1. (a) Interception

   (b) Fabrication and Modification

   (c)

   (d) Distributed Denial of Service

   (e) Zombies (or bots, hackerese for robots) are machines running pieces of malicious code under remote control.

   (f) HTTPS (HTTP Secure)

2. Think for a moment about how you might deny access in a computer network.

• One potential weakness is the capacity of the system. If demand is higher than the system can handle, some data will not move properly through the network. These attacks are also known as volume-based or volumetric attacks.

• Similarly to overwhelming basic network capacity, an attack can exhaust the application that services a particular network, in what is called an application based attack.

• Another way to deny service is to cut or disable the communications link between two points. Many users will be unable to receive service, especially if that link is a single point through which much traffic must pass.

• A final cause of denied access is a hardware or software failure. Although similar to a failure of a communications link, in this case the problem relates to machinery or programs, for which protection can involve concepts like fault tolerance.

NB; DOS can occur from excessive volume, a failed application, a severed link, or hardware or software failure.

3. Here are some e□amples of DoS attacks:

(b) Smurf/smurfing□ This attack is based on the Internet Control Message Protocol (ICMP) echo repl□ function. It is more commonl□ known as ping+ which is the command+line tool used to invoke this function. In this attack+ the attacker sends ping packets to the broadcast address of the network+ replacing the original source address in the ping packets with the source address of the victim+ thus causing a flood of traffic to be sent to the unsuspecting network device.

Fraggle This attack is similar to a Smurf attack. The difference is that it uses the User Datagram Protocol (UDP) instead of ICMP. The attacker sends spoofed UDP packets to broadcast addresses as in the Smurf attack. These UDP packets are directed to port 7 (echo) or port 19 (chargen). When connected to port 19+ a character generator attack can be run. Table 3.1 lists the most commonl e ploited ports.

(a) Ping flood This attack attempts to block service or reduce activit on a host b sending ping requests directl to the victim. A variation of this t pe of attack is the ping of death+ in which the packet si e is too large and the s stem doesn't know how to handle the packets. SYN flood This attack takes advantage of the TCP three+wa handshake. The source s stem sends a flood of s nchroni ation (SYN) requests and never sends the final acknowledgment (ACK)+ thus creating half+open TCP sessions. Because the TCP stack waits before resetting the port+ the attack overflows the destination computer's connection buffer+ making it impossible to service connection requests from valid users.

Land This attack e ploits a behavior in the operating s stems of several versions of Windows+ Uni + Macintosh OS+ and Cisco IOS with respect to their TCP/IP stacks. The attacker spoofs a TCP/IP s nchroni ation (SYN) packet to the victim s stem with the same source and destination IP address and the same source and destination ports. This confuses the s stem as it tries to respond to the packet.

(e) Teardrop This form of attack targets a known behavior of UDP in the TCP/IP stack of some operating s stems. The Teardrop attack sends fragmented UDP packets to the victim with odd offset values in subsequent packets. When the operating s stem attempts to rebuild the original packets from the fragments+ the fragments overwrite each other+ causing confusion. Because some operating s stems cannot gracefull handle the error+ the s stem will most likel crash or reboot.

(c)

Echo–Chargen

The **echo–chargen** attack works between two hosts. Chargen is an ICMP protocol that generates a stream of packets to test the network's capacity. Echo is another ICMP protocol used for testing; a host receiving an echo returns everything it receives to the sender.

The attacker picks two victims, A and B, and then sets up a chargen process on host A that generates its packets as echo packets with a destination of host B. Thus, A floods B with echo packets. But because these packets request the recipient to echo them back to the sender, host B replies by returning them to host A. As shown in Figure 6-20, this series puts the network infrastructures of A and B into an endless loop, as A generates a string of echoes that B dutifully returns to A, just as in a game of tennis. Alternatively, the attacker can make B both the source and destination address of the first packet, so B hangs in a loop, constantly creating and replying to its own messages.

(d)

SYN Flood

Another popular denial-of-service attack is the **SYN flood**. This attack uses the TCP protocol suite, making the session-oriented nature of these protocols work against the victim.

