Introduction to Designing Security for a Windows 2000 Network

CERTIFICATION OBJECTIVES

1.01 What is Designing Security for a Windows 2000 Network?
1.02 Overview of Exam 70-220
1.03 What We’ll Cover in This Book
1.04 What You Should Already Know

Two-Minute Drill

Q&A

Self Test
Welcome to Windows 2000 and one of Microsoft’s most important new elective topics for the Windows 2000 Microsoft Certified Systems Engineer (MCSE) certification track. With almost universal connectivity becoming a reality, and horror stories of hacker invasions making the front page of the newspaper on a regular basis, security is on the minds of everyone involved in computer networking today. Microsoft has recognized and addressed these concerns in designing Windows 2000. Understanding how to create a secure network environment is essential to performing the duties of an administrator in today’s business world, and should be mastered by those intending to work as a certified systems engineer in any organization that deals in any way with sensitive or confidential information.

Exam 70-220 is one of the three Design electives, along with Designing a Windows 2000 Network Infrastructure and Designing a Windows 2000 Directory Services Infrastructure. You are required to pass one of the three in order to complete the Windows 2000 certification track. Because there is a growing market for security specialists, the Security Design exam is an excellent choice for enhancing your marketability in the workplace. Others will choose this exam as their Design elective because it is the only one of the three that explores a new topic area not covered in any of the four core exams. (Directory services and network infrastructures are the subject of both an implementing/administering core and a designing elective, whereas this is the only exam that focuses on security issues.)

This exam covers a wide range of security-related topics, encompassing concepts that are part of Active Directory as well as those involved in designing and implementing the network infrastructure. For that reason, we recommend you first study and test on the core topics, prior to tackling this Design exam. This might, at first glance, seem to be a backward approach; after all, you must design the security for a network before you implement and administer the network. However, Microsoft sees the Design exams as topics requiring a higher level of knowledge and expertise, with the ability to gather the appropriate data, analyze and evaluate requirements and specifications, and conceptualize the “big picture” being the task of a true enterprise architect, a step beyond the duties of the engineer in the field who carries out those plans after they’ve been formulated.

Correlation Between the Windows 2000 and NT 4.0 Exams

Although it is possible to draw some sort of correlation between the Windows 2000 core exams and their Windows NT 4.0 counterparts (for instance, the Windows 2000 Professional and Windows NT Workstation exams, or the two Server exams,
What is Designing Security for a Windows 2000 Network?

or even the combination of Networking Essentials and TCP/IP compared to the Implementing and Administering a Network Infrastructure exam), it is impossible to map the Windows 2000 Design exams to anything in the Windows NT MCSE certification track.

You can expect the question format to be significantly different from the Windows NT 4.0 exams. The Design exams, especially, are expected to include case study questions that will require the exercise of analytical skills to a degree not found in more traditional question formats.

Purpose of the Design Exams

It has been rumored that the design exams are part of a long-range plan by Microsoft to create an “upper tier” MCSE certification, perhaps conferring the title enterprise architect. Whether or not this occurs, it is obvious that the company desires to raise the bar for the Microsoft Certified Systems Engineer certification itself, making it more difficult for the so-called “dumpers and crammers” (those who memorize test questions and answers from “brain dumps” distributed on the Internet or who cram “quick review” books as their primary source of study for the exams) to pass the exams.

CERTIFICATION OBJECTIVE 1.01

What is Designing Security for a Windows 2000 Network?

The American Heritage Dictionary defines security as “something that gives or assures safety,” and goes on to specify that in the context of computer science, the term means “prevention of unauthorized use of a program or device.”

The same source tells us that design means “to plan out in systematic, usually graphic form” or, as a verb, “to make or execute plans” and “to have a goal or purpose in mind.”

Designing security, then, involves creating and implementing a plan with the goal or purpose of preventing unauthorized use of our network resources—keeping them safe.

Why an entire exam devoted to designing a network security plan? Is security really such a big deal that it warrants its own examination? The answer is obvious to
those who have worked in an organization where data that travels across the network is sensitive. Security is important for confidential patient records in medical offices, client documents in law offices, trade secrets in manufacturing companies, secret formulae and code in intellectual property businesses, classified information in governmental agencies, financial data, the list goes on.

With the advent of the Internet as a major means of communication, company networks have been opened up, literally, to the world. Vulnerability to both accidental and malicious access by unauthorized personnel is a real and growing worry for organizations whose business viability, in many cases, depends on networked communications. Taking all that sensitive data offline is not an option, so methods must be devised to protect the integrity and privacy of information stored on networked computers or transmitted over network connections.

Although many of these security concerns and issues are the same ones encountered with Windows NT 4.0 networks, the Windows 2000 operating system family provides many new security functionalities with which you can address them. There are completely new features such as Kerberos, IPSecurity (IPSec), Active Directory object security, and file level encryption with the Encrypting File System (EFS). And vast improvements have been made to many of the security functions that were available in Windows NT, such as NTFS permissions, public key certificates, and virtual private networking. Windows 2000 is changing the world of networking, and the options administrators have for securing their network communications are changing and expanding as well.

To implement an effective security program on an enterprise level network, you must have a thorough understanding of how Windows 2000’s security features work. Then you must go a step further. To pass the Security Design exam, you will need to know more than the technical aspects of security mechanisms; you will also need to understand business models and company processes, and how the organization’s policies fit into the security plan. You should be able to analyze the existing network structure and identify security requirements, create a security baseline, and develop strategies that will balance the need for protection of sensitive data against the need for fast and easy accessibility.

Specifically, you will be expected to demonstrate the ability to design audit policies, authentication strategies, and plans for delegating administrative authority, applying group policy in the context of securing resources, and coming up with solutions for specific security-related scenarios.
What is Designing Security for a Windows 2000 Network?

The exam is comprehensive, covering security issues that arise in both local area networking and wide area networking environments, and addressing the special security needs associated with the growing practice of providing secure access to private networks over the very public Internet. Remote access connections are a popular means of keeping “in the loop” when employees are working at home or on the road, and maintaining security over Remote Access Service (RAS) connections will be another area of focus for this exam. Windows 2000 has also made it easy to implement terminal services as an alternative to upgrading old hardware, and the special considerations for securing the connections of terminal clients to the network through the terminal server will also be addressed.

Finally, areas that might not be traditionally thought of as security-related must be factored in. Domain Name System (DNS) security, security issues connected with Remote Installation Service (RIS), and security considerations when using the Simple Network Management Protocol (SNMP) and other monitoring tools must be factored into the design of the overall security plan. This book will cover each of these areas in detail.

Security Planning Strategies

Planning security for an enterprise network is not—or should not be—the sole province of one security expert. In order for the plan to be effective and workable, it must be a team effort, with input from different factions in the organization. A thorough understanding of both the risks and vulnerabilities of the organization and its needs and priorities is essential to developing a security strategy that helps, rather than hinders, the overall operation of the company’s network. Rarely does one person, regardless of how intelligent or technically competent he or she may be, have the complete big picture perspective necessary to accomplish this alone.

The security plan and its implications and implementation should be considered from both an administrative and a technical point of view, so it makes sense at the very least to involve representatives from those two areas of the organization in the process.

In most companies, there is a great deal of specialization. Those in management positions are there because of their business administrative skills, and may not be technically savvy or even aware of what is or isn’t possible, or the cost and time factors involved in implementing various network security options. Technical
personnel tend to be more focused on the how rather than the why, and may be oblivious to, for instance, the psychological effects that a particular security plan may have on employees (thus impacting overall company productivity).

A good security planning team will work together, tossing out ideas, questioning, challenging, and playing devil’s advocate, with the knowledge and viewpoint of each member complimenting that of the others. A team that works in this manner is more likely to end up with a security plan that truly meets the company’s needs than an outsider called in to set up a turnkey security solution. Even if consultants are hired to do the bulk of the work, company personnel should insist on being involved in the analysis and design phases (and if you are the consultant, you should welcome and emphasize to them the importance of their involvement).

