ELEC 377 – Operating Systems

Week 10 – Class 2

Last Class

- Finished Distributed Systems

Security

- Security
  - ◊ impossible in practice
  - ◊ accidental violations (easy to protect)
  - ◊ malicious (harder)
    - – Reading of data (info theft)
    - – Modification of data
    - – Destruction of data
    - – Denial of service
  - ◊ Cost tradeoffs

Security Levels

- Physical
  - ◊ bios on PC
- Human
  - ◊ social engineering
- Network
  - ◊ packet interception, denial of service
- OS
  - ◊ only level OS has control over

- first two are outside of OS control but necessary
- hardware protection for OS
- harder to add security than design for it

System Threats

- Denial of Service
  - ◊ Disable the service
  - ◊ password timeouts
  - ◊ network based

    - smurf attack

    - zombie attack (combined with worms)

    - oversize ICMP packet

    - Xmas Tree Packets
- Key Loggers

  ◊ software (permission to install?)

  ◊ hardware (physical security)

Human Security

- Social Engineering (manipulating people)
  - ◊ Kevin Mitnick
  - ◊ Password reset on banking/credit card
- Can be more elaborate (Patch update attack)...
- phishing
  - ◊ fake email from bank/PayPal/Microsoft
  - ◊ Nigerian 411/Lotto win
  - ◊ Harvard/UC Berkely Study

    23% did not look at addr/status bar, sec indicators

    68% ignored certificate warnings

    90% were fooled by good phishing websites

    no correlation with age, sex, previous exp, comp experience

Human Security

- Baiting
  - ◊ Free Screen Savers

- Quid pro quo
  - ◊ Calling back from Tech Support

- Fake Services
  - ◊ physical mail victim
  - ◊ “new” telephone banking number (1800...)
  - ◊ play back recorded prompts, record acct/pin numbers

Buffer Overflow

- Check the size of the buffer on the stack?

  ◊ offset is unsigned

```
while (offset > (unsigned)charsRd) {
  char buffer[1024];
  int charsSkpd;
  charsSkpd = offset - charsRd;
  if (charsSkpd > 1024)
     cbSkip = 1024;
  if (!Read(buffer, charsSkpd))
                           break;
    charsRd += charsSkpd;
}
```

Buffer Overflow

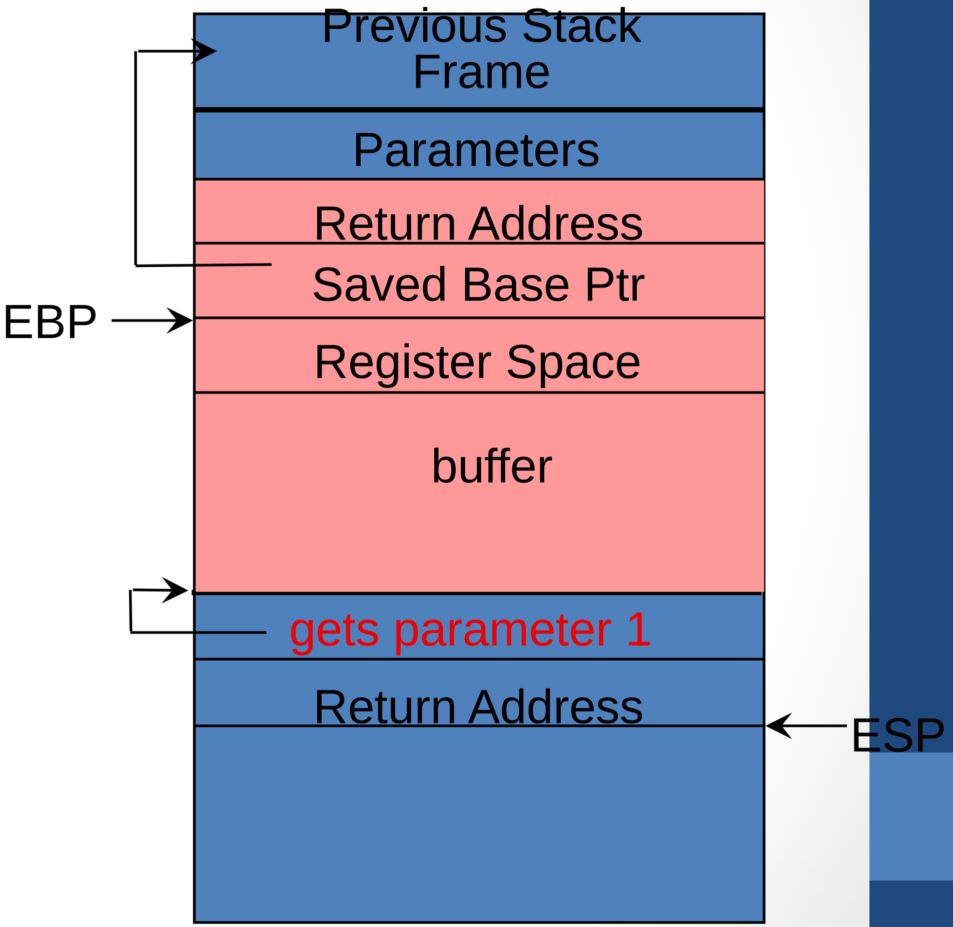
- Check the size of the buffer on the stack?
  - ◊ subtraction is unsigned
  - ◊ if stmt comparison is signed
  - ◊ offset > 2^31, then failure
  - ◊ file needs only be a bit longer than 1024 chars!!
    - – small file
  - ◊ should have used seek!!
    - – seek changes the file read position

Stack Overflow Attack

```
char * GetLine(){
   char buffer[130];
   gets(buffer);
   checkChars(buffer); // only A-Z0-9
}
```

