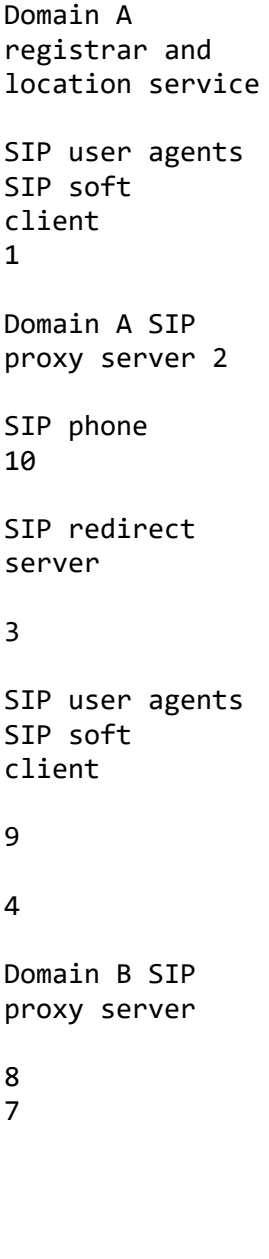
and the UAS. It also forwards requests generated by callers to their respective recipients. Proxy servers are also generally used for name mapping, which allows the proxy server to interlink an external SIP system to an internal SIP client.
• Registrar server Keeps a centralized record of the updated locations of all the
users on the network. These addresses are stored on a location server.

• Redirect server Allows SIP devices to retain their SIP identities despite changes
in their geographic location. This allows a device to remain accessible when its location is physically changed and hence while it moves through different networks. The use of redirect servers allows clients to remain within reach while
they move through numerous network coverage zones. This configuration is generally known as an intraorganizational configuration. Intraorganizational routing enables SIP traffic to be routed within a VoIP network without being transmitted over the PSTN or external network.



5
6

SIP phone

Domain B
registrar and
location
service

1. Call User B
2. Query “How do I get to User B, Domain B?”
3. Response “Address of proxy controller for domain”
4. Call “Proxied to SIP proxy for Domain B”
5. Query “Where is User B?”
6. User B’s address
7. Proxied call
8. Response
9. Response
10. Response
11. Multimedia channel established

Streaming Protocols
The Real Time Protocol (RTP) is a session layer protocol that carries data in media
stream format, as in audio and video, and is used extensively in VoIP, telephony,
video conferencing, and other multimedia streaming technologies. It provides endto-end delivery services and is commonly run over the transport layer protocol
UDP. RTP Control Protocol (RTCP) is used in conjunction with RTP and is also considered a session layer protocol. It provides out-of-band statistics and control
information to provide feedback on QoS levels of individual streaming multimedia sessions.

PART IV

Domain B.com

User A
calls
User B

IP Telephony Issues
VoIP’s integration with the TCP/IP protocol has brought about some security challenges
because it allows threat actors to leverage their TCP/IP experience to probe for flaws in
both the architecture and the implementation of VoIP systems. Also involved are the

traditional security issues associated with networks, such as unauthorized access, exploitation of communication protocols, and the spreading of malware. The promise of financial benefit derived from stolen call time is a strong incentive for most attackers. In short, the VoIP telephony network faces all the flaws that traditional computer networks have faced, plus the ones from legacy telephone systems too.

SIP-based signaling suffers from the lack of encrypted call channels and authentication of control signals. Attackers can tap into the SIP server and client communication to sniff out login IDs, passwords/PINs, and phone numbers. Once an attacker gets a hold of such information, she can use it to place unauthorized calls on the network. Toll fraud is considered to be the most significant threat that VoIP networks face, but illicit surveillance is also a threat for some organizations. If attackers are able to intercept voice packets, they may eavesdrop on ongoing conversations.

Attackers can also masquerade identities by redirecting SIP control packets from a caller to a forged destination to mislead the caller into communicating with an unintended end system. Like in any networked system, VoIP devices are also vulnerable to DoS attacks. Just as attackers would flood TCP servers with SYN packets on an IP network to exhaust a device's resources, attackers can flood RTP servers with call requests in order to overwhelm its processing capabilities. Attackers have also been known to connect laptops simulating IP phones to the Ethernet interfaces that IP phones use. These systems can then be used to carry out intrusions and DoS attacks. Attackers can also intercept RTP packets containing the media stream of a communication session to inject arbitrary audio/video data that may be a cause of annoyance to the actual participants.

Attackers can also impersonate a server and issue commands such as BYE, CHECKSYNC, and RESET to VoIP clients. The BYE command causes VoIP devices to close down while in a conversation, the CHECKSYNC command can be used to reboot VoIP terminals, and the RESET command causes the server to reset and reestablish the connection, which takes considerable time.

Combating VoIP security threats requires a well-thought-out infrastructure implementation plan. With the convergence of traditional and VoIP networks, balancing security while maintaining unconstrained traffic flow is crucial. VoIP calls can (and probably should) be encrypted over TLS. The use of authorization on the network is also an important step in limiting the possibilities of rogue and unauthorized entities on

the network. Authorization of individual IP terminals ensures that only prelisted devices
are allowed to access the network. Although not absolutely foolproof, this method can
prevent rogue devices from connecting and flooding the network with illicit packets.
The use of secure cryptographic protocols such as TLS ensures that all SIP packets
are conveyed within an encrypted and secure tunnel. The use of TLS can provide a secure channel for VoIP client/server communication and prevents the possibility of
eavesdropping and packet manipulation.

693
VoIP Security Measures Broken Down
Hackers can intercept incoming and outgoing calls, carry out DoS attacks, spoof phone calls, and eavesdrop on sensitive conversations. Many of the countermeasures to these types of attacks are the same ones used with traditional data-oriented
networks:

Multimedia Collaboration
The term multimedia collaboration is very broad and includes remotely sharing any combination of voice, video, messages, telemetry, and files during an interactive session. The term
encompasses conferencing applications like Zoom, WebEx, and Google Meetings but also
many other applications in disciplines such as project management, e-learning, science,
telemedicine, and military. What distinguishes multimedia collaboration applications

PART IV

• Keep patches updated on each network device involved with VoIP transmissions:
• The call-processing manager server
• The voicemail server
• The gateway server
• Encrypt VoIP traffic whenever possible.
• Identify unidentified or rogue telephony devices:
• Implement authentication so only authorized telephony devices are working on the network.
• Install and maintain
• Stateful firewalls
• VPN for sensitive voice data
• Intrusion detection
• Disable unnecessary ports and services on routers, switches, PCs, and IP telephones.
• Employ real-time monitoring that looks for attacks, tunneling, and abusive call patterns through IDS/IPS:
• Employ content monitoring.

• Use encryption when data (voice, fax, video) crosses an untrusted network.
• Use a two-factor authentication technology.
• Limit the number of calls via media gateways.
• Close the media sessions after completion.

is their need to simultaneously share a variety of data formats, each of which has different loss, latency, jitter, and bandwidth requirements. Of course, as we work to meet these performance requirements and allow maximum participation from authorized users (potentially around the world), we also have to ensure the security of this communication channel.

Meeting Applications

Imagine this scenario: You are hosting an online leadership meeting with your international partners to discuss the year ahead. Suddenly, a participant with a name you don't recognize starts sharing pornographic images and hate speech for all to see. You've just been "Zoom-bombed." (A term that doesn't necessarily mean you were using that particular platform.) This is what happens when access controls to your online meeting are inadequate. Many naïve users of meeting applications simply share a link with their guests, usually via e-mail or some other messaging application. Anyone with that link could then join the call if other precautions aren't taken.

The rise in popularity of meeting applications and their increased importance to the business of our organizations have put them in the crosshairs of a wide range of attackers beyond the Zoom-bombing troll we described. To prevent these attacks, consider the following best practices for securing online meeting applications:

• Don't use consumer-grade products. There is much wisdom in the old adage "you get what you pay for." Consumer-grade products are much cheaper than enterprise-grade ones (or even free), but they lack most security controls that we need to secure our organizational meetings.
• Use AES 256-bit encryption. It is rare to be able to support true end-to-end encryption for online meetings because most service providers need access to the traffic for things like recording, closed captioning, and echo cancelation. Still, you should ensure all call traffic is encrypted between each participant and the service provider.
• Control access to every meeting. Enterprise-grade conferencing services can integrate with your identity and access management service to ensure strong authentication. Failing that, ensure that, at a minimum, each meeting is password-protected.

• Enable the waiting room feature, particularly for external participants. Many services place participants in a virtual waiting room when they sign in to the meeting until the host lets them in. This gives you an opportunity to screen each participant prior to allowing them to join. At a minimum, ensure participants cannot connect to the call before the host does.
• Restrict participants' sharing of their screens or cameras as appropriate. This is particularly important when the meeting involves external parties such as partners or clients. While cameras may be desirable for a variety of reasons, it is rare for all participants to need unfettered screen sharing. Either way, ensure this is a deliberate decision by the host or organizer and enforceable by the platform.

Telepresence

Sometimes, you and other meeting participants need to do more than just see and hear each other and share slides remotely. Telepresence is the application of various technologies to allow people to be virtually present somewhere other than where they physically are. Consider a bomb disposal specialist trying to disarm an explosive device remotely using a robot, or a surgeon performing a delicate operation on a patient who would otherwise be inaccessible. The possibilities are endless and include the far more mundane applications that most of our organizations would consider, such as trade shows, pipeline inspections, and virtual reality (VR) training.

Because telepresence systems are not yet prevalent, there is no consensus yet on how to best secure them as a whole. Still, the secure design principles we've covered in this book (to which we'll return later in this chapter) apply to these systems.

Unified Communications

While meeting applications like videoconferencing systems have received a lot of attention recently, there is a broader application of multimedia collaboration services known as unified communications (UC). UC is the integration of real-time and non-real-time communications technologies in one platform. Real-time communications are those that are instantaneous and interactive, such as telephone and video conferencing. Non-real-time communications, on the other hand, don't require our immediate attention and are exemplified by technologies such as e-mail and text messaging. The whole point of UC is that it integrates multiple modes of communication, as shown in Figure 15-4.

