Modern Security Topics

CS 1500 - 003

Who are we?

Founders of the Computer and Network Security Club

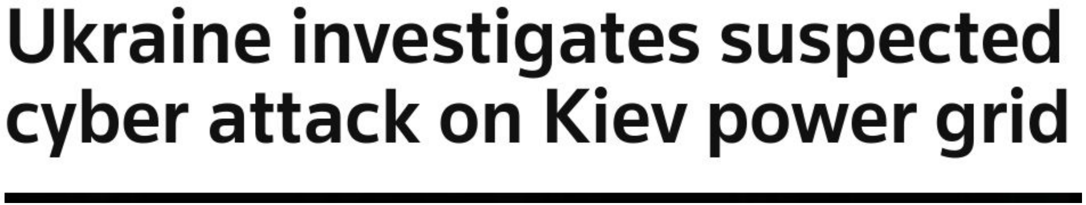
Collin Berman
Cryptographer for Capital One
Background in exploitation

Cyrus Malekpour
Security Engineer for Raytheon
Background in exploitation

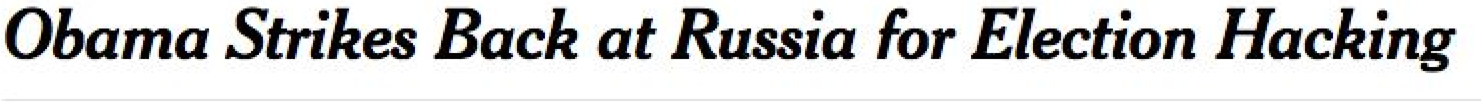
Syllabus Review

What is security?

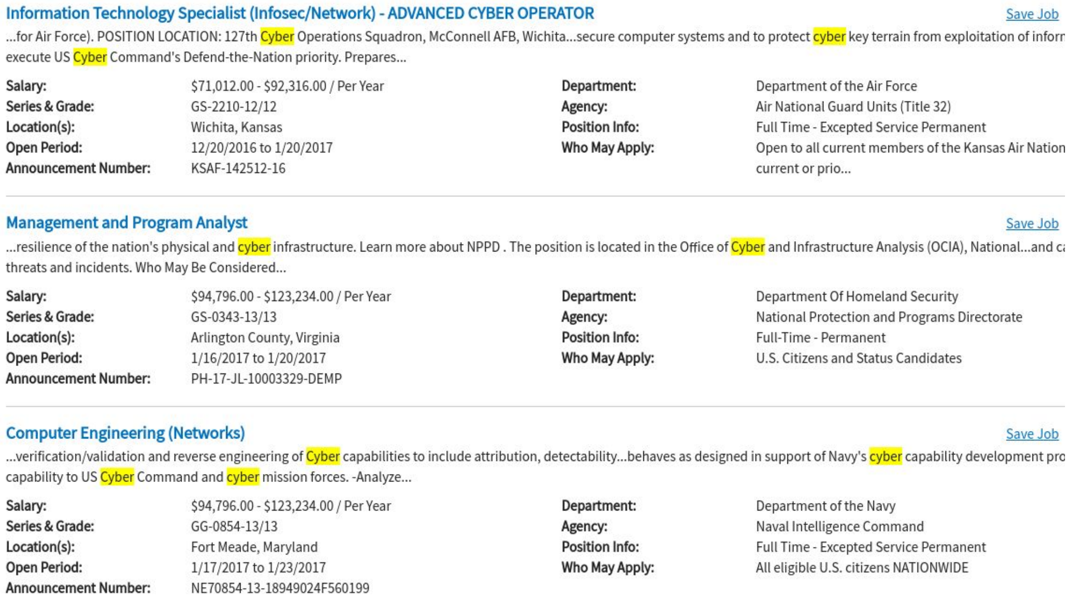
Why it’s important



Ukraine investigates suspected cyber attack on Kiev power grid



Obama Strikes Back at Russia for Election Hacking



Information Technology Specialist (Infosec/Network) - ADVANCED CYBER OPERATOR Save Job

...for Air Force). POSITION LOCATION: 127th Cyber Operations Squadron, McConnell AFB, Wichita...secure computer systems and to protect cyber key terrain from exploitation of inforr execute US Cyber Command's Defend-the-Nation priority. Prepares...