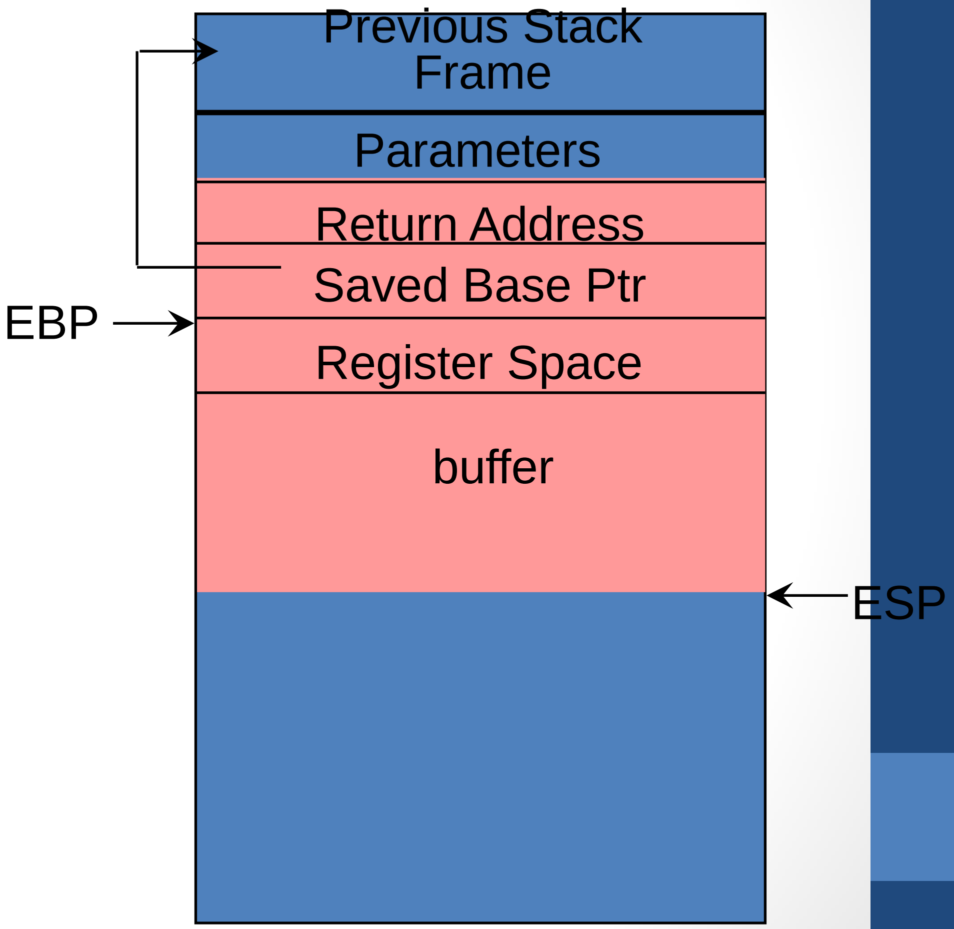
Stack Overflow Attack

```
getLine:
   push  ebp
   mov   ebp,esp
   sub   esp,152
   lea   eax,-152(ebp)
   pushl eax
   call  gets
   add   esp,4
   lea   eax,-152(ebp)
   pushl eax
   call  checkChars
   add   esp,4
     leave
   ret
```



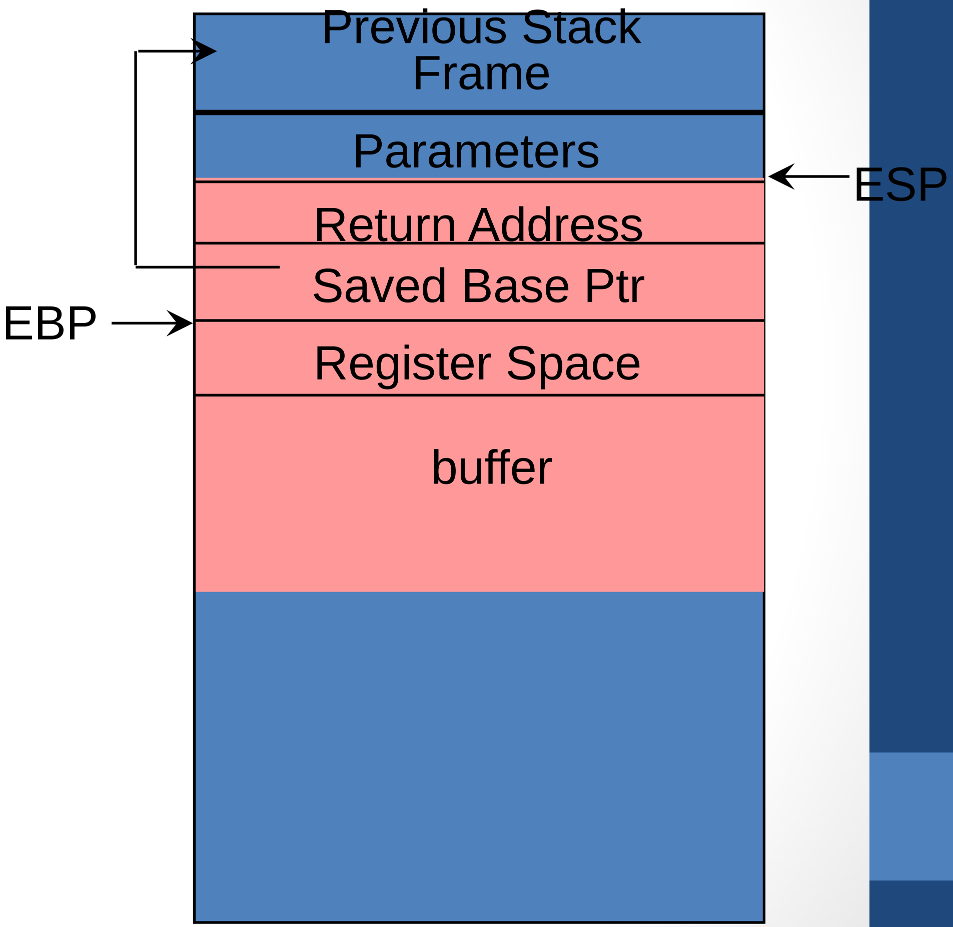
Stack Overflow Attack

```
getLine:
   push  ebp
   mov   ebp,esp
   sub   esp,152
   lea   eax,-152(ebp)
   pushl eax
   call  gets
   add   esp,4
   lea   eax,-152(ebp)
   pushl eax
   call  checkChars
   add   esp,4
     leave
   ret
```



Stack Overflow Attack

```
getLine:
   push  ebp
   mov   ebp,esp
   sub   esp,152
   lea   eax,-152(ebp)
   pushl eax
   call  gets
   add   esp,4
   lea   eax,-152(ebp)
   pushl eax
   call  checkChars
   add   esp,4
     leave
   ret
```



