4

Managing Networks and Security

If you find an error, please send it to me to receive extra credit. Indicate the page and line number, then state what the error is and how to fix it. Send it to panko@hawaii.edu. Begin with 431: Error Report for Chapter \*.

Do not send error reports as parts of other messages. They may be lost that way.

# Objectives

By the end of this chapter, you should be able to:

* Discuss network quality of service (QoS) and be able to specify service level agreement (SLA) guarantees.
* Design a network layout based on required traffic volumes between pairs of sites. Describe options for dealing with momentary traffic peaks.
* Describe the benefits and importance of centralized network management; discuss, compare and contrast three tools for centralizing network management: ping, traceroute, and the Simple Network Management Protocol (SNMP).
* Describe security management, including the plan-protect-respond cycle.
* Describe and apply strategic security planning principles.

Note: The section on Strategic Planning Principles will require you to do considerable thinking to apply the principles.

# Failures in the Target Breach

After every breach, companies should pause to draw lessons from the experience. This type of reflection, if it leads to appropriate changes, will reduce the odds of similar breaches in the future.

One lesson from the Target breach is that you cannot trust external businesses you deal with to have good security. In the case of Fazio Mechanical Services, an employee fell for a spear phishing attack. This could happen in any company. However, Fazio made it more likely. It used the free messages and attachments. If Fazio had used a commercial antivirus program for their e-mail, the employee might have seen a warning that the attachment was suspicious.

The breach also taught lessons about Target’s internally security. After gaining a foothold on the vendors’ server, attackers were able to move into more sensitive parts of the network in order to download malware onto the POS terminals, compromise a server to create a holding server, and hack another server to act as an extrusion server. The low-security and highly sensitive parts of the network should have been segregated. They were not, or at least not well.

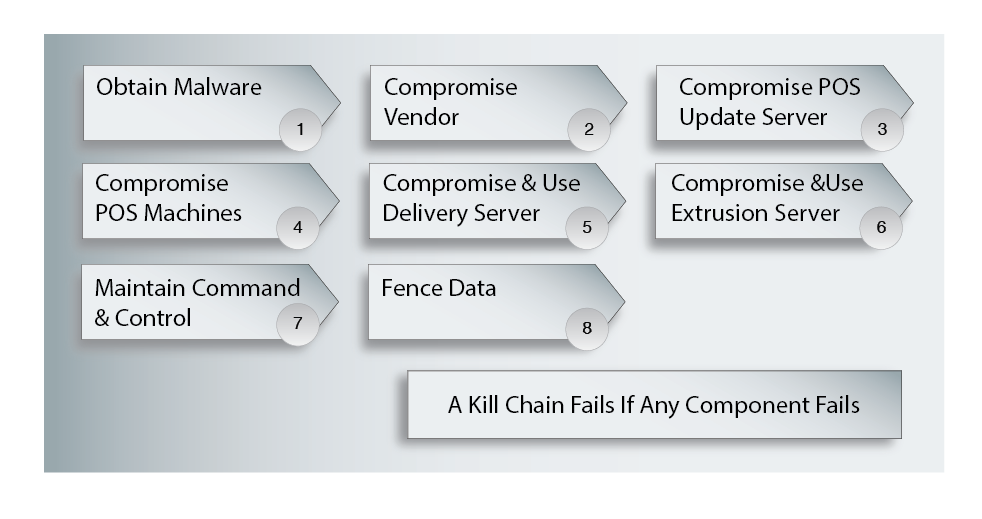
Another issue is that Target received explicit warnings when the attackers were setting up the extrusion server. The thieves had to download malware onto the extrusion server in order to take it over and to manage subsequent FTP transmission. Target used the FireEye intrusion detection program and even FireEye’s human analysis service. FireEye notified the Minneapolis security staff that a high-priority event had occurred on November 30, 2013.[[1]](#footnote-1) In addition, the thieves had trouble with the initial malware. They had to make additional updates on December 1 and December 3. These resulted in additional FireEye warnings being sent to Target’s Minneapolis security group. Had Target followed up on these warnings, they could have stopped or at least reduced the data extrusion, which began on December 2.[[2]](#footnote-2)

Target may also have been lax in addressing the specific danger of POS attacks. In April and August 2013, VISA had sent Target and other companies warnings about new dangers regarding POS data theft.[[3]](#footnote-3) It appears that Target’s own security staff expressed concern for the company’s exposure to charge card data theft.[[4]](#footnote-4) If target did not respond to this risk aggressively, this would have been a serious lapse.

Overall, Figure 3-1 showed that the thieves had to succeed at every step in a complex series of actions. Lockheed Martin’s Computer Incident Response Team[[5]](#footnote-5) staff called this a *kill chain*, which is a term borrowed from the military. The kill chain concept was designed to visualize all of the manufacturing, handling, and tactical steps needed for a weapon to destroy its target. Failure in a single step in a kill chain will create overall failure. Lockheed has suggested that companies should actively consider security kill chains and look for evidence that one of the steps is occurring. Success in identifying an operating kill chain may allow the company to stop it or at least disrupt or degrade it. The warnings when malware was installed three times on the extrusion server could have done exactly that.

The kill chain concept was designed to visualize all of the manufacturing, handling, and tactical steps needed for a weapon to destroy its target. Failure in a single step in a kill chain will create overall failure.

Figure 4-1: Kill Chain for a Successful Attack



Until one understands likely kill chains in depth, however, it is impossible to understand that events are part of each kill chain. Conversely, understanding the kill chain can allow the company to act before a kill chain fitting that pattern begins. For example, even cursory thinking about charge card data theft would lead the company to realize that thieves would probably use FTP transfers to unusual servers, that command communication would probably use certain ports in firewalls, and so forth.

Even well-defended companies suffer security compromises. However, when strategic planning is not done, if protections are not put into place, or if the security staff is not aggressive in doing the work required for the protections to work, the risk of compromises becomes a near certainty. Security expert Ben Schneier said that security is a process, not a product.”[[6]](#footnote-6) Boxes and software are not magic talismans.

Test Your Understanding

1. a) What security mistake did Fazio Mechanical Services make? b) Why do you think it did this? (This requires you to give an opinion.) c) How might segregation of the network have stopped the breach? d) Why do you think the Minneapolis security staff did not heed the FireEye warning? (This requires you to give an opinion.) e) What warnings had Target not responded to adequately? f) What happens in a kill chain if a single action fails anywhere in the chain? g) How can kill chain analysis allow companies to identify security actions it should take? h) Explain why "Security is a process, not a product.”

# Introduction

In the first three chapters, we looked at general network concepts and security. However, technology means nothing unless a company manages network and security well. In this chapter, we will look at network and security planning. Although the concepts are broad, they apply to everything networking professionals do at every level.

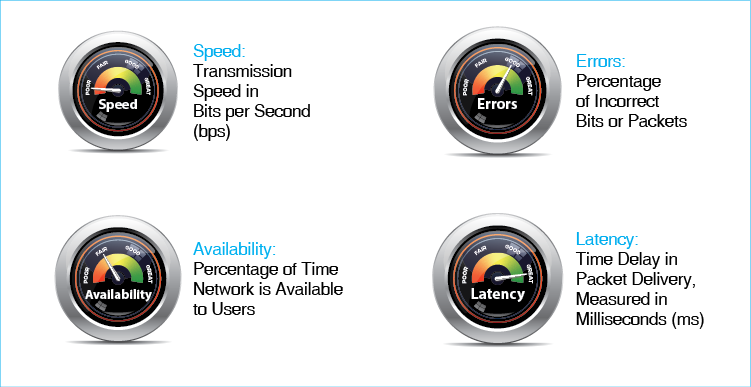
Management is critical. Today, we can build much larger networks than we can manage. Even a mid-size bank is likely to have 500 Ethernet switches and a similar number of routers. Furthermore, network devices and their users are often scattered over large regions—sometimes internationally. While network technology is exciting to talk about and concrete conceptually, it is chaos without good management.