Salary:	$71,012.00 - $92,316.00 / Per Year	**Department:**	Department of the Air Force
Series & Grade:	GS-2210-12/12	**Agency:**	Air National Guard Units (Title 32)
Location(s):	Wichita, Kansas	**Position Info:**	Full Time - Excepted Service Permanent
Open Period:	12/20/2016 to 1/20/2017	**Who May Apply:**	Open to all current members of the Kansas Air Nation current or prio...
Announcement Number:	KSAF-142512-16		

Management and Program Analyst Save Job

...resilience of the nation's physical and cyber infrastructure. Learn more about NPPD . The position is located in the Office of Cyber and Infrastructure Analysis (OCIA), National...and ca threats and incidents. Who May Be Considered...

Salary:	$94,796.00 - $123,234.00 / Per Year	**Department:**	Department Of Homeland Security
Series & Grade:	GS-0343-13/13	**Agency:**	National Protection and Programs Directorate
Location(s):	Arlington County, Virginia	**Position Info:**	Full-Time - Permanent
Open Period:	1/16/2017 to 1/20/2017	**Who May Apply:**	U.S. Citizens and Status Candidates
Announcement Number:	PH-17-JL-10003329-DEMP		

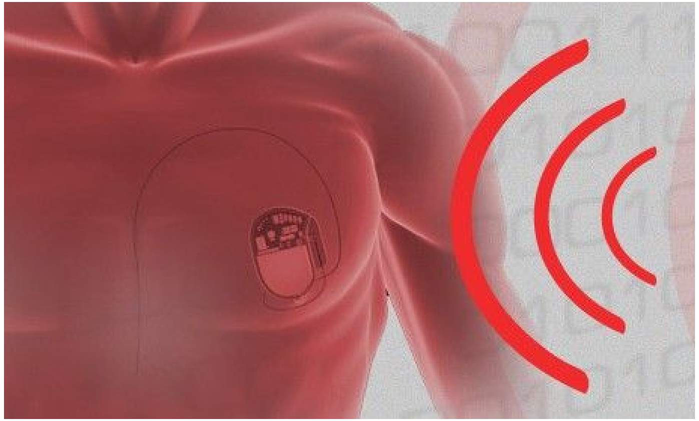
Computer Engineering (Networks) Save Job

...verification/validation and reverse engineering of Cyber capabilities to include attribution, detectability...behaves as designed in support of Navy's cyber capability development pro capability to US Cyber Command and cyber mission forces. -Analyze...