Previous Stack Frame

Parameters

Return Address

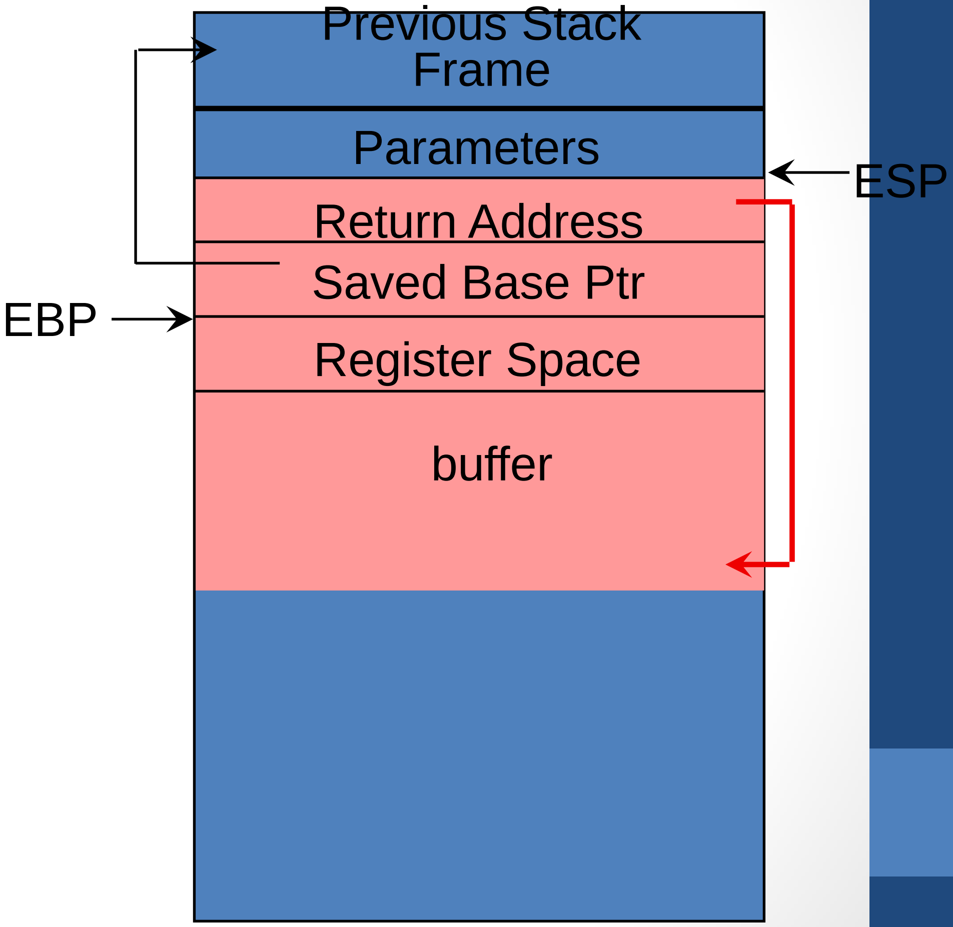
Saved Base Ptr

Register Space

buffer

Stack Overflow Attack

```
getLine:
   push  ebp
   mov   ebp,esp
   sub   esp,152
   lea   eax,-152(ebp)
   pushl eax
   call  gets
   add   esp,4
   lea   eax,-152(ebp)
   pushl eax
   call  checkChars
   add   esp,4
     leave
   ret
```

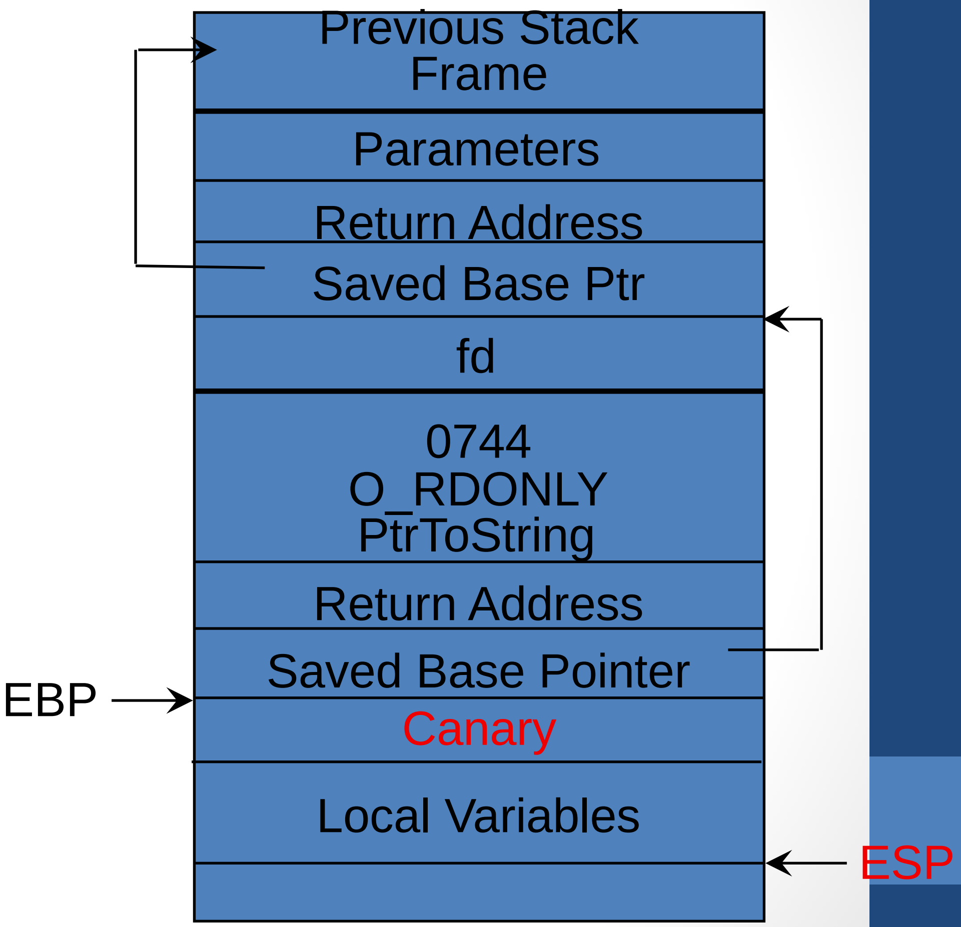


Canary Value

- Protection against Stack Overflow
  - ◊ Random value put on stack before local variables
  - ◊ check before return
  - ◊ If not the same, then has been modified by a stack overflow attack!!
- Compiler generated protection
  - ◊ OS provides random value.
  - ◊ read into global value during process startup.

