ECE 435 – Network Engineering
Lecture 5

Vince Weaver

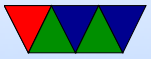
http://web.eece.maine.edu/~vweaver

vincent.weaver@maine.edu

12 September 2017

Announcements

- HW#2 was posted.

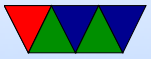


HW#1 Review

- Sockets Code
  - Need to clear out the old message and not print remnants.
  - How to copy a string in c?

    `strcpy(dest,src)` – potential buffer overflow if not terminated

    `strncpy(dest,src,size)` – better, but not always terminated `strlcpy()` – even better, not always available

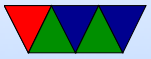


Custom coded: always dangerous:

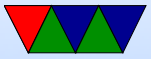
```
i=0; // important
while(src[i]) { dst[i]=src[i]; i++} dst[i]=0;
```

- Don't want to loop and accept over and over.
  What does `accept()` do?
  If you keep `accept()`ing, you get new connection each time This also leaks file descriptors (Though unless $>$ 4096 or more won't notice)

  What you want to do is loop reading from the file descriptor until it closes.



- Don't ignore compiler warnings.
  What if `toupper()` not found?
  manpage. Need to include `ctype.h`
- Poor Specifications
  - I wanted you to enter code on the client, have it echoed back to you by server.
  - When you type "bye" it would exit both sides.
    (bye by itself? cr/lf? byet?
  - Bye from client, not at keyboard, though Fancy code with select to watch for input on server/fd.
  - Idea was client send string, server would uppercase



and send it back, client would then print this.

- For something cool hoped you would send back updated version with ANSI chars, not just print in color on server.

  How do you insert at beginning of string in C?

  strcpy(), strcat()

  sprintf()

  Custom loop.

- Something Cool

  Command Line args argc=number. Always at least 1.

  argv[]. argv[0]=executable name

argv[1]=first argument

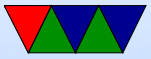
`atoi()/strtod()/strtol()` Why different?

`atoi()` has no way of reporting error, just returns 0.

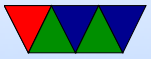
`strtod()` can report errors but is more complex.

- General
  - Error handling: don't just segfault. Even if can't do anything, print message and try to exit gracefully.
- comment your code!
- OSI reference model
  - Bits and voltages – physical layer (1?)

    Not hardware layer



- Routing packets – network layer (3?)

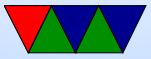


HW#2 Issues

- Typo in handout, says `test.html` but included `index.html`. Rename one or other to match.
- Get the header printing first, then worry about correctness of headers (dates, length))
- Know how to search for a string and point to location after it?
  - Find a string and point to beginning of it.

```
char *pointer;
pointer=strstr(haystack,needle);
```

  - Look for `"GET "`

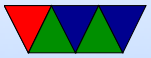


Actually points to beginning of GET. How to skip ahead?

- pointer+=4 is one way. (pointer math, ugh)
- How to get to first space?
- `strtok(pointer," ");`

  Will split the string into chunks, put 0 at end.
- Also can do this manually;

```
pointer2=pointer;
while(*pointer) {
   if (pointer==' ') {
      *pointer=0;
      break;
   }
   pointer++;
```

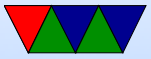


```
}
printf("%s\n",pointer2);
```

- Know how to construct a string on the fly? `strcat()`, `sprintf()`
  `strcpy()` first bit in.
  `strcat()` additional strings.
  If you want formatting you can do things like

```
sprintf(temp_string,"File size=%d\r\n",filesize);
strcat(out_string,temp_string);
```

  Create big enough buffer.
- How to find size of a file?
  Can read it in, and count. Or can use the stat (`man`

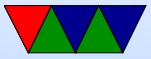


`stat.2`) need .2 (or `man -a`) as there's a command line tool called stat that comes ip first.

- How to read/write file. There are a large number of ways to do this. `open()/read()/write()/close` `fopen()/fread/fwrite/fclose` (careful! Buffered! And maybe need fdopen() to print to file descriptor).

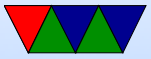
```
fd=open(filename,O_RDONLY);
if (fd<0) fprintf(stderr,"Error opening %s\n",filename);
while(1) {
    result=read(fd,buffer,256);
    if (result<=0) break;
    write(network_fd,buffer,resut);
}
```

Be sure to close afterward.



Questions from Last Time

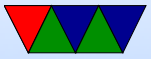
RSA security dongle – two factor authentication, not really any pub/private going on



Cryptographic Hash Functions

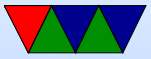
- Maps a document of arbitrary size to a fixed size
- Easy to calculate, hard to reverse. Only real feasible way to reverse is brute-force search
- Should not be able to find two different messages with same hash
- Small changes in document should lead to very different hashes
- Two items with same hash are called a *collision*

  Are collisions useful? If you can map documents of

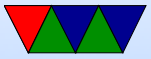


same filetype, or if somehow same document with lots of garbage on end

- Break file up into chunks, do a series of operations to "compress" it, often shift, xor, or, add, and, not
- md5 `md5sum`
  128-bit md5 hashes, create checksum, uniquely ID file
  Well, not really unique. It's been broken, can find (with great difficulty) collisions
- SHA-1
  Developed by NSA
  Used by git

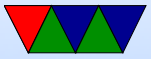


- Uses: passwords (/etc/shadow), (mostly) uniquely iding a file (git), verifying file contents (download, error checking), bitcoin?
- Problem: how do you verify the public key belongs to the person who they say it is? (on website? what if someone intercepts and replaces, mitm style)



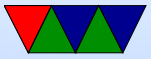
Certificate Authorities

- Certificate authorities
- Signed data block from official organization
- Hashed?
- Can be revoked
- Digital Signature Algorithm



SSL/TLS

- Secure Socket Layer / Transport Layer Security
- Handshake protocol followed by key exchange
- Browser says hello, which hashes/algorithms it supports
- Server picks one and sends back
- Server then sends a certificate (signed by authority) saying who it is, and what its public key is
- Client verifies certificate (via the CA public key it has stored)
- client generates a random number, encrypts with servers



public key, sends to server, used as symmetric key

- What could go wrong, what if someone gets a hold of server private key? could decrypt logged data. Diffie-Hellman key exchange – random number plus unique session key prevents problems if server private key leaked