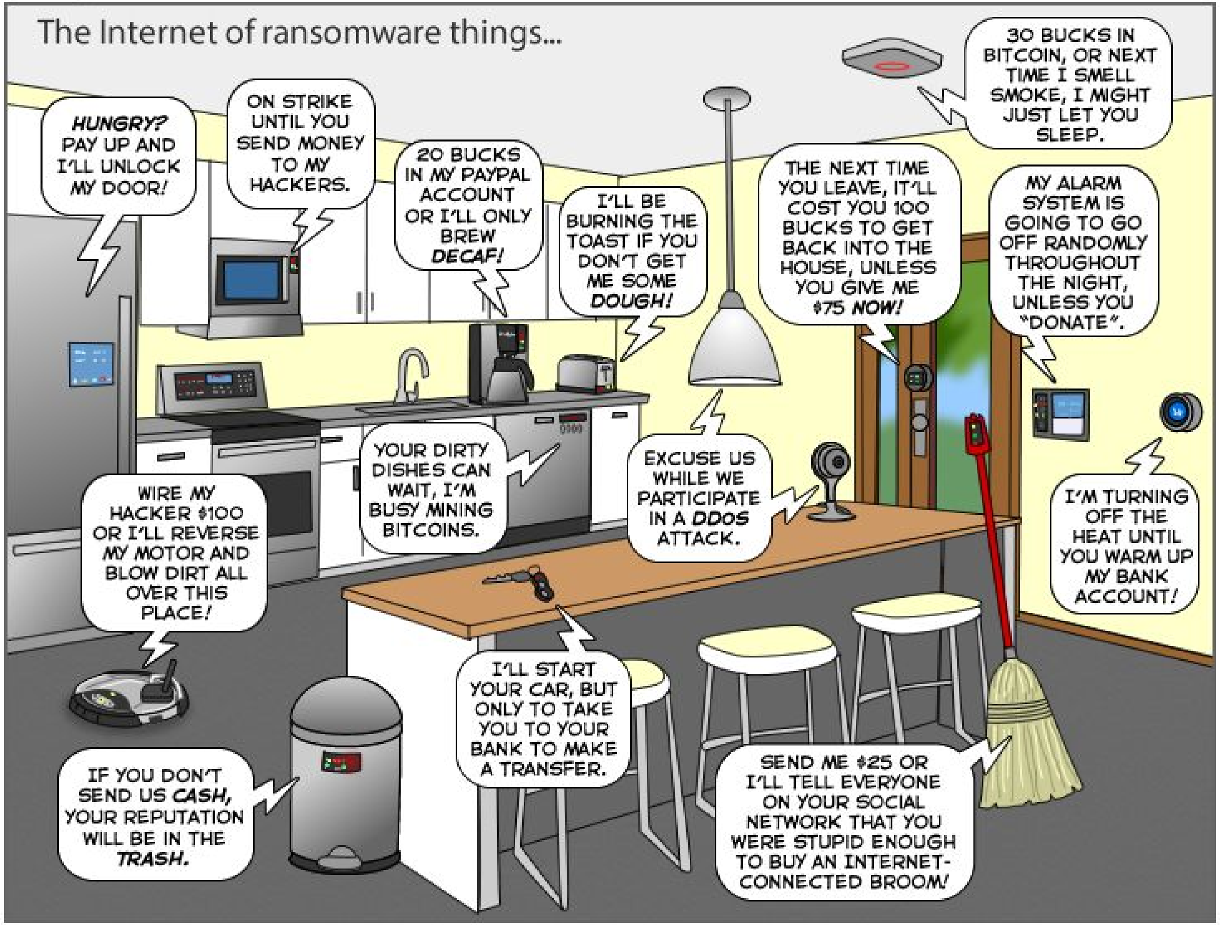
Salary:	$94,796.00 - $123,234.00 / Per Year	**Department:**	Department of the Navy
Series & Grade:	GG-0854-13/13	**Agency:**	Naval Intelligence Command
Location(s):	Fort Meade, Maryland	**Position Info:**	Full Time - Excepted Service Permanent
Open Period:	1/17/2017 to 1/23/2017	**Who May Apply:**	All eligible U.S. citizens NATIONWIDE
Announcement Number:	NE70854-13-18949024F560199		