For a protocol such as Telnet or SMTP, the protocol peers establish a virtual connection, called a session, to synchronize the back-and-forth, command–response nature of the interaction. A session is established with a three-way TCP handshake. Each TCP packet has flag bits, one of which is denoted SYN (synchronize) and one denoted ACK (acknowledge). First, to initiate a TCP connection, the originator sends a packet with the SYN bit on. Second, if the recipient is ready to establish a connection, it replies with a packet with both the SYN and ACK bits on. Finally, the first party completes the

in the SYN_RECV queue to try to identify the attacker. Second, the attacker wants to make the malicious SYN packets indistinguishable from legitimate SYN packets to establish real connections. Choosing a different (spoofed) source address for each one makes them unique, as ordinary traffic would be. A SYN–ACK packet to a nonexistent address results in an ICMP Destination Unreachable response, but this is not the ACK for which the TCP connection is waiting. (TCP and ICMP are different protocol suites, so an ICMP reply does not necessarily get back to the sender's TCP handler.)

These attacks misuse legitimate features of network protocols to overwhelm the victim, but the features cannot be disabled because they have necessary purposes within the protocol suite. Overwhelming network capacity is not the only way to deny service, however. In the next section we examine attacks that exhaust other available resources.

(f)

DNS Cache Poisoning

The **DNS cache poisoning** attack is a way to subvert the addressing to cause a DNS server to redirect clients to a specified address. A conceptually simple DNS poisoning attack is to forge a message to a DNS registrar, requesting that a particular domain name be changed from one address to another. These requests occur normally when a website is moved from one hosting provider to another or when an organization changes its address structure. However, a malicious attacker can use a DNS change request to redirect traffic intended for a particular domain name. Because of strong authentication requirements, registrars seldom succumb to such a forgery.

A more likely attack is to use the DNS protocol messages by which all Internet name servers coordinate their address translations. Dan Kaminsky [KAM08] expanded on some previously known methods to poison the DNS cache. The DNS protocol is complex, but you do not need to understand the details in order to appreciate this attack.

A client requiring the address corresponding to a domain name sends a query to its local DNS name server. If that server does not have the answer, it forwards the query to a root name server; the query is forwarded to more-specific name servers until one replies authoritatively with the address. That address is propagated through the chain of servers involved in resolving the query and eventually back to the client. The servers along the way cache the response so that they can respond directly to future queries for the same address.

Kaminsky noticed a flaw in this progression: namely, that these queries remain open until answered and that a response matching the ID number for the query will be cached. If an attacker can guess the sequence of query ID numbers, the attacker can forge a response that satisfies an open query's ID; that forged reply can provide any address as a response. Until the response is removed from the cache, all traffic for the requested address will be directed to the address given in the forged reply. Thus, by predicting sequence numbers correctly and generating network traffic to a specific name server, the attacker can redirect traffic silently to a selected address.

In cache poisoning an incorrect name-to-address DNS conversion is placed in and remains in a translation cache.

This example shows the vulnerability of predictable sequence numbers. A countermeasure for this type of attack is an *unpredictable* series of sequence numbers, preferably drawn from a large range of possibilities.

For years, the Internet governing bodies have been working to implement a protection against such replay and hijack attacks. This objective is addressed with **DNSSEC**, the DNS security extension (RFC 4033 [ARE05]). In June 2010, the first root DNS server was assigned a private key for signing DNS records; other root servers will be assigned keys. Every DNS record at the root level will be signed and published, along with the root administrator's public key, in the DNS itself. As root name servers' records are signed, other name servers will gradually acquire public keys and sign their records. Ultimately, a client's address request will also entail obtaining and checking the signatures of all records that were part of the name resolution path.

4. (a) Botnets, networks of bots, are used for massive denial-of-service attacks, implemented from many sites working in parallel against a victim. They are also used for spam and other bulk email attacks, in which an extremely large volume of email from any one point might be blocked by the sending service provider.

