Protection and Security

Protection

- (Chapter 14 in our book.)
- The goal is to protect the system from users, and protect users from each other.
  - It should be possible to limit the files, programs, devices, etc. that a given user can access.

Security

- Security is a broader area than protection.
- Protection is internal.
- Security requires protection, plus the ability to protect the system from external threats.
- First we will look at security threats.
- Then look at method of addressing threats.
  - Cryptography.
  - Other.

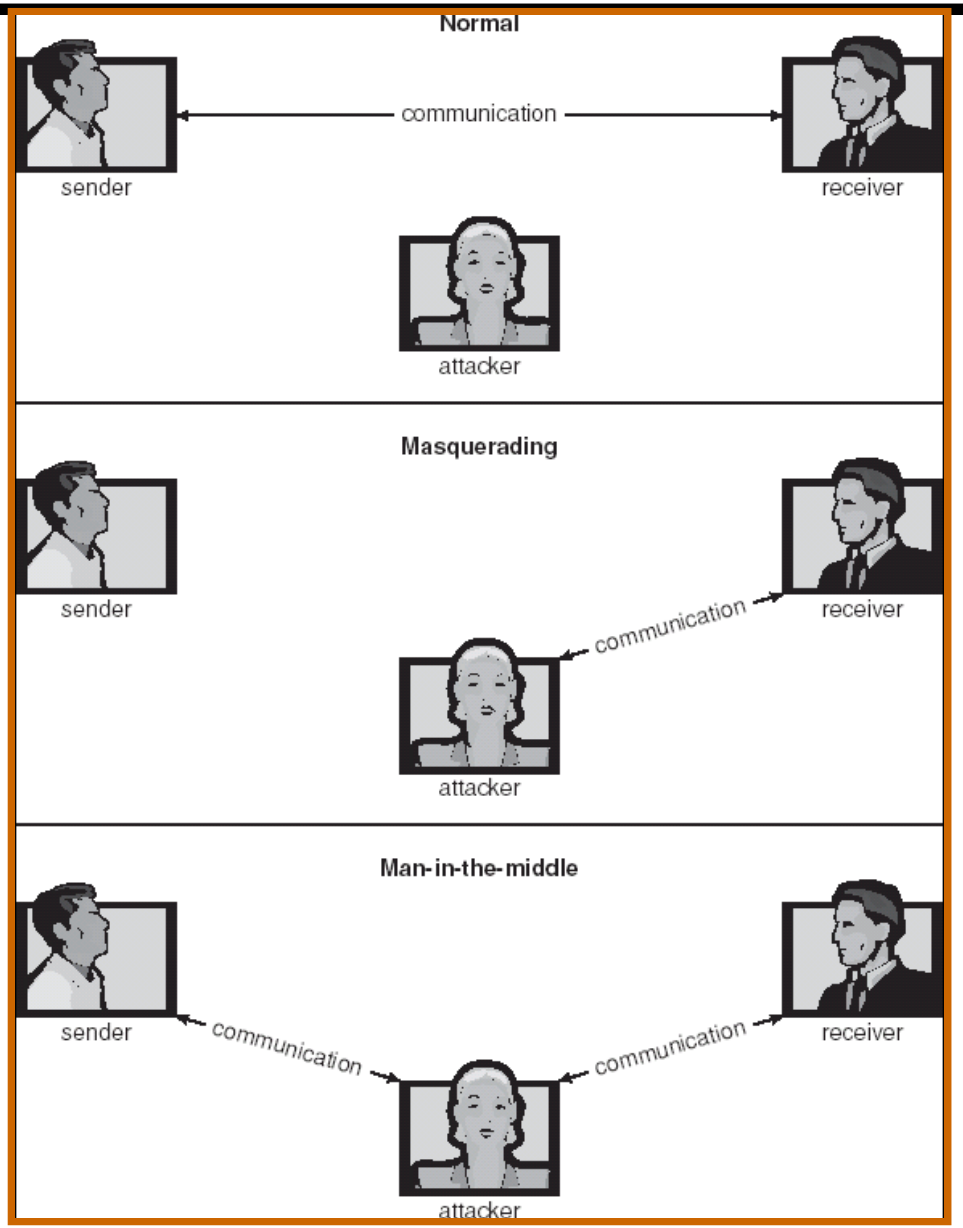
Categories of Security Violations

- Breach of confidentiality – stealing data.
- Breach of integrity – modifying data.
- Breach of availability – destruction of data.
- Theft of service.
- Denial of service – preventing legitimate use of the system.

Standard Methods of Attack

- Masquerading (breach authentication).
- Replay attack.
  - Message modification.
- Man-in-the-middle attack.
- Session hijacking.