Canary Values

```
push ebp
mov ebp,esp
push Canary
add esp,NumLocals
```

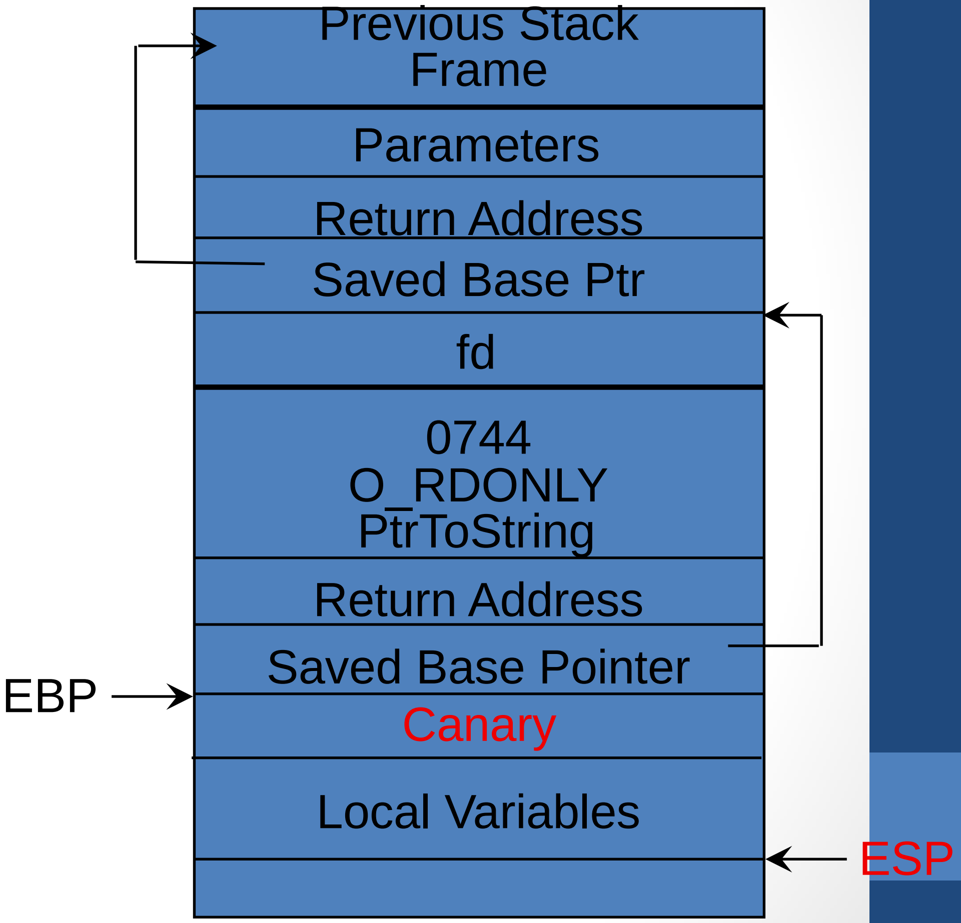


```
testl Canary,(ebp)
jne _stackErr_
leave
ret
```

Canary Values

```
push ebp
mov ebp,esp
push Canary
add esp,NumLocals
```

```
testl Canary,(ebp)
jne _stackErr_
leave
ret
```



Buffer Overflow

- Other Variants:

  ◊ Overflow to a local function pointer

  – protection: rearrange stack frame

  – put buffers above function pointers

  – can’t rearrange structures

```
struct xyzzy {
        void (*f)(int, int);
    char buffer[1024];
};
```