(b)

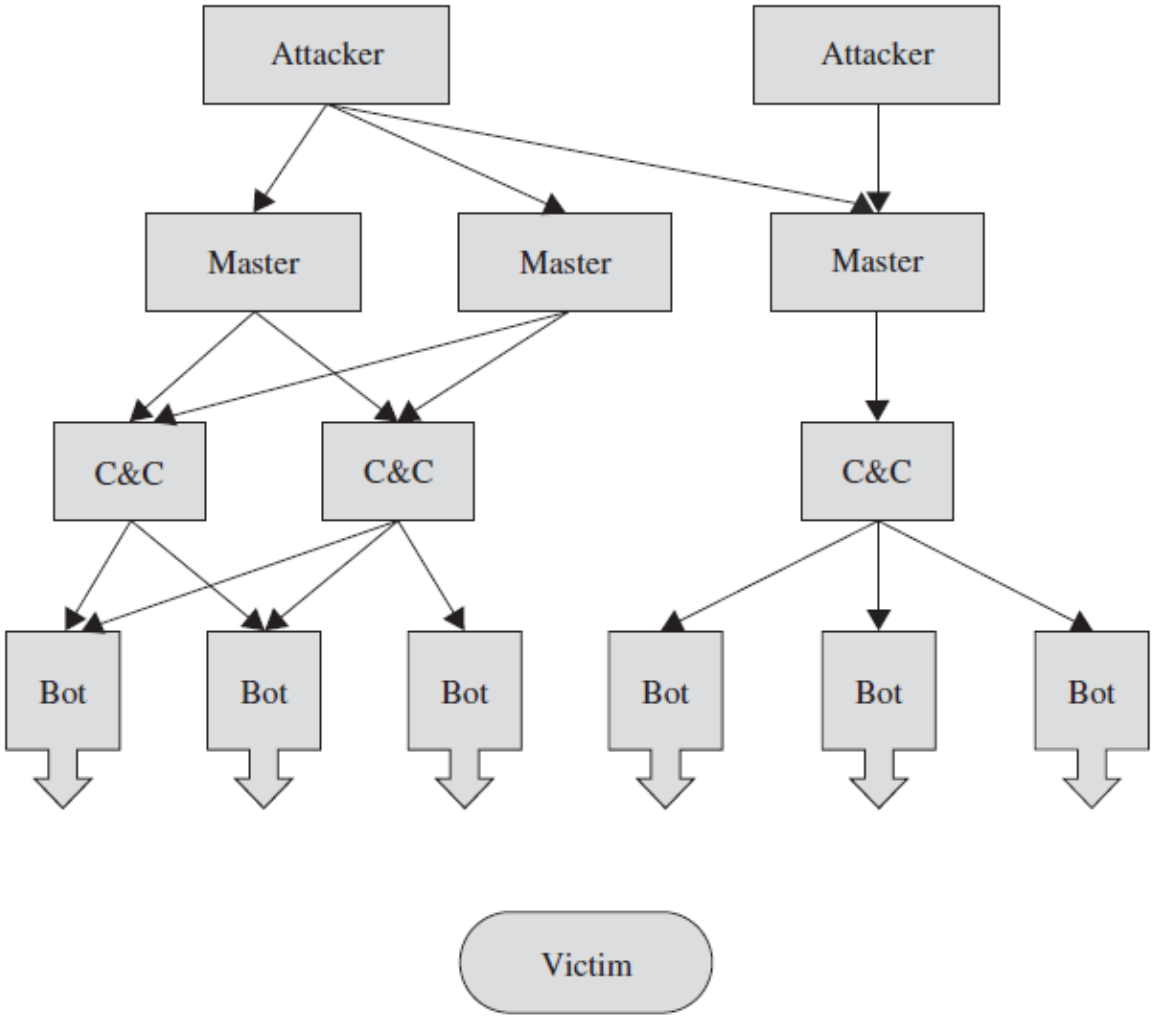

FIGURE 6-35 Botnet Command-and-Control Structure

NB: A botnet command-and-control center instructs specific machines to target a particular victim at a given time and duration.

(c)

Malicious Autonomous Mobile Agents

Bots belong to a class of code known more generally as **malicious autonomous mobile agents**. Working largely on their own, these programs can infect computers anywhere they can access, causing denial of service as well as other kinds of harm. Of course, code does not develop, appear, or mutate on its own; there has to be a developer involved initially to set up the process and, usually, to establish a scheme for updates. Such an agent is sometimes called an **inoculation agent**.

As bots or agents execute and acquire updates, not every agent will be updated at once. One agent may be on a system that is powered off, another on a system that currently has no external network connectivity, and still another may be running in a constrained resource domain. Thus, as agents run in and out of contact with their update services, some will be up to date and others will be running older versions. The problem of coordinating an army of disparate agents is an active research topic, based on the Byzantine generals problem [LAM82].

