Announcements

- Check class announcements daily
- You must implement programming projects by yourself
Security (Email)

- Least secure of internet protocols
- Avoid sending sensitive information (e.g., passwords) over e-mail
- Provide e-mail addresses in web sites in a way is not easily recognized by spam programs
  - Use at rather than @
  - Put an image with the e-mail
  - Avoid mailto
- Encrypt the message using PGP (Pretty Good Privacy) or GPG (GNU Privacy Guard)
- [http://www.wbwip.com/wbw/emailencoder.html](http://www.wbwip.com/wbw/emailencoder.html)
Security (Password-Protected Sites)

- **Approach not recommended**
  - Store encrypted password
  - Decrypt password and compare against user provided password

- **Better approach**
  - Store encrypted password
  - Encrypt provided password and compare against stored password
Security (Encryption)

- **Encryption** → process of converting plaintext into ciphertext
- **Decryption** → process of converting ciphertext into plaintext
- **Symmetric cryptography** → sender and receiver share the same key
- **Asymmetric (Public Key) cryptography** → sender and receiver have different, complementary keys

**Symmetric cryptography**

- Relatively fast compared to asymmetric

**Drawbacks**

- Keys must be change frequently
- How to distribute the key safely
Security (Encryption)

- Branches of public key cryptography
  - Public key encryption
  - Digital signatures
- Public key Encryption
  - Example algorithm: RSA
  - Relatively slowed compared to symmetric
  - How it works?
    - Each user has a public/private key pair.
    - Public key is widely known
    - Private key only known by user that generated it
    - If user A wants to send user B a message, user A encrypts message with B’s public key. B will decrypt the message with B’s private key. The only way to decrypt the message is by using B’s private key
- Digital signature
  - Message signed with sender’s private key can be verified by anyone with sender’s public key thereby proving message authenticity
Digital Certificates (Certificates)

- **Digital Certificates** → electronic documents that contain information about a public key and the owner (name, address, etc.)
- Employed to verify a public key corresponds to a particular organization
- Certificates must be issued by a trusted third party known as certificate authority (CA) which guarantees the information is correct
- **About certificates**
  - Have a validity period and can expire
  - They can be revoked
  - Browsers have a collection of root certificates
    - In Firefox – Tools → Options → Advanced → View Certificates
  - Main standard X.509
Message Digests

- Message digest → fixed-length representation of a message
- Expected properties for message digest ("Hashing") algorithm
  - Original message cannot be obtained from the digest
  - Two different messages should have different digests
- Example algorithms: MD5 and SHA
Need For Security

- SSL (Secure Sockets Layer) Protocol → Protocol that enable us to satisfy the need for security in client-web server transactions
- The algorithm provides support for confidentiality, integrity and authentication

SSL connection is established as follows:
- User connects to web server through the browser
- Browser and server exchange public keys and certificate information
- Browser checks server certificate validity (certificate not expired, issued by CA, etc.)
- Optional: server can request a valid certificate from the client
- Using public keys server and client determine a symmetric key to use
- Communication from this point on is through symmetric cryptography
**https**

- **https** → http where
  - A different default port (443) is used
  - An extra layer of encryption/authentication exists between HTTP and TCP
- **https** → is not a separate protocol but a combination of HTTP over encrypted SSL or TLS transport mechanism
- **TLS** → Transport Layer Security
  - IETF standard designed to standardize SSL as an Internet protocol
  - Slight differences between SSL 3.0 and TLS 1.0
Web Site Validation (whois servers)

- Importance of finding owner of web site
- Whois servers → databases that keep track of owners of domains
- Unix whois → provides domain information
  - Domain name
  - Registrar → Organization which registered the domain
  - Whois server → where you can find information about the domain
- Example using [http://www.internic.net/whois.html](http://www.internic.net/whois.html), Domain option and umd.edu
- Example using umd.edu and the Unix command
  - Run Unix whois command to determine whois server
  - Run Unix whois command with the –h option on whois server
Web Site Validation (whois servers)

[loompa 11] whois umd.edu

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered with many different competing registrars. Go to http://www.internic.net for detailed information.

Domain Name: UMD.EDU
Registrar: EDUCAUSE
Whois Server: whois.educause.net
Referral URL: http://www.educause.edu/edudomain
Name Server: NOC.UMD.EDU
Name Server: NS1.UMD.EDU
Name Server: NS2.UMD.EDU
Status: ok
Updated Date: 01-aug-2008
Creation Date: 31-jul-1985
Expiration Date: 31-jul-2009

>>> Last update of whois database: Thu, 16 Jul 2009 18:14:01 UTC <<<
ICANN

- ICANN → Internet Corporation for Assigned Names and Numbers
- [http://www.icann.org/](http://www.icann.org/)
- Responsibilities
  - Coordinates internet naming system
  - Ensures every IP address is unique
  - Oversees distribution of IP addresses and domain names
  - Accrediting domain name registrars
InterNIC web site

- Operated by ICANN
- [www.internic.net](http://www.internic.net)
- Provides public information regarding Internet domain name registration services
  - Find registrar’s details
  - Search domain information
  - Report incorrect whois data
  - File a registrar complaint
- Whois server for .mil domains – whois.nic.mil
- Whois server for .gov domains – whois.nic.gov
- [http://www.internic.net/faqs/domain-names.html](http://www.internic.net/faqs/domain-names.html)
  - Provides great information about domain names, ICANN and registrars.
Social Consequences of Security

- Recent report on how social security numbers can be predicted
- Confidentiality of medical information
- National Security Information
- What other scenarios can you think of?
Security Sites

- www.securityfocus.com/
- www.cert.org/