A pervasive issue in network management is cost. In networking, you never say, “Cost doesn’t matter.” Network budgets are always stretched thin. Networking and security professionals always need to accomplish important goals with limited budgets. One way to do this is to automate as much network management work as possible.

# Network Quality of Service (QoS)

In the early days of the Internet, networked applications amazed new users. However, these users soon added, “Too bad it doesn’t work better.” Today, networks are mission-critical for corporations. If the network breaks down, much of the organization comes to a grinding and expensive halt. Today, networks must not only work. They must work *well*. Companies are increasingly concerned with network quality-of-service (QoS) metrics, that is, quantitative measures of network performance. Figure 4-2 shows that companies use a number of QoS metrics. Collectively, these metrics track the service quality that users receive.

Figure 4-2: Quality-of-Service (QoS) Metrics



Test Your Understanding

2. a) What are QoS metrics? (Do not just spell out the acronym.) b) Why are QoS metrics important?

## Transmission Speed

There are many ways to measure how well a network is working. The most fundamental metric, as we saw in Chapter 1, is speed. While low speeds are fine for text messages, the need for speed becomes very high as large volumes of data must be delivered, and video transmission requires increasingly higher transmission speeds.

Rated Speed versus Throughput.  The term *transmission speed* is somewhat ambiguous. A transmission link’s rated speed is the speed it *should* provide based on vendor claims or on the standard that defines the technology. For a number of reasons, transmission links almost never deliver data at their full rated speeds. In contrast to rated speed, a network’s throughput is the data transmission speed the network *actually* provides to users.

A transmission link’s rated speed is the speed it should provide based on vendor claims or on the standard that defines the technology

Throughput is the transmission speed a network actually provides to users.

Figure 4-3: Rated Speed, Throughput, Aggregate Throughput, and Individual Throughput (Study Figure)

Rated Speed

The speed a system should achieve

According to vendor claims or to the standard that defines the technology

Throughput

The data transmission speed a system actually provides to users

Aggregate Throughput on Shared Lines

The throughput to all users is the aggregate throughput

Individual Throughput

The individual’s share of the shared aggregate throughput

Aggregate versus Individual Throughput.  Sometimes transmission links are shared. For example, if you are using a Wi-Fi computer in a classroom, you share the wireless access point’s throughput with other users of that access point. In shared situations, it is important to distinguish between a link’s aggregate throughput, which is the total it provides to all users who share it in a part of a network, and the link’s individual throughput that single users receive as their shares of the aggregate throughput. Individual throughput is always lower than aggregate throughput. As you learned as a child, despite what your mother said, sharing is bad.

Test Your Understanding

3. a) Distinguish between rated speed and throughput. b) Distinguish between individual and aggregate throughput. c) You are working at an access point with 20 other people. Three are doing a download at the same time you are. The rest are looking at their screens or sipping coffee. The access point channel you share has a rated speed of 150 Mbps and a throughput of 100 Mbps. How much speed can you expect for your download? (Check figure: 25 Mbps). d) In a coffee shop, there are 10 people sharing an access point with a rated speed of 20 Mbps. The throughput is half the rated speed. Several people are downloading. Each is getting five Mbps. How many people are using the Internet at that moment?

## Other Quality-of-Service Metrics

Although network speed is important, it is not enough to provide good quality of service. Figure 4-2 showed that there are other QoS categories. We will look briefly at three of them.

Availability.  One is availability, which is the percentage of time that the network is available for use. Ideally, networks would be available 100% of the time, but that is impossible in reality.

Error Rates.   Ideally, all packets would arrive intact, but a few will not. The error rate is the percentage of bits or packets that are lost or damaged during delivery. (At the physical layer, it is common to measure bit error rates. At the internet layer, it is common to measure packet error rates.

When the network is overloaded, error rates can soar because the network has to drop the packets it cannot handle. Consequently, companies must measure error rates when traffic levels are high in order to have a good understanding of error rate risks.[[7]](#footnote-7)

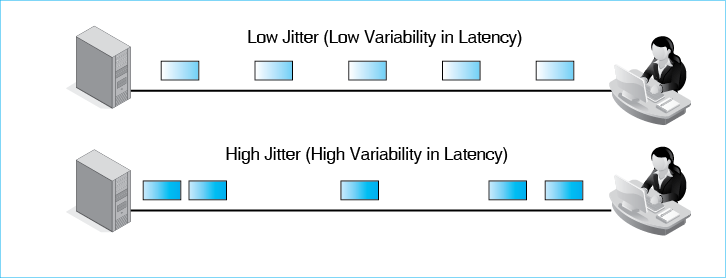
Latency.  When packets move through a network, they will encounter some delays. The amount of delay is called latency. Latency is measured in milliseconds (ms). A millisecond is a thousandth of a second. When latency reaches about 125 milliseconds, turn taking in telephone conversations becomes difficult. You think the other person has finished speaking, so you begin to speak—only to realize that the other party is still speaking.

The amount of network delay is called latency. It is measured in milliseconds (ms).

Jitter.  A related concept is jitter, which Figure 4-4 illustrates. Jitter occurs when the latency between successive packets varies. Some packets will come farther apart in time, others closer in time. While jitter does not bother most applications, VoIP and streaming media are highly sensitive to jitter. If the sound is played back without adjustment, it will speed up and slow down. These variations often occur over millisecond times. As the name suggests, variable latency tends to make voice sound jittery.[[8]](#footnote-8)

Jitter is the average variability in arrival times (latency)

Figure 4-4: Jitter



Engineering for Latency and Jitter.   Most networks were engineered to carry traditional data such as e-mail and database transmissions. In traditional applications, latency was only slightly important, and jitter was not important at all. However, as voice over IP (VoIP), video, and interactive applications have grown in importance, companies have begun to worry more about latency and jitter. They are finding that extensive network redesign may be needed to give good control over latency and jitter. This may include forklift upgrades for many of its switches and routers.

Test Your Understanding

4. a) What is availability? b) When should you measure error rates? Why? c) What is latency? d) In what units is latency measured? e) Give an example not listed in the text of an application for which latency is bad. f) What is jitter? g) Name an application not listed in the text for which jitter is a problem. h) Why may adding applications that cannot tolerate latency and jitter be expensive?

## Service Level Agreements (SLAs)

When you buy some products, you receive a guarantee that promises that they will work according to specifications and that lays out what the company must do if they do not. In networks, service providers often provide service level agreements (SLAs), which are contracts that guarantee levels of performance for various metrics such as speed and availability. If a service does not meet its SLA guarantees, the service provider must pay a penalty to its customers.

Service level agreements (SLAs) are contracts that guarantee levels of performance for various metrics such as speed and availability.

Figure 4-5: Service Level Agreements (SLA) (Study Figure)

Service Level Agreements (SLAs)

Guarantees for performance

Penalties if the network does not meet its service metrics guarantees

Guarantees Specify Worst Cases (No Worse than)

Lowest speed (e.g., no worse than 100 Mbps)

Maximum latency (e.g., no more than 125 ms)

SLAs are like insurance policies—take effect when something bad happens

Often Written on a Percentage Basis

E.g.: No worse than 100 Mbps 99% of the time

As the percentage increases, cost of engineering increases in order to achieve it

To specify 100% of the time would cost an infinite amount of money

Residential Services Are Rarely Sold with SLA Guarantees

It would be too expensive

Worst-Case Specification.  SLA guarantees are expressed as worst cases. For example, an SLA for speed would guarantee that speed will be *no lower* than a certain amount. If you are downloading webpages, you want at least a certain level of speed. You certainly would not want a speed SLA to specify a *maximum* speed. More speed is good. Why would you want to impose penalties on the network provider for exceeding some maximum speed? That would give them a strong incentive not to increase speed! Making things better is not the SLA’s job.

SLA guarantees are expressed as worst cases. Service will be no worse than a specific number.

For latency, in turn, an SLA would require that latency will be *no higher* than a certain value. You might specify an SLA guarantee of a maximum of 65 ms (milliseconds). This means that you will not get worse (higher) latency.