IT consultants find that clients often demand the impossible—and this is especially true in the area of network security. The ideal network environment is one in which all users who need access to resources can gain that access quickly and easily—and in which no one who shouldn’t have access can possibly “get in.” As I have explained on many occasions, security and ease of access are, in many ways, at opposite ends of a continuum. Prior to making a career change to network engineering several years ago, the author was a police officer and police academy defensive tactics trainer. Weapon security was an area of major concern. In the wake of numerous incidents in which police officers have had their own guns taken from them, they are always looking for the ultimate security holster that will keep their weapon secure. I continually reminded them that any holster that completely prevented a “bad guy” from removing the gun would also prevent the officer from being able to draw and use the gun when needed. Security, I told them, is always a trade-off, and I now find myself telling clients the same thing about computer and network security. The only way to ensure that unauthorized users absolutely have no chance of accessing data will also prevent authorized users from accessing it too.

Security Planning from the Management Point of View
Company managers who are responsible for the success or failure of the organization must concern themselves with many different factors, some of which are sure to be in conflict. Management ultimately decides on policies that impact the organization’s financial well being, its customers’ desire to do business with the company (or not),
What is Designing Security for a Windows 2000 Network?

and the job satisfaction of its employees. As if all this weren’t enough, managers must be acutely aware of the legal ramifications of their actions, both in terms of criminal law and civil lawsuits.

Although they have the broadest perspective and perhaps the best basis to know what needs to be accomplished in terms of securing the network, they often have no idea how to go about getting to that result.

Managers must juggle risk against cost: both monetary cost and the cost in terms of employee time, company morale, and perhaps internal political considerations.

The People Principle  If it weren’t for people, security measures would not be necessary. Unfortunately, no organization operates without people (at least, not yet). The people who work there are an organization’s biggest asset, and its greatest liability, or at least its greatest potential liability.

In developing security policies for an organization, managers must consider the people (the human resources, in popular terminology, or, to the technical folks, the users). How will the security policies and implementation of those policies impact the people who use the network? The users’ level of knowledge and capability to function with the new security system in place must be considered. If many of the network’s users may be unable to remember complicated security codes and procedures, perhaps smart card access or technologies such as fingerprint recognition would be more viable alternatives.

A somewhat delicate dilemma is how a sudden tightening of security will affect employees’ relationship with management. Part of developing the new security plan involves planning how it will be presented within the company. If done properly, employees can be made to understand the benefits of increased security to the organization and even to them personally. If presented poorly, or as often happens, not really presented at all but merely handed down as an edict from on high, the policy’s changes will be seen as insults to the employees’ integrity and evidence that they don’t have the trust of management. This is not just a matter of not wanting to hurt feelings; employees who feel unfairly mistrusted are more likely to rebel and attempt to circumvent what they see as unreasonable security measures, thereby creating a security risk that would not have otherwise existed.

Company Priorities  Although most companies (aside from non-profit organizations) are in business to make money, different companies have different
priorities and philosophies. One company may wish to present itself to the public as a rock of stability; another may wish to be seen as innovative, risk-taking, on the cutting edge. Likewise, companies have different philosophies when it comes to security issues. Corporation A may put a priority on “team spirit.” Internally, the attitude is “we’re all just one big happy family and we don’t keep secrets from one another.” In other organizations, the “sibling rivalry” between departments or project teams may border on paranoia.

Priorities may also be dictated by law, government administrative regulations, or professional oversight associations. For instance, attorneys are prohibited from revealing confidential client information, thus a law firm must place a high priority on securing files that contain that information, whether secrecy is in keeping with the firm’s personal philosophy or not. This leads us to the next factor.

**Legal Considerations** It may not be a bad idea to have a member of the company’s legal staff involved in the network security planning process. It is important to be cognizant of local, state, and federal laws that pertain to computer security, including those pertaining to unauthorized access. If yours is an international company, you must also consider those laws regulating exportation of encryption technologies and the applicable laws in the countries in which your company operates.

**Growth Strategies** Managers must always be looking ahead, taking the long-term approach. IT professionals are used to constant change and quick obsolescence. They may be less inclined to plan for what may happen years down the road, as they work in a field where it’s almost impossible to predict what new hardware and software solutions may be available in the near future.

The company’s projections in terms of near- and long-term growth will affect the network and may influence the decisions concerning the best and most cost effective security strategies. Some factors to be taken into account include the nature of the expected growth; different security strategies may be more appropriate, depending on whether all the growth is from within the company or due to a merger or an acquisition.

Special security issues are created when you attempt to combine existing networks into one. It is likely that company policies will not be identical, and even if the basic security levels and access policies are the same, the implementation may differ. Additionally, this type of growth is large and sudden, and its impact is thus
What is Designing Security for a Windows 2000 Network?

more apparent than the gradual growth that comes from within. For these reasons, it is important to take extra care in formulating your design plan in this situation.

**Bottom Line Factors** Traditionally, of course, management’s overriding concern has been the “bottom line” on the Profit and Loss statement. Careful planning will allow the security planning team to assess just what the true impact on the bottom line will be. They must take into account both the potential savings that can be attributed to the security plan as well as the cost of its implementation.

A security plan should be viewed somewhat like an insurance policy; you hope it will never be needed, but when it is, you’re very glad you have it.

**Security Planning from the Technical Point of View**

Technical personnel, such as the network administrators and security specialists, are likely to have a somewhat narrower (but more in depth) point of view than the company’s managers. As an IT professional, you may be more interested in the details of implementing a security plan than assessing why one is needed. Most IT workers enjoy implementing new hardware and software just for the fun of it. The technician must take care to keep the company’s needs in mind, and remember that the very biggest and best is not always necessary or even desirable for every situation.

**Ease of Implementation** Technical professionals will want to consider how easy a particular solution is for the IT staff to implement, and how long it will take to do so. Ease of implementation is especially important when the IT department is working to a tight, usually management-imposed, deadline.

Continued ease of maintenance, administration, and upgrading will also be factors in the decision-making process for those approaching security planning from the technical point of view.

**Cost of Implementation** Those in charge of the IT budget will be aware of cost factors and how they impact the total funds allocated to the department. Cost in this case may also refer to the cost in terms of manpower that will be taken away from other IT projects in order to implement and maintain the security plan.

**IT Administrative Structure** It will be important to consider the network administrative structure, that is, whether it is centralized in one IT department or
whether administrative authority is distributed throughout the organization based on geographic location, department, or other divisions of responsibility. Other considerations include company relationships with partners or subsidiaries, how much work is outsourced, and so forth.

The administrative model will influence how the security programs are implemented and the number of people who must be trained in the new technologies, and thus will impact the total cost of operations.

**Performance Factors** Finally, technical personnel would have difficulty, even if they wanted to, disregarding the issue of whether and how much security implementations will decrease network performance. Because the need for speed is a major concern in many of today’s fast-paced environments (at least in the minds of the network’s users), an analysis and cost-benefits comparison in this area is not only irresistible, it’s prudent.

**Security Planning Structure**

The structure and schedule of the security planning team will vary depending on the company and its priorities, workload, and staffing considerations. Each team member should have defined areas of responsibility, and the team should meet on a regular basis during the analysis and design phase.

Each organization will customize the planning process to fit its own needs, but breaking the team’s mission into specific phases, and tasks within those phases, will make for a smoother flow and easier transition to the new security model. It is likely that, whether formally defined or not, the planning process will go through the following steps:

- Information gathering and identification of needs and problems.
- Analysis of the existing structures and the administrative and technical requirements.
- Design of the new security solutions.
- Implementation of the plan.
- Assessment and evaluation (and revision, if necessary).
Information Gathering and Identification Phase
The first step in the establishment of any major policy is to gather information and identify the strengths and weaknesses of the current way of doing things and the areas where improvement is needed. This can be done by observing, by interviewing company personnel, by reviewing written records, or more likely by a combination of all three. Some of the information you will want to gather includes:

- What are the security measures currently in place?
- Have there been security breaches, and if so, of what nature (unauthorized access, denial of service attacks, IP spoofing, and so on)?
- What are the particular vulnerabilities of your network?
- What is the sensitivity level of the data stored on and transferred across the network?
- What are the accessibility requirements?

Analysis Phase
During the analysis stage, you put together the information gathered during phase one and draw conclusions based on the totality of the data. In the analysis phase, you determine what the problems are.

Design Phase
The design phase is where you put forth a solution or solutions to the problems identified in phase two. How can you best address the issues within the parameters of your organization’s budget, philosophy, and priorities?

There may be more than one possible solution, and you will need to assess the pros and cons of each and decide on a plan of action. It is a good idea to also have in place a contingency plan if Plan A doesn’t work.