Internet of Things

Internet of Things



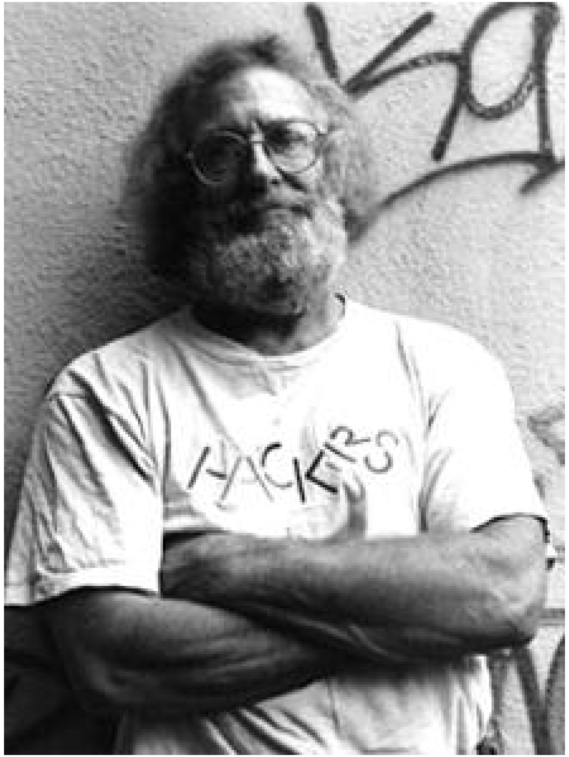
The Joy of Tech™ by Nitrozac & Snaggy


The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDoS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!

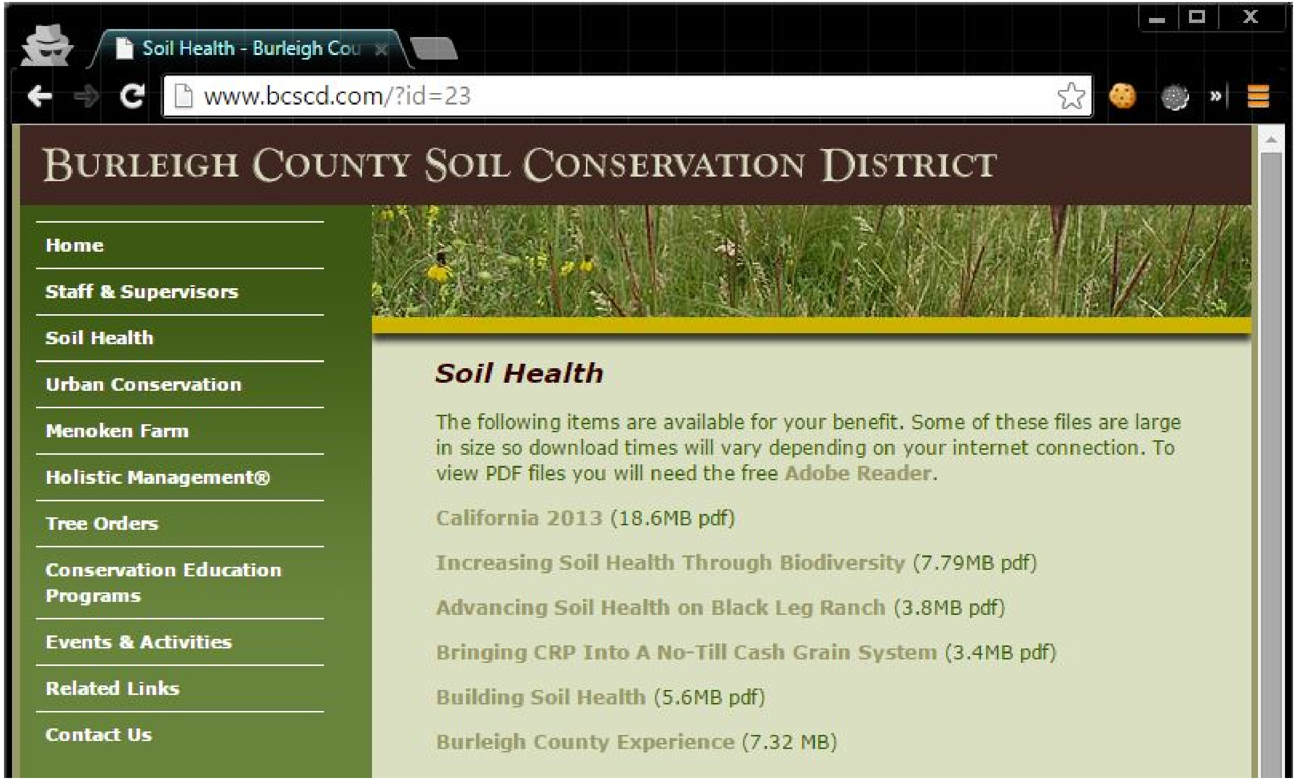
You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech

joyoftech.com

Injection



Injection



BURLEIGH COUNTY SOIL CONSERVATION DISTRICT

Soil Health

The following items are available for your benefit. Some of these files are large in size so download times will vary depending on your internet connection. To view PDF files you will need the free Adobe Reader.