One of the key features of UC is the concept of presence information, which is an

indicator of a subject’s availability and willingness to communicate. If you have ever used
a platform like Slack or Microsoft Teams, you will have noticed the presence icon next to
your teammates. It may show that they are available, sleeping, on a call, or on a meeting.
Presence information allows you to choose how to interact with your colleagues. If you

PART IV

• Keep your software updated. Online meeting software is no different than any other in the need for patch and update management. Even if you don’t use dedicated clients and use web browsers to connect, you should ensure whatever you use is up to date.
• Don’t record meetings unless necessary. It is helpful to record meetings, particularly
when some participants cannot join in real time and must watch it later. However, the recordings can contain sensitive data that could be stolen or lead to
other types of liability. If you do record the meeting, ensure it is for good reasons
and that the recorded data is encrypted.
• Know how to eject unwanted participants. If you do get Zoom-bombed, that is not the time to figure out how to eject (and lock out) an offending participant. Ensure all hosts know how to do this beforehand and, while they’re at it, learn also how to mute their microphones (and cameras) if needed.

Figure 15-4
Unified
communications
components

Voice

Messaging

Video

E-mail

User

Conferencing

Files

Presence

Directory

@

need to get a message to Mohammed, who happens to be in a meeting, you can send him a text message. If, on the other hand, you see that Carmen is available, you may want to reach out to her on a voice or video call. Presence information can also show where in the world your colleagues are. For example, if you want to meet Bob and notice that he happens to be in the same city as you are, you may opt for a face-to-face meeting request.

Securing UC involves similar security controls that we would apply to any other communications platform, but with a couple of important caveats. For starters, UC relies on centralized data and access controls. This means that, whether your organization hosts its services on premises or in the cloud, there is a hub that supports and enables them. You want to ensure that this hub is adequately protected against physical and logical threats. Obviously, you want to protect your data, whether at rest or in motion, with strong encryption, but this will only get you so far if you allow anyone to access it. Consequently, you want to apply strict access controls that still allow the business processes to run efficiently. Finally, you want to ensure that demand spikes don't cause self-inflicted denial-of-service conditions. Instead, ensure that you have enough spare capacity to handle these inevitable (if rare) spikes.

Remote Access

Remote access covers several technologies that enable remote and home users to connect to resources that they need to perform their tasks. Most of the time, these users must first gain access to the Internet through an ISP, which sets up a connection to the destination network. For many organizations, remote access is a necessity because it enables users to access centralized network resources; it reduces networking costs by using the Internet as the access medium instead of expensive dedicated lines; and it extends the workplace for employees to their home computers, laptops, and mobile devices. Remote access can streamline access to resources and information through Internet connections and provides a competitive advantage by letting partners, suppliers, and customers have closely controlled links.

VPN Authentication Protocols
While we’re talking about VPN configuration, let’s go over some of the authentication protocols you may come across, so you know what each brings to the table.
PAP The Password Authentication Protocol (PAP) is used by remote users to authenticate over Point-to-Point Protocol (PPP) connections such as those used in some VPNs. PAP requires a user to enter a password before being authenticated. The password and the username credentials are sent over the network to the authentication server after a connection has been established via PPP. The authentication server has a database of user credentials that are compared to the supplied credentials to authenticate users. PAP is one

We discussed VPNs in Chapter 13 as a general concept, but let’s circle back and see how to best employ them to provide secure remote connectivity for our staff members.
VPNs are typically implemented using a client application that connects to a VPN server (commonly called a concentrator) in our organization. In a perfect world, you would have enough bandwidth and concentrator capacity to ensure all your remote staff members can simultaneously connect over the VPN. Then, you could enforce always-on VPN, which is a system configuration that automatically connects the device to the VPN with no user interaction. Obviously, this would only be possible with devices owned by the organization, but it can provide strong access controls if properly implemented. For even better results, you can implement a VPN kill switch, which automatically cuts off Internet access unless a VPN session is established.
Alas, things are usually a bit more complicated. Perhaps you don’t have enough VPN capacity for your entire workforce, or you allow use of personal devices. If you cannot implement always-on VPN, the next best thing is to ensure you use multifactor authentication (MFA) and network access control (NAC). NAC is particularly important because you want to be able to check that the user device is safe before allowing it to access your corporate network. Since not everyone will be connecting to the VPN, you want to ensure that remote users have access to the resources they need and no

others,
possibly by putting them on the right VLANs and ensuring you have the right access
control lists (ACLs) in your internal routers.
Regardless, you want to ensure your VPN systems (clients and concentrators) are updated and properly configured. Many clients allow you to select the cryptosystem
to use, in which case you want to select the strongest option you can. Finally, carefully
consider whether you will allow split tunnels.
A VPN split tunnel is a configuration that routes certain traffic (e.g., to the corporate
data center) through the VPN while allowing other traffic (such as web searches) to
access the Internet directly (without going through the VPN tunnel). The advantage
of this approach is that users will be less likely to experience latency induced by an
overworked concentrator. It also allows them to print to their local printer at home while
on VPN. The disadvantage is that, should they pick up malware or otherwise become
compromised on the Internet, the adversary will automatically get a free ride into your
corporate network through the VPN. To prevent this from happening, you can enforce a
VPN full tunnel, which routes all traffic through the concentrators.

of the least secure authentication methods because the credentials are sent in cleartext,
which renders them easy to capture by network sniffers. PAP is also vulnerable
to manin-the-middle attacks. Although this protocol is not recommended for use anywhere,
some (improperly configured) systems can revert to PAP if they cannot agree on any
other authentication protocol.
EXAM TIP PAP has been considered insecure for decades. If you see it on the exam, consider it a bad choice.

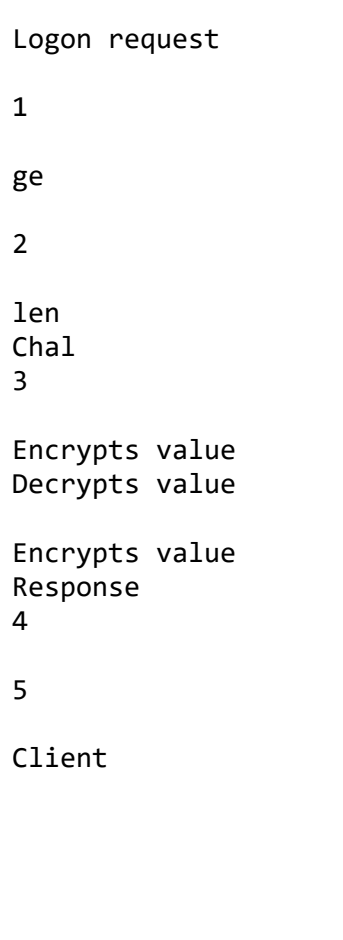
CHAP The Challenge Handshake Authentication Protocol (CHAP) addresses some of the
vulnerabilities found in PAP. It uses a challenge/response mechanism to authenticate
the user instead of having the user send a password over the wire. When a user wants
to establish a PPP connection and both ends have agreed that CHAP will be used for
authentication purposes, the user’s computer sends the authentication server a logon
request. The server sends the user a challenge (called a nonce), which is a random value.

This challenge is encrypted with the use of a predefined password as an encryption key, and the encrypted challenge value is returned to the server. The authentication server also uses the predefined password as an encryption key and decrypts the challenge value, comparing it to the original value sent. If the two results are the same, the authentication server deduces that the user must have entered the correct password and grants authentication. The steps that take place in CHAP are depicted in Figure 15-5.

Unlike PAP, CHAP is not vulnerable to man-in-the-middle attacks because it continues this challenge/response activity throughout the connection to ensure the authentication server is still communicating with a user who holds the necessary credentials.

EXAM TIP MS-CHAP is Microsoft's version of CHAP and provides mutual authentication functionality. It has two versions, which are incompatible with each other.

Figure 15-5 CHAP uses a challenge/response mechanism instead of having the user send the password over the wire.



Server
Authorize or fail
6
Compares values

699
EAP The Extensible Authentication Protocol (EAP) is also supported by PPP. Actually, EAP is not a specific authentication protocol as are PAP and CHAP. Instead, it provides a framework to enable many types of authentication techniques to be used when establishing network connections. As the name states, it extends the authentication possibilities from the norm (PAP and CHAP) to other methods, such as one-time passwords, token cards, biometrics, Kerberos, digital certificates, and future mechanisms. So when a user connects to an authentication server and both have EAP capabilities, they can negotiate between a longer list of possible authentication methods.
NOTE EAP has been defined for use with a variety of technologies and protocols, including PPP, Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), IEEE 802 wired networks, and wireless technologies such as 802.11 and 802.16.

There are many different variants of EAP, as shown in Table 15-1, because EAP is an extensible framework that can be morphed for different environments and needs.

Desktop Virtualization

Protocol

Description

EAP-TLS

Digital certificate–based authentication, considered one of the most secure EAP standards

EAP-PSK

Provides mutual authentication and session key derivation using a preshared key

EAP-TTLS

Tunneled TLS, which requires the server to have a CA-issued certificate, but makes this optional for the client

EAP-IKE2

Internet Key Exchange version 2 (IKE2), which provides mutual authentication and session key establishment using asymmetric or symmetric keys or passwords

PEAPv0/EAPMSCHAPv2

Similar in design to EAP-TTLS but only requires a server-side digital certificate

PEAPv1/EAP-GTC

Cisco variant based on Generic Token Card (GTC) authentication

EAP-FAST

Cisco-proprietary replacement for Lightweight EAP (LEAP) based on Flexible Authentication via Secure Tunneling (FAST)

EAP-SIM

For Global System for Mobile Communications (GSM), based on Subscriber Identity Module (SIM), a variant of PEAP for GSM

EAP-AKA

For Universal Mobile Telecommunication System (UMTS) Subscriber Identity Module (USIM) and provides Authentication and Key Agreement (AKA)

EAP-GSS

Based on Generic Security Service (GSS), uses Kerberos

Table 15-1

EAP Variants

PART IV

Desktop virtualization technologies allow users to remotely interact with computers as
if they were physically using them. In essence, these technologies present a virtual copy
of a desktop that is running on some computer (physical or virtual) somewhere else

in the network. IT staff frequently use desktop virtualization to manage rack-mounted
servers (without having to attach a monitor, keyboard, and mouse to each), to log into

jump boxes, and to manage and troubleshoot user workstations. In some organizations, remote desktop solutions allow staff to work from home and, through their personal devices, securely use an organizational computer. The upside of desktop virtualization is that the asset is protected by the organization's security architecture but still is accessible from almost anywhere. There are two main approaches to desktop virtualization: remote desktops and virtual desktop infrastructure.