Implementation Phase
The implementation phase is the phase in which you actually put the plan into action. Implementation may require hiring outside personnel, or you may be able to implement your plan with your current IT staff.
Although presented here as one phase in the overall design process, the implementation phase itself may have to be divided into phases, especially if you are making several major changes to strengthen the security on the network. There are many practical reasons for this. The budget may not allow for implementing all of your new security measures at the same time, or the “human factor” may dictate that users will more readily accept the changes if they are introduced gradually instead of in one big lump.

Assessment and Evaluation Phase

Often forgotten, the last and very important phase is the assessment and evaluation phase. In this phase, you test the security plan you’ve set in place and determine whether you have accomplished your goals, and whether the cost (both monetary and otherwise) of the higher security level is justified by the benefits to the company.

The evaluation phase may result in the pronouncement that the implementation of your security plan was a rousing success—or it may result in a trip back to the drawing board to revise and fine-tune, or even scrap the original plan and start over.

### SCENARIO & SOLUTION

| Why should the security plan be developed by a team rather than one individual? | It is highly unlikely that one person will have the broad perspective necessary to consider all aspects of implementing an enterprise-wide security policy. The plan should be approached with consideration for both the business and the technical points of view. |
| Who should be included as members of the security planning team? | Members of company management, members of IT administration, technicians, and perhaps legal experts and a representative of the end users. |
| How should the planning team gather information to form the basis of their analysis of the existing network security structure? | By observing, by interviewing network users and technical personnel, and by referring to written documentation. |
CERTIFICATION OBJECTIVE 1.02

Overview of Exam 70-220

The Microsoft Windows 2000 exams, more than ever, attempt to measure your ability to perform the job rather than just how well you memorize factoids. This is particularly challenging in the network design area, since the topics are less technical and perhaps a bit more subjective in nature than those covered by the core implementation and administration exams.

You will notice, when you examine Microsoft's stated objectives for this exam, that about half of the objectives use the verb **analyze** and the other half uses the verb **design**. This is a clue that your analytical skills will be very important. This is further supported by the new “case study” question format, demonstrated on Microsoft’s Web site. You **must** be able to read through a lot of information quickly, decide what is relevant and what can be discarded, and make decisions based on the information given. The scenario questions in the Windows NT 4.0 exams that asked you to determine whether a solution met required and desired results were Microsoft’s earlier attempt to measure these same skills; the tabbed case study format takes this to new heights. You can expect questions of this type on all the Design exams.

**Exam Watch**

*Before taking any of the Windows 2000 exams, and especially the Design electives, be sure you check out the new case study question format. You can download a demo of a case study sample question at [http://www.microsoft.com/trainingandservices/default.asp](http://www.microsoft.com/trainingandservices/default.asp).*

Analysis Issues

Your analytical skills will be tested in specific areas. We will discuss each area in this section, and provide a few tips for preparing to answer the exam questions.

**Analyzing Business Requirements**

The first step in designing your network security plan has little to do with the network itself, and everything to do with the organization as a whole. As a network
security designer, you function somewhat like a physician conducting a thorough physical examination. Unlike a doctor whose patient has come in with specific symptoms, you must step back and take a look at your “patient” (the network) as a whole, and assess where security issues might arise. Then you can practice preventative medicine in developing a plan that will head off problems later on.

You will need to analyze the existing model and also take into consideration any planned changes. A business model refers to the ways in which a company conducts its business. You will hear talk of the digital business model or the networked business model or the e-commerce model. Analysis of the model includes processes such as how information flows within the company, and the communication methods in place. Are interoffice communiqués disseminated through printed memoranda, e-mail, or accessed on an intranet Web site? Other questions to ask:

- What products or services does the company market?
- What are the life cycles of those products and services (that is, how often is a new version or model introduced)?
- How does the decision-making process work within this organization?

**Geographic Model** Where are the company’s resources located and how are they distributed among the locations? Determine which of the following describes the company’s scope of operations (a few years down the road, we may have to add interplanetary and intergalactic, but these are the current geographic models):

- **Local** The “mom and pop” corner store model, in which all or most business comes from members of the immediate neighborhood or community, or within a city.
- **Regional** The company operates within a confined area comprised of a state or specific region of the country.
- **National** The company does business all over the country, but rarely or never conducts business outside the national boundaries.
- **International** A global enterprise that does business in more than one country and perhaps has offices in different nations as well.

Remember to take into account where branch offices and subsidiaries are located, and the relationships of those offices to each other and to the company headquarters.
Management Model  An important facet of the overall business model is the company’s management model. How does the “chain of command” work within the company? Is management paternalistic, where control emanates from one person who may see him or herself as a benevolent dictator? Is the management style more team-oriented, where a group of upper level employees run the show (management by committee)?

Does the company’s management style fit one of the following two popular management theories?

Theory X  Theory X is the so-called traditional model, often used in government agencies, where there is a strict chain of command that employees are expected to follow. Going “over the heads” of superiors is frowned upon, or even formally prohibited, and the structure of the organization is paramilitary in nature. Employees are expected to follow the rules that are handed down from above.

Theory Y  Theory Y is the modern management theory that offers a kinder, gentler atmosphere in which employee input in decision-making is encouraged or even required. The company presents itself as one big, happy family where each member is equally valued (although not, of course, equally compensated in monetary terms). Creativity is considered a more valuable asset than going “by the book.”

Other Management Models  Other management “styles” or models that have been popularized in recent years include Management by Objectives (MBO) and Total Quality Management (TQM). Each of these theories or styles will impact how decisions are made in the organization and how information flows (or doesn’t), and thus directly or indirectly influences the process of designing a secure computer network.

Relationships Model  Another consideration involved in analyzing the business requirements of your organization hinges on the company’s relationships with the outside world—business partners, vendors, and customers. This is especially important if the company wishes to make information available to some or all of these through direct access to the company’s network.

Factors That Influence Company Strategies  Keep in mind that there are always a great many factors that influence company strategies. These must be
identified during the information gathering and analysis stages of the planning process. Otherwise the plan you develop, regardless of how technically brilliant it may be, may not meet your organization’s needs. Some common factors include:

- Company priorities
- Projected growth and the company’s growth strategy
- Relevant laws and regulations
- The company’s tolerance for risk
- The total cost of operations

Also, remember that although managers will ultimately make the decisions, much of the success of your security plan will depend on whether it is embraced by the end users, so you must not forget to analyze business and security requirements for the users.

The structure of IT management, in addition to the company’s overall management, should be considered as well, especially in terms of the administration. Is administration of the network centralized or decentralized? What is the funding model? How much of the IT work is outsourced to consultants? Also consider the decision-making process and the change-management process as they relate to the company’s information systems.

**Analyzing the Physical Model**

Assess the physical infrastructure of the network, and determine where the security issues exist and what can be done to address them. Your first line of defense against network intrusion is to physically secure your servers, the workstations that have access to those servers, the network media, and the network connectivity devices. The latter two categories are of special interest in a high-sensitivity environment.

**Security of Network Media Types and Hardware Devices**

Be aware that different media types offer more or less protection against “tapping” in and stealing data. Fiber optic cable is much more secure than copper wire; however, it is possible to insert an optical splitter in fiber cable to tap in and eavesdrop on the packets being transmitted.
It is sometimes possible to detect that a tap has been made (with either copper or fiber cable) by measuring the strength of the signal. If the signal has been split, this will weaken it, and the change can be detected by using a TDR (Time Domain Reflectometer) or for fiber optic media, an OTDR (Optical TDR). Of course, you must have previously established a baseline measurement against which you can compare the current signal strength.

Switches are more secure than hubs, because with a hub the communications go out every port, so by tapping into just one length of cable, all messages to all computers connected to the hub could be intercepted. With a switch, messages are sent out only on the port attached to the computer to which the packet is addressed.

Using optical cable and switches will provide a greater level of physical security. Because it is impossible to completely ensure that no one will be able to steal the packets, the next logical step is to create a situation in which even if those packets are intercepted, they can’t be read by unauthorized personnel. That’s where data encryption comes in. When the intruder attempts to read the message inside the packet, it will be scrambled and unreadable.

Securing the Servers and Central Connection Points It goes without saying that network servers should be in rooms that are locked and accessible only to authorized IT personnel. You should likewise lock the doors to wiring closets, labs, and other locations where hubs or routers are located.

