I have covid :(most notes from videos + slides

Mon, Feb 6 Memory Allocation

Stack space is limited!

Automatic variable lives on top of the stack

Heap can be accessed outside function it is made in

- There until you free it
- Slightly slower
- Lives in unused byte space

Malloc

- Uninitialized

See examples of functions

Infer - static analyzer

Valgrind - dynamic analyzer, while running

Bit map

- Size determines efficiency
- 1 bit per 4kb chunk
- Bit order: first hole on the list, next suitable
- Best fit: smallest hole that is larger than the desired region
- Worst fit: largest available hole
- Best fit leaves tiny holes

Buddy allocation: when a chunk is freed, check if it can be combined with its buddy to rebuild a larger chunk

Reallocation: outside in

Deallocation: outside out

Sudo apt install clang tools

Wed, Feb 8 Cryptography

Data and key (only known to authorized users)

Encryption: plain text + encryption key = cipher text

Decryption: cipher text + decryption key = plain text

Caesar cipher: shift by certain number of letters, very easy to break

Unbreakable codes

- One-time pad made by Claude Shannon
- Truly random string of bits and XOR with message
- Every possible output is equally probable, unknown without key

Modern encryption

- 1977 data encryption standard
    - Same key to en and decrypt
    - 2^55 keys
- Current algorithms AES uses at least 128 bit keys
    - Harder by 2x every bit

Attacking AES

- Infinity fast computer but it still consumes energy, breaking 128 bit AES would take the power of the US for more than a year
- Can’t be broken with brute force testing
- Broken with math
- Simon algorithm is currently unbreakable
    - Each bit dispersed around other bits

Simon

Public key cryptography

- Diffie-hellman key exchange
- Encrypt with public, decrypt with private
- Keys are inverses of each other
- Pretty slow
- Uses
    - Small amounts of data
    - Establishing shared key for symmetric encryption algorithms like AES

RSA

- Two large primes p and q (secret and temp)
- Attacking it requires factoring n
- phi(n) = (p-1)(q-1)
- Key gen
    - Two large primes
    - N = p times q
    - phi(n)
    - Random e such that gcd(e, phi(n)) = 1
- Private key
    - N and d
- Primality testing
- gcd, euler witness, miller rabin, Mod exp and mod inv
- Fibonacci in GMP
    - Hard to use

Attack modern cryptography by spying on the keys

Fri, Feb 10

Recursion

Function calls require creating a stack frame, takes time and space

Use when it makes sense, can make things more complicated too

Binary search

- Search ordered array in O(logn)
- Split in half, check less or greater
- Repeat

String table

- Allocate node
- Set children to null
- Room for string

- Copy string

Google maps uses depth first search
Recursion is good for search

Bit vectors and sets
Logical shifts left and right
C does not have rotators
Use high order nibble for rotating

- High order nibble in a byte means the most sig 4 bits
- Bit shift right 4 so that nibble takes the place of the low order nibble
- & 0x0F

Rotate right or left in c??