ANNOUNCEMENTS

- None

USABILITY: FRAMES

- **Frame**
  - Allows us to view several HTML documents in the same window.
  - A page can be loaded in a frame while other stay constant.
  - **Example:**
    http://java.sun.com/j2se/1.5.0/docs/api/index.html
- **Causes big problems from a usability point of view**
  - Bookmarking will not work as expected.
  - Search engines have difficulties with frames.
  - Printing can be problematic.
- Effects associated with frames can be achieved via CSS positioning and ** ** tag.

GUIDELINES FOR AN USABLE WEB SITE

- **Visual Consistency** - When a new page is selected in a site it should be easy to identify it belongs to the same site.
  - You can achieve consistency by
    - Using logos or banners.
    - Keeping a consistent layout and configuration of elements. For example:
      - Navigation bar is consistent in its placement and appearance.
      - Consistent coloring.
  - If the layout is not consistent you can use identical colors and shape elements to make pages appear consistent.
- **Navigation** – For an easily navigable site users should be clear about:
  - Where they will go when selecting a link.
  - Where they are in the site.
  - How to get back to a recognizable starting place.

GUIDELINES FOR AN USABLE WEB SITE

- **Navigation: Approaches to organize a site**
  - **Sequential Organization** – Pages follow a certain order and are linked to one another in order. Appropriate for scenarios were:
    - Sequence of steps needed to complete a task are described.
    - A story is told.
    - Chronological information is presented.
  - **Hierarchical Organization** – Appropriate for sites with a very large number of pages. A main page has categories with subcategories, etc. Users should know their position in the structure.
  - **Web-based Organization** – Most common organizational structure.
    - Web-like structure (should not force one of the organizations previously discussed).
    - Pages link to one another based on content
      - A page could be accessible only from one particular page.
      - A page can connect many pages.
      - Etc.

GUIDELINES FOR AN USABLE WEB SITE

- Links
  - Links names should be descriptive and indicate where the links go.
  - Rather than next, prev, up, down add a description of the nature of the page that will be reached.

    “next: Weather in the USA”

    “up: Courses at UMCP”
- Search
  - Search tools for an entire web site can help users find what they need.
  - The search should search the web site by default.

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).

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**
  - Example algorithms: DES, Triple-Des, RC4.
  - 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 Asymmetric.
  - 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 issue 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 revoke.
  - Browsers have a collection of root 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.

SECURITY SITES

- www.securityfocus.com/
- www.cert.org/
- http://rootshell.com/