Analyzing the Internal and External Security Risks Security risks can come from either outside or inside the organization. It is important that you assess the level of risk from each, and prepare a plan that addresses both.

Protecting the Network from Outside Intrusion In planning protection from outsiders, take a tip from firms specializing in home and office protection, and establish several security rings or lines of defense, one inside the other. Don’t depend on just one security solution to protect highly sensitive or critical data. You might put up an electrified fence to keep intruders off your property, but you would probably not think that because you had the fence, you could leave the front door
to the house unlocked. If someone gets past the fence, he still has another barrier preventing access to the house. And within the house, you might establish yet another perimeter in the form of a locked safe where you store your real valuables.

Similarly, you should create several layers of security to protect your network. These could include:

- Locks on doors to server closets, the use of secure media, and other physical security measures.
- Firewalls between the internal network and the public Internet.
- Strict access control, including the enforcement of strong password policies, closing of unneeded ports, and limitations on remote access to the network.
- Limited assignment of administrative privileges and delegation of authority.
- File level encryption using Windows 2000’s EFS or a third party product.
- Auditing to ensure accountability and detect breaches of security.

**Microsoft Proxy Server 2.0 can be used with Windows 2000 to provide some firewall functions, both to protect internal resources and to limit the access of LAN users to the Internet.** Proxy uses packet filtering to minimize risks on computers connected to the public network. If the local network is large or there is a great deal of traffic, multiple Proxy servers can be used in chains or arrays to handle the volume.

One popular option for creating a secure perimeter between the internal network and the outside world is to set up an area in the network infrastructure referred to as the demilitarized zone (DMZ), in which you place servers that are accessible from the public network and which do not have access to the internal network resources.

**Protecting the Network from Internal Threats** Security breaches often originate inside the organization, with persons who have legitimate physical access to the premises. This includes company employees, contract workers, maintenance personnel, and service workers. Internal security breaches may be intentional or accidental; either way, they should be addressed.

Remember that if a person has access to a client computer on the network, it becomes much easier for him to gain access to resources without authorization.
Again, strong password policies, encryption, and judicious assignment of administrative permissions will help protect against security threats that come from the inside, and auditing will help to make you aware of the problem if it does occur.

**Another way in which an intruder can intercept packets without having to physically tap into the cable is by using “sniffing” software (many such programs are available as free downloads on the Web). These programs are capable of setting the network adapter to run in “promiscuous” mode, if supported by the network interface card (NIC), so that all packets traversing the network—not just those going to or from the particular machine on which the software is installed—can be captured and analyzed. Again, the key is to provide an “interior perimeter” using encryption technology so that even if an intruder gets this far, the packets that he or she captures will be useless.**

**Analyzing Technical Requirements**

Another area in which you must be able to apply your analytical skills is that of the technical requirements associated with the company’s network, and how security measures will impact the technical aspects (performance, stability) of the network infrastructure.

First you should evaluate the company’s existing and planned technical environment, taking into account such factors as:

- Company size
- User and resource distribution
- Available connectivity between the geographic location of work sites and remote sites
- Net available bandwidth
- Performance requirements
- Methods in use for accessing data and systems
- Network roles and responsibilities (that is, administrative, user, service, resource ownership, and application)
- Technical support structure
- Existing and planned network and systems management
Chapter 1: Introduction to Designing Security for a Windows 2000 Network

After you assess the existing systems and applications and identify existing and planned software and hardware upgrades and rollouts, you should attempt to predict the impact of the security design on the existing and planned technical environment.

Analyzing Security Requirements

Now that you have done a thorough analysis of the company’s business and technical requirements, you can finally get down to the heart of the matter—analyzing the organization’s security requirements.

The first step in this process is to establish a security baseline for your Windows 2000 network. A baseline is a reference point, measured before changes are made, that then allows you to compare the effects of the new design to the extant security model. This should include domain controllers, operations masters, application servers, file and print servers, RAS servers, desktop computers, portable computers, and kiosks.

Then, tedious as it may sound, the team should identify the required level of security for each resource. Examples of network resources include printers, scanners, modems, shared files and folders, Internet connections, and dial-in connections.

If your network is large or complex, it may require more than one security plan. This is especially true if the network encompasses different geographic locations, or consists of different user groups that need distinctly different security policies.

Determining Types of Security Risks

In analyzing the requirements of your organization, you should determine what types of security risks you want to protect against, and establish priorities. Common types of security risks in a corporate environment include:

- **Identity interception** In which unauthorized access is gained by using the valid credentials of someone else.

- **Impersonation** Which is the ability of an unauthorized person to present credentials that appear to be valid (see replay attack).

- **Replay attack** In which the unauthorized user records the exchange of packets between an authorized user and the server, and plays back the records later.
- **Masquerading** Where an unauthorized user uses the IP address of a trusted system account or device.
- **Data interception** Which consists of monitoring and capturing data as it is transferred across the network.
- **Manipulation** Which means unauthorized modification of unencrypted data.
- **Repudiation** In which the identity of the sender cannot be verified.
- **Denial of service attacks** In which the server is flooded with numerous requests that use all the bandwidth or resources so that the server cannot communicate.
- **Trojan horse** Which is a virus or malicious program that is disguised as a harmless program.

### SCENARIO & SOLUTION

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is a social engineering attack?</td>
<td>This is the term used for breaking into a network by simply “outwitting” employees and convincing them to reveal their passwords. Often the intruder pretends to be with the company’s IT department and tells the users that he is verifying their password or that there is a problem with their network account.</td>
</tr>
<tr>
<td>What is meant by malicious code?</td>
<td>This is a method of attacking a network by embedding ActiveX, VBScript, or a Java applet in a Web page or e-mail message, which when executed will provide the intruder with a way to access information on the network which he or she is not authorized to access.</td>
</tr>
<tr>
<td>What are macro viruses?</td>
<td>Macros are small programs that run inside other programs; for example, macros can be written to automate commonly used functions in Microsoft Word and other word processing programs. A macro virus uses this capability to invade a system and cause damage or gain unauthorized access to data.</td>
</tr>
</tbody>
</table>
Design Issues

The second half of the exam objectives address design issues. Specifically, you need to be able to demonstrate the following skills:

- Design a Windows 2000 Security Solution
- Design a Security Solution for Access between Networks (Internetworking)
- Design Security Solutions for Communication Channels (with an emphasis on Server Message Block signing and IPSec)

Let’s take a look at each of those in a bit more detail.

Designing a Windows 2000 Security Solution

**Auditing**, to monitor the results of your security implementations, is an important part of any security policy. You will be expected to design an effective audit policy for an enterprise network.

A new feature in Windows 2000’s new Active Directory domain structure is the ability to delegate administrative authority. You can assign administrative permissions over objects in an organizational unit (OU) to a user without making him or her an administrator elsewhere in the domain. The exam requires that you be able to design a strategy for delegating administrative authority.

Active Directory’s group policy feature is a major player in the Windows 2000 security model. You will need to know how to design and plan the placement of security policies for sites, domains and OUs, and how to control (force or block) inheritance of policies by child containers from the parent containers in which they reside.

The Encrypting File System (EFS) is another security feature that is new in Windows 2000. You will need to understand how EFS works and how to best plan a strategy for the use of file level encryption in your organization’s network communications.

**Authentication** of a user’s or system account’s credentials is a key element in securing the network. You will need to be familiar with common authentication methods available in Windows 2000, including:

- Certificate-based authentication
- Kerberos authentication
- Use of clear-text passwords
- Digest authentication
Smart card authentication
- NTLM (NT LAN Manager) authentication
- Remote Authentication Dial-In User Service (RADIUS)
- Secure Sockets Layer (SSL)

Additionally, you will need to be able to design an authentication strategy for integration with other operating systems and platforms.

Windows 2000 uses security groups for more efficient assignment of permissions. Exam 70-220 requires that you be able to design a sound strategy for the use of security groups.

The entities called “security groups” in Windows 2000 terminology serve the same function as plain old “groups” in Windows NT. However, Windows 2000 distinguishes between two types of groups: security groups, to which access permissions can be assigned; and distribution groups, which are used for sending messages to multiple users and which do not have a security function. Security groups in Windows 2000 can be one of three types: domain local groups, global groups, and (if the domain is running in native mode) universal groups.