Attacks


Normal
communication
sender
receiver
attacker
Masquerading
sender
communication
receiver
attacker
Man-in-the-middle
sender
communication
communication
receiver
attacker

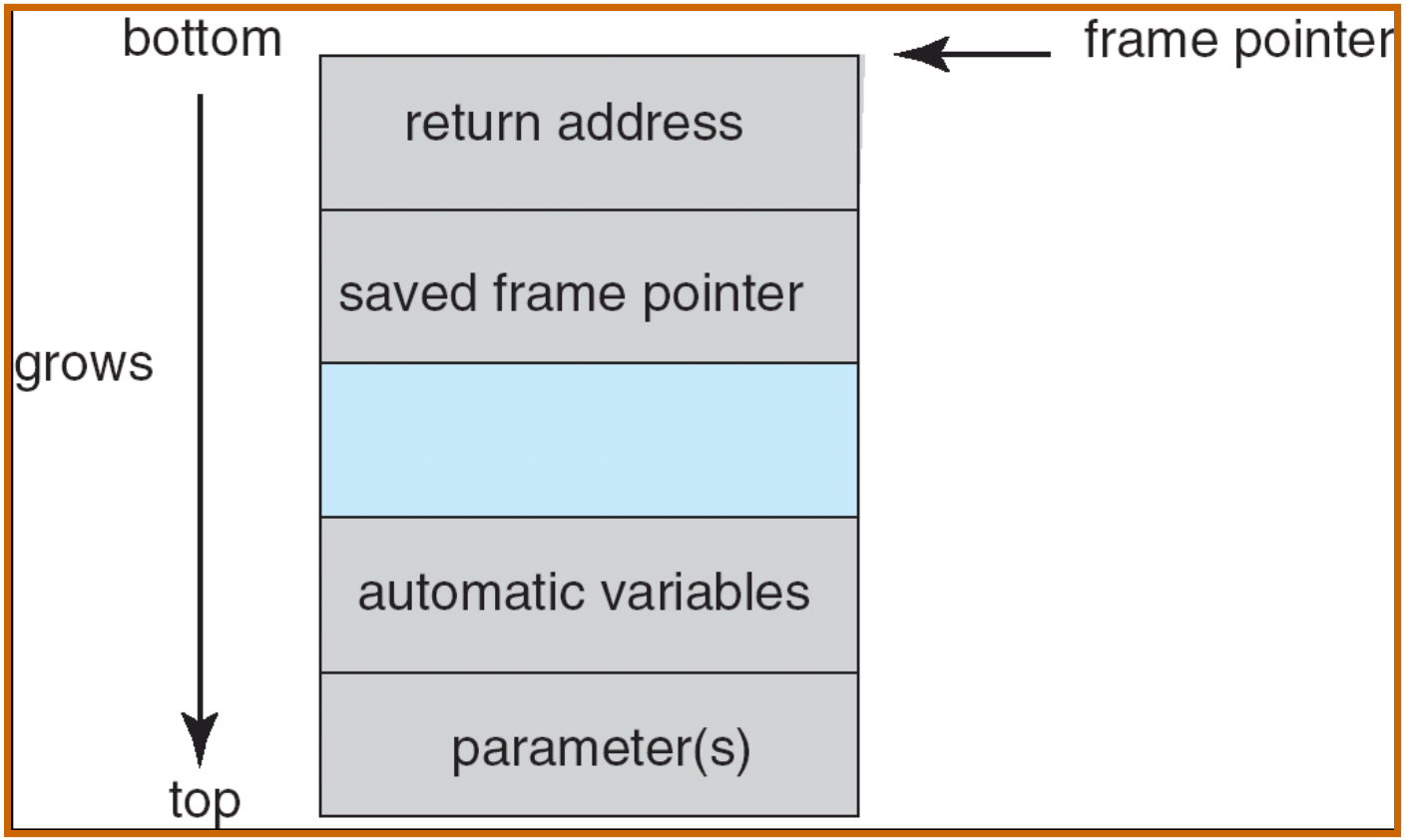
Program Threats

- Trojan Horse
  - (Why you should not have . in your path.)
- Trap Door
  - Specific user identifier or password that circumvents normal security procedures.
- Logic Bomb
  - Program that initiates a security incident under certain circumstances.
- Stack and Buffer Overflow
  - Exploits a bug in a program (overflow either the stack or memory buffers).
- Viruses

C Program With Buffer Overflow

```
#include <stdio.h>
#define BUFFER_SIZE 256
int main(int argc, char *argv[])
{
  char buffer[BUFFER_SIZE];
  if (argc < 2)
     return -1;
  else {
     strcpy(buffer,argv[1]);
     return 0;
  }
}
```