Percentage-of-Time Elements.  In addition, most SLAs have percentage-of-time elements. For instance, an SLA on speed might guarantee a speed of at least 480 Mbps 99.9% of the time. This means that the speed will nearly always be at least 480 Mbps but may fall below that 0.1% of the time without incurring penalties. A smaller exception percentage might be attractive to users, but it would require a more expensive network design. Nothing can be guaranteed to work properly 100% of the time, and beyond some point, cost grows very rapidly with increasing percentage guarantees.

Corporations versus Individuals.  Companies that use commercial networks expect SLA guarantees in their contracts, despite the fact that engineering networks to meet these guarantees will raise costs and prices. Consumer services, however, rarely have SLAs because consumers are more price sensitive. In particular, residential Internet access service using DSL, cable modem, or cellular providers rarely offer SLAs. This means that residential service from the same ISP may vary widely across a city.

Test Your Understanding

5. a) What are service level agreements? b) Does an SLA measure the best case or the worst case? c) Would an SLA specify a highest speed or a lowest speed? d) Would an SLA specify a highest availability or a lowest availability? e) Would an SLA specify highest latency or lowest latency? f) Would an SLA guarantee specify a highest jitter or a lowest jitter? g) What happens if a carrier does not meet its SLA guarantee? h) If carrier speed falls below its guaranteed speed in an SLA, under what circumstances will the carrier *not* have to pay a penalty to the customers? i) Does residential ISP service usually offer SLA guarantees? Why or why not? j) A business has an Internet access line with a maximum speed of 100 Mbps. What two things are wrong with this SLA?

# Network Design

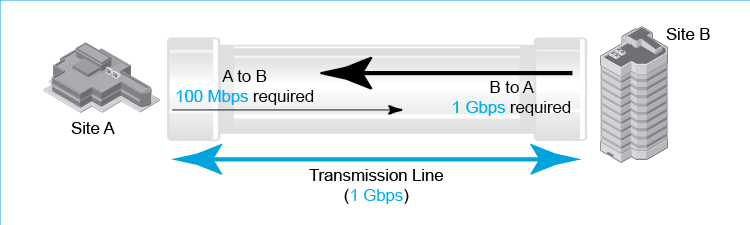
Network design, like troubleshooting, is a core skill in networking. The more you know about networking and your corporation’s situation, the better your design will be. However, if there is something you do not know, your design is likely to be a poor one. Network designers are governed by their worst moments.

## Traffic Analysis

Network design always begins with traffic requirements. Traffic analysis asks how much traffic must flow over each of the network’s many individual transmission links. Figure 4-6 shows a trivial traffic analysis. A company only has two sites, A and B. A needs to be able to transmit to B at 100 Mbps. B needs to be able to transmit to A at 1 Gbps. Transmission links usually are symmetric, meaning that they have the same speed in both directions. Therefore, the company must install a transmission link that can handle 1 Gbps.

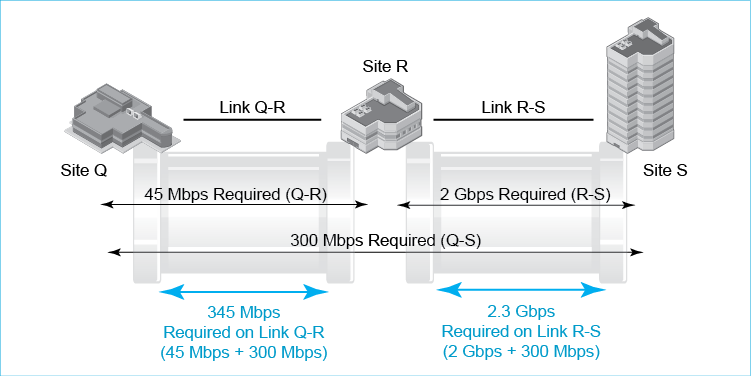
Traffic analysis asks how much traffic must flow over each of the network’s many individual transmission links.

Figure 4-6: Two-Site Traffic Analysis



As soon as the number of sites grows beyond two, traffic analysis becomes challenging. Figure 4-7 shows a three-site traffic analysis. For simplicity, we will assume that transmission is symmetric between each pair of sites.

Figure 4-7: Three-Site Traffic Analysis



The figure shows that Site Q attaches to Site R, which attaches to Site S. Site Q is west of Site R. Site S is east of Site R. Site Q needs to be able to communicate with Site R at 45 Mbps. Site R needs to be able to communicate with Site S at 2 Gbps. Site Q needs to be able to communicate with Site S at 300 Mbps. There are two links—Link Q-R and Link R-S.

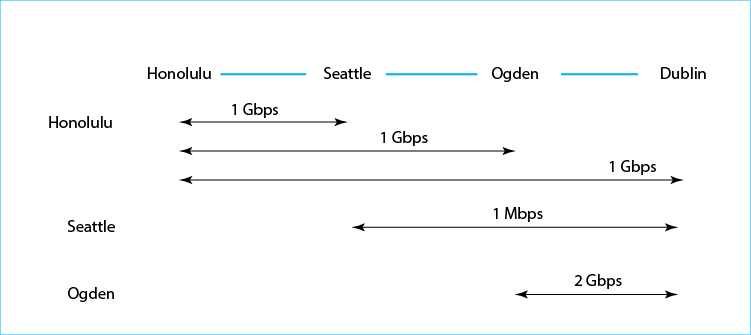
Are you overwhelmed by the last paragraph? Anyone would be! In traffic analysis, it is critical to draw the picture. Figure 4-7 shows how the three sites are laid out and what links connect them. After laying out the sites and links, you draw the three required traffic flows.

Note that the link between Q and R must handle both Q–R traffic (45 Mbps) and the Q–S traffic (300 Mbps). It does not handle any of the traffic between R and S, however. Consequently, Link Q-R must be able to handle 345 Mbps.

Similarly, Link R-S must be able to handle R–S traffic (2 Gbps) and Q–S traffic (300 Mbps). This means that the transmission link between R and S must be able to handle 2.3 Gbps.

Four Sites. Here is another, slightly more complex example. (Master the previous example before doing this one). A company has offices in Honolulu, Seattle, Ogden, and Dublin, Ireland. There are transmission links between Honolulu and Seattle, Seattle and Ogden, and Ogden and Dublin. Honolulu needs to communicate at 1 Gbps with each other site. Seattle and Dublin only need to communicate with each other at 1 Mbps. Ogden and Dublin need to communicate at 2 Gbps. How much traffic will each transmission link have to carry? The analysis in Figure 4-8 shows how to calculate this.

Figure 4-8: A More Complex Traffic Analysis



The first step is to draw a picture showing the sites and transmission lines. Figure 4-8 shows this information at the top.

Next, draw traffic requirements between pairs of sites. Just below the sites and transmission lines, the figure shows traffic from Honolulu to the other three sites. The arrows show speeds and sites being connected. Each connection is one gigabit per second.

Below the Seattle traffic, the figure shows traffic between Seattle and other sites. Traffic flowing between Honolulu and Seattle has been counted in the previous step. Seattle only communicates with Dublin.

Finally, Ogden adds a 2 Gbps transmission link to Dublin. Other Ogden and Dublin pairs have been captured in previous steps.

Once the traffic data has been shown, the next thing to do is examine what traffic must flow over each line. All traffic between Honolulu and other sites passes over the transmission link Honolulu–Seattle. Consequently, this line must have at least 3 Gbps in transmission speed.

Many Sites. If a company has just a few sites, doing traffic analysis calculations manually becomes impossible. Companies use simulation programs that try different options for using links to connect its many sites. For each case, traffic analysis is done on each link. However, you need to understand what the program is doing, and the way to do that is to work through a few examples with only a few sites.

Test Your Understanding

6. Do a three-site traffic analysis for the following two scenarios. a) In Figure 4-8, add traffic of 392 Mbps for Seattle-Ogden traffic. Using a picture like the one in the figure, show your work. b) In Figure 4-7, remove the link between Q and R but add a link between Q and S. Using a picture like the one in the figure, show your work.