A public key infrastructure (PKI) is a system of digital certificates, certificate authorities, and other registration authorities that verify and authenticate the validity of each party involved in an electronic transaction. This is done using public key cryptography, in which a public key, published and made widely available, is used to encrypt data and a corresponding private key, kept secret, is used for decryption. This exam requires you to be able to design a public key infrastructure, including the design of certificate authority (CA) hierarchies, identification of certificate server roles, management and mapping of certificates, and integration with third-party certificate authorities.

Windows 2000 is built around its network services; after all, networking is what the new operating system was made to do. The sharing of resources on a network, however (and especially implementation of sophisticated services designed to enhance connectivity and access), always presents a security risk. In order to pass Exam 70-220, you will need to understand Windows 2000 networking concepts and have a good grasp of network services, especially the following:

- Domain Name System (DNS) structure and implementation
24 Chapter 1: Introduction to Designing Security for a Windows 2000 Network

- Remote Installation Service (RIS)
- Simple Network Management Protocol (SNMP)
- Windows 2000 Terminal services

You will need to demonstrate your ability to provide solutions for securing all of the preceding connection types.

**Designing a Security Solution for Access Between Networks**

*Internetworking* refers to connecting two or more networks. This concept is the foundation of the global Internet, as well as private large enterprise networks. With Internet connectivity becoming a necessity rather than a luxury, and most major (and many, many minor) companies “on the net,” it is important to know how to secure your internal, private LAN from unauthorized access originating on the public network to which it is connected.

You must be able to provide authorized external (remote) users the ability to establish a secure connection and access the resources of the private network, while preventing other users of the public network from gaining access without authorization. You must be able to connect two private networks in a secure manner that protects the confidentiality of the communications. It is also essential that you be able to provide for secure access within a local network, as well as across a wide area network. Designing a security plan that will give remote users the access they need while protecting the integrity of the network’s security can be a special challenge. All of these issues are addressed in the objectives for Exam 70-220.

**Designing Security for Communication Channels**

Finally, the exam will focus on designing a plan for establishing secure communication channels. The emphasis will be on two areas: SMB signing and IPSec.

SMB is the *Server Message Block* protocol, used in Windows networks for file sharing across the network, and sometimes referred to as the *core protocol*. SMB signing requires that every packet be signed for and verified. This guards against *man-in-the-middle* attacks, where an intruder intercepts packets in transit and changes the security credentials to *administrator*, thereby allowing administrative functions on the server. Designing an SMB signing solution will be a part of the Security Design exam.
Since SMB signing requires that every packet in the stream be verified, enabling SMB signing can result in decreased performance on the server. This may be an acceptable tradeoff in an environment where sensitive data is subject to attack, but is a side effect of which you should be aware if your network’s functions require optimum performance.

Internet Protocol Security (IPSec) is a suite of protocols that is designed to allow for secure encrypted communications over a network that is not itself secure. IPSec encrypts the data at the network layer, unlike higher-level encryption protocols that require that applications be aware of and support the encryption method. IPSec uses a special algorithm to generate a “shared secret” (that is, the same encryption key at each end of the connection). This means the key itself is never transmitted over the network. IPSec can protect your network against data manipulation, interception, and replay attacks.

For Exam 70-220, you will need to be able to demonstrate your ability to design an IP Security solution, including an IPSec encryption scheme and management strategy. Further, you will need to be able to design negotiation policies. IPSec communications begin security negotiations using a protocol called the Internet Key Exchange (IKE) protocol, and then the two computers involved in the secure connection will exchange authentication information based on the method designated in the security rule. This could be Kerberos, public key certificates, or a pre-shared key value. IKE establishes security associations between the computers and generates a shared secret key for each association.

You should know how to plan the implementation of and configure IPSec filters, with which you can specify exactly which types of incoming TCP/IP traffic are processed for each IP interface. Each filter defines a particular subset of inbound or outbound network traffic that should be secured.
Chapter 1: Introduction to Designing Security for a Windows 2000 Network

Analyzing Existing and Planned Business Models: Chapter 2

Chapter 2 will address the analysis of your company’s business model, including the analysis of the geographic model (local, regional, national, or international), and the company processes and information flow patterns. This chapter will also deal with communication processes, life cycles of products and services, and the decision-making process.

Analyzing Business Requirements: Chapter 3

In Chapter 3, we will continue the discussion of the analytical skills required for the exam by examining methods for analyzing the company’s business requirements. This will include the analysis of existing and planned organizational structures, management models, and company organization. We will explore the implications of the company’s relationships with vendors, partners, and customers. In this chapter, we discuss acquisition plans, and how IT departments can be eliminated or integrated in the acquisition process. We will also talk about how to define security standards for the organization.

We will provide information on how you can analyze the many factors that influence company strategies. This includes company priorities, projected growth and the strategies that have been developed for handling that growth, the importance of relevant laws and the rules of regulatory agencies, and the company’s tolerance for risk, along with how the total cost of operations is impacted.

Other topics addressed in Chapter 3 include how to analyze the structure of the company’s IT management, and understanding different IT administrative models (centralized versus decentralized). We will talk about outsourcing, the decision-making process, and the change management process within the IT structure. Finally, we will wrap up with a discussion of both internal and external security risks.

Analyzing End User Computing Requirements: Chapter 4

In Chapter 4, we take a look at the needs and requirements of the network’s users. We will focus on analyzing both the business requirements and the security requirements of end users, and will define classes of users, such as executives, technical personnel, and administrative personnel.
We will discuss how the user’s physical location influences his or her needs, and how the requirements of local users differ from those of remote users. We will also talk a little about user applications, the roles they play, and the requirements of common applications.

Next we turn to an examination and analysis of the physical model and the existing information security model. We will discuss physical security, including facilities issues, protection of servers and the data center, and how to secure user workstations. We will also discuss protection of the data on local hard disks and on the servers, as well as the special problem of protecting data created by or accessed by remote users.

The authentication methods supported by Windows 2000 for remote access include Point to Point Protocol (PPP) challenge/response; Custom Extensible Authentication Protocol (EAP) for stronger authentication using token cards, smart cards, or biometric hardware; and EAP Transport Layer Security (EAP-TLS) based on digital certificates and smart cards.

Analyzing Technical Requirements: Chapter 5

Our focus changes in Chapter 5, moving away from the business aspects to the technical aspects of providing security for our Windows 2000 network. Here we will discuss how to evaluate a company’s existing technical environment, as well as any planned changes to that environment. Some considerations we will address include the size of the company, distribution of its users and resources, and the status of connectivity between onsite and remote locations.

We will explore a topic near and dear to the heart of most network professionals—network bandwidth—and we’ll talk about how to assess the available net bandwidth. We will share methods of analyzing performance requirements based on the applications and usage of the network, and we will discuss how to analyze the methods used in the company to access the data and systems.

Then we will address the important topic of network roles and responsibilities, including the administrative role, the role of users, and the issues of network services, resource ownership, and applications.

We will learn to analyze the impact of the security design on the technical environment, both existing and planned.
28 Chapter 1: Introduction to Designing Security for a Windows 2000 Network

Designing a Security Baseline: Chapter 6

Chapter 6 will focus on the concept of security baselines and how to establish them. In this chapter, we will establish a framework for understanding the details of establishing and using a baseline. Specifically, we will discuss the baseline as it applies to domain controllers, operations masters, and other Windows 2000 servers, including application servers, file servers, print servers, and remote access servers. We will also look at how the baseline applies to desktop computers (workstations), portable/mobile computers, and special-purpose computers such as kiosks.

Analyzing Security Requirements: Chapter 7

Chapter 7 will introduce you to the process of determining what level of security is required for each resource on the network. We will address the security issues involved in sharing printers, files, and other shares, as well as those involved in sharing Internet or dial-in access connections.

This chapter will cover Active Directory concepts related to security, including the basic operation of the directory services, the roles of the schema and global catalog in a Windows 2000 network, how trust relationships work in a Windows 2000 domain structure, and the security implications of the Active Directory namespace. We will look at Active Directory security boundaries, including sites, domains, and organizational units (OUs). We will talk about directory replication from the security standpoint, and how group policies can be used to secure access to network resources.

We will talk about how to use Active Directory permissions to secure the directory, controlling permissions inheritance, the implications of object ownership, and how administrative control can be delegated and even customized.

Designing a Security Solution: Chapter 8

In Chapter 8 we will address some important security concepts applicable to Windows 2000. Specifically, we’ll discuss how the placement of security policies impacts the network, and how policies are inherited, as well as how you can change the default inheritance behaviors.