NOTE A jump box (also called a jump host or jump server) is a hardened host that acts as a secure entry point or gateway into a sensitive part of a network.

Remote Desktops

Two of the most common approaches to providing remote desktops are Microsoft's Remote Desktop Protocol (RDP) and the open-source Virtual Network Computing (VNC) system. At a high level, both are very similar. They both require that a special server is running on the computer that will be controlled remotely and that the remote device has a software client installed and connected to the server, by default over port 3389 for RDP and 5900 for VNC. Although there are clients and servers for every major operating system, RDP is more common in Windows environments and VNC is more common in Linux environments.

The most important security consideration when deploying either RDP or VNC is to ensure that the connections are encrypted. Neither of these systems has robust security controls, so you have to tunnel them over a secure channel. If you are providing this service to remote users outside your organizational network, then you should ensure they are connected to the VPN. Having external RDP or VNC servers is a recipe for a security disaster, so their corresponding ports should be blocked at your firewall.

One of the advantages or disadvantages (depending on how you look at it) of RDP and VNC is that they allow a client to remotely control a specific computer. That computer must be provisioned somewhere on the network, specifically configured to allow remote access, and then must remain available. If it is powered off or is otherwise unavailable, there is nothing to remotely control.

Virtual Desktop Infrastructure

By combining virtualization and remote desktop technologies, we can create an environment in which users access the desktops of virtual machines (VMs) that look and behave exactly as the users have configured them, but that can be spun up or down,

migrated,
wiped, and re-created centrally as needed. Virtual desktop infrastructure (VDI) is a technology that hosts multiple virtual desktops in a centralized manner and makes them
available to authorized users. Each virtual desktop can be directly tied to a VM (very
similarly to the remote desktops described in the previous section) or can be a composite of multiple virtual components, such as a desktop template combined with virtual

Secure Shell
We don’t always need a graphical user interface (GUI) to interact with our devices. In
fact, there are many advanced use cases in which users, especially experienced and administrative ones, are more productive using a command-line interface (CLI). The tool of
choice in many of these cases (particularly in Linux environments) is Secure Shell (SSH),
which functions as a type of tunneling mechanism that provides terminal-like access to
remote computers. SSH is the equivalent of remote desktops but without the GUI. For
example, the program can let Paul, who is on computer A, access computer B’s files, run
applications on computer B, and retrieve files from computer B without ever physically
touching that computer. SSH provides authentication and secure transmission over vulnerable channels like the Internet.
NOTE SSH can also be used for secure channels for file transfer and port redirection.

SSH should be used instead of Telnet, FTP, rlogin, rexec, or rsh, which provide the same type of functionality SSH offers but in a much less secure manner. SSH is a
program and a set of protocols that work together to provide a secure tunnel between
two computers. The two computers go through a handshaking process and exchange (via
Diffie-Hellman) a session key that will be used during the session to encrypt and protect
the data sent. The steps of an SSH connection are outlined in Figure 15-6.

applications running on multiple different VMs. This flexibility allows organizations
to tailor desktops to specific departments, roles, or even individuals in a scalable and
resource-effective manner.
VDI deployments can be either persistent or nonpersistent. In a persistent VDI,

a
given user connects to the same virtual desktop every time and is able to customize it
as allowed by whatever organizational policies are in place. In a persistent model, users’
desktops look the same at the beginning of one session as they did at the end of the last
one, creating continuity that is helpful for long-term use and for complex workflows.
By contrast, users of a nonpersistent VDI are presented with a standard desktop that is
wiped at the end of each session. Nonpersistent infrastructures are useful when providing
occasional access for very specific purposes or in extremely secure environments.
VDI is particularly helpful in regulated environments because of the ease with which
it supports data retention, configuration management, and incident response. If a user’s
system is compromised, it can quickly be isolated for remediation or investigation, while
a clean desktop is almost instantly spawned and presented to the user, reducing the
downtime to seconds. VDI is also attractive when the workforce is highly mobile and
may log in from a multitude of physical devices in different locations. Obviously, this
approach is highly dependent on network connectivity. For this reason, organizations
need to consider carefully their own network speed and latency when deciding how (or
whether) to implement it.

SSH steps to establish a
secure connection:
1. Client requests SSH connection
2. Handshake to find out protocol version
3. Alogrithm negotiation and key exchange
4. Secure session setup
5. Client runs remote application

Figure 15-6

SSH is used for remote terminal-like functionality.

EXAM TIP Telnet is similar in overall purpose to SSH but provides none of the latter’s security features. It is insecure and probably not the right answer to any question.

Once the handshake takes place and a secure channel is established, the two

computers
have a pathway to exchange data with the assurance that the information will be encrypted
and its integrity will be protected.

Secure channel

Data Communications
Up to this point in this chapter, we've been focused on communications channels used
by users. It is probably a good idea to also consider machine to machine data communications. Recall from Chapter 7 that there are multiple system architectures that require
quite a bit of backend chatter between system components. For example, in an n-tier
architecture, you may have an application server communicating quite regularly with a
database. We must also map out and secure all these not-so-obvious data communications channels.

Network Sockets
A network socket is an endpoint for a data communications channel. A socket is a layer
4 (transport) construct that is defined by five parameters: source address, source port,
destination address, destination port, and protocol (TCP or UDP). At any given time, a
typical workstation has dozens of open sockets, each representing an existing data communications channel. (Servers can have thousands or even tens of thousands of them.)
Each of these channels represents an opportunity for an attacker to compromise our
systems. Do you know what all your data channels are?
This is one of the reasons why understanding our systems architectures is so critical.
Many systems use default installation configurations that are inherently insecure. In
addition to the proverbial (weak) default password, a brand-new server probably includes
a number of services that are not needed and could provide an open door to attackers.
Here are some best practices for securing sockets-based communications channels:

One of the challenges of securing data communications channels is that they rely on service accounts that usually run with elevated privileges. Oftentimes, these service
accounts are excluded from the password policies that are enforced for user accounts. As
a result, service account passwords are seldom changed and sometimes are documented

in an unsecure manner. For example, we know of organizations that keep a list of their
service accounts and passwords on a SharePoint or Confluence page for their IT team.
These passwords should be protected just like any other privileged account and securely
stored in a password vault.

Remote Procedure Calls
Moving up one level to the session layer (layer 5), a remote procedure call (RPC) allows a
program somewhere in your network to execute a function or procedure on some other
host. RPC is commonly used in distributed systems because it allows systems to divide
larger tasks into subtasks and then hand those subtasks to other systems. Although the
IETF defined an RPC protocol for Open Network Computing (ONC), the RPC concept
can take many different forms in practice. In most networks (especially Windows
ones), RPC services listen on TCP port 135. RPC use is ubiquitous in many enterprise
environments because it is so powerful. However, by default, it doesn’t provide
any security beyond basic authentication.

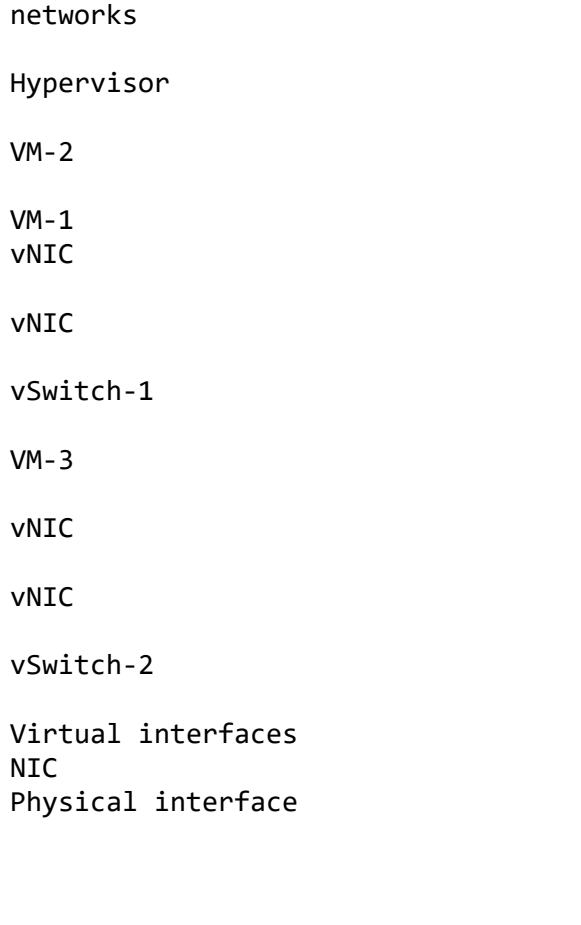
PART IV

- Map out every authorized data communications channel to and from each server.
- Apply ACLs to block every connection except authorized ones.
- Use segmentation to ensure servers that communicate with each other regularly are in the same network segment.
- Whenever possible, encrypt all data communications channels.
- Authenticate all connection requests.

If your organization uses RPC, then you should really consider upgrading its security.
Secure RPC (S-RPC) provides authentication of both users and hosts as well as traffic
encryption. As of February 9, 2021, Windows Active Directory (AD) systems require
S-RPC. The IETF also released a standard for RPC security (RPCSEC) years ago, but because it is difficult to implement, it was never widely adopted. Instead, many
organizations require TLS for authenticating hosts and encrypting RPC traffic. Other,
vendor-specific implementations of RPC security exist, so you should research whatever
versions are being used in your environment and ensure they are secure.