Network Security

- Eavesdropping

  ◊ WAR driving

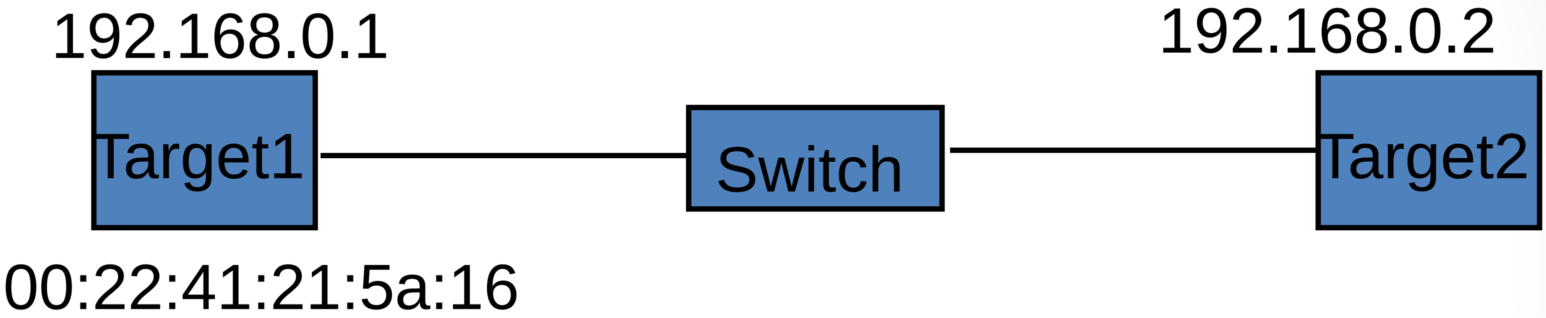
  ◊ WEP Vulnerability

  ◊ Switches only route to specific ethernet addresses

  - ARP poisoning

Network Security

- ARP Poisoning



192.168.0.1

Target1

Switch

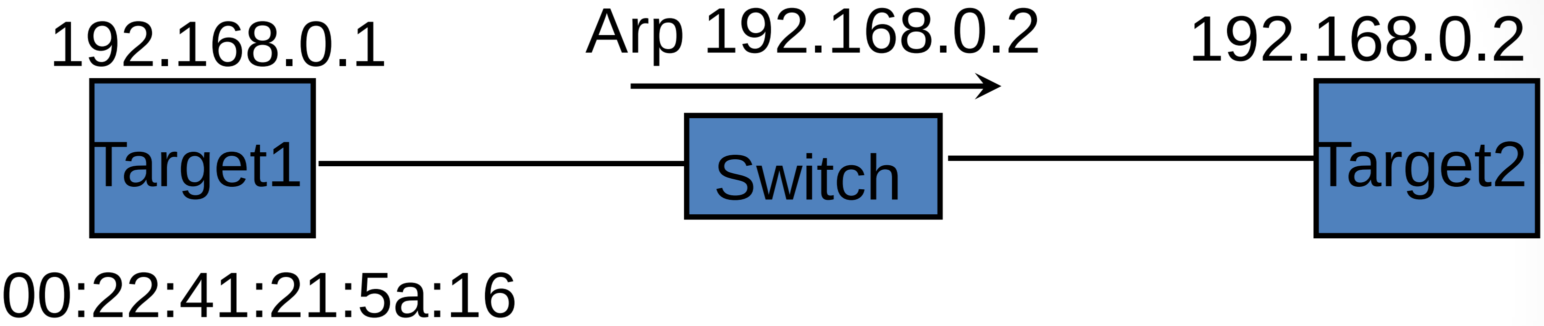
192.168.0.2

Target2

00:22:41:21:5a:16

Network Security

- ARP Poisoning



192.168.0.1

Arp 192.168.0.2

192.168.0.2

Target1

Switch

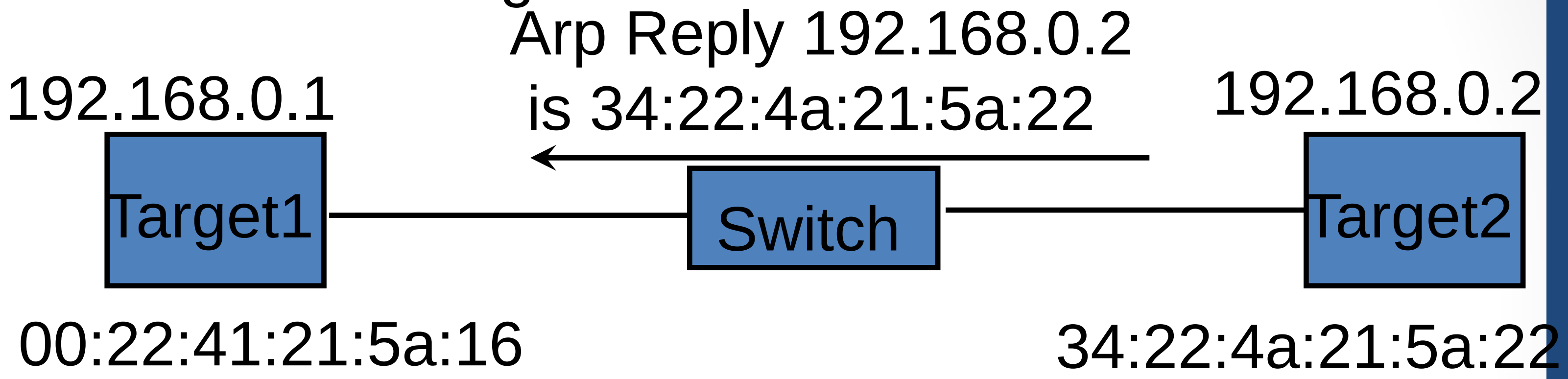
Target2

00:22:41:21:5a:16

Note: Arp is a broadcast packet

Network Security

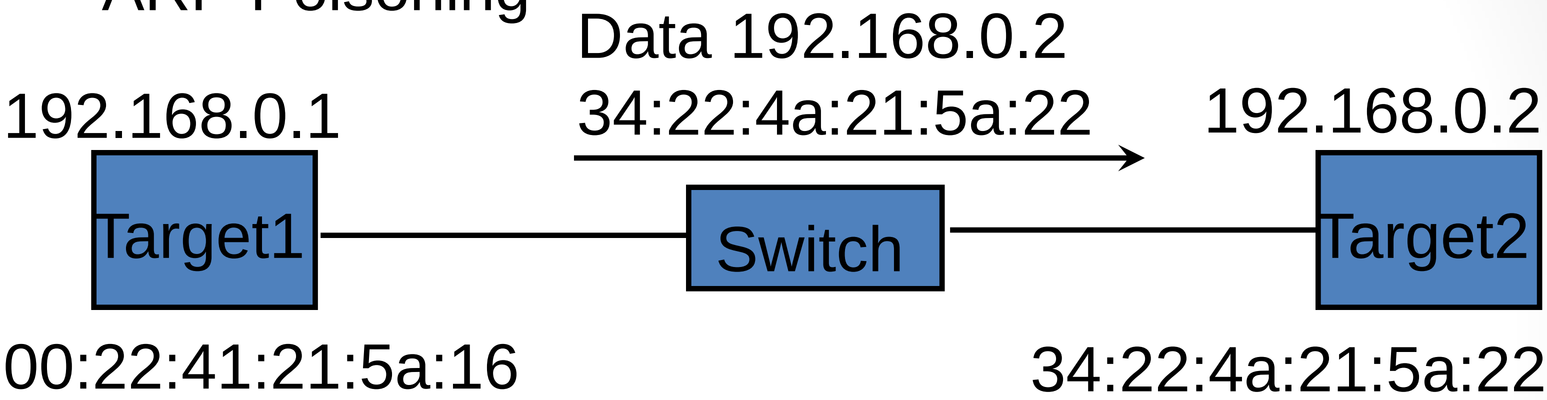
- ARP Poisoning



Arp Reply 192.168.0.2 is 34:22:4a:21:5a:22

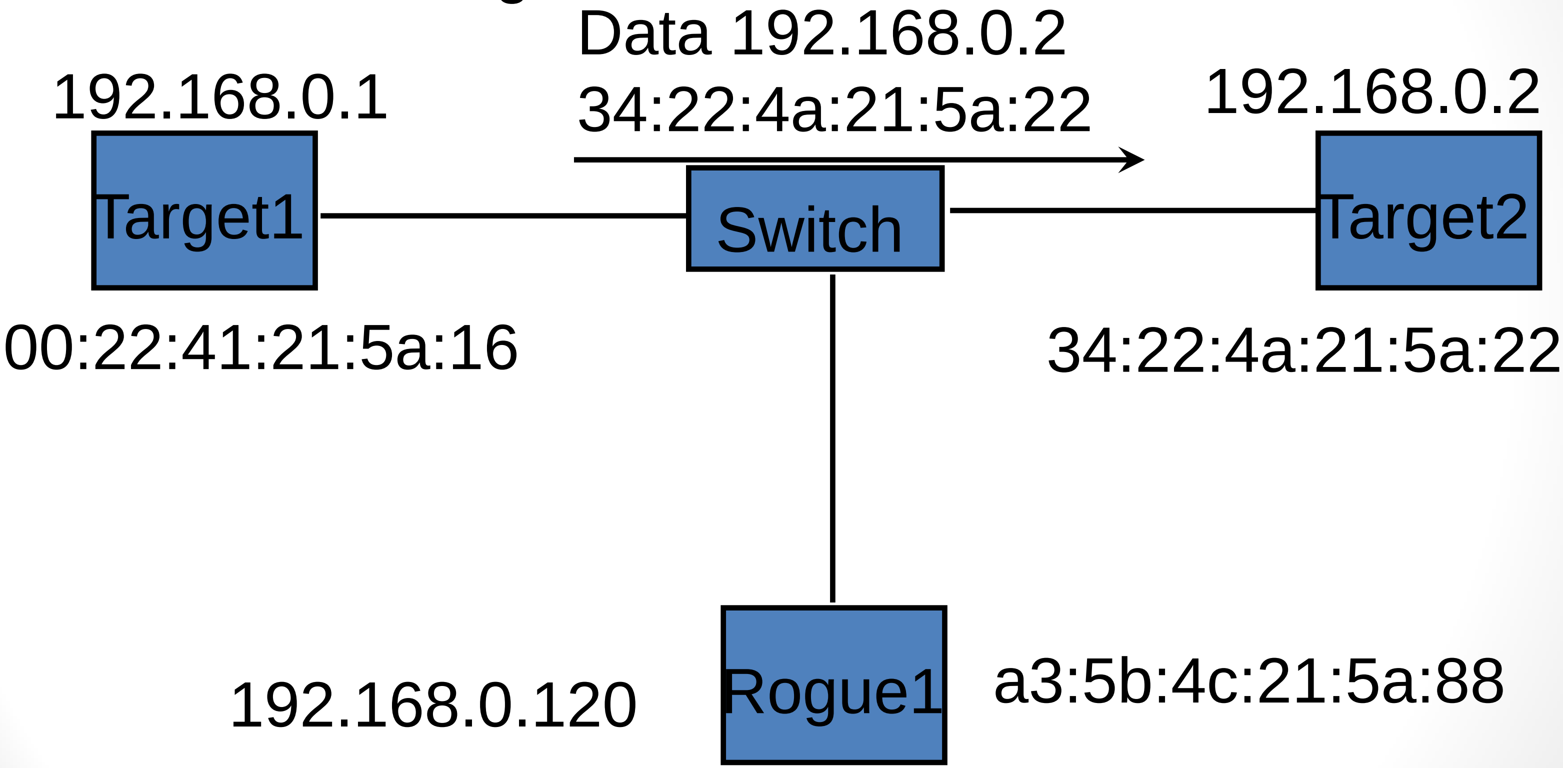
Network Security

- ARP Poisoning



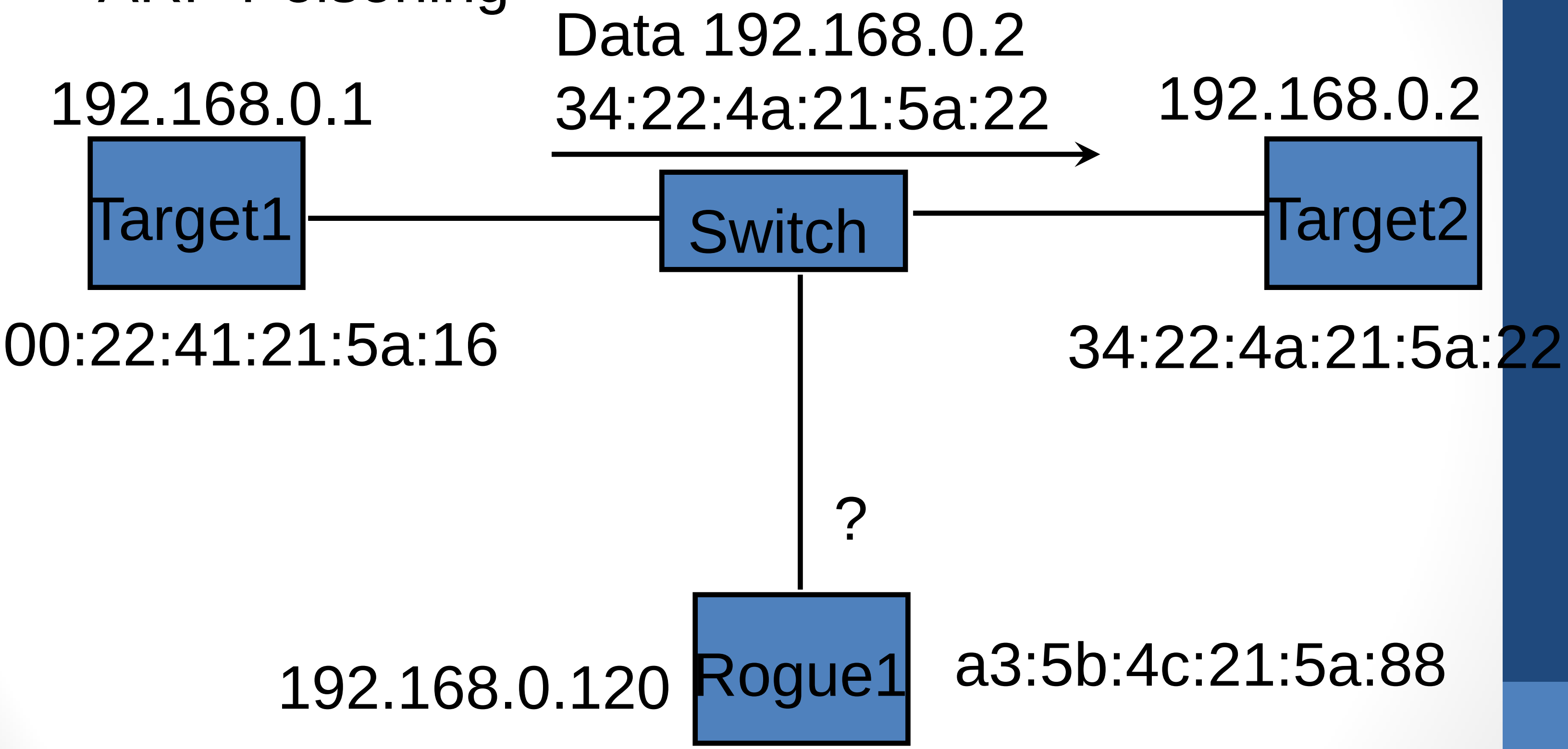
Network Security

- ARP Poisoning



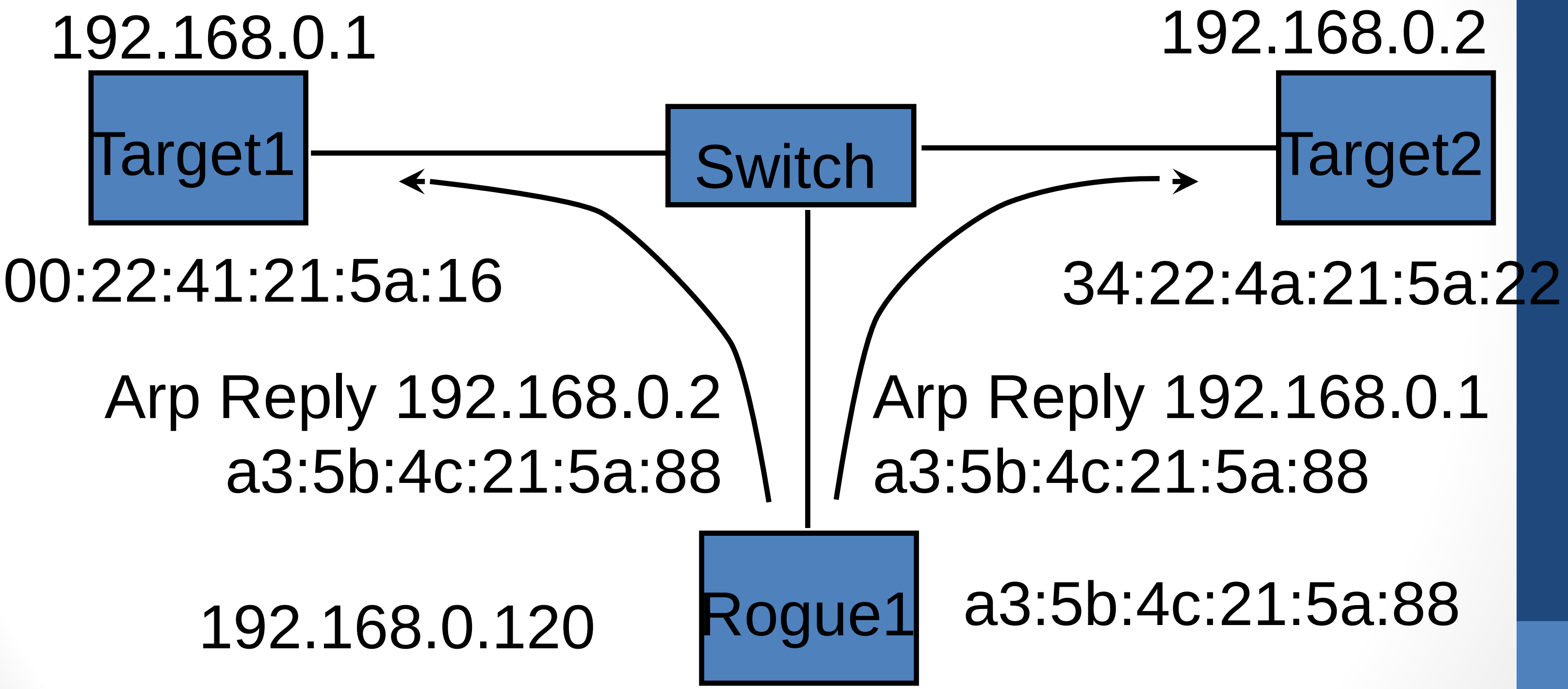
Network Security

- ARP Poisoning



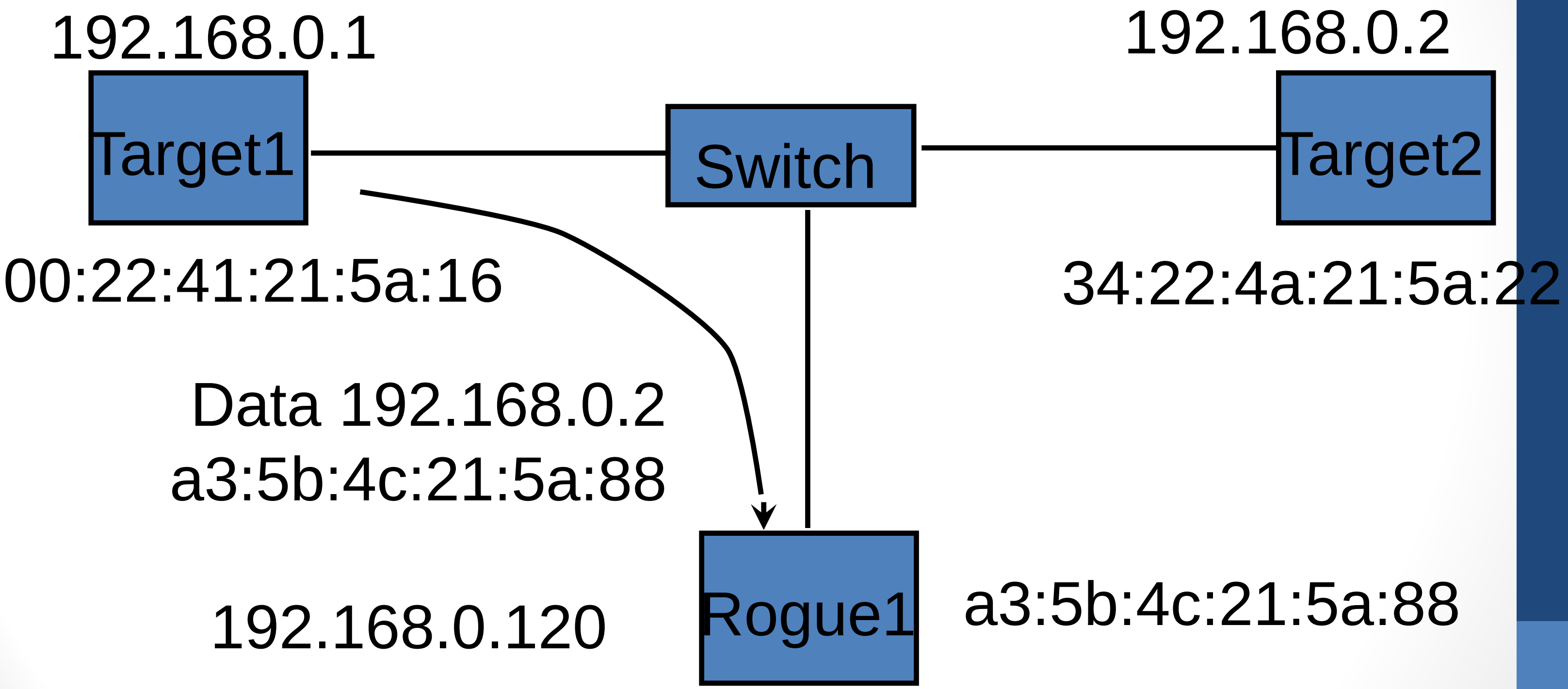
Network Security

- ARP Poisoning



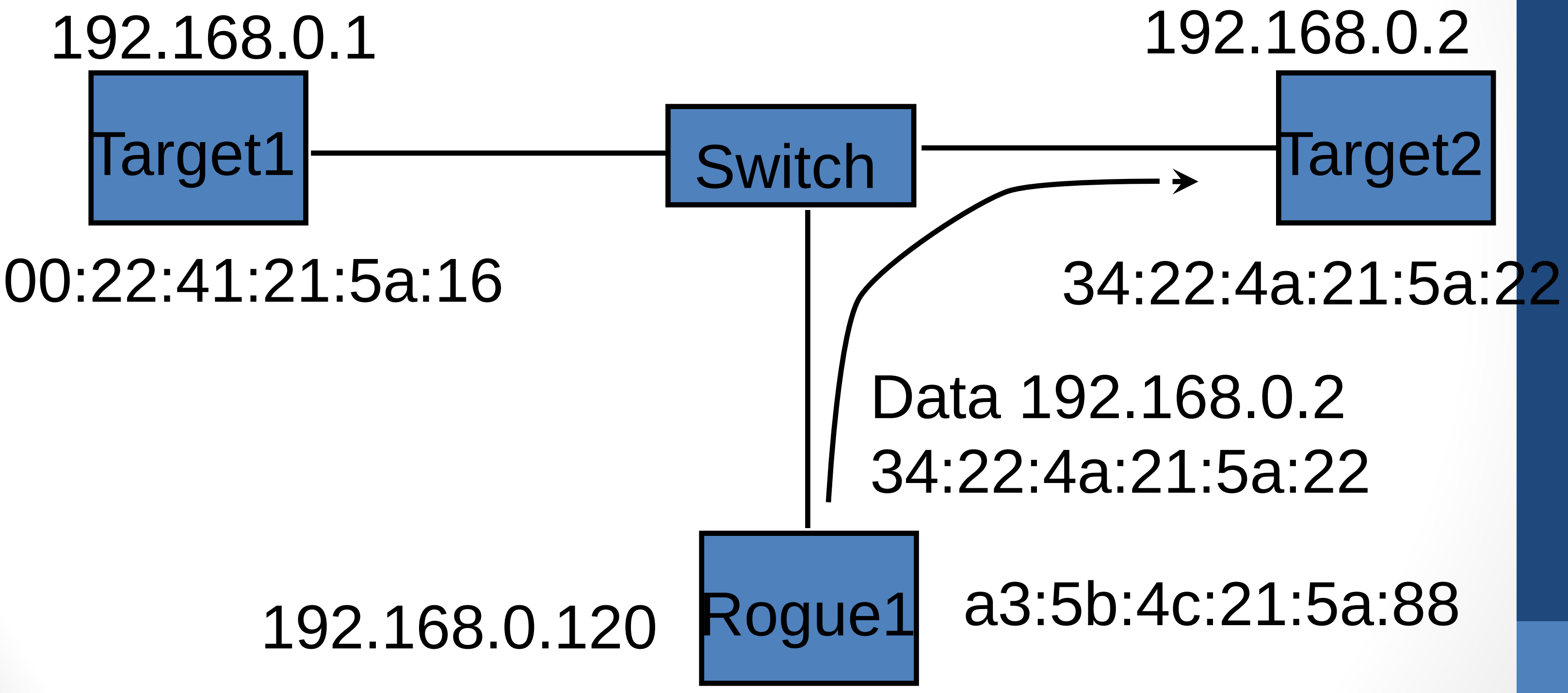
Network Security

- ARP Poisoning



Network Security

- ARP Poisoning



Arp Poisoning

- Protections
  ◊ Don’t use replies you did not ask for.
  ◊ If MACs change unexpectedly, log changes, so a record available.

Network Security

- Eavesdropping

  ◊ WAR driving

  ◊ WEP Vulnerability

  ◊ Switches only route to specific ethernet addresses

