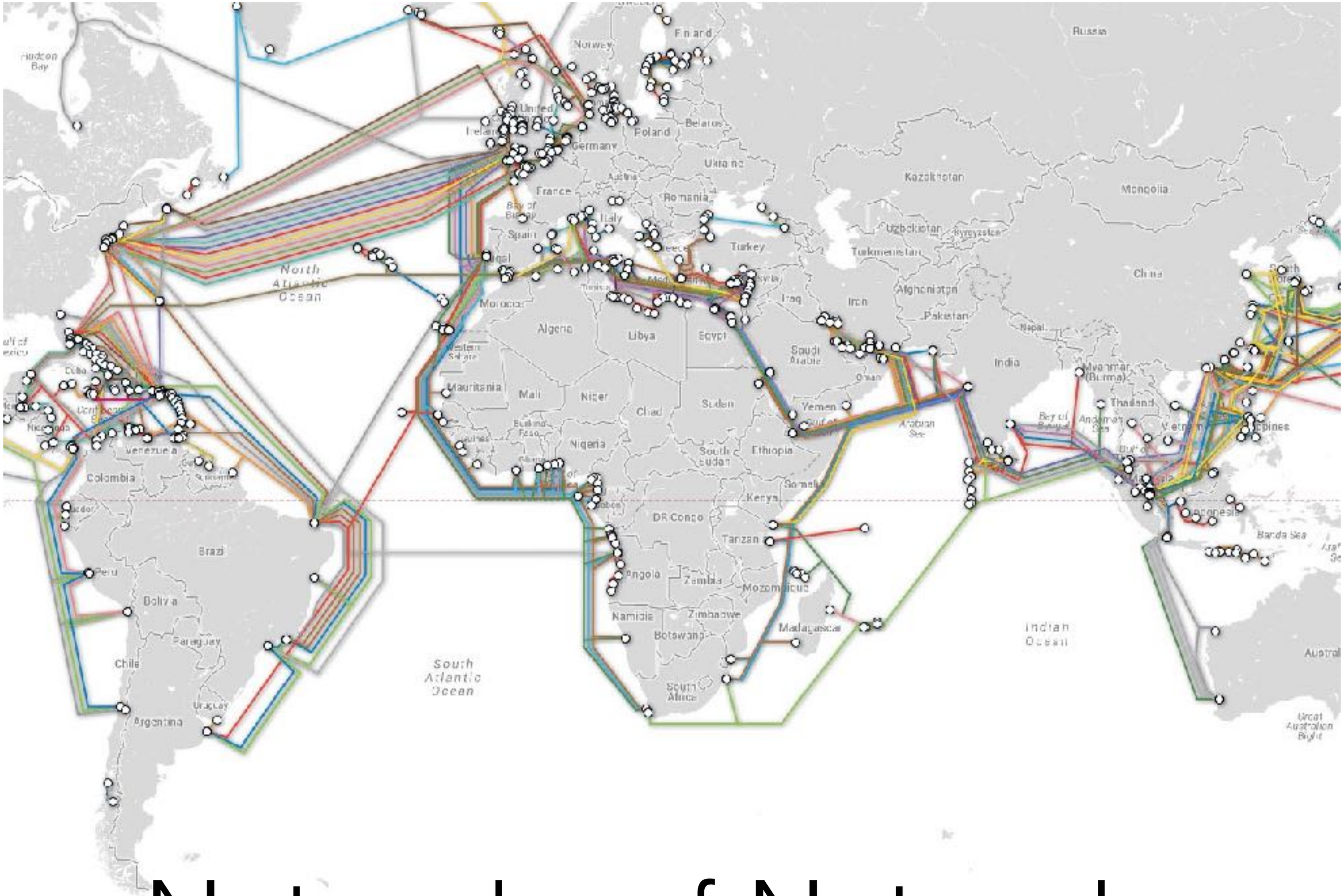
Offensive and Defensive Security

WHITE

HAT

Agenda

- The Internet
- What is Ethical Hacking
- Red Team vs. Blue Team
- Role in todays world
- Balance of both approaches
- Bug Bounties and the future of Ethical Hacking
- Defending the Network, Data and the Internet



Networks of Networks

Internet Service Providers

- Tier 1, Tier 2 and Tier 3
- Peering Agreements
- Large cables laid on the sea floor
- India has only one Tier 1 network. Tata Communications

Ethical Hacking

- Fancy word

- Offensive security is more precise

Thinking like a thief

But why?

- Extremely helpful
- Helps in finding issues before they happen
- Ensures proper programming practices are followed
- Pen Test
- Security Assessment
- Code Review. Etc…

Validation

Penetration Testing

- Black box testing
- You are trying to learn in the same way an attacker would
- Kali Linux is a popular choice
- Use tools to test for corner cases of a software/hardware
- If you find a flaw. **Report it!**
- **Reporting or not reporting is what makes it legal or illegal**

Red Team vs Blue Team

- My favorite approach
- The Red Team tries to break in
- The Blue Team patches the problem before the Red Team can break in
- Results in most issues being fixed very soon

Fix the average case

Given enough resources. Anything is breakable

Know what you are defending against

Vulnerabilities

In computer security, a vulnerability is a weakness which allows an attacker to reduce a system's information assurance.

Vulnerability is the intersection of three elements:

a system susceptibility or flaw,
attacker access to the flaw, and
attacker capability to exploit the flaw

Lets talk Vulnerabilities

- Problems in software
- Introduced by Developers who don't keep security in mind
- Mostly introduced by not considering how a user might use the program

Buffer Overflows

```
main() {
    char buf[6];

    gets(buf);

    printf("You typed: %s", buf);
}
```

What happens when you give large input?