We will discuss the design of an authentication strategy and how to select from among the authentication methods supported by Windows 2000. The pros and cons
What We’ll Cover in This Book

and characteristics of each authentication method will be examined. Methods include certificate-based authentication, Kerberos, clear-text password authentication, digest authentication, the use of so-called smart cards for authentication, NTLM authentication (as used with older Microsoft operating systems), RADIUS authentication for remote users, and Secure Sockets Layer (SSL) authentication for secure Web transactions. We will talk about how to design an authentication strategy for integration with other operating systems and platforms, and the compatibility issues involved.

Smart card authentication is called a “two factor authentication method.” This refers to the fact that a user must do two things: present a physical object (the card) and supply a password. The most common example of this type of technology is the ATM card, which you “swipe” through the card reader; you then enter a PIN (personal identification number).

Next, we will look at how to design a public key infrastructure, including the structuring of Certificate Authority hierarchies. We will identify the roles of certificate servers, and discuss the management and mapping of certificates. We’ll also look at how to integrate Windows 2000 certificate services with third-party certificate authorities.

Finally, we will talk about Windows 2000 network services and how they can be secured. This discussion will cover security issues involving DNS, RIS, SNMP, and terminal services.

Understanding Group Policies: Chapter 9

In Chapter 9 we will attempt to give you an overview of how group policies work. This chapter will focus on the technical aspects of group policy, in preparation for the design details in the following chapter.

Chapter 9 will discuss audit policies, the Active Directory structure, and the use of Active Directory permissions for securing object access. The use of organizational units and how user and computer accounts fit into the group policy strategy will also be covered. We will talk about how to design a strategy for using security groups to control access, and this will include discussion of group types and scopes, and how to create and delete groups. We will explore best practices and strategies for implementing security groups based on such factors as the organizational structure, the administrative model, and the application model.
Chapter 10: Introduction to Designing Security for a Windows 2000 Network

We will talk about security templates and how to use them, the Microsoft Management Console (MMC) group policy snap-in and how it works, the role of local policies, and how to use the Event Log and the Registry in conjunction with group policy implementation. We will discuss how to design a group policy, and how to configure group policy settings. We'll discuss group policy objects, containers, and templates, and we'll explore the rules of group policy inheritance and the processing order of multiple policies. Then we will explore how to apply group policies, including creation of a GPO, managing permissions and inheritance, using the group policy console, and how to use templates and scripts.

Designing and Implementing Group Policy Strategies: Chapter 10

Chapter 10 will build on the technical information in Chapter 9, focusing on strategy. Delegation of administrative authority, ownership and inheritance, access control entries, and assignment of the special NTFS permissions will all be discussed.

Then we will look at an often-overlooked aspect of security planning: disaster recovery. We will look at the options Windows 2000 provides for creating fault tolerant volumes on dynamic disks. We will also discuss how to use the built-in backup utility, and how to create and use an Emergency Repair Disk.

The next section of this chapter deals with the design of a strategy for implementing the Windows 2000 Encrypting File System (EFS) on your network. We will provide an overview of EFS concepts, discuss encryption and decryption methods, and explore the cipher command included in Windows 2000. We will also talk about using the Recovery Agent, which gives administrators the ability to recover encrypted files.

In order to implement EFS, there must be a public key infrastructure established on the network. At least one administrator must have an EFS data recovery certificate. In order to encrypt a file, the author must have an EFS certificate. Finally, only files and folders located on NTFSv5 drives can be encrypted with EFS. If an EFS encrypted file is moved or copied by the owner to a FAT16 or FAT32 partition, the encryption will be lost.
The last chapter of this book will cover issues pertaining to securing internetworked connections. We will talk about how to provide secure access to public networks, such as the global Internet, from a private network, such as a company LAN. We will also address ways to provide external users (for example, employees working from a remote location) with secure access to the resources of the private network. Then we will discuss how to establish a secure link between two or more private networks, to allow for secure transfer of traffic between the two.

We will talk about security issues with the local area network and security issues within a wide area network, as well as how to provide for secure private connections across a public network, using virtual private networking with the Point-to-Point Tunneling Protocol (PPTP) or Layer 2 Tunneling Protocol (L2TP) supplied with Windows 2000.

We will learn to design secure connections for remote access users, and we will discuss the protocols used in establishing secure RAS connections and authenticating remote users. This includes both inbound and outbound connections, and addresses both virtual private network (VPN) and dial-in connectivity.

Wrapping up this chapter, and the book, we will discuss SMB signing as a security solution, and we will look at an exciting new protocol suite that provides IP security—IPSec.

### SCENARIO & SOLUTION

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>What protocols does Windows 2000 support for VPN connections?</td>
<td>Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP)</td>
</tr>
<tr>
<td>Which of the tunneling protocols was also supported in Windows NT 4.0?</td>
<td>PPTP</td>
</tr>
<tr>
<td>Which of the tunneling protocols works with IPSec to ensure secure end-to-end communications?</td>
<td>L2TP</td>
</tr>
</tbody>
</table>
Chapter 1: Introduction to Designing Security for a Windows 2000 Network

**CERTIFICATION OBJECTIVE 1.04**

**What You Should Already Know**

Before you embark on your journey through this book, there are some fundamental terms and concepts with which you should be familiar.

**Security Terminology**

A good grasp of the terminology associated with computer security issues will be helpful in understanding the concepts and practices discussed in this book. Following are a few of the terms with which you should be familiar before plunging into the technical chapters of this book:

- **Authentication** The process of validating the identity of a user or a device such as a server or router. There are a number of different methods of authenticating identity, including Kerberos, NTLM, RADIUS, and others.

- **Certificate** A message that has a digital signature that is associated with the private key of a trusted third party, and confirms that a particular public key belongs to the party (user or device) that claims to own it.

- **Certificate authority** An entity, such as Verisign, that is entrusted with the authority to sign digital certificates confirming the identity of a user or device.

- **CHAP (Challenge Handshake Authentication Protocol)** A protocol used for authentication over a Point to Point Protocol (PPP) connection.

- **Cipher** An algorithm used to encrypt text to make it unreadable to unauthorized persons. The word comes from the Arabic word *sifr*, which means *empty* or *zero*. 

**IPSec policies can be defined separately for each domain or OU on the network. You can also set local IPSec policies for computers that do not have domain IPSec policies assigned to them.**
Cryptography  The study of creating and deciphering encoded or encrypted messages. The word comes the Greek kryptos, which means hidden.

DES (Data Encryption Standard)  A method of cryptography that uses a secret (private) key, originated by IBM and later adopted by the U.S. government.

Encryption  Scrambling of information so that it will not be readable until it is decrypted.

Firewall  Either hardware or software that provides a security boundary or barrier between two networks by filtering incoming and outgoing packets.

Hash (hashing algorithm)  A mathematical calculation applied to a string of text, resulting in a string of bits of a fixed size, which cannot be done in reverse to arrive back at the original source data.

IPSec (IPSecurity)  A set of protocols used to protect packets produced by the Internet Protocol (IP), which works at the Network layer of the Open Systems Interconnection (OSI) model, thus allowing security to be handled without requiring awareness by user applications.

Kerberos  A network authentication protocol that uses a secret (private) key, which was developed by the Massachusetts Institute of Technology (MIT) and is an important component of Windows 2000’s new security system.

Password  A string of characters (text, numbers, or symbols) that is kept private and used to authenticate a user’s identity.

PAP (Password Authentication Protocol)  A simple authentication method used over PPP connections, which is less secure than CHAP.

Private key  A digital code that can be used to decrypt information, which works in conjunction with a corresponding public key.

Public key  A digital code used to encrypt information, which is then decrypted by a private key.

RADIUS (Remote Authentication Dial-In User Service)  A client/server protocol used for authentication of dial-in clients that allows centralized authentication and control of remote users.
Chapter 1: Introduction to Designing Security for a Windows 2000 Network

- **Secret key**: A digital code or password shared by two parties, used for both encryption and decryption of messages.
- **SSL (Secure Sockets Layer)**: A protocol that provides security at the socket level and is used for securing Web access.
- **Smart card**: A device similar to a credit card, which contains an embedded chip (also called a *token*) that stores digital certificates and is used for authentication.
- **Trust relationship**: A logical relationship established between Windows domains to allow pass-through authentication, in which a trusting domain honors the logon authentications of a trusted domain.