Virtualized Networks
A lot of the network functionality we have covered in this chapter can take place in virtual environments. You should remember from our coverage of virtual

machines (VMs)
in Chapter 7 that a host system can have virtual guest systems running on it, enabling
multiple operating systems to run on the same hardware platform simultaneously. But
the industry has advanced much further than this when it comes to virtualized
technology. Routers and switches can be virtualized, which means you do not actually purchase
a piece of hardware and plug it into your network, but instead you deploy
software products that carry out routing and switching functionality. Obviously, you still need a robust
hardware infrastructure on which to run the VMs, but virtualization can save you a lot
of money, power, heat, and physical space.
These VMs, whether they implement endpoints or networking equipment,
communicate with each other over virtual networks that behave much like their real
counterparts, with a few exceptions. In order to understand some of these, let us first
consider the simple virtual infrastructure shown in Figure 15-7. Let’s suppose that VM-1
is an endpoint (perhaps a server), VM-2 is a firewall, and VM-3 is an IDS on the external
side of the firewall. Two of these devices (VM-1 and VM-3) have a single virtual NIC
(vNIC), while the other one (VM-2) has two vNICs. Every vNIC is connected to a
virtual port on a virtual switch. Unlike the real world, any data that flows from one vNIC
Figure 15-7
Virtualized
networks



Third-Party Connectivity

We can’t wrap up our discussion of securing the multitude of communications channels in our systems without talking about third parties. In Chapter 2, we covered the risks that third parties bring to our organizations and how to mitigate them. These third parties cover a broad spectrum that includes suppliers, service providers, and partners. Each of them may have legitimate needs to communicate digitally with our organizations, potentially in an automated manner. How can we provide this required connectivity to third parties without sacrificing our security? The answer can be found by applying the secure design principles we’ve been revisiting throughout the book:

- Threat modeling Always start by identifying the threats. What might malicious (or just careless) third parties be able to do with the communications channels we provide that would cause us harm? What are their likeliest and most dangerous actions? This deliberate exercise in understanding the threats is foundational.
- Least privilege Third parties will have legitimate connectivity requirements that we should minimally provide. If a contractor needs to monitor and control our HVAC systems remotely, we should segment those systems on the same VLAN and ensure that only specific calls from specific hosts to specific devices are allowed, and nothing more.

to another vNIC is usually just copied from one memory location (on the physical host) to another; it only pretends to travel the virtual network.

The single physical NIC in our example is connected to vSwitch-2, but it could just as easily have been directly connected to a vNIC on a VM. In this virtual network, VM-2 and VM-3 have connectivity to the physical network but VM-1 does not. The hypervisor stores in memory any data arriving at the physical NIC, asks the virtual switch where to send it, and then copies it into the memory location for the intended vNIC.

This means that the hypervisor has complete visibility over all the data traversing its virtualized networks, whether or not it touches the physical NIC.

It should come as no surprise that one of the greatest strengths of virtualization, the hypervisor, is potentially also its greatest weakness. Any attacker who compromises the hypervisor could gain access to all virtualized devices and networks within it.

So, both
the good and the bad guys are intensely focused on finding any vulnerabilities in these
environments. What should you do to ensure the security of your virtualized networks
and devices? First, just as you should do for any other software, ensure you stay on
top of any security patches that come out. Second, beware of third-party add-ons that
extend the functionality of your hypervisor or virtual infrastructure. Ensure these are
well tested and acquired from reputable vendors. Last, ensure that whoever provisions
and maintains your virtualized infrastructure is competent and diligent, but also check
their work. Many vulnerabilities are the result of misconfigured systems, and hypervisors
are no different.

• Defense in depth Based on the threat model, we put in place controls to mitigate risks. But what happens if the first layer of controls fails to contain the
threat? If that HVAC contractor is compromised in an island-hopping attack and the adversary is able to escape the VLAN, how do we detect the breach and then contain the attack?
• Secure defaults While ensuring that default configurations are secure is generally a best practice, it is particularly important on systems that will be used by third parties. One of the keys here is to enforce strict configuration management. For any system that will be accessible by a third party, we must ensure that all defaults are secure by testing them.
• Fail securely Speaking of testing, we should test the system under a range of conditions to see what happens when it breaks. For example, stress testing (under heavy usage loads), fuzzing, and power and network failure testing can show us what happens when a system fails. This is not specific to third-party systems, by the way.
• Separation of duties Giving third parties the least privileges needed actually makes separating duties easier. For example, it may be that the HVAC contractor does not normally start or stop the furnace, but this may be occasionally required.
Because this can have an impact on our facility, the action must be approved by our site manager.
• Keep it simple This principle is centered on the statement of work (SoW) that describes the agreement with the third party and in the processes we build to support that work. A policy of “deny by default, allow by exception” can keep things simple, supports the least-privilege principle, and should be paired with a simple process for handling exceptions.
• Zero trust It goes without saying that we should not trust third parties when it comes to access to our systems. For every interaction of third parties with our
systems, we must ensure that authentication, nonrepudiation, and audit controls are sufficient to detect and mitigate any threat (deliberate or otherwise) that

they
introduce into our environments.
• Privacy by design If we use this principle to guide the development of our entire security architecture (and we really ought to), then we really shouldn’t have
to do anything else to account for third parties using our systems, particularly if
we couple privacy with least privilege in the first place.
• Trust but verify We already talked about auditability in the context of zero trust, but there is a difference between logging activities and analyzing those logs
periodically (or even continually). What is the process by which our security staff
verifies that the actions of third parties are appropriate? How are suspicious or
malicious activities handled?
• Shared responsibility Finally, who is contractually responsible for what? As the saying goes, “good fences make good neighbors.” It is important to define responsibilities in the service or partnership agreement so that there are no misunderstandings and, should someone fail, we can take financial or legal actions to recover our losses.

Chapter Review
With this chapter, we have finished our coverage of the fourth domain of the CISSP
Common Body of Knowledge, Communication and Network Security, by discussing the myriad of technologies that allow us to create secure communications channels in
our organizations. Though most people (particularly in the technology fields) would not
consider voice to be their primary means of communication, it remains important for
many reasons, not the least of which is the fact that traditional voice channels are more
commonly used nowadays for digital data traffic. It is important to understand how these
technologies blend in different ways so that we can better secure them.
The COVID-19 pandemic forced most organizations around the world to quickly move toward (or improve their ability at) supporting a remote workforce largely based
in home offices. While the news media regularly featured stories on the vulnerabilities
and attacks on our multimedia collaboration and remote access systems, it is remarkable
how well these held up to the sudden increase in use (and attacks). We hope that this
chapter has given you a better understanding of how security professionals can continue
to improve the security of these systems while supporting a remote workforce and thirdparty connectivity.

• The public switched telephone network (PSTN) uses circuit switching instead of packet routing to connect calls.
• The Signaling System 7 (SS7) protocol is used for establishing and terminating calls in the PSTN.
• The main components of a PSTN network are signal switching points (SSPs) that terminate subscriber loops, signal transfer points (STPs) that interconnect SSPs and other STPs to route calls through the network, and service control points (SCPs) that control advanced features.
• A digital subscriber line (DSL) is a high-speed communications technology that simultaneously transmits analog voice and digital data between a home or business and a PSTN service provider's central office.
• Asymmetric DSL (ADSL) has data rates of up to 24 Mbps downstream and 1.4 Mbps upstream but can only support distances of about a mile from the central office without signal boosters.
• Very high-data-rate DSL (VDSL) is a higher-speed version of ADSL (up to 300 Mbps downstream and 100 Mbps upstream).
• G.fast is DSL that runs over fiber-optic cable from the central office to a distribution point near the home and then uses legacy copper wires for the last few hundred feet to the home or office. It can deliver data rates of up to 1 Gbps.
• Integrated Services Digital Network (ISDN) is an obsolescent pure digital technology that uses legacy phone lines for both voice and data.

PART IV

Quick Review

• Basic Rate Interface (BRI) ISDN is intended to support a single user with two channels each with data throughput of 64 Kbps.
• Primary Rate Interface (PRI) ISDN has up to 23 usable channels, at 64 Kbps each, which is equivalent to a T1 leased line.
• Cable modems provide high-speed access to the Internet through existing cable coaxial and fiber lines, but the shared nature of these media result in inconsistent throughputs.
• Internet Protocol (IP) telephony is an umbrella term that describes carrying telephone traffic over IP networks.
• The terms "IP telephony" and "Voice over IP" are used interchangeably.
• Jitter is the irregularity in the arrival times of consecutive packets, which is problematic for interactive voice and video communications.
• The H.323 recommendation is a standard that deals with audio and video calls over packet-based networks.
• The Session Initiation Protocol (SIP) is an application layer protocol used for call setup and teardown in IP telephony, video and multimedia conferencing, instant messaging, and online gaming.
• The Real-time Transport Protocol (RTP) is a session layer protocol that carries data in media stream format, as in audio and video, and is used extensively

in VoIP, telephony, video conferencing, and other multimedia streaming technologies.
• RTP Control Protocol (RTCP) is used in conjunction with RTP and is also considered a session layer protocol. It provides out-of-band statistics and control information to provide feedback on QoS levels of individual streaming multimedia sessions.
• Multimedia collaboration is a broad term that includes remotely and simultaneously
sharing any combination of voice, video, messages, telemetry, and files in an interactive session.
• Telepresence is the application of various technologies to allow people to be virtually present somewhere other than where they physically are.
• Unified communications (UC) is the integration of real-time and non-real-time communications technologies in one platform.
• An always-on VPN is a system configuration that automatically connects the device to the VPN with no user interaction.
• A VPN kill switch is a system configuration that automatically cuts off Internet
access unless a VPN session is established.
• A VPN split tunnel is a configuration that routes certain traffic through the VPN
while allowing other traffic to access the Internet directly.

Questions
Please remember that these questions are formatted and asked in a certain way for a
reason. Keep in mind that the CISSP exam is asking questions at a conceptual level.
Questions may not always have the perfect answer, and the candidate is advised against
always looking for the perfect answer. Instead, the candidate should look for the best
answer in the list.
1. In which type of networks is the Signaling System 7 (SS7) protocol used?
A. Integrated Services Digital Network (ISDN)
B. IP telephony network
C. Real-time Transport Protocol (RTP) network
D. Public switched telephone network (PSTN)

• The Password Authentication Protocol (PAP) is an obsolete and insecure authentication protocol that sends user credentials in plaintext and should not be allowed.
• The Challenge Handshake Authentication Protocol (CHAP) uses a challenge/response mechanism using the password as an encryption key to authenticate the user instead of having the user send a password over the wire.
• The Extensible Authentication Protocol (EAP) is a framework that enables many types of authentication techniques to be used when establishing network connections.

