Lecture 14 - Review

CSE543 - Fall 2006
Computer and Network Security
Professor Jaeger
October 24, 2006
Security Terminology

- Adversary
- Risks
- Vulnerability
- Threats
- Compromise
- Trust
- Trust Model
- Threat Model
Cryptography

- Encryption, Decryption
- Symmetric Key Systems
  - DES
  - One-time pads
- Public Key Systems
  - RSA
  - Diffie-Hellman
- Hash Functions
  - Uses
  - Properties
- Combinations of these into protocols
- Threats to crypto systems (use)
What is a key?

• A key is an input to a cryptographic algorithm used to obtain confidentiality, integrity, authenticity or other property over some data.
  – The security of the cryptosystem often depends on keeping the key secret to some set of parties.
  – The keyspace is the set of all possible keys
  – Entropy is a measure of the variance in keys
    • typically measure in bits

• Keys are often stored in some secure place:
  – passwords, on disk keyrings, ...
  – TPM, secure co-processor, smartcards, ...

• ... and sometimes not, e.g., certificates
Authentication

- Key distribution
  - Needham-Schroeder
  - Secret and public key
- Kerberos
  - Protocol Basics
  - Extensions to NH
- Kerberos Flaws
- Public Key Infrastructure
  - Use
  - Limitations
- Protocol Analysis
  - What can we do? What can’t we do?
Trusted Computing

• Hardware for Security
  – Protected Storage
  – Hash Extends
  – Sealed Storage

• Model
  – What can really be done?

• Issues
  – Lots
Systems Security

• Access Control Fundamentals
  – Protection State
  – Protection System
  – Reference Monitor
  – Access Matrix

• Policies
  – Goals
  – How represented, how achieved?

• ACLs and Capabilities
  – Functions and issues

• System Architectures
  – Impact on access control enforcement