Autonomous Mobile Protective Agents

Suppose a security engineer decodes the logic of an agent; the engineer might then enlist the agent to fight for the good guys by modifying it to look normal to its siblings but in fact to spread a counterinfection. So, for example, a modified agent might look for other hostile agents and pass them an "update" that in fact disabled them.

This concept is not as far-fetched as it sounds. In the same way that attackers have developed networks for harm, security researchers have postulated how good agents could help heal after a malicious code infection.

A German teenager, Sven Jaschen, wrote and released a worm called NetSky in February 2004. He claimed his intention was to remove infections of the widespread MyDoom and Bagle worms from infected computers by closing the vulnerabilities those worms exploit. NetSky spread by email. However, Jaschen soon became engaged in a battle with the creators of Bagle and MyDoom, who produced better versions of their code, which led to new versions of NetSky, and so on, for a total of 30 separate strains of NetSky. According to one security expert, Mikko Hypponen of f-Secure, NetSky was more effective at reducing the flow of spam than anything that had happened in the U.S. Congress or courts. Unfortunately, it also consumed large amounts of system resources and bombarded numerous commercial clients with email. Later versions of the worm launched denial-of-service attacks against places Jaschen disliked. Two years after the virus's release, it was still the most prevalent virus infection worldwide, according to security firm Sophos [SOP04].

Two months after releasing NetSky, on his eighteenth birthday, Jaschen wrote and released a highly destructive Internet-based virus named Sasser that forced computers to reboot constantly. He was arrested by German authorities, and convicted and sentenced to a 31-month suspended sentence and three years' probation.

(d) Bots are co-opted by an agent who exploits a vulnerability, typically one already known. Vulnerable machines can be discovered by scanning.

5 Tips for DDoS Attack Prevention

Prevention is the best medicine, and this couldn't be more true for DDoS attacks. Prepare your organization with the following tips to avert a devastating DDoS attack.

1. Organize a DDoS Attack Response Plan. Don't be caught blindsided by DDoS attacks; have a response plan ready in case of a security breach so your organization can respond as promptly as possible. Your plan should document how to maintain business operations if a DDoS attack is successful, any technical competencies and expertise that will be necessary, and a systems checklist to ensure that your assets have advanced threat detection.

Additionally, establish an incident response team in case the DDoS is successful and define responsibilities, such as notifying key stakeholders and ensuring communication throughout the organization.

2. Secure your Infrastructure with DDoS Attack Prevention Solutions. Equip your network, applications, and infrastructure with multi-level protection strategies. This may include prevention management systems that combine firewalls, VPN, anti-spam, content filtering and other security layers to monitor activities and identity traffic inconsistencies that may be symptoms of DDoS attacks.

If you're looking for protection by leveraging cloud-based solutions, many providers allow for advanced protection resources for additional charges. Other options allow for businesses to go "full cloud," entrusting sensitive data with a reputable cloud provider that offers heightened security protocols, both virtual and physical.

3. Perform a Network Vulnerability Assessment. Identify weakness in your networks before a malicious user does. A vulnerability assessment involves identifying security exposures so you can patch up your infrastructure to be better prepared for a DDoS attack, or for any cybersecurity risks in general.

Assessments will secure your network by trying to find security vulnerabilities. This is done by taking inventory of all devices on the network, as well as their purpose, system information, and any vulnerabilities associated with them, and including what devices need to be prepared for upgrades or future assessments. Doing so will help define your organization's level of risk so you can optimize any security investments.

4. Identify Warning Signs of a DDoS Attack. If you can identify the symptoms of a DDoS attack as early as possible, you can take action and hopefully mitigate damage. Spotty connectivity, slow performance, and intermittent web crashes are all signs that your business may be coming under attack from a DDoS criminal. Educate your team on signs of DDoS attacks so everyone can be alert for warning signs.

Not all DDoS attacks are extensive and high volume; low-volume attacks that launch for short durations are just as common. These attacks can be particularly nefarious because they are more likely to go under the radar as just a random incident rather than a potential security breach. Low-volume DDoS attacks are likely distractions for damaging malware; while your IT security staff is distracted by a low-volume attack, malicious software like ransomware can infiltrate your network.