• Desktop virtualization technologies, such as remote desktops and virtual desktops,
allow users to remotely interact with computers as if they were physically using them.
• Two of the most common approaches to providing remote desktops are Microsoft's Remote Desktop Protocol (RDP) and the open-source Virtual Network Computing (VNC) system.
• Virtual desktop infrastructure (VDI) is a technology that hosts multiple virtual
desktops in a centralized manner and makes them available to authorized users.
• Secure Shell (SSH) is a secure tunneling mechanism that provides terminal-like access to remote computers.
• A network socket is an endpoint for a data communications channel, defined by five parameters: source address, source port, destination address, destination port,
and protocol (TCP or UDP).
• Remote procedure calls allow a program somewhere in your network to execute a function or procedure on some other host.

2. Which of the following is true about the Session Initiation Protocol (SIP)?
A. Used to establish virtual private network (VPN) sessions
B. Framework for authenticating network connections
C. Session layer protocol for out-of-band statistics
D. Application layer protocol used in online gaming communications

3. Which of the following is not considered a best practice for securing multimedia
collaboration platforms?
A. Don't record meetings unless necessary
B. Use consumer-grade products
C. Use AES 256-bit encryption
D. Restrict participants' sharing of their screens or cameras as appropriate

4. How could you best protect a unified communications (UC) platform?
A. Protect it as you would any other systems
B. Enable Password Authentication Protocol (PAP)
C. Use the Session Initiation Protocol (SIP) for every new session
D. Ensure the hub is protected against physical and logical threats

Use the following scenario to answer Questions 5–7. You are the CISO of a research and
development company that is transitioning to a 100 percent remote workforce, so your
entire staff will be working from home. You don't have enough laptops for all your staff,
so those without one will be using their personal computers and printers for work. Your
VPN concentrators are sufficient to support the entire workforce, and you will be requiring all staff members to connect to the VPN.
5. Which authentication protocol would be best for your VPN connections?
A. Password Authentication Protocol (PAP)

B. Challenge Handshake Authentication Protocol (CHAP)
C. Extensible Authentication Protocol (EAP)
D. Session Initiation Protocol (SIP)

6. Which of the following additional VPN configurations should you also enable?
A. Split tunneling
B. Full tunneling
C. VPN kill switch
D. Hybrid tunneling

7. Which of the following will best protect the confidentiality of your sensitive
research data?
A. Secure Shell (SSH)
B. Virtualized networks
C. Virtual desktop infrastructure (VDI)
D. Remote Procedure Calls (RPC)

8. During a recent review of your enterprise architecture, you realize that many of your mission-critical systems rely on Remote Procedure Call (RPC). What measures should you take to ensure remote procedure calls are secured?
A. Implement ITU standard H.323
B. Tunnel RPC through Transport Layer Security (TLS)
C. Use the Password Authentication Protocol (PAP) for authentication
D. Enforce client-side authentication

9. Which of the following is not an advantage of virtual desktops?
A. Reduced user downtime during incident response
C. Support for both physical and remote logins
D. Better implementation of data retention standards

Answers
1. D. The SS7 protocol is used in a PSTN to set up, control, and disconnect calls.
2. D. SIP is an application layer protocol used for call setup and teardown in IP telephony, video and multimedia conferencing, instant messaging, and online gaming.
3. B. Consumer-grade products almost always lack the security controls and management features that we need to properly secure multimedia collaboration platforms.
4. D. Securing UC involves similar security controls that we would apply to any other communications platform, but with a couple of important caveats. Unified communications rely on a central hub that integrates, coordinates, and synchronizes the various technologies. You want to ensure that this hub is adequately protected against physical and logical threats.
5. C. EAP is considered much more secure than both PAP (which is not secure at all)
and CHAP. SIP does not provide authentication mechanisms at all.
6. A. Because your staff will be using printers on their home networks, you will have
to enable split tunneling, which allows some traffic to be sent over the VPN and

other traffic to go to the local network or to the Internet directly.

PART IV

B. Support for both persistent and nonpersistent sessions

↟CISSP All-in-One Exam Guide

712
7. C. VDI allows your sensitive data to remain in your protected network even as users are able to work with it over a virtual desktop. Properly configured, this infrastructure prevents any sensitive research data from being stored on the remote user’s computer.
8. B. Since many implementations of RPC lack security controls, many organizations
require TLS for authenticating hosts and encrypting RPC traffic.
9. C. VDI is particularly helpful in regulated environments because of the ease with which it supports data retention, configuration management, and incident response through persistent and nonpersistent sessions. However, since VDI relies on VMs in a data center, there is not a computer at which a user could physically log in.

↟PART V

Identity and Access
Management
Chapter 16
Chapter 17

Identity and Access Fundamentals
Managing Identities and Access

↟This page intentionally left blank

↟16

CHAPTER

Identity and Access
Fundamentals
This chapter presents the following:
• Identification, authentication, authorization, and accountability
• Credential management
• Identity management
• Federated identity management with a third-party service

The value of identity of course is that so often with it comes purpose.
—Richard Grant
The concept of identity is foundational to controlling access to our assets because everyone (and everything) that touches them must have a legitimate purpose in doing so.
What makes access control tricky is that most of us have multiple identities that depend
on the context in which we find ourselves. A person could simultaneously be an

asset
owner, custodian, and processor (roles we discussed in Chapter 5), depending on which
asset we consider and at what time. On top of the challenge of handling multiple identities, we also have to ensure that each identity belongs to the person claiming it.
In this chapter, we discuss the fundamentals of user identification, authentication,
and authorization. We do this while considering a variety of real-world contexts, such
as complex enterprise environments and the interaction with third parties. Of course,
we must be able to verify that things are being done correctly, so we also talk about
accountability in these efforts. This all sets the stage for the next chapter, in which we
delve into how to actually manage identities and access.

Identification, Authentication, Authorization, and Accountability

For users to be permitted to access any resource, they first must prove they are who they
claim to be, have the necessary credentials, and have been given the necessary rights or
privileges to perform the actions they are requesting. Once these steps are completed
successfully, it is necessary to track users' activities and enforce accountability for their

actions. Identification describes a method by which a subject (user, program, or process) claims to have a specific identity (username, account number, or e-mail address).
Authentication is the process by which a system verifies the identity of the subject, usually by requiring a piece of information that only the claimed identity should have. This
piece could be a password, passphrase, cryptographic key, personal identification number
(PIN), physiological characteristic, or token. Together, the identification and authentication information (for example, username and password) make up the subject's credentials.
These credentials are compared to information that has been previously stored for this
subject. If these credentials match the stored information, the subject is authenticated.
But we are not done yet.
Once the subject provides its credentials and is properly authenticated, the system
it is trying to access needs to determine if this subject has been given the necessary

rights and privileges to carry out the requested actions. The system may look at an access control matrix or compare security labels to verify that this subject may indeed access the requested resource and perform the actions it is attempting. If the system determines that the subject may access the resource, it authorizes the subject.

Although identification, authentication, authorization, and accountability have close and complementary definitions, each has distinct functions that fulfill a specific requirement in the process of access control. A user may be properly identified and authenticated to the network, but may not have the authorization to access certain files on the file server. On the other hand, a user may be authorized to access the files on the file server, but until she is properly identified and authenticated, those resources are out of reach. Figure 16-1 illustrates the four steps that must happen for a subject to access an object.

1. Identification

2. Authentication

3. Authorization

Resource

4. Accountability

Figure 16-1 Four steps must happen for a subject to access an object: identification, authentication, authorization, and accountability.

Race Condition

A race condition occurs when processes carry out their tasks on a shared resource in an incorrect order. A race condition is possible when two or more processes use a shared resource, such as data within a variable. It is important that the processes carry out their functionality in the correct sequence. If process 2 carried out its task on the data before process 1, the result would be much different than if process 1 carried out its tasks on the data before process 2.

In software, when the authentication and authorization steps are split into two functions, there is a possibility an attacker could use a race condition to force the

authorization step to be completed before the authentication step. This would be a
flaw in the software that the attacker has figured out how to exploit. A race condition
occurs when two or more processes use the same resource and the sequence of steps
within the software can be carried out in an improper order, something that can
drastically affect the output. So, an attacker can force the authorization step to take
place before the authentication step and gain unauthorized access to a resource.

EXAM TIP The words “logical” and “technical” can be used interchangeably in this context. It is conceivable that the CISSP exam would refer to logical and technical controls interchangeably.

An individual’s identity must be verified during the authentication process. Authentication usually involves a two-step process: entering public information (a
username, employee number, account number, or department ID), and then entering private information (a static password, smart token, cognitive password, one-time
password, or PIN). Entering public information is the identification step, while entering
private information is the authentication step of the two-step process. Each technique
used for identification and authentication has its pros and cons. Each should be properly
evaluated to determine the right mechanism for the correct environment.

PART V

The subject needs to be held accountable for the actions taken within a system or
domain. The only way to ensure accountability is if the subject is uniquely identified and
the subject’s actions are recorded.
Logical access controls are technical tools used for identification, authentication,
authorization, and accountability. They are software components that enforce access
control measures for systems, programs, processes, and information. The logical access
controls can be embedded within operating systems, applications, add-on security packages, or database and telecommunication management systems. It can be challenging
to synchronize all access controls and ensure all vulnerabilities are covered without
producing overlaps of functionality. However, if it were easy, security professionals would
not be getting paid the big bucks!

Identification and Authentication

Once a person has been identified through the user ID or a similar value, she must be authenticated, which means she must prove she is who she says she is. Three main types of factors can be used for authentication: something a person knows, something a person has, and something a person is. Sometimes, these factors are combined with two additional factors: somewhere a person is (logical or physical location) and something a person does (behavioral factor). These location and behavioral factors may not be all that strong by themselves, but when combined with other factors they can significantly improve the effectiveness of the authentication process.

