1 General nomenclature

Security has several important components.

- Privacy (secrecy): Private data should not be disclosed to unauthorized parties.
- Protection: Data (and programs) should not be modified by unauthorized parties.
- Service: Software should not become nonfunctional in normal use.
- Authentication: Parties should be able to reliably determine with whom they are communicating.

2 Browser issues

Over the years, many security-related flaws have appeared in web browsers. The developers fix them, but one can expect more to appear.

- ActiveX controls. IE can be configured to run programs embedded in web pages called **ActiveX controls**. These programs can accept data from untrusted sources (other than the server) and access local data. The user can set IE security levels to prevent security errors, but the ActiveX control can register itself as secure and avoid this hurdle. Reference: [http://msdn.microsoft.com/workshop/components/activex/safety.asp](http://msdn.microsoft.com/workshop/components/activex/safety.asp).
Security settings and Java applets (eg file permissions) Most browsers can be configured to run applets, which are programs embedded in web pages. These applets can be coded in any language, but the browser must support that language. Java is the typical language for applets. The browser runs applets in a sandbox, that is, an environment with restricted permissions. Applets cannot open client-side files or create network connections except to the originating host. If the applet is signed and the user accepts the signature, then the restrictions are reduced. Reference: http://java.sun.com/sfaq/.

- JavaScript Most browsers can be configured to run scripts, which are programs embedded in web pages coded in JavaScript. Scripts can access and modify data presented on web pages and entered by users on forms. They can also build a connection back to the originating host and use it to send and receive data. JavaScript has been designed to avoid security risks.

- Cross-frame attacks. Most browsers can show unrelated documents in various windows and frames. There have been security problems with JavaScript accessing documents across frames; these problems have been fixed. Reference: http://msdn.microsoft.com/workshop/author/om/xframe_scripting_security.asp.

- Other script and applet attacks. Code embedded in a web page might be able to place an image in such a way that it obscures important information in the browser, such as the URL window, allowing the script to pretend not to be doing something.

- Executing hidden embedded code (malformed JPEG for instance) Browsers often depend on libraries to perform standard operations such as decoding JPEG pictures and performing bidirectional Unicode layout. These libraries might have security flaws that are elicited by web pages containing offending data.

- Executing downloaded files (Word, .EXE) Browsers can be set to automatically invoke external software to deal with some document types. The external software might be insecure. The general problem is treating data (information on the web) as program. Obvious cases are .EXE files; less obvious are Word files, which can contain macros, or PDF files, which can contain executable parts.

- Spoofing URLs (Unicode) It is easy to build a URL that looks similar to a legitimate URL, different only in a single letter.
Often users don’t look at the URL very closely when they follow a link. Different Unicode characters are often displayed identically, such as the Latin and the Cyrillic “a” character. URLs with characters outside the Latin range are not always flagged as problematic by the browser.

- Tracking cookies. Browsers can be configured to store information in the form of cookies presented by the originating host and later queried by that host. Cookies help the host associate one web request with another. However, cookies can also be used to track what sites a user has visited.

3 Secure communication

- Network communication is by nature insecure in that unauthorized parties can snoop the traffic, whether by listening into wireless channels, attaching to physical ether, or subverting either the sending or receiving host, or the mapping service that converts domain addresses to IP addresses.

- Therefore, confidential communication should always use cryptographic techniques to assure security.

- The standard method has three stages.
  - public-key encryption to establish an authenticated channel between the two parties.
  - exchange of a session key on that authenticated channel.
  - private-key encryption from that point forward using the session

- Authenticating the server requires that the client know the server’s public key. There are too many servers for anyone to store all their public keys. Instead, servers present a certificate to the client that includes their public key, signed by a recognized authority, of which there are about 20.

- The browser should ask the user if it cannot recognize the signing authority, if the certificate has expired, or if the certificate is not for that server; the user might blindly choose to accept a certificate that is in fact forged, inappropriate, or no longer secure.
The signing authority might not apply due scrutiny to the application for a certificate.

Some encryption methods (such as DES) are too weak to be trusted, but browsers (and other software) still support them.

4 Server vulnerabilities

There are situations in which clients can attack servers.

- CGI scripting.
  - The CGI script that runs on the server might have permissions to read or write any file on the server; in this case, it must be very careful to only access the right files.
  - However, careful configuration of the web server usually limits the privilege of CGI scripts to the user who owns the script.
  - It is important not to trust any information that the client provides in forms handled by the script. In particular, such data must never be passed directly to shells as invocation parameters, because the data might contain characters like ";" or "&" that have meaning to the shell.
  - Perl has a -T flag that taints all data derived from outside the program. Perl refuses to let tainted data affect anything outside the program, including parameters to program calls. This flag also enables other important restrictions, such as verifying that path directories aren't writable by others.

- Unnecessary open ports
  - Network services listen for connections from clients on ports. Some of these ports have a standard interpretation; others don’t.
  - It is wise not to run any services that you don’t need on your computer, because every service provides a target for an attack.
  - There are web sites that can test your computer for open ports. Reference: google:shields up.

- Denial-of-service (DOS) attacks
  - Every attempt to connect to a network service requires CPU cycles, even if there is no open port.
Malicious parties can overwhelm a server by making many connection requests, or, worse, sending large amounts of data on opened connections.

The malicious party might control a large, dispersed, swarm of infected computers that engage in the DOS attack.

It is not possible to defend against a well-orchestrated DOS attack; one needs to shut down the traffic outside the server, usually by manually analyzing its behavior and installing filters in nearby routers.

5 Social engineering

- Phishing privacy

A phishing attack is an attempt to get a user to divulge private information to a host that pretends to be a trusted server. These attacks use clever means to hide the fact that the server is not authenticated. They use URLs that are similar to legitimate ones and web content that is indistinguishable from legitimate content.

- Nigerian scams

The standard Nigerian scam tries to convince the user to enter into a shady financial deal. Users are then enticed into fronting increasing amounts of money to make the deal work. This sort of attack is really a confidence scheme and has little to do with network security, except that the initial contact is made via email.

6 Protective measures

- Lists of bad guys

  - Firefox uses a list to warn about known phishing sites.
  - Firefox plugin to avoid advertisements, which are occasionally malicious.
  - Blacklisting and greylisting to reduce incoming spam.

- Firewall software
A firewall is software that applies rules to determine whether to permit a network connection to be established.

- The rules are represented as a list of entries; the first entry that matches is effective.
- An entry can include the name of the local software, the remote IP address, the local port number, and the remote port number; it can use a wildcard for any of these. The entry indicates whether to allow or disallow the connection.
- Free firewall software is available for Microsoft, Linux, and Mac operating systems.

Network address translation (NAT)

- A remote site can only attack your computer if it knows your IP address.
- If your computer is behind NAT box (typically a router), then when you make an outward connection, the remote machine only sees the NAT box’s IP address, which it cannot use to contact your machine.
- NAT boxes recognize reverse traffic, though, and connect return connections from servers that you have recently contacted back to your computer.
- Unless the NAT box is configured to route connection attempts from remote machines to certain inbound port numbers into your machine, remote hosts cannot initiate any connections to your machine, which therefore is protected against many attacks.

Prompt attention to security-related software updates

- Once an attack vector is discovered, it is often released to vendors first, and they have time to fix their software.
- Some attacks are not first given to vendors; they are called zero-day attacks.
- Whenever a vendor publishes a security upgrade, you should install it as soon as you can. The fact that they have published the upgrade tells malicious people how to attack unpatched machines. Most successful attacks target software that should have been upgraded but was not.
- Of course, you need to verify that your upgrade is legitimate.