## Traffic Requirements versus Leased Lines

If the sites are far apart, they will be connected by leased lines from a telephone carrier. Figure 4-9 shows the most common leased line speeds in the United States. If you need a transmission speed of 30 Mbps between two sites, you cannot lease a 30 Mbps line. You would need a T3 line.

Figure 4-9: Leased Line Speeds in the United States

|  |  |
| --- | --- |
| **Line** | **Transmission Speed** |
| T1 | 1.544 Mbps |
| T3 | 44.7 Mbps |
| OC-3 | 155.58 Mbps |
| OC-12 | 622.08 Mbps |
| OC-48 | 2,488 Mbps |
| OC-192 | 9,953 Mbps |

Test Your Understanding

7. For the preceding three examples and the situations in the previous test-your-understanding question, what leased line would each link require?

## Momentary Traffic Peaks

Traffic volume varies randomly. Consequently, there will *inevitably* be occasional momentary traffic peaks that exceed capacity. These only last milliseconds or a second or two, but they can be disruptive. Traffic will be delayed, creating latency. Some traffic may even be discarded. Figure 4-10 shows three ways to deal with momentary traffic peaks.

Figure 4-10: Addressing Momentary Traffic Peaks

|  |  |  |  |
| --- | --- | --- | --- |
| Lack of Capacity | Amelioration | Description | Considerations |
| Chronic | Add more capacity | As it sounds. | There is no choice. |
| Momentary (milliseconds to a few seconds) | Add more capacity | As it sounds. | Expensive in terms of transmission cost.  But no ongoing management labor. |
|  | Prioritize traffic | Send higher-priority traffic through first. | Delay-intolerant high-priority traffic such as voice gets through immediately.  Delay tolerant traffic such as e-mail will get lower priority, so if it is delayed briefly, harm is minimal.  Requires ongoing management labor. |
|  | Give QoS guarantees | QoS guaranteed capacity for certain traffic | Like reserved seating in a sports stadium.  Traffic with a QoS guarantee will absolutely get through, up to the amount of capacity reserved.  Other traffic only gets what is left over—even if the guaranteed traffic is not using its capacity. |

Chronic Lack of Capacity.  Although we are dealing with momentary lack of capacity, it is important realize that this is not the same thing as chronic lack of capacity, when a network is overloaded a considerable amount of time. This is like traffic jams on a freeway. The only way to address a chronic lack of capacity is to add more capacity. Taxpayers may tolerate congested freeways, but networked applications cannot. Chronic lack of capacity is a sign of very poor management.

The only way to address a chronic lack of capacity is to add more capacity.

Adding More Capacity.  Figure 4-9 shows three techniques for addressing momentary traffic peaks. The first is to add more capacity. Ideally, one would add enough more capacity to eliminate momentary traffic peaks entirely. Given the nature of randomness, momentary traffic peaks will still occur sometimes, but they will be rare and far shorter in duration. Adding more capacity will be expensive in terms of transmission facilities, but it adds no ongoing management labor. Given the cost of labor, this is often a good tradeoff.

Priority.  A second approach to dealing with momentary traffic peaks is to assign a priority level to frames or packets, based on their tolerance for latency and loss. Voice over IP is extremely latency intolerant. Any noticeable delay will be compromise the user experience substantially. On the other hand, e-mail can easily tolerate a delay of several seconds. Consequently, VoIP frames and packets get high priority, so that they will get through immediately. E-mail gets low priority because a delay of a few seconds is not a problem in e-mail. All switches and routers in corporations come with the ability to use priority, so priority does not increase capital expense. Priority makes momentary traffic peaks tolerable to all types of uses, unless the peak is quite long. On the negative side, assigning priority to different applications and managing priority on switches and routers requires considerable ongoing management labor, which is expensive.

Momentary traffic peaks can be addressed by assigning a priority level to frames or packets, based on their tolerance for latency and loss.

Quality of Service Guarantees.  An extreme approach is to give QoS guarantees to certain traffic flows such as VoIP. Regardless of momentary traffic peaks, this traffic will always get through. It is like having season ticket seats for a sports team. To provide QoS guarantees, the company must allocate reserved capacity on each switch, router, and transmission line. This is great for traffic flows with QoS guarantees. However, it means that all other traffic only gets what is left over, even if the reserved capacity is not being used.

QoS guarantees reserve capacity for certain traffic flows such as VoIP. Regardless of momentary traffic peaks, this traffic will always get through.

Test Your Understanding

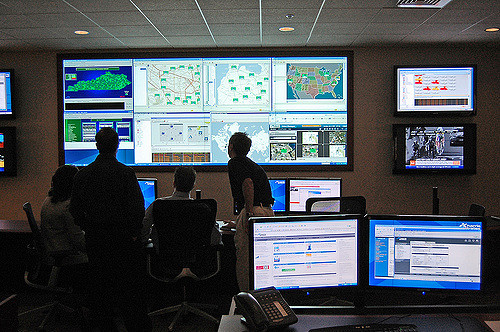
8. a) Distinguish between chronic lack of capacity and momentary traffic peaks. b) How long do momentary traffic peaks last? c) What two problems do they create? d) What three choices do you have for reducing the impact of delays for latency intolerant traffic? e) What is the advantage of each compared to the others? f) What is the disadvantage of each compared to the others? g) Compared to e-mail and voice over IP, what priority would you give to network control messages sent to switches and routers? (The answer is not in the text.) Explain your reasoning.

# Centralized Network Management

Given the complexity of networks, network managers need to turn to network management software to support much of their work. Many of these are network visibility tools, which allow managers working at computers in centralized network operation centers (NOCs) to comprehend (and sometime change) what is going on throughout their networks.

Network visibility tools allow managers working at computers comprehend (and sometime change) what is going on throughout their networks.

Figure 4-11: Centralized Network Management at a Network Operations Center (NOC)



Network visibility tools are critical in large and distributed networks. If a network manager had to travel to each device and transmission line to collect operating data for diagnosis when problems occurred or because he or she wished to optimize the network, the cost would be prohibitive. Network visibility tools and network management tools in general, are costly to purchase and require considerable labor to operate, they save more money than they cost.

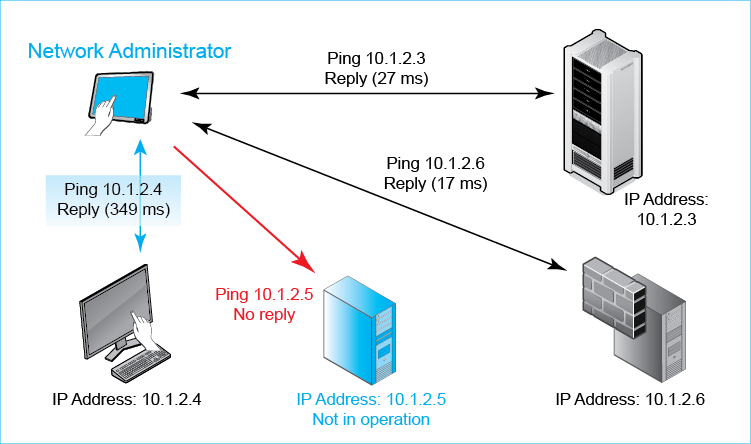
Test Your Understanding

9. a) What do network visibility tools allow a manager to do? b) Why do they save money? c) Do they cost more money than they save?

## Ping

The oldest network visibility tool is the basic ping command available in all operating systems. If a network is having problems, a network administrator can simply ping a wide range of IP addresses in the company. When a host receives a ping, it should send back a reply. If it replies, it is obviously in operation. If it does not, it may not be. In Figure 4-12, host 10.1.2.5 does not respond to its ping. This signals a potential problem.

Figure 4-12: Ping



By analyzing which hosts and routers respond or do not respond, then drawing the unreachable devices on a map, the administrator is likely to be able to see a pattern that indicates the root cause of the problem. Of course, manually pinging a wide range of IP addresses could take a prohibitive amount of time. Fortunately, there are many programs that ping a range of IP addresses and portray the results.

