one block of ciphertext is propagated to all subsequent blocks of plaintext in PCBC mode (see Figure F.2 in Appendix F). 4.4 Suppose that, in PCBC mode, blocks Ci and Ci+1 are interchanged during transmission. Show that this affects only the decrypted blocks Pi and Pi+1 but not subsequent blocks. 4.5 In addition to providing a standard for public-key certificate formats, X.509 specifies an authentication protocol. The original version of X.509 contains a security flaw. The essence of the protocol is A S B: A {tA, rA, IDB} B S A: B {tB, rB, IDA, rA} A S B: A {rB} where tA and tB are timestamps, rA and rB are nonces, and the notation X {Y} indicates that the message Y is transmitted, encrypted, and signed by X. The text of X.509 states that checking timestamps tA and tB is optional for three-way authentication. But consider the following example: Suppose A and B have used the preceding protocol on some previous occasion, and that opponent C has intercepted the preceding three messages. In addition, suppose that timestamps are not used and are all set to 0. Finally, suppose C wishes to impersonate A to B. C initially sends the first captured message to B: C S B: A {0, rA, IDB} B responds, thinking it is talking to A but is actually talking to C: B S C: B {0, r B = , IDA, rA} C meanwhile causes A to initiate authentication with C by some means. As a result, A sends C the following: A S C: A {0, rA = , IDC} C responds to A using the same nonce provided to C by B. C S A: C {0, r B = , IDA, rA = } A responds with A S C: A {r B = } This is exactly what C needs to convince B that it is talking to A, so C now repeats the incoming message back out to B. C S B: A {r B = } So B will believe it is talking to A, whereas it is actually talking to C. Suggest a simple solution to this problem that does not involve the use of timestamps. 158 chapter 4 / Key Distribution and User Authentication 4.6 Consider a one-way authentication technique based on asymmetric encryption: A S B: IDA B S A: R1 A S B: E(PRa, R1) a. Explain the protocol. b. What type of attack is this protocol susceptible to? 4.7 Consider a one-way authentication technique based on asymmetric encryption: A S B: IDA B S A: E(PUa, R2) A S B: R2 a. Explain the protocol. b. What type of attack is this protocol susceptible to? 4.8 In Kerberos, how do servers verify the authenticity of the client using the ticket? 4.9 In Kerberos, how does an authentication server protect a ticket from being altered by the client or opponent? 4.10 How is ticket reuse by an opponent prevented in Kerberos? 4.11 What is the purpose of a session key in Kerberos? How is it distributed by the AS? 4.12 The 1988 version of X.509 lists properties that RSA keys must satisfy to be secure, given current knowledge about the difficulty of factoring large numbers. The discussion concludes with a constraint on the public exponent and the modulus n: It must be ensured that e 7 log2(n) to prevent attack by taking the eth root mod n to disclose the plaintext. Although the constraint is correct, the reason given for requiring it is incorrect. What is wrong with the reason given and what is the correct reason? 4.13 Find at least one intermediate certification authority's certificate and one trusted root certification authority's certificate on your computer (e.g., in the browser). Print screenshots of both the general and details tab for each certificate. 4.14 NIST defines the term "cryptoperiod" as the time span during which a specific key is authorized for use or in which the keys for a given system or application may remain in effect. One document on key management uses the following time diagram for a shared secret key. Originator Usage Period Recipient Usage Period Cryptoperiod Explain the overlap by giving an example application in which the originator's usage period for the shared secret key begins before the recipient's usage period and also ends before the recipient's usage period. 4.8 / Key Terms, Review Questions, and Problems 159 4.15 Consider the following protocol, designed to let A and B decide on a fresh, shared session key KAB = . We assume that they already share a long-term key KAB. 1. A S B: A, NA 2. B S A: E(KAB, [NA, KAB =]) 3. A S B: E(KAB = , NA) a. We first try to understand the protocol

designer's reasoning: ■■ Why would A and B believe after the protocol ran that they share KAB = with the other party? ■■ Why would they believe that this shared key is fresh? In both cases, you should explain both the reasons of both A and B, so your answer should complete the following sentences. A believes that she shares KAB = with B since . . . B believes that he shares KAB = with A since . . . A believes that KAB = is fresh since . . . B believes that KAB = is fresh since . . . b. Assume now that A starts a run of this protocol with B. However, the connection is intercepted by the adversary C. Show how C can start a new run of the protocol using reflection, causing A to believe that she has agreed on a fresh key with B (in spite of the fact that she has only been communicating with C). Thus, in particular, the belief in (a) is false. c. Propose a modification of the protocol that prevents this attack. 4.16 List the different management functions of the PKIX model. 4.17 Explain the entities and data flows of generic identity management architecture. 4.18 Consider the following protocol: A S KDC: IDA } IDB }N1 KDC S A: E(Ka, [KS } IDB }N1 } E(Kb, [KS } IDA])) A S B: E(Kb, [KS } IDA]) B S A: E(KS, N2)A S B: E(KS, f(N2)) a. Explain the protocol. b. Can you think of a possible attack on this protocol? Explain how it can be done. c. Mention a possible technique to get around the attack—not a detailed mechanism, just the basics of the idea. Note: The remaining problems deal with a cryptographic product developed by IBM, which is briefly described in a document at this book's Web site in IBMCrypto.pdf. Try these problems after reviewing the document. 