  - ARP poisoning
  - MAC Flooding

  ◊ unencrypted protocols

  - ftp, telnet

  ◊ encrypted protocols

  - sftp, scp, ssh

Network Security

- Other Network Attacks...
  - smurf attack
    - ping response....
  - oversize ICMP packet
    - ICMP packet that is too big....
  - Xmas Tree Packets
    - turn on all of the flags
      - ACK, SYN, etc..

Network Security

- pharming

  ◊ reverse proxy for a online bank/Paypal

  ◊ compromise a DNS server/Or DHCP server

  - new attack, DNS poisoning

  ◊ point bank/Paypal at your reverse proxy

  ◊ pass transactions through to the bank

  - but record information for later use.
  - security images???

  ◊ compromise router

  - backbone routers
  - cosumer grade routers

- DLINK advertising...

Authentication

- Passwords
  - ◊ main login
  - ◊ access to resources (databases, Unix groups)
- Vulnerable
  - ◊ guessing - most user chosen passwords are easy to remember, short, easy to guess
    -WPA interface
  - ◊ shoulder surfing (ATM hack)
  - ◊ packet sniffing (conferences)
  - ◊ masquerade
  - ◊ account sharing
- System generated?
  - ◊ too hard to remember?

Passwords

- Must store to verify?
  - ◊ If passwords are stored on OS must be secure
  - ◊ encrypted passwords
  - ◊ one way encryption
    - how to check?
    - safe???