Even if a host responds, you must check the latency. If it is substantial, there may be communication problems that need to be solved. This appears to be the case with Host 10.1.2.4. Another network visibility too, traceroute, lets you see latency between each jump between routers along the route. Subtracting the total latency between adjacent pairs of routers can help you determine where a latency problem lies.

Figure 4-13: Traceroute

|  |  |
| --- | --- |
| **Router** | **Latency (ms)** |
| 1 | 1 |
| 2 | 7 |
| 3 | 7 |
| 4 | 7 |
| 5 | 8 |
| 6 | 10 |
| 7 | 12 |
| 8 | 13 |
| 9 | 29 |
| 10 | 34 |
| 11 | 38 |
| 12 | 110 |
| 13 | 111 |
| 14 | 111 |
| 15 | 111 |
| 16 | 114 |
| 17 | 117 |
| 18 | 117 |

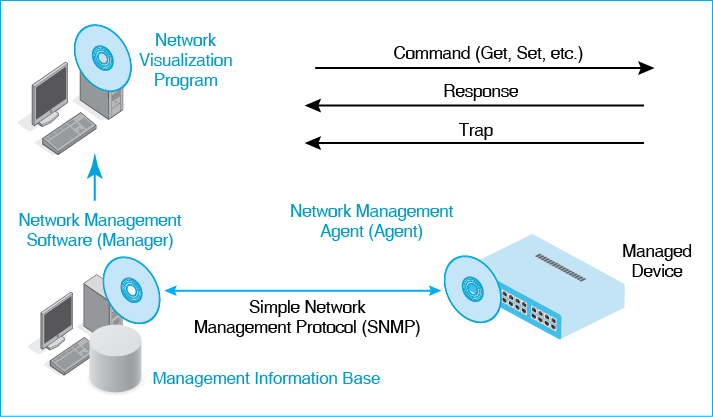
Test Your Understanding

10. a) If you ping a host and it does not respond, what can you conclude? b) What *two* things does ping tell you about a host that replies? c) If a router fails, how can you diagnose this with ping? d) Distinguish between ping and traceroute. e) In Figure 4-13, what jump causes the most latency? Show your calculations as a table.

## The Simple Network Management Protocol (SNMP)

Ping can tell you if a host is reachable and, if so, the round-trip latency in communicating with that host. Although this is useful information, it is extremely limited. For remote device management, network operation centers also use more powerful network visualization products based on the simple network management protocol (SNMP), which is illustrated in Figure 4-14. In the network operations center, a computer runs a program called the manager. This manager works with a large number of managed devices, such as switches, routers, servers, and PCs.

Figure 4-14: Simple Network Management Protocol (SNMP)



Agents.  Actually, the manager does not talk directly with the managed devices. Rather, each managed device has an agent, which is hardware, software, or both. The manager talks to the agent, which in response talks to the managed device. To give an analogy, recording stars have agents who negotiate contracts with studios and performance events. Agents provide a similar service for devices.

Get Commands and the Management Information Base (MIB).  The network operations center constantly collects data from the managed devices using SNMP Get commands. It places this data in a management information base (MIB). Data in the MIB allows the network operation center managers to understand the traffic flowing through the network. This can include failure points, links that are approaching their capacity, or unusual traffic patterns that may indicate attacks on the network.

Set.  In addition, the manager can send Set commands to the switches and other devices within the network. Set commands can reroute traffic around failed equipment or transmission links, reroute traffic around points of congestion, or turn off expensive transmission links during periods when less expensive links can carry the traffic adequately.

Trap.  Normally, the manager sends a command and the agent responds. However, if the agent senses a problem, it can send a Trap command on its own initiative. The trap command gives details of the problem.

Network Visualization Program.  There is one more program in the figure—a network visualization program. This program takes results from the MIB and interprets the data to display results in maps, find root causes for problems, and do other tasks. Note that this functionality is *not* included in the simple network management protocol. SNMP simply collects the data in a way that network visualization programs can use. This lack of specification allows network visualization program vendors to innovate without being constrained by standards.

Automation.   Many other network management chores can be automated to reduce the amount of work that network managers need to spend on minutia. For example, many routers are given a standard corporate configuration when they are installed. Doing this manually can take an hour or more per router. However, it may be possible to create a standard configuration, store it, and simply download it onto new routers. In addition, if corporate standard configurations change or a patch must be installed on all routers, it may be possible simply to “push out” these changes to all routers. Automation saves a great deal of expensive labor.

Test Your Understanding

11. a) List the main elements in SNMP. b) Does the manager communicate directly with the managed device? Explain. c) Distinguish between Get and Set commands. d) Where does the manager store the information it receives from Get commands? e) What kind of message can agents initiate? f) Why is network automation important? g) What does a network visualization program do? h) Why is the ability to push changes to remote devices useful?

# Security Management

## Security Is a Management Issue

People tend to think of security as a technology issue, but security professionals know that security is primarily a management issue. Unless a firm does excellent planning, implementation, and day-to-day execution, the best security technology will be wasted. As noted earlier, security is a process, not a product. Unless firms have good security processes in place, the most technologically advanced security products will do little good.

Security is primarily a management issue, not a technology issue.

One thing that sets security management apart from other aspects of network management and IT management in general is that the security team must battle against *intelligent adversaries*, not simply against human mistakes and technical unreliability. Companies today are engaged in an escalating arms race with attackers, and security threats and defenses are evolving at a frightening rate.

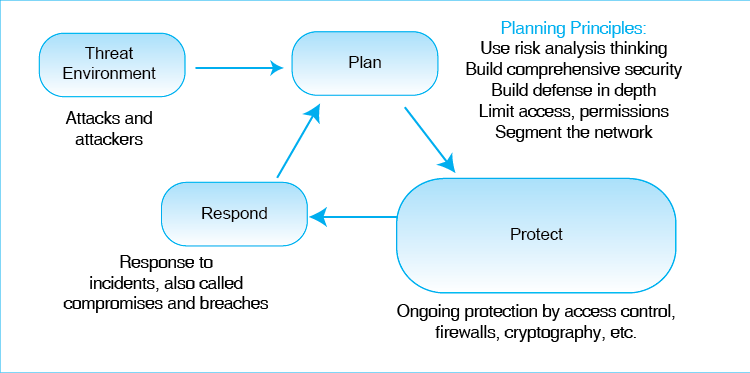
Test Your Understanding

12. a) Why is security primarily a management issue, not a technology issue? b) What sets security management apart from other aspects of network management and IT management in general?

## The Plan–Protect–Respond Cycle

Figure 4-15 shows the overall process that companies follow to deal with threats. On the left is the threat environment, which consists of the attackers and attacks the company faces. We looked at the threat environment in Chapter 3.

Figure 4-15: The Threat Environment and the Plan-Protect-Respond Cycle



The rest of the figure illustrates how companies mount their defenses against the threats they face. The figure shows that companies constantly cycle through three phases of security management. This is the plan–protect–respond cycle.

Planning.  In the plan phase, companies assess the threat environment and decide how they will meet these threats. Investors invest in a portfolio of investments that will give the maximum yield for the amount invested. Companies must do the same for security, selecting a portfolio of security projects that will give the highest results from their limited security budgets. In our discussion of the planning stage, we will focus on core principles that companies adopt to make their planning effective.

Protecting.  In the protect phase, companies provide actual protections on a day-to-day basis. We looked at protections such as firewalls in Chapter 3. In Figure 4-15, the protect phase bubble is larger than the other three. This emphasizes the fact that the protect phase is much larger than the other two phases in terms of time spent and resource expenditure. However, without extensive and insightful planning, it is possible to spend a great deal of time and effort mounting protections without being very effective.

Responding.  In the response phase, the company must respond when it suffers a successful security attack. We call successful attacks compromises, incidents, or breaches. It would be nice if compromises never occurred. In fact, they will. Like fire departments, security teams must respond immediately and effectively. This requires careful planning and rehearsal because every second counts in reducing the cost of breaches.