**Security Fundamentals**

Before you start your study of security design in earnest, you will find the topics covered on this exam much easier to understand if you review some fundamental networking security concepts. These include:

- The elements of a secure networking environment
- Cryptography basics

**The Elements of a Secure Networking Environment**

Network security consists of both *physical* and *logical* security. That is, in order to secure network communications, physical access to the network computers, cable or other media, and network devices must be controlled. Logical security barriers, such as user authentication methods, encryption, and so on, should also be in place. Another way to think of these two divisions is *hardware security* and *software security*.

Windows 2000 provides for *distributed security*. This means the operating system includes numerous security functions that work together or separately to provide for a secure network environment.

Some basics of secure networking include:

- **Single Sign-on**: The ability of users to provide one username and password to access all authorized network resources rather than having to be authenticated separately for multiple servers and applications.
Access Control  The method of protecting resources by assigning or denying permissions.

Data Integrity  Protecting network data against tampering and modification or destruction.

Data Confidentiality  The ability to encrypt data before it is transferred over the network so that it cannot be read by someone eavesdropping or “tapping” the network.

Physical Security  Protection of the network’s physical assets (servers, workstations, cable, hubs, and so on) from intruders.

User Education  The best security plan in the world will fail if users are not educated to keep their passwords secret and guard against distribution of confidential information.

Cryptography Basics

Cryptography is the study of writing and reading messages that are encoded to prevent unauthorized users from understanding them. Cryptographic methods use algorithms, which are mathematical functions or formulae, along with a value known as a key. The key is a string of bits, and the longer the key, the more difficult it will be to break the code by guessing the value.

There are various types of encryption:

Secret key encryption (also called symmetric encryption)  Both parties use the same shared secret key to encrypt and decrypt the data.

Public key encryption (also called asymmetric encryption)  Two different but corresponding keys (called a key pair) are used; one—the public key—is used to encrypt the data and is not kept secret but is published to all wishing to send an encrypted message to the owner. The second key—the private key—is known only by the owner and is used to decrypt data that was encrypted with the corresponding public key.

Digital signatures  These are message digests that are hashed and attached to a document, and used to verify the identity of the sender and the fact that the data in the document has not been tampered with.
Chapter 1: Introduction to Designing Security for a Windows 2000 Network

Basic Windows 2000 Networking Concepts

Be sure, before you attempt to take Exam 70-220, that you also have a good grasp of the following basic Windows 2000 networking concepts:

- Active Directory Security and Administrative Concepts
  - Active Directory Domain Structure
  - Group Policy
- Authentication methods
  - Certificate-based authentication
  - Kerberos authentication
  - NTLM authentication
  - Clear-text password authentication
  - Smart card authentication
  - RADIUS
  - Secure Sockets Layer (SSL)
- Windows 2000 Public Key Infrastructure
- Windows 2000 Network Services
  - Domain Name System (DNS)
  - Remote Installation Service (RIS)
  - Simple Network Management Protocol (SNMP)
  - Windows 2000 Terminal Services
- Windows 2000 Remote Access Service (RAS)
CERTIFICATION SUMMARY

In this chapter, we provided an overview of what is to come as you work your way through the book and prepare yourself for Exam 70-220, Designing Security for a Windows 2000 Network. We’ve given you some ideas about security planning, both from the manager’s and the technical point of view, and discussed the formation and operation of a security planning team. We examined the phases of the typical planning process: information gathering, analysis, design, implementation, and assessment/evaluation.

We went into an overview of the exam itself, based on Microsoft’s examination objectives. We talked about how to analyze business requirements, the physical model, and the technical requirements of a particular organization in relation to its network. This led us naturally to the analysis of the security requirements.

We provided a brief synopsis of what will be covered in each chapter of this book, and then added some tips on what you should already know before you tackle the individual content chapters, including security-related terminology, fundamentals of network security and cryptography, and Windows 2000 networking basics.
TWO-MINUTE DRILL

What is Designing Security for a Windows 2000 Network?

- Designing security involves creating and implementing a plan with the goal or purpose of preventing unauthorized use of network resources.
- The Windows 2000 operating system family provides many new security functionalities that were not included in Windows NT 4.0, such as Kerberos, IPSec, Active Directory security, and the Encrypting File System (EFS).
- Planning security for an enterprise network should be a team effort, incorporating personnel who can provide the points of view of both management and IT.
- The management viewpoint is broader, taking into account the people principle, overall company priorities, legal considerations, growth factors, and the ever-popular “bottom line” on the financial statement.
- The technical point of view is more focused and specialized, but must consider ease of implementation, cost of implementation (both in terms of money and manpower allocation), the IT administrative structure, and performance factors.
- Security planning can, and usually should, be done in phases: information gathering and identification of needs and problems; analysis of existing structures and the administrative and technical requirements; design of the security solutions; implementation of the plan; and assessment and evaluation of the outcome (including revisions, if necessary).

Overview of Exam 70-220

- The stated objectives for Exam 70-220 can be divided into two broad categories: those addressing analysis issues, and those addressing design issues.
- A business model refers to the ways in which a company conducts business, and includes the geographic model, the management model, relationships with other entities, and factors that influence company strategies.
Some of the factors that influence strategy include the company’s priorities, projected growth and growth strategies, relevant laws and regulations, tolerance for risk, and the total cost of operations.

What We’ll Cover in This Book

- The first line of defense in a security plan involves physically securing the network’s computers (both servers and workstations), cable or other media, connectivity devices, and other hardware components.
- Security threats can be divided into two types: internal and external. Each must be addressed in order to provide for secure communications over the network.
- Designing a security plan requires the establishment of a security baseline for your network which includes domain controllers, operations masters, application servers, file and print servers, RAS servers, desktop and portable machines, and special purpose computers such as kiosks.
- Key elements in security design that take advantage of Windows 2000’s built-in security features include auditing, delegating of authority, authentication, encryption, security groups, the public key infrastructure, and the network services.

What You Should Already Know

- Terms with which you should be familiar before reading further in this book include authentication, certificate, certificate authority, CHAP, cipher, cryptography, DES, encryption, firewall, hash algorithm, IPSec, Kerberos, Password, PAP, private key and public key, RADIUS, secret key, SSL, smart card, and trust relationship.
- Basics of secure networking are: single sign-on (SSO), access control, data integrity, data confidentiality, physical security, and user education.
- Secret key encryption uses the same shared key for encrypting and decrypting, whereas public key encryption uses key pairs—two different, but related keys—with a public key used to encrypt and a private key used to decrypt.
SELF TEST

The following questions will help you measure your understanding of the material presented in this chapter. Read all of the choices carefully, as there may be more than one correct answer. Choose all correct answers for each question.

What is Designing Security for a Windows 2000 Network?

1. Which of the following are security features incorporated into Windows 2000 that were not part of the Windows NT operating system out-of-the-box? (Choose all that apply.)
   - A. NTLM authentication
   - B. IPSec
   - C. Kerberos authentication
   - D. File level permissions

2. Which of the following is true of designing a security plan for an enterprise organization?
   - A. One person should do the work of analyzing and designing, in order to maintain consistency.
   - B. The duties should be divided between two persons, one who does the analysis tasks and one who does the design tasks.
   - C. Both analysis and design should be undertaken as a team effort, with representatives from management, IT, and perhaps the legal department.
   - D. The design phase is the last phase in security planning.

3. Which of the following usually is a concern from the management point of view in developing a security plan? (Choose all that apply.)
   - A. The effect of tightened security on company employees’ relationship with management.
   - B. The effect of security measures on network bandwidth and throughput.
   - C. The monetary cost of implementing security measures.
   - D. How security measures fit into the current IT structure.

4. Observing, interviewing company personnel, and consulting written records are key elements of which phase of the security planning process?
A. Information gathering and identification phase
B. Analysis phase
C. Design phase
D. Implementation phase

5. The “way in which a company conducts its business” is the definition of which of the following?
   A. Business cycle
   B. Business model
   C. Security model
   D. Management model

What We’ll Cover in This Book

6. The geographic model refers to which of the following? (Choose all that apply.)
   A. How large the company is in terms of number of employees.
   B. Where the company’s branch offices and subsidiaries are located.
   C. Whether the company does business on a local, regional, national, or international basis.
   D. How the company’s headquarters offices are laid out.