  - ◊ brute force attack (Dictionary Attack)
  - ◊ public file?

    /etc/secure

Passwords

- One Time Passwords
  - ◊ challenge response
    - – hardware key
  - ◊ one time pad
    - – list of random numbers
    - – early on-line banking

- Biometrics
  - ◊ Fingerprints, retina, iris
  - ◊ replay attacks?
  - ◊ major disadvantage

Passwords

- Biometrics
  - ◊ Fingerprints, retina, iris
  - ◊ accuracy

    - false positives (identifies me as you)

    - false negatives (denies you)
  - ◊ anonymity (my yahoo account is anoymous)
  - ◊ multiple accounts

    high security/low security

    - limited number of biometric keys

Passwords

- Biometrics
  - ◊ false sense of security
    - - thermal sensors
    - - repudiation
  - ◊ replay attacks?
  - ◊ fake fingers
    - - silicone fingers

  Tsutomu Matsumoto of Yokohama National University

  - - Gelatin fingers (same electrical characteristics as flesh)
  - - can be made from finger prints left on any object

About Accuracy

- accuracy - what does it mean?
- 300 Million People in the USA
- Assume 1000 terrorists (1 per 300,000 = .00033%)
- Assume 40 percent positive detection (finds 40%) (400 terrorists)
- Assume 0.01% misidentification (30,000 people)

So What is the chance that someone identified as a terrorist is a terrorist?

About Accuracy

- accuracy - what does it mean?
