time passwords
  - Encryption

Passwords

- Vulnerabilities
  - Easily guessable
  - Observable
  - Human nature
- Alternatives
  - One-time passwords
  - Encryption
  - Frequent changes

Passwords

- Vulnerabilities
  - Easily guessable
  - Observable
  - Human nature
- Alternatives
  - One-time passwords
  - Encryption
  - Frequent changes
  - Biometrics

Programmatic threats

- Trojan horses

Programmatic threats

- Trojan horses
- Trap doors

Programmatic threats

- Trojan horses
- Trap doors
- Logic bombs

Programmatic threats

- Trojan horses
- Trap doors
- Logic bombs
- Buffer overflows

Programmatic threats

- Trojan horses
- Trap doors
- Logic bombs
- Buffer overflows
- Worms

Programmatic threats

- Trojan horses
- Trap doors
- Logic bombs
- Buffer overflows
- Worms
- Virii

Programmatic threats

- Trojan horses
- Trap doors
- Logic bombs
- Buffer overflows
- Worms
- Virii
- (D)DOS

Safety measures

- Cryptography

Safety measures

- Cryptography
  - Authentication

Safety measures

- Cryptography
  - Authentication
  - Secure file systems

Safety measures

- Cryptography
  - Authentication
  - Secure file systems
  - IPSec

Safety measures

- Cryptography
  - Authentication
  - Secure file systems
  - IPSec
- Explicit security policy

Safety measures

- Cryptography
  - Authentication
  - Secure file systems
  - IPSec
- Explicit security policy
- Security scans (i.e., vulnerability assessment)

Safety measures

- Cryptography
  - Authentication
  - Secure file systems
  - IPSec
- Explicit security policy
- Security scans (i.e., vulnerability assessment)
- Firewalls

Safety measures

- Cryptography
  - Authentication
  - Secure file systems
  - IPSec
- Explicit security policy
- Security scans (i.e., vulnerability assessment)
- Firewalls
- Intrusion detection

Safety measures

- Cryptography
  - Authentication
  - Secure file systems
  - IPSec
- Explicit security policy
- Security scans (i.e., vulnerability assessment)
- Firewalls
- Intrusion detection
- Logging

Classifications

- **D** No guarantees

Classifications

C.
   1. Users control protection

D. No guarantees

Classifications

C
1. Users control protection
2. C1 + control granularity @ individual users

D No guarantees

Classifications

B
1. C2 + sensitivity labels on objects

C
1. Users control protection
2. C1 + control granularity @ individual users

D No guarantees

Classifications

B
1. C2 + sensitivity labels on objects
2. B1 + sensitivity labels on resources

C
1. Users control protection
2. C1 + control granularity @ individual users

D. No guarantees

Classifications

B
1. C2 + sensitivity labels on objects
2. B1 + sensitivity labels on resources
3. B2 + exclusionary access control

C
1. Users control protection
2. C1 + control granularity @ individual users

D No guarantees

Classifications

A. B3 + formal design and verification

B.
   1. C2 + sensitivity labels on objects
   2. B1 + sensitivity labels on resources
   3. B2 + exclusionary access control

C.
   1. Users control protection
   2. C1 + control granularity @ individual users

D. No guarantees