Test Your Understanding

13. a) What happens in each stage of the Plan–Protect–Respond cycle? b) Which stage consumes the most time and resources?

# Security Planning Principles

Perhaps more than any other aspect of IT, effective security depends on effective planning. Security planning is a complex process that we can discuss only briefly. We will focus on some key planning principles that must be observed in all security thinking. Figure 4-16 summarizes these security planning principles.

Figure 4-16: Seven Security Planning Principles

|  |  |  |
| --- | --- | --- |
| Principle | Description | Category |
| Apply risk analysis thinking | You cannot stop every threat  Even if possible, it would cost far more to do so than the losses it would avoid  Protect to the extent that is economical  Risk management, not risk elimination | Overall |
| Provide comprehensive security | Close all avenues of attack to each resource | Broad design principles |
| Provide defense in depth | Create a series of countermeasures the attacker must overcome  If one fails, still protected |
| Limit access with minimum permissions | Just because authenticated, do not give permission to do anything desired  Limit permissions to the minimum permissions needed to do the job | Access control principles |
| Segment the network | Give different parts of the network different access and permissions for different people  Prevent someone from jumping from an unsecure segment to a secure segment |
| Identify and protect single points of takeover | Single resources that can control much of the network or network security. (SNMP, e.g.)  Identify and harden extremely well. | Analysis of vulnerabilities |
| Identify and protect weakest links, | A weakest link is a failure point that would give the attacker access even if everything else works well  Identify each weakest link, harden it as far as possible, and check it frequently. |

## Apply Risk Analysis Thinking

Many believe that the goal of security is to stop all threats to the corporation. Surprisingly, that is not true. Stopping all attacks is impossible. Despite strong security efforts, there will still be some risk of a compromise. There has always been crime in society, and there always will be. The same is true of security incidents. No matter how much money a company spends on security, it cannot stop all threats. It would go bankrupt trying. Rather, the goal of security is to reduce the risk of attacks to the extent that is economically feasible.

The goal of security is to reduce the risk of attacks to the extent that is economically feasible.

Risk analysis is the process of balancing risks and protection costs. Corporate security planners have to ask whether investing in a countermeasure against a particular threat is economically justified. For example, if the probable annual loss from a threat is $10,000 but the security measures needed to thwart the threat will cost $200,000 per year, the firm obviously should *not* spend the money. Instead, it should accept the probable loss.

Risk analysis is the process of balancing risks and protection costs.

Figure 4-17 gives an example of a risk analysis for a hypothetical situation. Without a countermeasure, the damage per successful attack is expected to be $1,000,000, and the annual probability of a successful attack is 20%. Therefore, the annual probable damage is $200,000 without a countermeasure. The probable net annual outlay therefore is $200,000 if no action is taken.

Figure 4-17: Risk Analysis Calculation

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Countermeasure | | |
| None | A | B |
| Damage in Successful Attack | $1,000,000 | $500,000 | $1,000,000 |
| Annual Probability | 20% | 20% | 15% |
| Annual Probable Damage | $200,000 | $100,000 | $150,000 |
| Annual Cost of Countermeasure | $0 | $20,000 | $60,000 |
| Annual Outlay | $200,000 | $120,000 | $210,000 |
| Countermeasure Value | NA | $80,000 | (10,000) |

Countermeasure A cuts the damage from a successful attack in half.

Countermeasure A does not reduce the annual probability of a compromise.

Countermeasure B does not reduce the damage from a successful attack.

Countermeasure B reduces the probability of a successful attack by a quarter.

Countermeasure A is designed to cut the damage of a successful attack in half. So the damage per successful attack is expected to be $500,000 instead of a million dollars. The countermeasure will not reduce the probability of a successful attack, so that continues to be 20%. With Countermeasure A, then, the annual probable damage will be $100,000. However, the countermeasure is not free. It will cost $20,000 per year. Therefore, the net annual probable outlay is $120,000 with the countermeasure.

Countermeasure A, then, will reduce the net annual probable outlay from $200,000 to $120,000. The countermeasure has a value of $80,000 per year. This is positive, so Countermeasure A is justified.

There is also a second candidate countermeasure, Countermeasure B. This countermeasure will reduce the probability of a successful attack by 25%, from 20% to 15%. The loss would not be reduced at all. This countermeasure would cost $60,000 annually, giving a net annual probable outlay of $210,000. This exceeds the no-countermeasure’s figure of $200,000. The annual probable outlay is negative $10,000 if the countermeasure is used. This countermeasure would not make sense even if it was the only candidate countermeasure.

Security professionals may be tempted to think of costs in terms of hardware and software spending. However, most countermeasures require extensive security labor. In fact, labor is often the biggest cost. More broadly, security often increases labor costs for users. If users spend even a few extra minutes each time they must use a particular resource, this can lead to substantial cost. It could tip the scales against installing the countermeasure.

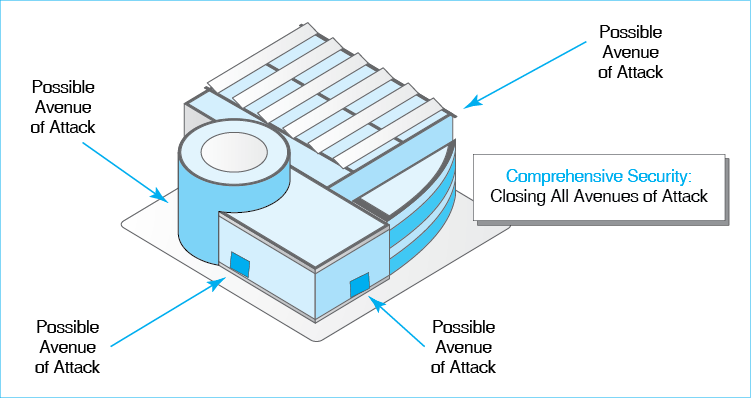
Test Your Understanding

14. a) Comment on the statement, “The goal of security is to eliminate risk.” b) Why do you think Target did not take action to protect its POS terminal? c) Repeat the risk analysis in Figure 4-11, this time with Countermeasure C, which reduces damage severity by a quarter and the likelihood of attack by 75%. The annual cost of Countermeasure C is $175,000. Show the full table. What do you conclude? Justify your answer.

## Provide Comprehensive Security

To be safe from attack, a company must close off *all* avenues of attack. Figure 4-18 illustrates this principle. In contrast, an attacker only needs to find one unprotected avenue to succeed. Although it is difficult to achieve comprehensive security, it is essential to come as close as possible.

Figure 4-18: Comprehensive Security



Comprehensive security is closing off all avenues of attack.

Test Your Understanding

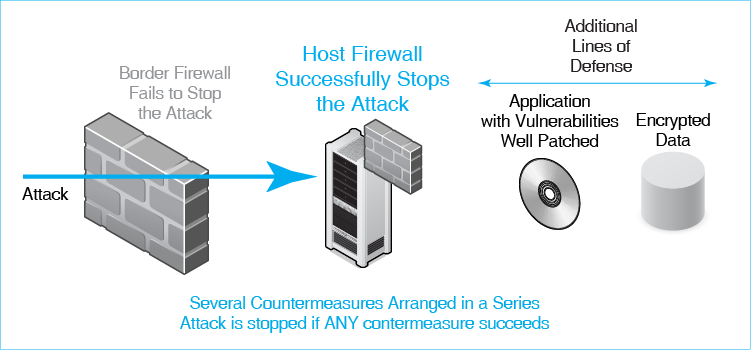
15. a) What is comprehensive security? b) Why is it important? c) Which avenues into and out of its network did Target fail to protect adequately? d) Give your own example of a failure in comprehensive security.

## Provide Defense in Depth

Another critical planning principle is defense in depth. Every protection will break down occasionally. If attackers have to break through only one line of defense, they will succeed during these vulnerable periods. However, if an attacker has to break through two, three, or more lines of defense, the breakdown of a single defense technology will not be enough to allow the attacker to succeed. Having successive lines of defense that must *all* be breached for an attacker to succeed is called defense in depth. Figure 4-19 illustrates the principle.

