Difference between Internet and WWW:

Internet: a network of network that interconnects millions of machines.

WWW: a distributed program that is running on top of Internet.

Web Servers: www.binghamton.edu

Web browsers: Chrome

Router: 路由器

Internet services provider are internet company, such as ATT、sprint

TCP: Connection-oriented, data will not be lost or reordered

UDP: Connectionless, data may be lost or reordered, but faster

Router: transfer the data over different network

Bridge: transfer the data in the same network

Get:

1. Request can be cached;
2. Request is in browser history;
3. Request can be bookmarked;
4. Data is added to URL;
5. Length restriction on data;

Post:

1. Cannot be cached;
2. Not in browser history;
3. Cannot be bookmarked;
4. Not added to URL;
5. No length restriction;

HTTP 1.0: every time you use http 1.0,like web sends request to server, and then server response the request to web, you need to built the connection every time, because after the response to the web, the server will terminate the connection.

HTTP 1.1: one connection can be used for multiple requests, because the connection won’t be terminated by the server.

Function:

**Accept** – media type supported by web browser; ”order” defines preferences.

**ETag (entity tag)** – checks if a cached version of the requested web page is identified to the current web page.

Status Code:

200 – OK

400 – bad request

404 – not find

HTTP server:

1. Admin requests a certificate from a trusted certificate authority;
2. Web browsers are distributed with the public key of trusted certificated authority;

SSL:

## In handshake protocol, client and server exchange the key, what kind of key is that? It said it is public key. It seems we should learn a lot of public key and private key.

The virus designed for Linux cant execute in Windows Systems. Same to Windows’ s Virus.

The Windows virus are more than Linux’s because of the larger number of users in Windows

How to distinguish whether the program has been infected: check the size of the program, if it is infected, it has a larger size than it should be.

So, we can compress the program when we try to infect it by virus. Compress(prog)=size (Prog’+pendings+virus)

Polymorphic Virus: contains encryption copy of virus and decryption module.

Master boot record:

1. 1st sector of hard disk;
2. Created when the computer is partitioned;
3. Boot loader a partition table

User Mode Rootkits:

1. W - who is using the computer and what they are doing;
2. df - display available disk spacs;
3. ps - process status;
4. who - who is using the computer;
5. top - top cpu process;
6. last – last few login/logout activities (activities after computer file was created)

attacker can modify the pointer (syscall 产生一个pointer，然后pointer指向我们需要的syscall), then the pointer gets the syscall and return to the virus rather than it should be.

Bank:

1. E(Ks,(PI || DS || OIMD)) ; E(Pub,Ks)->for digital envelop
2. E(Ks`, E(Priv-m, Transaction-ID)) –> authorization block; E(Pub,Ks’)->digital Envelop
3. Certificate of merchant and cardholds