5. Adopt Cloud-Based Service Providers. There are several benefits to outsourcing DDoS attack prevention to the cloud.

Cloud providers who offer high levels of cybersecurity, including firewalls and threat monitoring software, can help protect your assets and network from DDoS criminals.

The cloud also has greater bandwidth than most private networks, so it is likely to fail if under the pressure of increased DDoS attacks.

5. SSL/TLS uses both asymmetric and symmetric encryption to protect the confidentiality and integrity of data-in-transit. Asymmetric encryption is used to establish a secure session between a client and a server, and symmetric encryption is used to exchange data within the secured session.
6.

SSL Session

Because SSL is commonly used with web pages, it is often referred to as HTTPS (HTTP Secure), and you will see the https: prefix in the address bar of a browser, as well as a closed padlock in the corner whenever SSL is in operation. To use SSL, the client requests an SSL session. The server responds with its public key certificate so that the client can determine the authenticity of the server. The client returns a symmetric session key encrypted under the server's public key. Both the server and client compute the session key, and then they switch to encrypted communication, using the shared session key.

After an SSL session has been established, the details of the session can be viewed. For example, Figure 6-41 shows an SSL connection established to https:login.yahoo.com.

7. ,,,
8. ,,,
9. Port scanning tells an attacker three things: which **standard ports or services** are running and responding on the target system, what **operating system** is installed on the target system, and what **applications and versions of applications** are present.
10. (a) Strengths of WPA over WEP
    - Non-Static Encryption Key
    - Authentication
    - Strong Encryption
    - Integrity Protection
    - Session Initiation

Security Tip (ST05-003)

(b)Securing Wireless Networks

Wireless networks introduce additional security risks. If you have a wireless network, make sure to take appropriate precautions to protect your information.

In today's connected world, almost everyone has at least one internet-connected device. With the number of these devices on the rise, it is important to implement a security strategy to minimize their potential for exploitation (see Securing the Internet of Things). Internet-connected devices may be used by nefarious entities to collect personal information, steal identities, compromise financial data, and silently listen to—or watch—users. Taking a few precautions in the configuration and use of your devices can help prevent this type of activity.

What are the risks to your wireless network?

Whether it's a home or business network, the risks to an unsecured wireless network are the same. Some of the risks include:

Piggybacking

If you fail to secure your wireless network, anyone with a wireless-enabled computer in range of your access point can use your connection. The typical indoor broadcast range of an access point is 150–300 feet. Outdoors, this range may extend as far as 1,000 feet. So, if your neighborhood is closely settled, or if you live in an apartment or condominium, failure to secure your wireless network could open your internet connection to many unintended users. These users may be able to conduct illegal activity, monitor and capture your web traffic, or steal personal files.

Wardriving

Wardriving is a specific kind of piggybacking. The broadcast range of a wireless access point can make internet connections available outside your home, even as far away as your street. Savvy computer users know this, and some have made a hobby out of driving through cities and neighborhoods with a wireless-equipped computer—

sometimes with a powerful antenna—searching for unsecured wireless networks. This practice is known as “wardriving.”

Evil Twin Attacks

In an evil twin attack, an adversary gathers information about a public network access point, then sets up their system to impersonate it. The adversary uses a broadcast signal stronger than the one generated by the legitimate access point; then, unsuspecting users connect using the stronger signal. Because the victim is connecting to the internet through the attacker’s system, it’s easy for the attacker to use specialized tools to read any data the victim sends over the internet. This data may include credit card numbers, username and password combinations, and other personal information. Always confirm the name and password of a public Wi-Fi hotspot prior to use. This will ensure you are connecting to a trusted access point.

Wireless Sniffing

Many public access points are not secured and the traffic they carry is not encrypted. This can put your sensitive communications or transactions at risk. Because your connection is being transmitted “in the clear,” malicious actors could use sniffing tools to obtain sensitive information such as passwords or credit card numbers. Ensure that all the access points you connect to use at least WPA2 encryption.

Unauthorized Computer Access

An unsecured public wireless network combined with unsecured file sharing could allow a malicious user to access any directories and files you have unintentionally made available for sharing. Ensure that when you connect your devices to public networks, you deny sharing files and folders. Only allow sharing on recognized home networks and only while it is necessary to share items. When not needed, ensure that file sharing is disabled. This will help prevent an unknown attacker from accessing your device’s files.