Having several lines of defense that must all be breached for an attacker to succeed is called defense in depth.

Figure 4-19: Defense in Depth



Defense in depth is a way to increase security by having a series of protections so a single failure will not compromise security. In contrast, many *individual protections* consist of a series of internal steps that must *all* work if the protection is to succeed. If one fails, the countermeasure fails. For example, an antivirus program may protect a user by identifying a malicious attachment. However, if the user fails to use good judgment and opens the attachment anyway, there is no protection.

In the figure, there are four protections in succession. The first is a border firewall at the connection between the company site and the Internet. The second is a host firewall on a particular server. The third is the use of good practice in patching application vulnerabilities. The fourth is encrypting all data for confidentiality so that the attacker cannot read sensitive information even all if other defenses fail.

The figure shows what happens if the border firewall does not stop an attack. In this case, the host firewall catches the attack and stops it. The company should fix the border firewall quickly, so that it becomes part of the effective defense, but attack packets will not get through to the target data while the border firewall is being fixed.

Test Your Understanding

16. a) What is defense in depth? b) Why is defense in depth necessary? c) Give your own example of defense in depth inside or outside of networking.

## Limit Access with Minimum Permissions

Security planners constantly worry about access to resources. People who get access to resources can do damage to those resources. Not surprisingly, companies work very hard to control access to their resources. Access control is limiting who may have access to each resource and limiting his or her permissions when using the resource.

Access control is limiting who may have access to each resource and limiting his or her permissions when using the resource.

Figure 4-20: Least Permissions in Access Control

Access Control

If attackers can’t get access to a resource, they cannot exploit it

Access control is limiting who may have access to each resource

And limiting his or her permissions when using the resource

Authentication versus Authorizations (Permissions)

Authentication: Proof of identity

Authorizations: Permissions a particular authorized user is given with a resource

Just because a user is authenticated does not mean that he or she will be permitted to do everything

Principle of Least Permissions

Give each authenticated user only the minimum permissions he or she needs to do his or her job

Cannot compromise security by doing unauthorized things

Examples of Limited Permissions

Create files but not delete files

Cannot access files above a specified level of sensitivity

Read files but not edit them

See files in own folder but not in other folders

Connect to the person’s department server but not to the Finance server

Do certain things but cannot give others permission to do them

One aspect of access control that we saw in the previous chapter is authentication, which is requiring users requesting access to prove their identities. However, just because you know who someone is does not mean that he or she should have unfettered access to your resources. (There undoubtedly are several people you know whom you would not let drive your car.)

Authorizations or permissions are the actions that an authenticated user is allowed to take on the resource. For example, although everyone is permitted to view the U.S. Declaration of Independence, no one is allowed to add his or her own signature at the bottom.

Authorizations or permissions are the actions that an authenticated user is allowed to take on the resource.

An important principle in assigning permissions is to give each person least permissions—the minimum permissions that the user needs to accomplish his or her job. In the case of access to team documents, for example, most team members may be given read-only access, in which the user can read team documents but not change them. It is far less work to give the user extensive or full permissions so that he or she does not have to be given additional permissions later. However, it is a terrible security practice. If even one unnecessary permission is assigned to a person, this may be a security risk.

Least permissions are the minimum permissions that the user needs to accomplish his or her job.

Figure 4-20 shows some examples of limited permissions for particular resources. These resources include files, folders, servers, and network elements. To know what resources should be assigned to different individuals and groups, you must understand how each resource should be used.

Test Your Understanding

17. a) Distinguish between authentication and authorizations. b) What is another term for authorizations? c) What is the principle of least permissions? d) Why is it important? e) To assign least permissions to someone, what must you know? f) Give your own example of a least permissions inside or outside of networking.

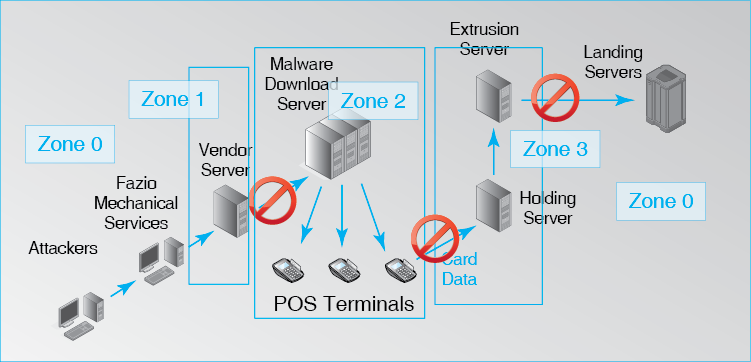
## Segment the Network

In a building, there are many areas. Each will have different requirements for authentication and authorizations. In addition, travel between one area and another may require further authentication and authorizations, such as doors requiring security cards.

Figure 4-21 shows that the same is true in networks. This network segmentation hypothetically divides the Target situation into four zones.

* Zone 0 is the world outside Target. The other three are internal.
* Zone 1 is a medium-security zone for the vendor server and other assets that require good security but not the highest security.
* Zone 2 is a high-security zone that contains the POS system and other high-risk assets. It has the individual POS terminals as well as the POS download server and connections between them.
* Zone 3 has medium-high security hosts of various types.

Figure 4-21: Segmenting the Network



There should be a strong default policy banning communication between assets in different zones, and this policy should be enforced by strong technology. While exceptions must be possible, these should be limited, with each exception considered carefully. Unauthorized communications between zones should be monitored diligently and treated as transmissions requiring immediate attention.

Figure 4-21 illustrates how this hypothetical zone structure might have helped Target. Connections between Zone 0 devices and Zone 1 devices are likely to be the most common form of inter-zone communication. At Target, a compromised Fazio Mechanical Services computer is suspected of having logged into the vendor server. Stronger authentication such as two-factor authentication might have made such connections unlikely.

The break-in probably required a connection between a Zone 1 computer and a Zone 2 host, most likely to the POS update server. This inter-zone connection should have been impossible by default, and it should have generated a strong alert. Within Zone 2, furthermore, all connections should have been required very strong security. The POS terminals, for instance, might have been given a white list of downloads that they would accept. The malware program would not have been on that whitelist.

Zone 3 would have the holding and extrusion servers (assuming that they were not in Zone 2). They should never have been allowed to communicate with the outside world in Zone 0 without a specific exception being granted.

This hypothetical example of network segmentation demonstrates how good network segregation might have been able to break the kill chain at Target. If a single link in the exploitation process had been stopped, the attackers would have failed. Of course, network segmentation is difficult and is never complete, but by making each exploit more difficult and noisy and by providing defense in depth, even incomplete network segmentation is powerful.

Test Your Understanding

18. a) Why is it important to segment different parts of the network and provide access control limits on each path between segments? b) How would network segmentation have stopped the attack on Target? Be specific. c) Give your own example of segmenting communication to provide security inside or outside of networking.

## Identifying and Protecting Single Points of Takeover and Single Points of Failure

In some cases, if an attacker can take over or damage a single resource, he or she can take control of a critical set of resources.

* The SNMP manager is a good example of a single point of takeover. If an attacker compromises this computer, he or she can use the powerful Set command to reconfigure network components in ways needed to take over a target resource or even to cause the network to collapse in chaos.
* A border firewall can be an example of a single point of failure. If a border firewall put out of service in an attack, the firm must either suspend communication to the outside world or permit communication without a firewall.

It is important for firms to identify possible single points of takeover and single points of failure. Until it identifies them, it cannot give them the protection they deserve. This level of protection must be very high.

Test Your Understanding

19. a) Come up with an example of a single point of takeover inside or outside of networking. b) Come up with an example of a single point of failure inside or outside of networking.