0x00000000

vuln.c -> a.out

Bash Shell

Program B

Program A

0xFFFFFFFF

Temp Variables

Local Variable 3

Local Variable 2

Local Variable 1

Return Address

EBP

Function Arguments

0x00000000

vuln.c -> a.out

Bash Shell

Program B

Program A

0xFFFFFFFF

Local Variable 3

Local Variable 2

Return Address

EBP

Function Arguments

Problems

- Value of Variable 2 can change the value of variable 1

- If there is any condition that checks variable 2. That can be bypassed via value of Variable 1

- You are forcing the program to take inputs that were not intended

```
#include <stdio.h>
#include <string.h>

main() {
  char buf[10]; # Some buffer
  int pass = 0; # Flag for password check

  printf("\nEnter a password: ");
  gets(buf); # get a password from user

   # Check if password is correct
  if(strcmp(buf,"jaincollege")) {
    printf("\nWrong Password\n");
  }
  else {
    printf("\nCorrect Password");
    pass = 1; # Set flag if password is correct
  }

  if(pass) {
     # Grant extra access if password flag is set
    printf("\n**You have been granted special access**\n");
  }
}
```

0x00000000

vuln.c -> a.out

Bash Shell

Program B

Program A

0xFFFFFFFF

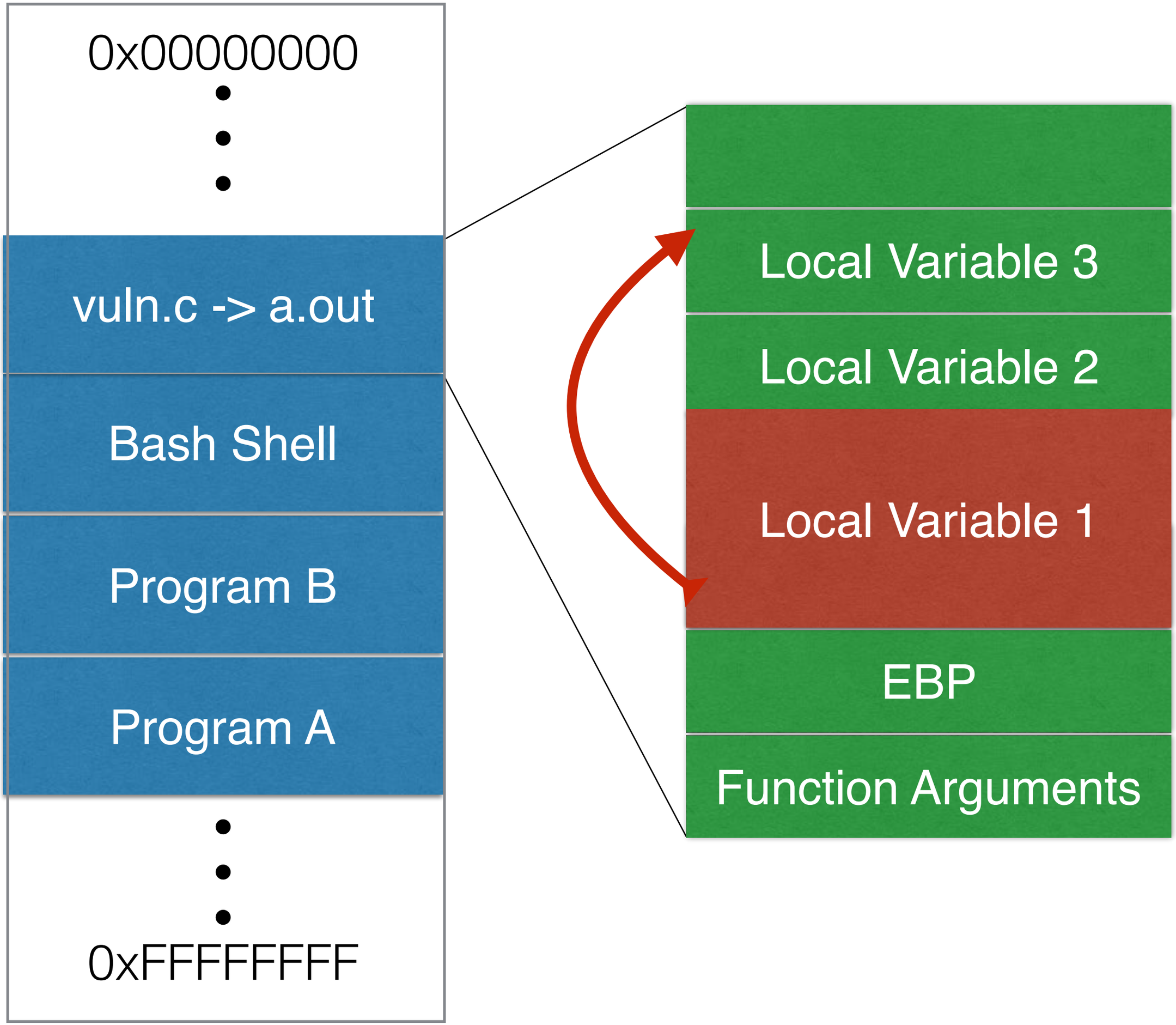
Local Variable 3

Local Variable 2

Local Variable 1

EBP

Function Arguments


0x00000000
vuln.c -> a.out
Bash Shell
Program B
Program A
0xFFFFFFFF
Local Variable 3
Local Variable 2
Local Variable 1
EBP
Function Arguments

Zero Days

- Problems unknown to software maker
- Can be used to compromise anyone who uses the software
- Remote exploits that entirely defeat the security of an Android or Windows Phone device go for as much as $100,000 (65 Lakh Rs)
- Very very very difficult to find

Bug Bounties

- Companies welcome white hat hackers
- Facebook, Google, etc..
- Find flaws in their product
- Report it
- They pay you
- Sometimes a LOT