



Modern Security Topics

CS 1500 - 003

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 inform execute US **Cyber** Command's Defend-the-Nation priority. Prepares...

Salary: \$71,012.00 - \$92,316.00 / Per Year
Series & Grade: GS-2210-12/12
Location(s): Wichita, Kansas
Open Period: 12/20/2016 to 1/20/2017
Announcement Number: KSAF-142512-16

Department: Department of the Air Force
Agency: Air National Guard Units (Title 32)
Position Info: Full Time - Excepted Service Permanent
Who May Apply: Open to all current members of the Kansas Air Nation current or prio...

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 c: threats and incidents. Who May Be Considered...

Salary: \$94,796.00 - \$123,234.00 / Per Year
Series & Grade: GS-0343-13/13
Location(s): Arlington County, Virginia
Open Period: 1/16/2017 to 1/20/2017
Announcement Number: PH-17-JL-10003329-DEMP

Department: Department Of Homeland Security
Agency: National Protection and Programs Directorate
Position Info: Full-Time - Permanent
Who May Apply: U.S. Citizens and Status Candidates

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...

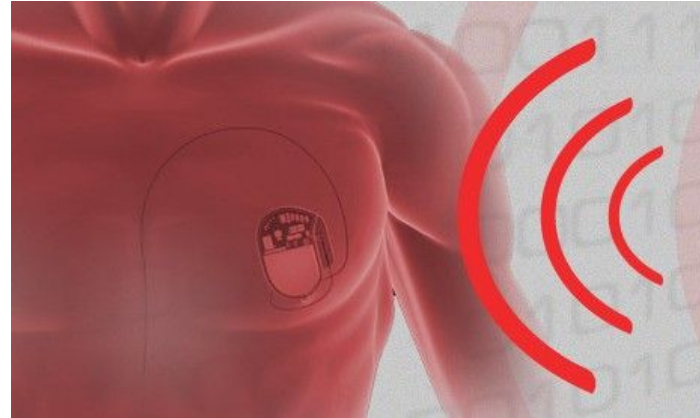
Salary: \$94,796.00 - \$123,234.00 / Per Year
Series & Grade: GG-0854-13/13
Location(s): Fort Meade, Maryland
Open Period: 1/17/2017 to 1/23/2017
Announcement Number: NE70854-13-18949024F560199

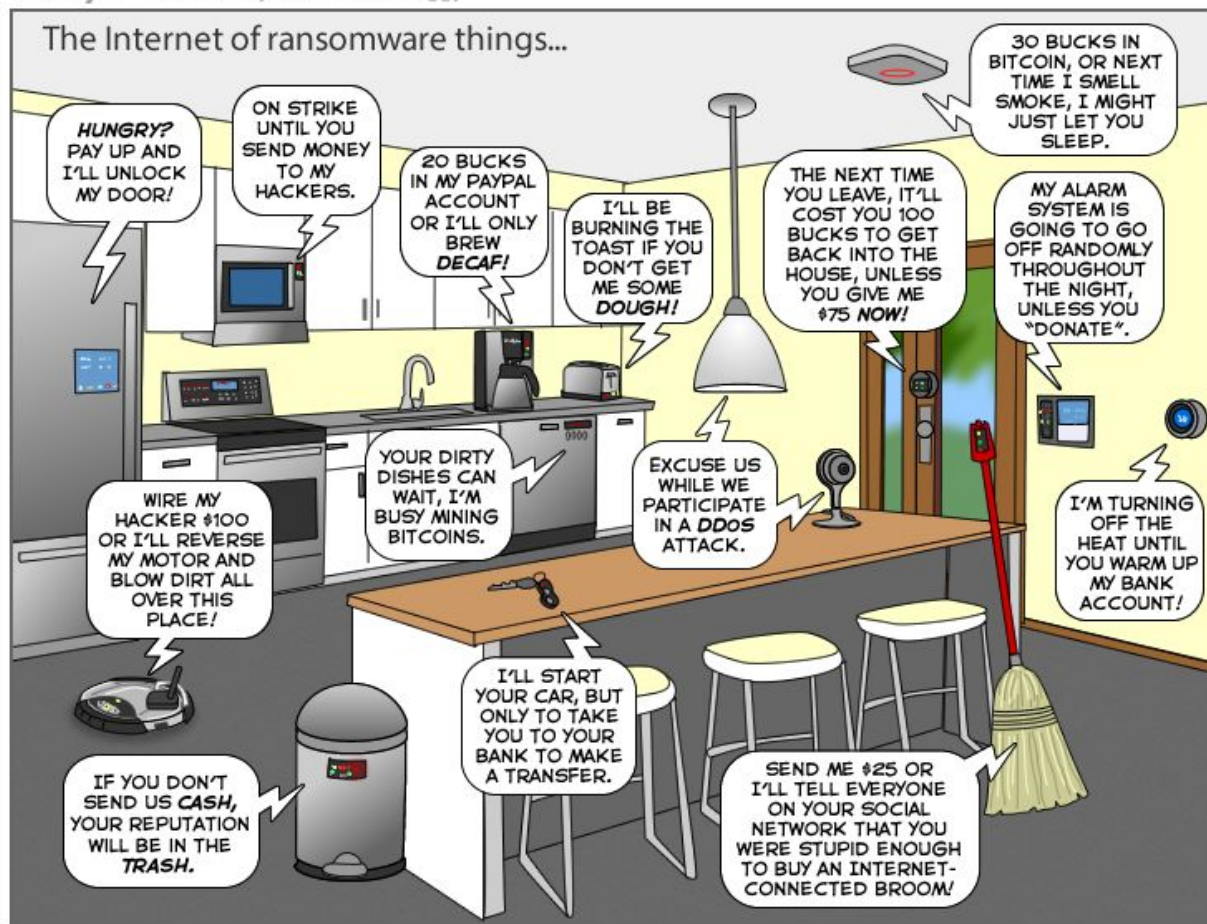
Department: Department of the Navy
Agency: Naval Intelligence Command
Position Info: Full Time - Excepted Service Permanent
Who May Apply: All eligible U.S. citizens NATIONWIDE

Internet of Things



Internet of Things





Injection



Injection



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:

```
--- 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

```
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;  
}
```

```
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?

```
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?

$$\begin{array}{r} 0111\ 1111\ 1111\ 1111 \\ + \hspace{15em} 1 \\ \hline 1000\ 0000\ 0000\ 0000 \end{array}$$

```
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?

$$\begin{array}{r} 0111\ 1111\ 1111\ 1111 \\ + \hspace{15em} 1 \\ \hline 1000\ 0000\ 0000\ 0000 \end{array}$$

- `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);  
}
```