

Services 2

Telnet Trick

Text

Many services use a textual dialog between the client and server -- short phrases sent back and forth as lines of text.

Telnet

Telnet to the appropriate port number, and just type the commands by hand...
`% telnet host port`

"Transparency"

Systems are easier to debug if their state is visible and accessible. This is an advantage of text-based protocols.

ASCII standard

Using plain ASCII characters also provides portability. Every system in the world understands ASCII, and because each letter is a single byte, it does not depend on big-endian little-endian issues that make binary data harder to port between systems.

Telnet - POP

(things typed by me are in bold)

`[localhost:~] nick% telnet pobox6.stanford.edu 110`

Trying 171.64.14.86...

Connected to pobox6.stanford.edu.

Escape character is '^'].

+OK pobox6.Stanford.EDU Cyrus POP3 v2.0.12 server ready

USER nick

+OK Name is a valid mailbox

PASS foobar

+OK Maildrop locked and ready

STAT

+OK 2 1242

+OK

QUIT

Connection closed by foreign host.

Telnet - HTTP

`[localhost:~] nick% telnet www.stanford.edu 80`

Trying 171.64.14.237...

Connected to www.lb-a.stanford.edu.

Escape character is '^'].

HEAD / HTTP/1.0

HTTP/1.1 200 OK

Date: Mon, 23 Apr 2001 18:24:04 GMT
 Server: Stronghold/2.4.2 Apache/1.3.6 C2NetEU/2412 (Unix) mod_fastcgi/2.2.4
 Connection: close
 Content-Type: text/html

Connection closed by foreign host.

Security

Most of our security coverage will come at the end of the quarter, but we'll do a little bit now to understand the security scheme in HW1

Authentication

Prove who you are

3 ways

Something you know -- a password

Something you are -- fingerprint retinal scan (these methods have some serious disadvantages)

Something you have -- a little gadget which knows the password for you

Traditional Password Auth

"Shared Secret"

The password is a secret thing known to the client and server (or whoever the parties are).

Knowing the shared secret defines authenticity -- only Bob knows the secret.

Therefore, if X claims to be Bob, and X knows the secret, then X is Bob.

Password demand

The server asks the client for the password. The client provides it, the server checks it against the server's copy of the password.

One-Way Hash Function

Hash

Given a string as input, combine/hash the bits together in a regular way to produce a "hash" value.

Function of input

The hash value depends on every bit in the input. Changing the input a little results in a different hash value.

Not-invertible

Given the hash value, it should not be possible to compute the "inverse" -- figure out what the original input was to result in that hash.

MD5 is a standard hash function.

Hash password DB trick

It's traditional for the server to not store the password directly. Instead, the server will store a hash of the password.

When the client sends over a password, the server hashes it, and compares the hash value to the stored value to see if they match.

Advantages

The server cannot impersonate the client.
 Someone who breaks in to the server and steals the password db cannot impersonate the client.

Problem -- passwords in the clear

If the client sends the password to the server just as plain text, then a bad guy who was eavesdropping could pick up the password, and later impersonate the client.

Solution -- challenge/response

Challenge

The server sends a "challenge" to the client: a random number R.

Client

The client computes $\text{hash}(R+\text{password})$ and sends the hash to the server

Verify

The server knows R and knows the password, so the server can also compute $\text{hash}(R+\text{password})$ and see if it matches what the client sent.

Safe

Note that the bad guy can intercept R and $\text{hash}(R+\text{password})$, but in theory cannot invert the hash function to find the original password.

Problem Bad Passwords

Most ordinary people choose low quality passwords -- obvious names, words, dates, ...

In fact, mostly bad passwords aren't a problem, since most online activities are not important -- there's a lack of motive.

A motivated case: a bad guy breaks into a person's ebay account, and uses their good standing to do auction fraud.

In an increasingly electronic world, this will be more of a problem.

Problem -- password guessing

Bad guy

Knows R from observing the challenge

Knows $\text{hash}(R+\text{password})$ from observing the response

Cannot invert $\text{hash}(R+\text{password})$

Can guess all possible passwords

Guess all possible passwords, and try $\text{hash}(R+\text{guess})$ for each one until a match is found to $\text{password}(R+\text{password})$

Somewhat feasible

Say there are around 50,000 words ($5e4$) in the English language

Combinations of two words = $5e4 * 5e4 = 2.5 e9 = 2.5 \text{ billion combinations}$

A large number, but not infeasible

If each letter may be upper/lower case, could increase the space by, say, a factor of 1000

Put the odds on your side by inserting letters, digits, punctuation randomly for important passwords. Don't use plain words, but slightly messed up words are ok.

Future problem

Password guessing will be a larger problem as computers get faster while the human capacity to remember random strings is fixed (or diminishing in my case!).

Future gadget

Eventually, we will need our ring/watch/pendant to do our authentication for us. This will make logins etc. more convenient -- you walk up to the computer, and it just knows it's you.

Encrypted Connection

Another solution would be to bring up the connection between the client and server so that all the traffic on it is encrypted. Then the bad guy cannot intercept anything, and we could go back to just sending the password. This still suffers from the "man in the middle" attack -- we'll study all these issues in detail later.