California 2013 (18.6MB pdf)

Increasing Soil Health Through Biodiversity (7.79MB pdf)

Advancing Soil Health on Black Leg Ranch (3.8MB pdf)

Bringing CRP Into A No-Till Cash Grain System (3.4MB pdf)

Building Soil Health (5.6MB pdf)

Burleigh County Experience (7.32 MB)

```
select title, text from pages where id=$id
```

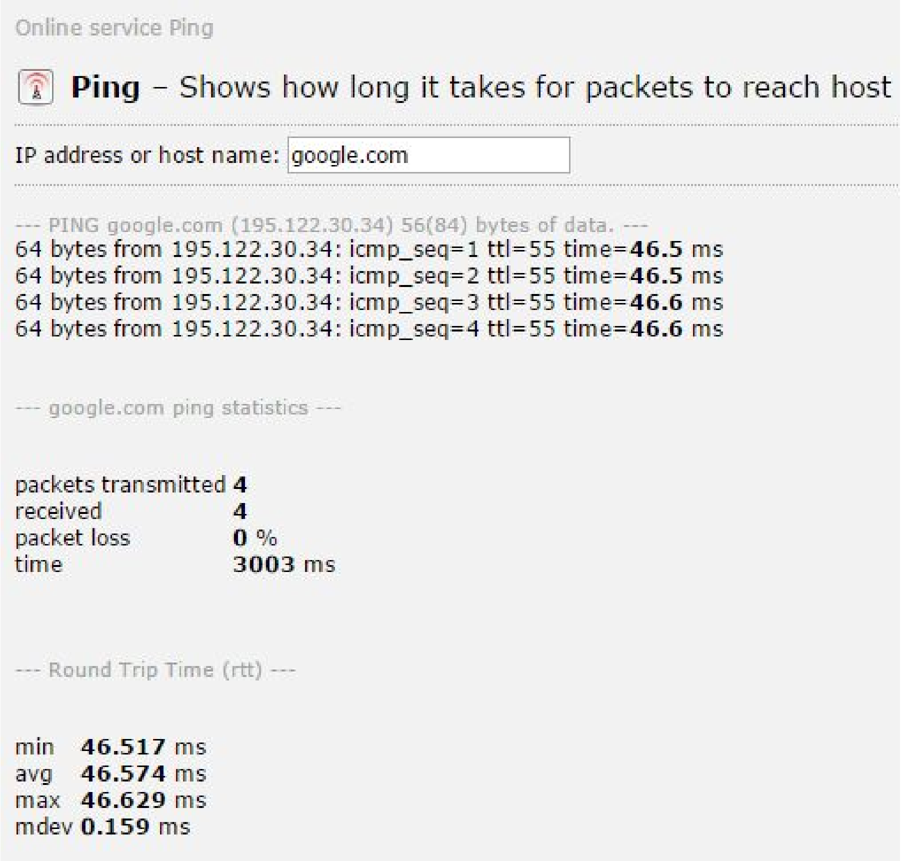
Injection

```
select title, text from pages where id=23
```

```
select title, text from pages where id=23 or 1=1
```

```
select title, text from pages where id=23; drop table news
```

Injection



Online service Ping

Ping – Shows how long it takes for packets to reach host

IP address or host name: google.com

```
--- PING google.com (195.122.30.34) 56(84) bytes of data. ---
64 bytes from 195.122.30.34: icmp_seq=1 ttl=55 time=46.5 ms
64 bytes from 195.122.30.34: icmp_seq=2 ttl=55 time=46.5 ms
64 bytes from 195.122.30.34: icmp_seq=3 ttl=55 time=46.6 ms
64 bytes from 195.122.30.34: icmp_seq=4 ttl=55 time=46.6 ms


--- google.com ping statistics ---


packets transmitted 4
received            4
packet loss         0 %
time                3003 ms


--- Round Trip Time (rtt) ---


min   46.517 ms
avg   46.574 ms
max   46.629 ms
mdev 0.159 ms
```

```
ping -c 4 $host
```