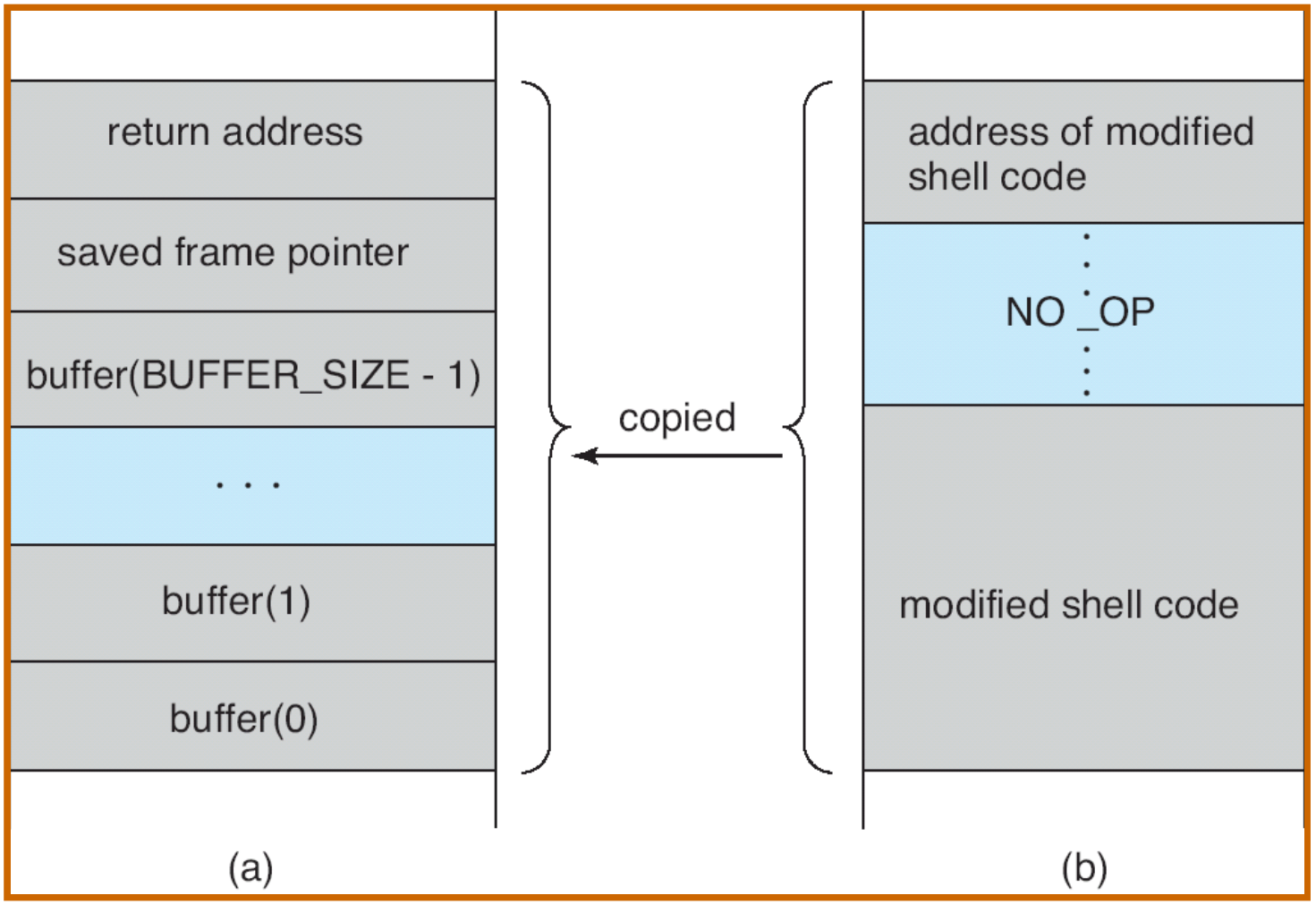
Layout of a Stack Frame



Modified Shell Code

```
#include <stdio.h>
int main(int argc, char *argv[])
{
  execvp(‘‘\bin\sh’’,‘‘\bin \sh’’, NULL);
  return 0;
}
```

Result of the Attack



System and Network Threats

- Worms
- Port scanning
  - Automated attempt to connect to a range of ports on one or a range of IP addresses
- Denial of Service
  - Overload the targeted computer preventing it from doing any useful work.
  - Distributed denial-of-service (DDOS) come from multiple sites at once.

Security Measures

- Security must occur at four levels to be effective:
  - Physical.
  - Human.
    - Avoid **social engineering, phishing, dumpster diving.**
  - Operating System.
  - Network.

Cryptography

- Broadest security tool available
  - Source and destination of messages cannot be trusted without cryptography.
  - Means to constrain potential senders (sources) and / or receivers (destinations) of messages.
- Based on secrets (**keys**)
- Symmetric encryption:
  - Sender and receiver must share a key.
- Asymmetric (public key) encryption:
  - Two keys, one public, one private.
  - They “undo” each other.

Other Security Measures

- Defense in depth - multiple layers of security.
- Security policy describes what is being secured.
- Vulnerability assessment compares real state of system / network compared to security policy.
- Intrusion detection endeavors to detect attempted or successful intrusions
  - Signature-based detection spots known bad patterns.
  - Anomaly detection spots differences from normal behavior.
    - Can detect zero-day attacks.
  - False-positives and false-negatives a problem.

Other Security Measures

- Virus protection.
- Auditing, accounting, and logging of all or specific system or network activities.
- Firewalls.

Acknowledgments

- Portions of these slides are taken from Power Point presentations made available along with:
  - Silberschatz, Galvin, and Gagne. Operating System Concepts, Seventh Edition.
- Original versions of those presentations can be found at:
  - http://os-book.com/