Something a person knows (knowledge-based authentication [KBA]) can be, for example, a password, PIN, mother's maiden name, or the combination to a lock. Authenticating a person by something that she knows is usually the least expensive method to implement. The downside to this method is that another person may acquire this knowledge and gain unauthorized access to a resource.

Something a person has (ownership-based authentication) can be a key, swipe card, access card, or badge. This method is common for accessing facilities but could also be used to access sensitive areas or to authenticate systems. A downside to this method is that the item can be lost or stolen, which could result in unauthorized access.

Something specific to a person (biometric authentication) becomes a bit more interesting. This is not based on whether the person is an American, a geek, or an athlete—it is based on a physical attribute. Authenticating a person's identity based on a unique physical attribute is referred to as biometrics.

Strong authentication contains two or all of these three methods: something a person knows, has, or is. Using a biometric system by itself does not provide strong authentication because it provides only one out of the three methods. Biometrics supplies what a person is, not what a person knows or has. For a strong authentication process to be in place, a biometric system needs to be coupled with a mechanism that checks for one of the other two methods. For example, many times the person has to type a PIN into a keypad before the biometric scan is performed. This satisfies the "something the person knows" category. Conversely, the person could be required to swipe a magnetic card through a

One-to-One and One-to-Many
Verification 1:1 is the measurement of an identity against a single claimed identity.
The conceptual question is, “Is this person who he claims to be?” So if Bob provides
his identity and credential set, this information is compared to the data kept in an
authentication database. If they match, we know that it is really Bob. If the identification is 1:N (many), the measurement of a single identity is compared against
multiple identities. The conceptual question is, “Who is this person?” An example is
if fingerprints were found at a crime scene, the cops would run them through their
database to identify the suspect.

reader prior to the biometric scan. This would satisfy the “something the person has”
category. Whatever identification system is used, for strong authentication to be in the
process, it must include multiple factors.
TIP Strong authentication is also sometimes referred to as multifactor authentication (MFA), which just means that more than one authentication method is used. While two-factor authentication (2FA) is common, threefactor authentication (for example, smart card, PIN, and retinal scan) is sometimes used.

Identity is a complicated concept with many varied nuances, ranging from the philosophical to the practical. A person may have multiple digital identities. For example,
a user could be JPublic in a Windows domain environment, JohnP on a Unix server, JohnPublic on the mainframe, JJP in instant messaging, JohnCPublic in the certification
authority, and JohnnyPub on Facebook. If the organization that employs that user wants
to centralize all of its access control, these various identity names for the same person may
cause the security administrator undue stress.
NOTE Mutual authentication is when the two communicating entities must authenticate to each other before passing data. For example, an authentication server may be required to authenticate to a user’s system before allowing data to flow back and forth.

Identification Component Requirements
When issuing identification values to users, the following should be in place:

- Each identifier should be unique, for user accountability.
- A standard naming scheme should be followed.
- The value should be nondescriptive of the user’s position or tasks.
- The value should not be shared between users.

PART V

While most of this chapter deals with user authentication, it is important to realize system-based authentication is possible also. Computers and devices can be identified, authenticated, monitored, and controlled based upon their hardware addresses (media access control) and/or Internet Protocol (IP) addresses. Networks may have network access control (NAC) technology that authenticates systems before they are allowed access to the network. Every network device has a hardware address that is integrated into its network interface card (NIC) and a software-based address (IP) that either is assigned by a Dynamic Host Configuration Protocol (DHCP) server or locally configured.

Knowledge-Based Authentication

We start off our discussion of authentication methods by looking at the most commonly used approach: using something that a person knows. This knowledge-based approach typically uses a password, passphrase, or cognitive password. Let’s take a closer look at each.

Passwords

User identification coupled with a reusable password is the most common form of system identification and authorization mechanisms. A password is a protected string of characters that is used to authenticate an individual. As stated previously, authentication factors are based on what a person knows, has, or is. A password is something the user knows, and in order to ensure its effectiveness for authentication, it must be kept secret.

Password Policies Although passwords are prevalent, they are also considered one of the weakest security mechanisms available. Why? Users usually choose passwords that are easily guessed (a spouse’s name, a user’s birth date, or a dog’s name), or tell others their passwords, and many times write the passwords down on a sticky note and hide it under the keyboard. To most users, security is usually not the most important or interesting part of using their computers—except when someone hacks into their computer and steals confidential information, that is. Then security is all the rage.

This is where password policies step in. If passwords are properly generated, updated,

and kept secret, they can provide effective security. Password generators can be used to create passwords for users. This ensures that a user will not be using “Bob” or “Spot” for a password, but if the generator spits out “kdjasijew284802h,” the user will surely scribble it down on a piece of paper and stick it to the monitor, which defeats the whole purpose.

If a password generator is going to be used, the tools should create uncomplicated, pronounceable, nondictionary words to help users remember them so they aren’t tempted to write them down.

If users can choose their own passwords, the operating system should enforce certain password requirements. The operating system can require that a password contain a certain number of characters, unrelated to the user ID, and not be easily guessable. The operating system can keep track of the passwords a specific user generates so as to ensure no passwords are reused. In March of 2020 the National Institute of Standards and Technology (NIST) updated its guidelines concerning passwords in SP 800-63B. These include the following recommendations:

- Increased password length The longer the password, the harder it is to guess. The recommended minimum password length is 8 characters for user-selected ones and 6 characters for computer-generated passwords. The maximum recommended length is 64 characters.
- Allow special characters Users should be allowed to use any special character, and even emojis, in their passwords. Special characters, however, should not be required.
- Disallow password hints On the surface, password hints may seem to make sense because they allow users to remember complex passwords and reduce reliance on password resetting features. However, they mostly help attackers.

If an attacker is after a password, she can try a few different techniques:

- Electronic monitoring Listening to network traffic to capture information, especially when a user is sending her password to an authentication server. The password can be copied and reused by the attacker at another time, which is called a replay attack.
- Access the password file Usually done on the authentication server. The password file contains many users’ passwords and, if compromised, can be the source of a lot of damage. This file should be protected with access control mechanisms and encryption.
- Brute-force attacks Performed with tools that cycle through many possible character, number, and symbol combinations to uncover a password.
- Dictionary attacks Comparing files of thousands of words to the user’s password

until a match is found.
• Social engineering Falsely convincing an individual that she has the necessary authorization to access specific resources.
• Rainbow table Using a table that contains all possible passwords already in a hash format.

NOTE Clipping level is an older term that just means threshold. If the number of acceptable failed login attempts is set to three, three is the threshold (clipping level) value.

Policies can also specify other conditions that make passwords more difficult to exploit.
Many organizations maintain a password history so users cannot reuse passwords within
a certain timeframe. A variation on this is having the system remember the last n (where
n is some number greater than or equal to one) passwords to prevent their reuse. Policies
can also specify maximum age (that is, expiration) and minimum age (so the password
can’t be changed immediately to bypass the other policies) requirements.
As with many things in life, education is the key. Password requirements, protection,
and generation should be addressed in security awareness programs so users understand

PART V

Certain techniques can be implemented to provide another layer of security for passwords and their use. After each successful logon, a message can be presented to a
user indicating the date and time of the last successful logon, the location of this logon,
and whether there were any unsuccessful logon attempts. This alerts the user to any
suspicious activity and whether anyone has attempted to log on using his credentials.
An administrator can set system parameters that allow a certain number of failed logon
attempts to be accepted before a user is locked out; this is a type of clipping level. The
user can be locked out for five minutes or a full day, for example, after the threshold (or
clipping level) has been exceeded. It depends on how the administrator configures this
mechanism. An audit trail can also be used to track password usage and both successful
and unsuccessful logon attempts. This audit information should include the date, time,
user ID, and workstation the user logged in from.

what is expected of them, why they should protect their passwords, and how passwords
can be stolen. Users should be an extension to a security team, not the opposition.
NOTE Rainbow tables contain passwords already in their hashed format. The attacker just compares a captured hashed password with one that is listed in the table to uncover the plaintext password. This takes much less time than carrying out a dictionary or brute-force attack.

Password Checkers Several organizations test user-chosen passwords using tools that
perform dictionary and/or brute-force attacks to detect the weak passwords. This helps
make the environment as a whole less susceptible to dictionary and exhaustive attacks
used to discover users' passwords. Many times the same tools employed by an attacker to
crack a password are used by a network administrator to make sure the password is strong
enough. Most security tools have this dual nature. They are used by security professionals
and IT staff to test for vulnerabilities within their environment in the hope of uncovering
and fixing them before an attacker finds the vulnerabilities. An attacker uses the same
tools to uncover vulnerabilities to exploit before the security professional can fix them. It
is the never-ending cat-and-mouse game.
If a tool is called a password checker, it is used by a security professional to test the
strength of a password. If a tool is called a password cracker, it is usually used by a hacker;
however, most of the time, these tools are one and the same.
You need to obtain management's approval before attempting to test (break) employees'
passwords with the intent of identifying weak passwords. Explaining you are trying to
help the situation, not hurt it, after you have uncovered the CEO's password is not a
good situation to be in.
Password Hashing and Encryption In most situations, if an attacker sniffs your password from the network wire, she still has some work to do before she actually knows
your password value because most systems hash the password with a hashing algorithm,
commonly Message Digest 5 (MD5) or Secure Hash Algorithm (SHA), to ensure passwords are not sent in cleartext.
Although some people think the world is run by Microsoft, other types of operating
systems are out there, such as Unix and Linux. These systems do not use registries and
SAM databases but contain their user passwords in a file cleverly called "shadow." This
shadow file does not contain passwords in cleartext; instead, your password is

run through
a hashing algorithm, and the resulting value is stored in this file. Unix-type systems zest
things up by using salts in this process. Salts are random values added to passwords prior
to hashing to add more complexity and randomness. The more randomness entered
into the hashing process, the harder it is for the bad guy to decrypt and uncover your
password. The use of a salt means that the same password can be encrypted into several
thousand different hashes. This makes it much more difficult for an adversary to attack
the passwords in your system using approaches like rainbow tables.
Limit Logon Attempts A threshold can be set to allow only a certain number of
unsuccessful logon attempts. After the threshold is met, the user's account can be locked
for a period of time or indefinitely, which requires an administrator to manually unlock

the account. This protects against dictionary and other exhaustive attacks that continually
submit credentials until the right combination of username and password is discovered.