## Identifying and Protecting Weakest Links

In defense in depth, we have seen that an attack has have to break through several countermeasures to succeed. Failure at a single point destroys the kill chain. In some cases, in contrast, a single countermeasure may have multiple components, each of which must succeed to stop an attack. A firewall, for example, can only succeed in frustrating attack if it is the right kind of firewall, if it is configured properly, if it is constantly updated, and if its log files are read frequently to detect new attacks. If one of these components is done wrong, attacks will continue. For example, if an SPI firewall administrator opens Port 80 access to any internal server running the protocol instead of just permitting HTTP connections to a few known and approved webservers, this will allow many attacks to succeed.

Figure 22: Defense in Depth versus Weakest Links

|  |  |  |
| --- | --- | --- |
|  | **Defense in Depth** | **Weakest link** |
| Number of Countermeasures Involved | Several arranged in series | One, with several components |
| Criterion for Effective Defense | Only one must succeed to stop attacks | All components must succeed to avoid a compromise |

Test Your Understanding

20. a) What are the two things that distinguish defense in depth from weakest links? b) Come up with an example of a weakest link inside or outside of networking.

# Conclusion

## Synopsis

This is the last of four introductory chapters. In this chapter, we looked at network and security management. Technology is never enough. How well people manage the firm’s networks and security makes all the difference in the world.

Networks today must work well. Networks must meet goals for quality-of-service (QoS) metrics. We looked at speed, availability, error rates, latency, and jitter. After discussing individual QoS metrics, we looked at service level agreements (SLAs), which guarantee performance levels for QoS metrics, usually for a certain percentage of time. Many find it confusing that QoS metrics specify that service will be *no worse* than certain values. For example, SLAs will specify a minimum speed, not a maximum speed.

Designing networks is a complex process. We looked at basic principles of traffic analysis, which identifies the traffic that various transmission links must sustain, including redundancy in case of link failures. We also looked at strategies for addressing the common problem of momentary traffic peaks that exceed the network’s capacity.

We next looked at centralized management. By simplifying and automating many actions, centralized management prevents labor costs from increasing as rapidly as the number of networking and security devices. We began with ping, which is in the toolbox of every network administrator. Advanced network management depends heavily on the Simple Network Management Protocol (SNMP).

Security management follows the plan–protect–respond cycle. Planning prepares the company for day-to-day protection both now and in the future. Response happens when protections break down, as they inevitably do. Of course, experience in managing protections and responses feeds back into the planning process.

Strategic security planning uses the following planning principles that must be considered in every project plan:

* *Adopt Risk Analysis Thinking*. The purpose of security is to reduce risk to a degree that is economically justified.
* *Provide Comprehensive Security*. Stop all avenues of attack.
* *Provide Defense in Depth*. Make the attacker overcome multiple countermeasures to succeed.
* *Limit Access with Minimum Permissions.* Make it hard to get access to resources, and give those with access minimum capabilities to use the resource, consistent with their jobs.
* *Segment the Network.* Divide the network into zones with different security and strongly limit and manage inter-zone communication.
* *Identify and Protect Single Points of Takeover.* This type of takeover allows attacker to do extensive damage by taking over a single resource and using it to cause misbehavior in it and other parts of the network.
* *Identify and Protect Single Points of Failure.* This type of attack attacker to do extensive damage by causing an important resource to fail.

## End-of-Chapter Questions

Thought Questions

4-1. Your home is connected to the Internet. You get to create SLAs that the ISP must follow. Being reasonable, write SLAs you would like to have for the following things: a) Write an SLA for speed. b) Write an SLA for availability. c) Write an SLA for latency. **Do not just say what each SLA should include; actually write the SLAs as the ISP would write them in the form of specific guarantees**. **Failure to do this will result in a substantial grading penalty.**

4-2. Redo the analysis in Figure 4-8. Remove the link between Ogden and Seattle but add a link between Seattle and Dublin.

4-3. a) Suppose that an attack would do $100,000 in damage and has a 15% annual probability of success. Spending $11,000 per year on Countermeasure A would cut the annual probability of success in half and reduce the damage of a successful attack by 25%. Do a risk analysis to compare benefits and costs. Show your work clearly. b) Should the company spend the money? Explain. c) What is the maximum a company should be willing to pay for Countermeasure A?

|  |  |  |
| --- | --- | --- |
|  | Base | A |
| Damage | $100,000 | $75,000 |
| Annualized Rate of Occurrence | 15% | 7.5% |
| Annualized Damage | $15,000 | $5,625.0 |
| Annualized Cost of Countermeasure | | $11,000 |
| Outlay | $15,000 | $16,625.0 |
|  |  |  |
| Damage | $100,000 | $75,000 |
| Annualized Rate of Occurrence | 15% | 7.5% |
| Annualized Damage | $15,000 | $5,625.0 |
| Annualized Cost of Countermeasure | | **$9,375** |
| Outlay | $15,000 | $15,000 |

4-4. An executive opened an e-mail attachment because the content looked like it came from a subordinate. In addition, the executive knew that the company did antivirus filtering. Actually, this was a spear phishing attempt, and the attachment contained malware. What security planning principle does this breakdown represent?

4-5. Edward Snowden, a server administrator, was able to copy many CIA secret and top secret files to a USB RAM stick. What security planning principle breakdown allowed this?

4-6. For the following table, list the security planning principle involve in each example and justify your choices. More than one principle may be involved.

|  |  |  |
| --- | --- | --- |
| **Example** | **Principle** | **Justification** |
| Deciding whether to place a combination lock on the door to the computer center. |  |  |
| Protecting a building with many entry points. |  |  |
| Two-factor authentication for a debit card—the card itself and a PIN |  |  |
| Parental controls on a television |  |  |
| Compromising a client PC’s password. |  |  |
| Failing to sanction an employee for tailgating—following another employee through a door without swiping his or her access card. |  |  |
| Taking over a firm’s login system. |  |  |
| Failing to update antivirus signatures. |  |  |
| In a public storage facility, the elevator has a different combination for each customer. It will only take the person to the floor that contains his or her storage locker. |  |  |
| Attacking your systems itself in order to identify vulnerabilities before attackers can. |  |  |
| Compromising a border firewall. |  |  |

Perspective Questions

4-7. What was the most surprising thing you learned in this chapter?

4-8. What was the most difficult part of this chapter for you?

1. Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack, “Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It”, *Bloomberg Businessweek*, March 13, 2014. *http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data*. [↑](#footnote-ref-1)
2. Aviv Raff, “PoS Malware Targeted Target,” *Seculert*, January 16, 2014. *http://www.seculert.com/blog/2014/01/pos-malware-targeted-target.html*. [↑](#footnote-ref-2)
3. Jim Finkle and Mark Hosenball, “Exclusive: More Well-Known U.S. Retailers Victims of Cyber Attacks – Sources,” *Reuters*, January 12, 2014. *http://www.reuters.com/article/2014/01/12/us-target-databreach-retailers-idUSBREA0B01720140112*. [↑](#footnote-ref-3)
4. Danny Yadron, Paul Ziobro, Devlin Barrett, “Target Warned of Vulnerabilities Before Data Breach,” *The Wall Street Journa*l, February 14, 2014. *http://online.wsj.com/news/articles/SB10001424052702304703804579381520736715690.* [↑](#footnote-ref-4)
5. Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, Lockheed Martin, 2011. http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf. [↑](#footnote-ref-5)
6. Ben Schneier, Computer Security: Will We Ever Learn? Crypto-Gram Newsletter, May 15, 2000. https://www.schneier.com/crypto-gram-0005.html. [↑](#footnote-ref-6)
7. The impact of even small error rates can be surprisingly large. TCP tries to avoid network congestion by sending TCP segments slowly at the beginning of a connection. If these segments get through without errors, TCP sends the following segments more quickly. However, if there is a single error, the TCP process assumes that the network is overloaded. It falls back to its initial slow start rate for sending TCP segments. This can produce a major drop in throughput for applications. [↑](#footnote-ref-7)
8. The technical term for jitter is IP packet delay variation, but jitter is almost always used to designate the phenomenon. RFC 3393 describes how jitter can be measured. Do not attempt to read it unless there is headache medicine nearby. [↑](#footnote-ref-8)