Lab Puzzle

```
static OSStatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer signedParams,
                                 uint8_t *signature, UInt16 signatureLen)
{
    OSStatus        err;
    SSLBuffer       hashOut, hashCtx, clientRandom, serverRandom;
    uint8_t         hashes[SSL_SHA1_DIGEST_LEN + SSL_MD5_DIGEST_LEN];

                ■■■■

    if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
        goto fail;
        goto fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;

        err = sslRawVerify(ctx,
                           ctx->peerPubKey,
                           dataToSign,                          /* plaintext */
                           dataToSignLen,                  /* plaintext length */
                           signature,
                           signatureLen);
        if(err) {
                sslErrorLog("SSLDecodeSignedServerKeyExchange: sslRawVerify "
                    "returned %d\n", (int)err);
                goto fail;
        }

fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
    return err;

}
```

ECE 220
Honors Lab Section

Lab 5: Pseudo-Hacking

Miscellanea

- No lab March 8th (next week)
- A lab assignment will still be posted

- To run tests for labs
  - make test
  - To run individually
    - ./bin/<exec> test/testx
  - To debug individually
    - gdb ./bin/<exec>
    - b main
    - run tests/testx

- One line code blocks
  - if, for, while

Program Inputs

- int main(int argc, const char *argv[])
  - argc – number of strings pointed to by argv
  - argv – pointer array to command line arguments

- From previous slide
  - ./bin/<exec> test/testx
    - argc = 2
    - argv[0] = “./bin/<exec>”
    - argv[1] = test/testx
    - argv[2] = ¯_(ツ)_/¯

Pseudo-Hacking

- Government files:
  - http://champaigncountyclerk.com/government/sei_search.php
- Input parsing is important!
- _scanf, fgets, gets problems?
  - Overflow allocated buffer
- Certain websites limit string length for input
  - http://www.jeremytunnell.com/posts/swab-password-policies-and-two-factor-authentication-a-comedy-of-errors
- Time estimator: https://www.grc.com/haystack.htm

Buffer Overflow

- What can we do with a buffer overflow?
  - Overwrite a local variable
  - Overwrite parameter of a different stack frame
  - Overwrite a return address
  - Gain sudo access (Do this in ECE419/CS460 Security Lab)

- Demo!
  - (Note to self: upload files now)