Passphrase
A passphrase is a sequence of characters that is longer than a password (thus a "phrase")
and, in some cases, takes the place of a password during an authentication process. The
user enters this phrase into an application, and the application transforms the value
into a virtual password, making the passphrase the length and format that are required
by the application. (For example, an application may require your virtual password to
be 128 bits to be used as a key with the AES algorithm.) If a user wants to authenticate
to an application, such as Pretty Good Privacy (PGP), he types in a passphrase, let's say
StickWithMeKidAndYouWillWearDiamonds. The application converts this phrase into
a virtual password that is used for the actual authentication. The user usually generates
the passphrase in the same way a user creates a password the first time he logs on to a
computer. A passphrase is more secure than a password because it is longer, and thus
harder to obtain by an attacker. In many cases, the user is more likely to remember a
passphrase than a password.

Cognitive Password

EXAM TIP Knowledge-based authentication means that a subject is authenticated based upon something she knows. This could be a PIN, password, passphrase, cognitive password, personal history information, or through the use of a CAPTCHA, which is the graphical representation of data. A CAPTCHA is a skewed representation of characteristics a person must enter to prove that the subject is a human and not an automated tool as in a software robot.

Biometric Authentication
Biometrics verifies an individual's identity by analyzing a unique personal characteristic,
which is one of the most effective and accurate methods of verifying identification.
Biometrics is a very sophisticated technology; thus, it is much more expensive and complex than the other types of identity verification processes. Biometric systems typically

PART V

Cognitive passwords are fact- or opinion-based information used to verify an individual's
identity. A user is enrolled by answering several questions based on her life experiences.
Passwords can be hard for people to remember, but that same person will not likely forget
the first person they kissed, the name of their best friend in 8th grade, or their favorite
cartoon character. After the enrollment process, the user can answer the questions asked
of her to be authenticated instead of having to remember a password. This authentication process is best for a service the user does not use on a daily basis, because it takes
longer than other authentication mechanisms. This can work well for help-desk services.
The user can be authenticated via cognitive means. This way, the person at the help desk
can be sure he is talking to the right person, and the user in need of help does not need
to remember a password that may be used once every three months.

base authentication decisions on physical attributes (such as iris, retina, or fingerprint),
which provides more accuracy because physical attributes typically don't change, absent
some disfiguring injury, and are harder to impersonate.
Biometrics is typically broken up into two different categories:

• Physiological This category of biometrics uses physical attributes unique to a specific individual to verify that person's identity. Fingerprints are a common

example of a physiological trait used in biometric systems. Physiological is "what you are."

• Behavioral This approach is based on something an individual does uniquely to confirm her identity. An example is signature dynamics. Behavioral is "what you do."

A biometric system scans a person's physiological attribute or behavioral trait and compares it to a record created in an earlier enrollment process. Because this system inspects the grooves of a person's fingerprint, the pattern of someone's retina, or the pitches of someone's voice, it must be extremely sensitive. The system must perform accurate and repeatable measurements of anatomical or behavioral characteristics. This type of sensitivity can easily cause false positives or false negatives. The system must be calibrated so these false positives and false negatives occur infrequently and the results are as accurate as possible.

When a biometric system rejects an authorized individual, it is called a Type I error (false rejection rate [FRR]). When the system accepts impostors who should be rejected, it is called a Type II error (false acceptance rate [FAR]). The goal is to obtain low numbers for each type of error, but Type II errors are the most dangerous and thus the most important to avoid.

When comparing different biometric systems, many different variables are used, but one of the most important metrics is the crossover error rate (CER). This rating is stated as a percentage and represents the point at which the FRR equals the FAR. This rating is the most important measurement when determining the system's accuracy. A biometric system that delivers a CER of 3 will be more accurate than a system that delivers a CER of 4.

NOTE

Crossover error rate (CER) is also called equal error rate (EER).

What is the purpose of this CER value anyway? Using the CER as an impartial judgment of a biometric system helps create standards by which products from different vendors can be fairly judged and evaluated. If you are going to buy a biometric system, you need a way to compare the accuracy between different systems. You can just go by the different vendors' marketing material (they all say they are the best), or you can compare the different CER values of the products to see which one really is more accurate than

the others. It is also a way to keep the vendors honest. One vendor may tell you, “We
have absolutely no Type II errors.” This would mean that their product would not allow

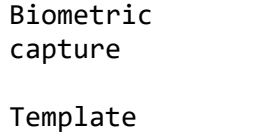
any imposters to be improperly authenticated. But what if you asked the vendor how
many Type I errors their product had and the rep sheepishly replied, “We average around
90 percent of Type I errors.” That would mean that 90 percent of the authentication
attempts would be rejected, which would negatively affect your employees’ productivity.
So you can ask a vendor about their product’s CER value, which represents when the
Type I and Type II errors are equal, to give you a better understanding of the product’s
overall accuracy.
Individual environments have specific security level requirements, which will dictate
how many Type I and Type II errors are acceptable. For example, a military institution
that is very concerned about confidentiality would be prepared to accept a certain rate of
Type I errors, but would absolutely not accept any false accepts (Type II errors). Because
all biometric systems can be calibrated, if you lower the Type II error rate by adjusting
the system’s sensitivity, it will typically result in an increase in Type I errors. The military
institution would obviously calibrate the biometric system to lower the Type II errors to
zero, but that would mean it would have to accept a higher rate of Type I errors.
Biometric authentication is the most expensive method of verifying a person’s identity,
and it faces other barriers to becoming widely accepted. These include user acceptance,
enrollment timeframe, and throughput. Many people are reluctant to let a machine read
the pattern of their retina or scan the geometry of their hand. The enrollment phase
requires an action to be performed several times to capture a clear and distinctive reference
record. People are not particularly fond of expending this time and energy when they are
used to just picking a password and quickly typing it into their console. When a person

attempts to be authenticated by a biometric system, sometimes the system will request an action to be completed several times. If the system is unable to get a clear reading of an iris scan or cannot capture a full voice verification print, the individual may have to repeat the action. This causes low throughput, stretches the individual's patience, and reduces acceptability.

During enrollment, the user provides the biometric data (e.g., fingerprint, voice print, or retina scan), and the biometric reader converts this data into binary values. Depending on the system, the reader may create a hash value of the biometric data, or it may encrypt the data, or do both. The biometric data then goes from the reader to a backend authentication database where the user's account has been created. When the user needs to later authenticate to a system, she provides the necessary biometric data, and the binary format of this information is compared to what is in the authentication database. If they match, then the user is authenticated.

In Figure 16-2, we see that biometric data can be stored on a smart card and used for authentication. Also, you might notice that the match is 95 percent instead of 100 percent. Obtaining a 100 percent match every time is very difficult because of the level of sensitivity of the biometric systems. A smudge on the reader, oil on the person's finger, and other small environmental issues can stand in the way of matching 100 percent. If your biometric system was calibrated so it required 100 percent matches, this would mean you would not allow any Type II errors and that users would commonly not be authenticated in a timely manner.

Figure 16-2 Biometric data is turned into binary data and compared for identity validation.



extraction

Image
processing

10110011
01011000
11001011
01101101
01011000

10110011
01011000
11001011
01101101
01011000

Biometric
matching

95%

Processing Speed
When reviewing biometric devices for purchase, one component to take into consideration is the length of time it takes to actually authenticate users. From the time
a user inserts data until she receives an accept or reject response should take five to
ten seconds.
The following is an overview of the different types of biometric systems and the physiological or behavioral characteristics they examine.

Fingerprint
Fingerprints are made up of ridge endings and bifurcations exhibited by friction ridges
and other detailed characteristics called minutiae. It is the distinctiveness of these minutiae that gives each individual a unique fingerprint. An individual places his finger on a
device that reads the details of the fingerprint and compares this to a reference file. If the
two match, the individual’s identity has been verified.
NOTE Fingerprint systems store the full fingerprint, which is actually a lot of information that takes up hard drive space and resources. The finger-scan technology extracts specific features from the fingerprint and stores just that information, which takes up less hard drive space and allows for quicker database lookups and comparisons.

Palm Scan
The palm holds a wealth of information and has many aspects that are used to identify
an individual. The palm has creases, ridges, and grooves throughout that are

unique to a
specific person. The palm scan also includes the fingerprints of each finger. An individual
places his hand on the biometric device, which scans and captures this information. This
information is compared to a reference file, and the identity is either verified or rejected.

Hand Geometry
The shape of a person's hand (the shape, length, and width of the hand and fingers)
defines hand geometry. This trait differs significantly between people and is used in
some biometric systems to verify identity. A person places her hand on a device that has
grooves for each finger. The system compares the geometry of each finger, and the hand
as a whole, to the information in a reference file to verify that person's identity.

Retina Scan
A system that reads a person's retina scans the blood-vessel pattern of the retina on the
backside of the eyeball. This pattern is unique for each person. A camera is used to
project a beam inside the eye and capture the pattern and compare it to a reference file
recorded previously.
NOTE Retina scans are extremely invasive and involve a number of privacy issues. Since the information obtained through this scan can be used in the diagnosis of medical conditions, it could very well be considered protected health information (PHI) subject to healthcare information privacy regulations such as HIPAA.

The iris is the colored portion of the eye that surrounds the pupil. The iris has unique
patterns, rifts, colors, rings, coronas, and furrows. The uniqueness of each of these characteristics within the iris is captured by a camera and compared with the information
gathered during the enrollment phase. Of the biometric systems, iris scans are the most
accurate. The iris remains constant through adulthood, which reduces the type of errors
that can happen during the authentication process. Sampling the iris offers more reference coordinates than any other type of biometric. Mathematically, this means it has a
higher accuracy potential than any other type of biometric.
NOTE When using an iris pattern biometric system, the optical unit must be positioned so the sun does not shine into the aperture; thus, when the system is implemented, it must be properly placed within the facility.