- 300 Million People in the USA
- Assume 1000 terrorists (1 per 300,000 = .00033%)
- Assume 40 percent positive detection (finds 40%) (400 terrorists)
- Assume 0.01% misidentification (30,000 people)

So What is the chance that someone identified as a terrorist is a terrorist?

400/30,000 = 1.32 %

About Accuracy

- 300 Million People in the USA
- Assume 1000 terrorists (1 per 300,000 = .00033%)
- Assume 70% positive detection (700 terrorists)
- Assume 0.01% misidentification (30,000 people)

So What is the chance that someone identified as a terrorist is a terrorist?

About Accuracy

- 300 Million People in the USA
- Assume 1000 terrorists (1 per 300,000 = .00033%)
- Assume 70% positive detection (700 terrorists)
- Assume 0.01% misidentification (30,000 people)

So What is the chance that somone identified as a terrorist is a terrorist?

700/30,000 = 2.3%

Program Threats

- Trojan Horse
  - ◊ game program that sends the contents your mail box to another server
  - ◊ utility that wipes out your accounting program (DOS)

- Masquerade
  - ◊ special type of trojan horse
  - ◊ pretends to be a valid service
  - ◊ login masquerade
  - ◊ web site masquerade (spelling error/email)

Program Threats

- Trap Door/Back Door
  - ◊ Intentional hole left by programmer
  - ◊ Hard coded account numbers or Ids
  - ◊ War Games (Matthew Broderick)