7. Which of the following is defined as the traditional business model, in use in most government agencies, where a strict chain of command is followed and employees are expected to follow rules without question and go “by the book”?
   A. Management by objectives (MBO)
   B. The theory X management model
   C. The theory Y management model
   D. Total Quality Management (TQM)

8. Which of the following is true of fiber optic cabling?
   A. It is less secure than copper cabling.
   B. It is harder to “tap” into than copper, but it is possible to do so.
   C. It is impossible to “tap” into and thus is completely secure.
   D. It offers about the same security as copper cable.
Chapter 1: Introduction to Designing Security for a Windows 2000 Network

9. Why do switches provide more data security than hubs?
   A. Switches use only optical cable, which is inherently more secure than the copper cable used by hubs.
   B. Switches have fewer ports than hubs, thus less of the total network traffic is exposed.
   C. Switches send messages out only on the ports associated with the destination address, whereas hubs send every message out of every port.
   D. Switches do not provide more data security than hubs.

10. Which of the following is a popular way of securing communication between the internal local network and the connection to the public Internet? (Choose all that apply.)
   A. Set up a proxy server between the LAN and the Internet.
   B. Establish a DMZ (demilitarized zone) in which the servers accessible to the “outside” are placed.
   C. Ensure that every computer on the LAN has its own registered IP address rather than using address translation to connect.
   D. Use commercial firewall software on the server that connects to the Internet.

11. The reference point that includes the company’s domain controllers, operations masters, application servers, file and print servers, RAS servers, desktop computers, portable computers, and special purpose computers is called which of the following?
   A. Security model
   B. Security reference
   C. Security design
   D. Security baseline

What You Should Already Know

12. Which of the following is a security risk in which data is monitored and captured, then analyzed, by unauthorized personnel?
   A. Masquerading
   B. Interception
   C. Impersonation
   D. Manipulation
13. Which of the following describes an attack in which the unauthorized user records the exchange of packets between a user and server?
   A. Replay attack
   B. Denial of service attack
   C. Identity attack
   D. Trojan horse attack

14. A system of digital certificates and certificate authorities that verify and authenticate the validity of parties involved in electronic transactions is which of the following?
   A. Domain Name System
   B. Public Key Infrastructure (PKI)
   C. Address Resolution Protocol
   D. IP Security

15. Which of the following is defined as the study of creating and deciphering encoded messages?
   A. Cipher
   B. DES
   C. Cryptography
   D. Hashing
SELF TEST ANSWERS

What is Designing Security for a Windows 2000 Network?

1. ✓ B and C. Both IP Security and industry-standard Kerberos authentication are included in Windows 2000, but were not a part of the Windows NT 4.0 operating system.
   ✗ A is incorrect because NT LAN Manager (NTLM) authentication is the method used by Windows NT. D is incorrect because Windows NT provided for file level assignment of permissions to shares located on NTFS partitions.

2. ✓ C. Best practice is to create a security planning team, consisting of members of various departments in the organization who can provide different perspectives.
   ✗ A is incorrect because designing a security plan for an enterprise organization should not be the province of only one person. B is incorrect because dividing the tasks this way would be inefficient and ineffective because the two parts of the process are dependent upon one another. D is incorrect because after the design phase comes the implementation phase, and after that you must assess and evaluate the effectiveness of the plan.

3. ✓ A and C. Managers must consider how the tightened security will impact employees psychologically, because this can affect worker productivity and even determine whether the security plan works or becomes something to circumvent. The monetary cost of implementing security measures as it affects the company’s bottom line is also a concern of management.
   ✗ B is incorrect because bandwidth and throughput are technical issues that are of more concern to IT personnel than to managers. Likewise, D is incorrect because the way security measures will fit into the current IT structure is usually more of a concern at the departmental level, rather than from the broader perspective of company management.

4. ✓ A. Observing, interviewing, and consulting written records are part of gathering the necessary information on which an analysis can be based.
   ✗ B, C, and D are incorrect because although these activities may be performed at any phase in the process, they are less prominent parts of the later phases. The key element of analysis is sorting through all the data gathered; the key element of design is developing a solution based on the analysis; and the key element of implementation is actually putting the plan into practice.

5. ✓ B. The business model refers to the overall conduct of business, or the strategy a business has adopted for success; an example would be the e-commerce model in which the business uses the Internet for most or all of its customer transactions.
A is incorrect because a business cycle refers to the seasonal changes in the financial status of the business. C is incorrect because the security model refers to how the business protects its assets, and may impact how it conducts business but is not focused on it. D is incorrect because the management model is only a subset of the overall business model, which refers to the chain-of-command structure within the organization.

What We’ll Cover in This Book

6. B and C. The geographic model refers to the scope of the business: local, regional, national, or international, and its branch offices and subsidiaries.

A is incorrect because, although company size and number of employees may increase as the geographic scope broadens, these factors do not determine the geographic model. D is incorrect because the layout of company headquarters would be a facilities design issue, not a part of the overall geographic model.

7. B. The theory X management model is the paramilitary model followed by government agencies and “old fashioned” companies.

A and D are incorrect because MBO and TQM are modern management models designed to address specific issues. C is incorrect because the theory Y model is a more open, team-oriented approach to management in which employee input and challenges are solicited and welcomed.

8. B. Fiber optic cable is more secure than copper cable because it is more difficult to physically “tap” into the line and steal the data; however, it can be done with an optical splitter.

A and D are incorrect, because they contradict the correct answer. C is incorrect because fiber optic does not offer complete security, just more security than traditional copper wire.

9. C. Switches send messages out only on the ports associated with the destination address, whereas hubs send every message out of every port.

A is incorrect because switches can use copper cable. B is incorrect because switches do not have fewer ports, and even if they did, this would provide no data security. D is incorrect because switches are in fact more secure than hubs.

10. A, B, and D. A proxy server provides both address translation and some firewall protection from outside access. Creating a DMZ is a popular way to set up a perimeter barrier between the LAN and the Internet. Commercial firewall software is available that filters incoming and outgoing traffic to provide security for communications between the LAN and the WAN.
Chapter 1: Introduction to Designing Security for a Windows 2000 Network

☒ C is incorrect because ensuring that each computer has a registered IP address will not increase security and will, in fact, make the LAN computers more vulnerable if some other protective measures are not in place.

11. ☑ D. The reference point that includes the company’s domain controllers, operations masters, application servers, file and print servers, RAS servers, desktop computers, portable computers, and special purpose computers is called the security baseline.
☒ A is incorrect because the security model refers to the overall security strategy or way of providing security. B is incorrect because security reference is not a commonly used term. C is incorrect because security design encompasses all aspects of both physical and logical security issues.

What You Should Already Know

12. ☑ B. Data interception refers to monitoring, capturing, and analyzing data without authorization.
☒ A is incorrect because masquerading is the use of the IP address of a trusted system or device to gain access. C is incorrect because impersonation is the presentation by an unauthorized person of credentials that appear to be valid. D is incorrect because manipulation refers to unauthorized modification of data.

13. ☑ A. A replay attack consists of recording the exchange of packets between a user and the server, and playing it back later to gain unauthorized access.
☒ B is incorrect because a denial of service attack refers to flooding the server with an overload of requests that use all its resources. C is incorrect because an identity attack, or identity interception, describes using the valid credentials of someone else to gain unauthorized access. D is incorrect because a Trojan horse attack involves sending a malicious program or a virus disguised as a harmless utility.

14. ☑ B. PKI is a system of digital certificates and certificate authorities that verify and authenticate the validity of parties involved in electronic transactions.
☒ A is incorrect because the Domain Name System (DNS) is a means of resolving fully qualified domain names to IP addresses. C is incorrect because the Address Resolution Protocol (ARP) is used to match IP addresses with Media Access Control (MAC) addresses. D is incorrect because IPSec is a means of providing secure end-to-end communications over an IP connection using encryption at the network layer.
15. ☑ C. Cryptography is the study of creating and deciphering encoded messages.
☒ A is incorrect because a cipher is the algorithm used to encrypt text. B is incorrect because Data Encryption Standard (DES) is a cryptography method developed by IBM and later adopted by the U.S. government. D is incorrect because hashing refers to applying a mathematical computation to a string of text to produce a fixed length result which can be compared to that of the original, and cannot be reverse engineered to determine the original text string.