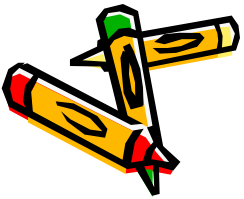
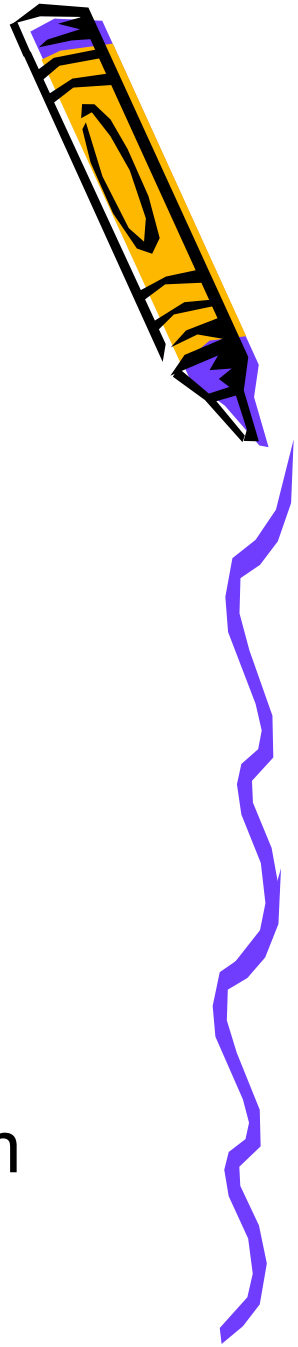
Traditional Security Issues

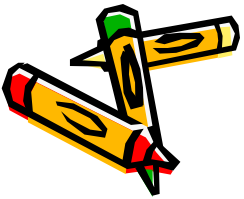
- Confidentiality
  - Prevent unauthorized access or reading of information
- Integrity
  - Insure that writing or operations are allowed and correct
- Availability
  - System functions cannot be denied



Security in the Real World

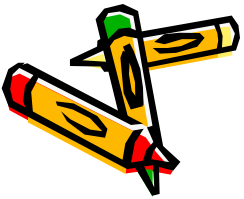


- Professionals must address:
  - Specification/Policy
    - Requirements, analysis, planning,…
  - Implementation/mechanisms
    - Algorithms, protocols, components, etc.
  - Correctness/assurance
    - Proof, testing, verification, attacks, etc.
  - The Human Factor
    - Protecting against “bad” users and clever attackers
- All critical: CS453 focuses on the 2nd item

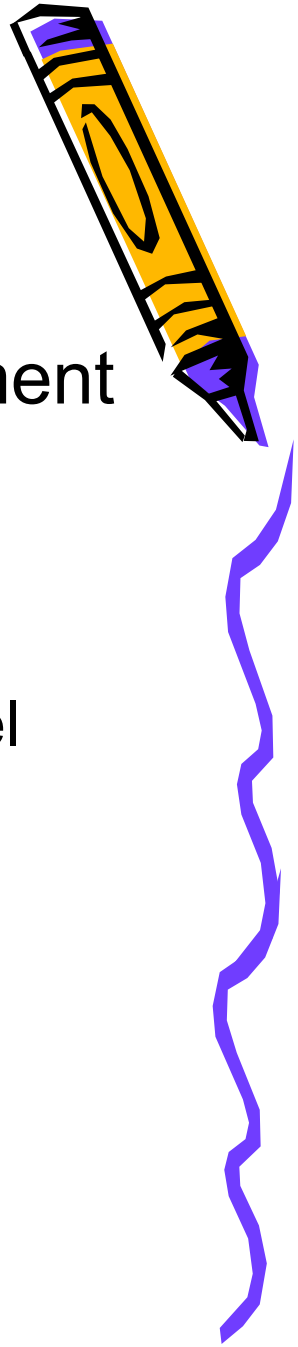


Terms for Activities Related to E-Commerce Security

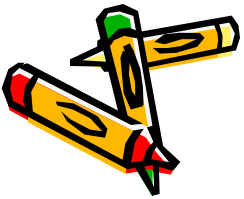
- Authentication
  - Identification of a user for access
- Authorization
  - Defining and enforcing rules or levels of access
- Repudiation
  - A party later denying a transaction has occurred
  - Goal: insuring non-repudiation



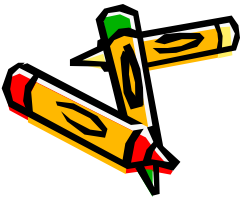
Briefly: Security Policy



- You should define a security policy document for your site or application
  - A form of non-functional requirements
- Might include:
  - General philosophy toward security (high-level goals etc.)
  - Items to be protected
  - Who's responsible for protecting them
  - Standards and measures to be used: how to measure to say you've built a secure system

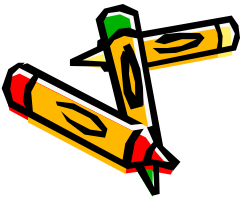


What's Coming in this Unit?



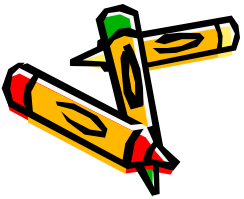
Authentication

- Proving a user is who they say they are
- Methods?
  - Passwords
  - Digital signatures, digital certificates
  - Biometrics (fingerprint readers etc.)
  - Smart cards and other HW
- We'll discuss
  - Cryptography
  - Mechanisms: algorithms, web servers, biometrics, SSL



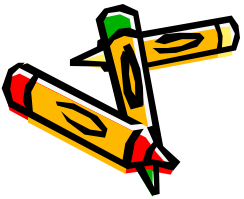
Authorization

- We won't say much about this
- Approaches include:
  - Access control lists
  - Capabilities
  - Multi-level security systems



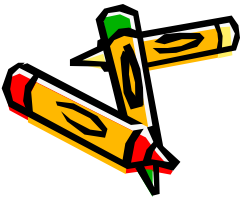
Non-Repudiation

- Non-repudiation of origin
  - proves that data has been sent
- Non-repudiation of delivery
  - proves it has been received
- Digital signatures
  - And more crypto



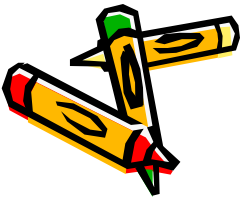
Digital Certificates

- "On the Internet, no one knows you're a dog."
  - Or do they?
  - For commerce, we can't always allow anonymity
- How does UVa's NetBadge work?
  - http://www.itc.virginia.edu/netbadge/
- Public Key Infrastructure (PKI)
- Certifying Authorities in the commercial world
  - E.g. VeriSign



SSL: Secure Socket Layer

- A network protocol layer between TCP and the application. Provides:
- Secure connection – client/server transmissions are encrypted, plus tamper detection
- Authentication mechanisms
  - From both client's point of view and also server's
  - Is the other side trusted, who they say they are? Using certificates
  - Is the Certificate Authority trusted?



Cryptography

- Cryptography underlies much of this
- Interesting computer science
  - And historical interest too
- We'll touch on that
  - But always try to come back to the practical and e-commerce
- Topics:
  - Symmetric Key Crypto.; Public Key Crypto.; Digital Signatures; Digital Certificates; SSL