Signature Dynamics
When a person writes a signature, usually they do so in the same manner and at the same

speed each time. Writing a signature produces electrical signals that can be captured by

PART V

Iris Scan

a biometric system. The physical motions performed when someone is signing a document create these electrical signals. The signals provide unique characteristics that can
be used to distinguish one individual from another. Signature dynamics provides more
information than a static signature, so there are more variables to verify when confirming
an individual’s identity and more assurance that this person is who he claims to be.
Signature dynamics is different from a digitized signature. A digitized signature is just
an electronic copy of someone’s signature and is not a biometric system that captures the
speed of signing, the way the person holds the pen, and the pressure the signer exerts to
generate the signature.

Keystroke Dynamics
Whereas signature dynamics is a method that captures the electrical signals when a person signs a name, keystroke dynamics captures electrical signals when a person types a
certain phrase. As a person types a specified phrase, the biometric system captures the
speed and motions of this action. Each individual has a certain style and speed of typing,
which translate into unique signals. This type of authentication is more effective than
typing in a password, because a password is easily obtainable. It is much harder to repeat
a person’s typing style than it is to acquire a password.

Voice Print
People’s speech sounds and patterns have many subtle distinguishing differences. A biometric system that is programmed to capture a voice print and compare it to the information held in a reference file can differentiate one individual from another. During
the enrollment process, an individual is asked to say several different words. Later, when
this individual needs to be authenticated, the biometric system jumbles these words and
presents them to the individual. The individual then repeats the sequence of words given.
This technique is used so others cannot attempt to record the session and play it back in

hopes of obtaining unauthorized access.

Facial Scan
A system that scans a person’s face takes many attributes and characteristics into account.
People have different bone structures, nose ridges, eye widths, forehead sizes, and chin
shapes. These are all captured during a facial scan and compared to an earlier captured
scan held within a reference record. If the information is a match, the person is positively
identified.
A naïve implementation of this technology could be fooled by a photograph of the legitimate user. To thwart this approach, the scanner can perform a three-dimensional
measurement of the user’s face by projecting thousands of infrared dots on it. This is how
Apple’s Face ID works.

Hand Topography
Whereas hand geometry looks at the size and width of an individual’s hand and fingers,
hand topology looks at the different peaks and valleys of the hand, along with its overall
shape and curvature. When an individual wants to be authenticated, she places her hand
on the system. Off to one side of the system, a camera snaps a side-view picture of the

Biometric Issues and Concerns
Biometric systems are not without their own sets of issues and concerns. Because they depend upon the specific and unique traits of living things, problems can arise.
Living things are notorious for not remaining the same, which means they won’t present static biometric information for every login attempt. Voice recognition can
be hampered by a user with a cold. Retinas can detach. Someone could lose a finger.
Or all three could happen. You just never know in this crazy world.
Some biometric systems actually check for the pulsation and/or heat of a body part to make sure it is alive. So if you are planning to cut someone’s finger off or
pluck out someone’s eyeball so you can authenticate yourself as a legitimate user, it
may not work. Although not specifically stated, this type of activity definitely falls
outside the bounds of the CISSP ethics you will be responsible for upholding once
you receive your certification.

hand from a different view and angle than that of systems that target hand

geometry, and
thus captures different data. This attribute is not unique enough to
authenticate individuals by itself and is commonly used in conjunction with hand
geometry.

Ownership-Based Authentication

One-Time Password
A one-time password (OTP), also called a dynamic password, is used for
authentication
purposes and is valid only once. After the password is used, it is no longer
valid; thus, it
can’t be reused if a hacker obtains it. The password is generated by a token
device, which
is something the person owns (or at least carries around). This device is the
most common implementation mechanism for OTP and generates the one-time password
for the
user to submit to an authentication server. It is commonly implemented in three
formats:
as a dedicated physical device with a small screen that displays the OTP, as a
smartphone
application, and as a service that sends an SMS message to your phone. The
following sections explain the concepts behind this technology.
NOTE SMS was deprecated as a means of providing 2FA by the NIST in
2017. It is widely considered an insecure channel but is unfortunately still in
common use.

PART V

Authentication can also be based on something that the subject has. This is
almost always
some sort of physical or logical token. It can be a device such as a phone,
identification
card, or even an implanted device. It can also be a cryptographic key, such as a
private
key in public key infrastructure (PKI). Sometimes, access to the token is
protected by
some other authentication process, such as when you have to unlock your phone to
get
to a software-based token generator.

The Token Device The token device, or password generator, is usually a handheld
device that has a display and possibly a keypad. This hardware is separate from
the
computer the user is attempting to access. The token device and authentication
service
must be synchronized in some manner to be able to authenticate a user. The token
device
presents the user with a list of characters to be entered as a password when
logging on
to a computer. Only the token device and authentication service know the meaning

of
these characters. Because the two are synchronized, the token device presents the exact
password the authentication service is expecting. This is a one-time password, also called
a token, and is no longer valid after initial use.
Synchronous A synchronous token device requires the device and the authentication
service to advance to the next OTP in sync with each other. This change can be triggered
by time (e.g., every 30 seconds a new OTP is in play) or by simply going down a
preagreed sequence of passwords, each of which is used only once before both the device
and the server advance to the next one. The device displays the OTP to the user, who
then enters this value and a user ID. The authentication service decrypts credentials and
compares the OTP to the value it expects. If the two match, the user is authenticated and
allowed to access the system.

RSA SecurID
RSA SecurID, from RSA Security LLC, is a well-known time-based token. One
version of the product generates the OTP by using a mathematical function on the
time, date, and ID of the token card. Another version of the product requires a PIN
to be entered into the token device.
RSA SecureID Time-Synchronous Two-Factor Authentication

UserID: asmith
PIN:kzw08
Token code: 345734

UserID: asmith
PIN:kzw08
Token code: 345734

RSA
authentication
agent

RSA
authentication
manager
345734
RAS, VPN,
SSL-VPN, WLAN,
Web, and more

Algorithm
Time

Seed

Same algorithm
Same time

Used by permission of RSA Security, Inc., © Copyright RSA Security, Inc. 2012

Same seed

EXAM TIP Synchronous token-based OTP generation can be time-based or counter-based. Another term for counter-based is event-based. Counterbased and event-based are interchangeable terms, and you could see either or both on the CISSP exam.

Asynchronous A token device using an asynchronous token–generating method employs a challenge/response scheme to authenticate the user. In this situation, the authentication server sends the user a challenge, a random value, also called a nonce. The user enters this random value into the token device, which encrypts it and returns a value the user uses as an OTP. The user sends this value, along with a username, to the authentication server. If the authentication server can decrypt the value and it is the same challenge value sent earlier, the user is authenticated, as shown in Figure 16-3.
EXAM TIP The actual implementation and process that these devices follow can differ between different vendors. What is important to know is that asynchronous is based on challenge/response mechanisms, while synchronous is based on time- or counter-driven mechanisms.

Both token systems can fall prey to masquerading if a user shares his identification information (ID or username) and the token device is shared or stolen. The token device can also have battery failure or other malfunctions that would stand in the way of a successful authentication. However, this type of system is not vulnerable to electronic eavesdropping, sniffing, or password guessing.
PART V

6.

1.

2.

4.

5.
Authentication

server

3.

1. Challenge value displayed on workstation.
2. User enters challenge value and PIN into token device.
3. Token device presents a different value to the user.
4. User enters new value into the workstation.
5. Value sent to authentication service on server.
6. AS sends an “allow access” response.

Figure 16-3 Authentication using an asynchronous token device includes a workstation, token device, and authentication service.

If the user has to enter a password or PIN into the token device before it provides an OTP, then strong authentication is in effect because it is using two factors—something the user knows (PIN) and something the user has (the token device).

NOTE One-time passwords can also be generated in software, in which case a piece of hardware such as a token device is not required. These are referred to as soft tokens and require that the authentication service and application contain the same base secrets, which are used to generate the OTPs.

Cryptographic Keys

Another way to prove one’s identity is to use asymmetric cryptography and let the users’ private keys show they are who they claim to be. Recall that the private key is kept secret by an individual and should never be shared. So, if the authentication server has (or gets a hold of) the user’s public key, it can use that key to encrypt a challenge and send it to the user. Only the person owning the corresponding private key would be able to decrypt it and respond to it. Ideally, the user then encrypts the response using the server’s public key to provide mutual authentication. This approach is commonly used in Secure Shell (SSH) instead of passwords, which are the weakest form of authentication and can be easily sniffed as they travel over a network.

Memory Cards

The main difference between memory cards and smart cards is their capacity to process information. A memory card holds information but cannot process information. A smart card holds information and has the necessary hardware and software to actually process

that information. A memory card can hold a user's authentication information so the user only needs to type in a user ID or PIN and present the memory card, and if the data that the user enters matches the data on the memory card, the user is successfully authenticated. If the user presents a PIN value, then this is an example of two-factor authentication—something the user knows and something the user has. A memory card can also hold identification data that is pulled from the memory card by a reader. It travels with the PIN to a backend authentication server.

An example of a memory card is a swipe card that must be used for an individual to be able to enter a building. The user enters a PIN and swipes the memory card through a card reader. If this is the correct combination, the reader flashes green and the individual can open the door and enter the building. Another example is an ATM card. If Buffy wants to withdraw $40 from her checking account, she needs to slide the ATM card (or memory card) through the reader and enter the correct PIN.

Memory cards can be used with computers, but they require a reader to process the information. The reader adds cost to the process, especially when one is needed per computer, and card generation adds cost and effort to the whole authentication process. Using a memory card provides a more secure authentication method than using a password because the attacker would need to obtain the card and know the correct PIN. Administrators and management must weigh the costs and benefits of a memory

token–based card implementation to determine if it is the right authentication mechanism for their environment.

Smart Card

A smart card has the capability of processing information because it has a microprocessor and integrated circuits incorporated into the card itself. Memory cards do not have this type of hardware and lack this type of functionality. The only function they can perform is simple storage. A smart card, which adds the capability to process information stored on it, can also provide a two-factor authentication method because the user may have to enter a PIN to unlock the smart card. This means the user must provide something she