Shoulder Surfing

In public areas malicious actors can simply glance over your shoulder as you type. By simply watching you, they can steal sensitive or personal information. Screen protectors that prevent shoulder-surfers from seeing your device screen can be purchased for little money. For smaller devices, such as phones, be cognizant of your surroundings while viewing sensitive information or entering passwords.

Theft of Mobile Devices

Not all attackers rely on gaining access to your data via wireless means. By physically stealing your device, attackers could have unrestricted access to all of its data, as well as any connected cloud accounts. Taking measures to protect your devices from loss or theft is important, but should the worst happen, a little preparation may protect the data inside. Most mobile devices, including laptop computers, now have the ability to fully encrypt their stored data—making devices useless to attackers who cannot provide the proper password or personal identification number (PIN). In addition to encrypting device content, it is also advisable to configure your device's applications to request login information before allowing access to any cloud-based information. Last, individually encrypt or password-protect files that contain personal or sensitive information. This will afford yet another layer of protection in the event an attacker is able to gain access to your device.

What can you do to minimize the risks to your wireless network?

Change default passwords. Most network devices, including wireless access points, are pre-configured with default administrator passwords to simplify setup. These default passwords are easily available to obtain online, and so provide only marginal protection. Changing default passwords makes it harder for attackers to access a device. Use and

periodic changing of complex passwords is your first line of defense in protecting your device. (See Choosing and Protecting Passwords.)

Restrict access. Only allow authorized users to access your network. Each piece of hardware connected to a network has a media access control (MAC) address. You can restrict access to your network by filtering these MAC addresses. Consult your user documentation for specific information about enabling these features. You can also utilize the “guest” account, which is a widely used feature on many wireless routers. This feature allows you to grant wireless access to guests on a separate wireless channel with a separate password, while maintaining the privacy of your primary credentials.

Encrypt the data on your network. Encrypting your wireless data prevents anyone who might be able to access your network from viewing it. There are several encryption protocols available to provide this protection. Wi-Fi Protected Access (WPA), WPA2, and WPA3 encrypt information being transmitted between wireless routers and wireless devices. WPA3 is currently the strongest encryption. WPA and WPA2 are still available; however, it is advisable to use equipment that specifically supports WPA3, as using the other protocols could leave your network open to exploitation.

Protect your Service Set Identifier (SSID). To prevent outsiders from easily accessing your network, avoid publicizing your SSID. All Wi-Fi routers allow users to protect their device’s SSID, which makes it more difficult for attackers to find a network. At the very least, change your SSID to something unique. Leaving it as the manufacturer’s default could allow a potential attacker to identify the type of router and possibly exploit any known vulnerabilities.

Install a firewall. Consider installing a firewall directly on your wireless devices (a host-based firewall), as well as on your home network (a router- or modem-based firewall). Attackers who can directly tap into your wireless network may be able to circumvent your network firewall—a host-based firewall will add a layer of protection to the data on your computer (see Understanding Firewalls for Home and Small Office Use).

Maintain antivirus software. Install antivirus software and keep your virus definitions up to date. Many antivirus programs also have additional features that detect or protect

against spyware and adware (see Protecting Against Malicious Code and What is Cybersecurity?).

Use file sharing with caution. File sharing between devices should be disabled when not needed. You should always choose to only allow file sharing over home or work networks, never on public networks. You may want to consider creating a dedicated directory for file sharing and restrict access to all other directories. In addition, you should password protect anything you share. Never open an entire hard drive for file sharing (see Choosing and Protecting Passwords).

Keep your access point software patched and up to date. The manufacturer of your wireless access point will periodically release updates to and patches for a device's software and firmware. Be sure to check the manufacturer's website regularly for any updates or patches for your device.

Check your internet provider's or router manufacturer's wireless security options. Your internet service provider and router manufacturer may provide information or resources to assist in securing your wireless network. Check the customer support area of their websites for specific suggestions or instructions.

Connect using a Virtual Private Network (VPN). Many companies and organizations have a VPN. VPNs allow employees to connect securely to their network when away from the office. VPNs encrypt connections at the sending and receiving ends and keep out traffic that is not properly encrypted. If a VPN is available to you, make sure you log onto it any time you need to use a public wireless access point.