Injection

```
ping -c 4 google.com
```

```
ping -c 4 google.com -W 0 -i 0 -c 999999999
```

```
ping -c 4 google.com; cat /etc/passwd
```

```
ping -c 4 google.com; rm -rf /
```

Course Slack

- https://uva-compsci.slack.com
- #modern-security-s17

How do I pass this course?

- No more than 2 unexcused absences
- Complete at least 8 out of 12 homework assignments
- Linux environment will be needed for several assignments

Review of C concepts

C and Pointers

```c
int main() {
    int x = 5;
    int *y = &x;
    int **z = &y;

    printf("%d\n", **z);
    printf("%d\n", **&*z);
    first(x); printf("%d\n", x);
    second(y); printf("%d\n", x);
    return 0;
}
```

```c
void first(int x) {
    x = 3;
}

void second(int *x) {
    *x = 3;
}
```

C and Buffers

- What's wrong with this code?
- How can we take advantage of it?
- How can we fix it?

```c
int main() {
  char name[256];
  printf("Enter your name: ");
  gets(name);
  printf("Hello %s", name);
  return 0;
}
```

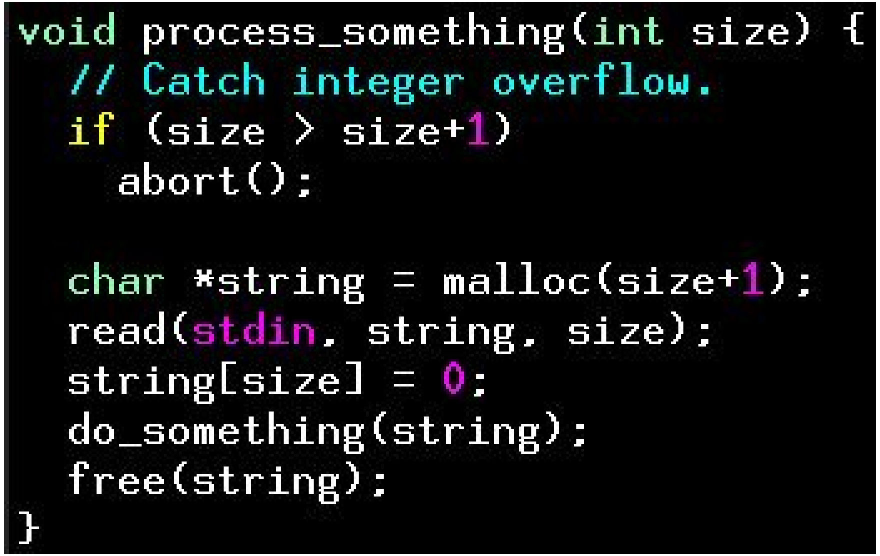
C and Memory

- Where are local variables and function arguments stored in memory?
- Where are dynamic buffers stored in memory?
- How do we create a dynamic buffer?

```
void do_things(int which) {
    void (*call_me)();
    switch(which) {
        case 1:
            call_me = foo;
            break;
        case 2:
            call_me = bar;
            break;
    }
    call_me();
}
```

Undefined Behavior

- What if `size` is `INT_MAX`?



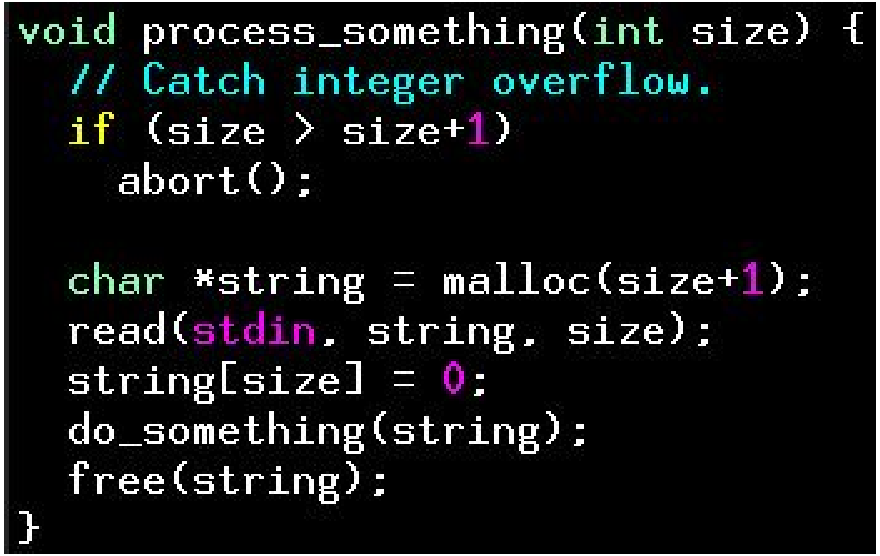
```
void process_something(int size) {
  // Catch integer overflow.
  if (size > size+1)
    abort();

  char *string = malloc(size+1);
  read(stdin, string, size);
  string[size] = 0;
  do_something(string);
  free(string);
}
```

Undefined Behavior

- What if `size` is `INT_MAX`?

  -
    ```
     0111 1111 1111 1111
    +                   1
    ---------------------
     1000 0000 0000 0000
    ```



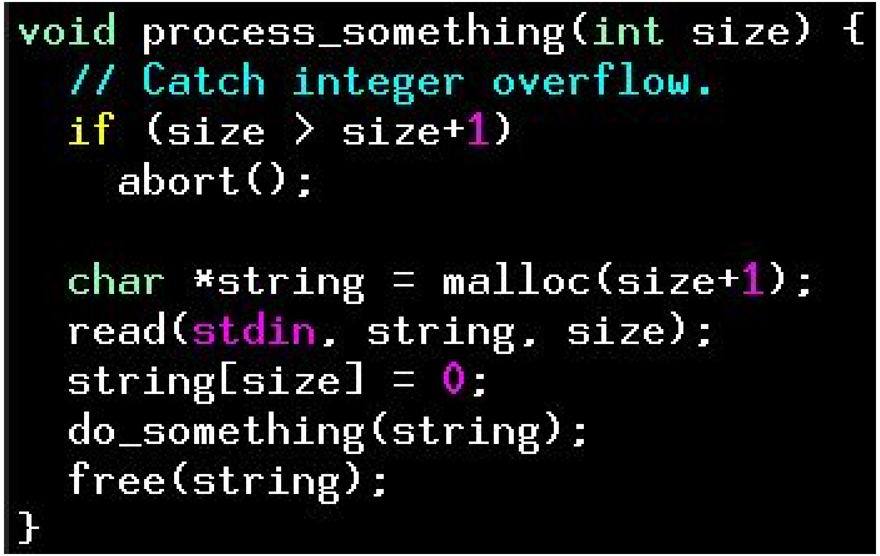
```
void process_something(int size) {
  // Catch integer overflow.
  if (size > size+1)
    abort();

  char *string = malloc(size+1);
  read(stdin, string, size);
  string[size] = 0;
  do_something(string);
  free(string);
}
```

Undefined Behavior

- What if `size` is `INT_MAX`?

  -
    ```
     0111 1111 1111 1111
    +                  1
    --------------------
     1000 0000 0000 0000
    ```
- `size > size+1` is optimized to “false”



```
void process_something(int size) {
  // Catch integer overflow.
  if (size > size+1)
    abort();

  char *string = malloc(size+1);
  read(stdin, string, size);
  string[size] = 0;
  do_something(string);
  free(string);
}
```