4.19 What is the effect of adding the instruction EMKi ? EMKi : X S E(KMHi , X) i = 0, 1 4.20 Suppose N different systems use the IBM Cryptographic Subsystem with host master keys KMH[i](i = 1, 2, c, N). Devise a method for communicating between systems without requiring the system to either share a common host master key or to divulge their individual host master keys. Hint: Each system needs three variants of its host master key. 4.21 The principal objective of the IBM Cryptographic Subsystem is to protect transmissions between a terminal and the processing system. Devise a procedure, perhaps adding instructions, which will allow the processor to generate a session key KS and distribute it to Terminal i and Terminal j without having to store a key-equivalent variable in the host. 160 5.1 Network Access Control Elements of a Network Access Control System Network Access Enforcement Methods 5.2 Extensible Authentication Protocol Authentication Methods EAP Exchanges 5.3 IEEE 802.1X Port-Based Network Access Control 5.4 Cloud Computing Cloud Computing Elements Cloud Computing Reference Architecture 5.5 Cloud Security Risks and Countermeasures 5.6 Data Protection in the Cloud 5.7 Cloud Security as a Service 5.8 Addressing Cloud Computing Security Concerns 5.9 Key Terms, Review Questions, and Problems Chapter Network Access Control and Cloud Security 5.1 / Network Access Control 161 This chapter begins our discussion of network security, focusing on two key topics: network access control and cloud security. We begin with an overview of network access control systems, summarizing the principal elements and techniques involved in such a system. Next, we discuss the Extensible Authentication Protocol and IEEE 802.1X, two widely implemented standards that are the foundation of many network access control systems. The remainder of the chapter deals with cloud security. We begin with an overview of cloud computing, and follow this with a discussion of cloud security issues. 5.1 Network Access Control Network access control (NAC) is an umbrella term for managing access to a network. NAC authenticates users logging into the network and determines what data they can access and actions they can perform. NAC also examines the health of the user's computer or mobile device (the endpoints). Elements of a Network Access Control System NAC systems deal with three categories of components: ■■ Access requestor (AR): The AR is the node that is attempting to access the network and

may be any device that is managed by the NAC system, including workstations, servers, printers, cameras, and other IP-enabled devices. ARs are also referred to as supplicants, or simply, clients. ■■ Policy server: Based on the AR's posture and an enterprise's defined policy, the policy server determines what access should be granted. The policy server often relies on backend systems, including antivirus, patch management, or a user directory, to help determine the host's condition. Learning Objectives After studying this chapter, you should be able to: ◆ Discuss the principal elements of a network access control system. ◆ Discuss the principal network access enforcement methods. ◆ Present an overview of the Extensible Authentication Protocol. ◆ Understand the operation and role of the IEEE 802.1X Port-Based Network Access Control mechanism. ◆ Present an overview of cloud computing concepts. ◆ Understand the unique security issues related to cloud computing. 162 chapter 5 / Network Access Control and Cloud Security ■■ Network access server (NAS): The NAS functions as an access control point for users in remote locations connecting to an enterprise's internal network. Also called a media gateway, a remote access server (RAS), or a policy server, an NAS may include its own authentication services or rely on a separate authentication service from the policy server. Figure 5.1 is a generic network access diagram. A variety of different ARs seek access to an enterprise network by applying to some type of NAS. The first step is generally to authenticate the AR. Authentication typically involves some sort of secure protocol and the use of cryptographic keys. Authentication may be performed by the NAS, or the NAS may mediate the authentication process. In the latter case, authentication takes place between the supplicant and an authentication server that is part of the policy server or that is accessed by the policy server. The authentication process serves a number of purposes. It verifies a supplicant's claimed identity, which enables the policy server to determine what access privileges, if any, the AR may have. The authentication exchange may result in the Figure 5.1 Network Access Control Context Supplicants Network access servers Authentication server DHCP server VLAN server Policy server Patch management Network resources Quarantine network Antivirus Antispyware Enterprise network 5.1 / Network Access Control 163 establishment of session keys to enable future secure communication between the supplicant and resources on the enterprise network. Typically, the policy server or a supporting server will perform checks on the AR to determine if it should be permitted interactive remote access connectivity. These checks—sometimes called health, suitability, screening, or assessment checks—require software on the user's system to verify compliance with certain requirements from the organization's secure configuration baseline. For example, the user's antimalware software must be up-to-date, the operating system must be fully patched, and the remote computer must be owned and controlled by the organization. These checks should be performed before granting the AR access to the enterprise network. Based on the results of these checks, the organization can determine whether the remote computer should be permitted to use interactive remote access. If the user has acceptable authorization credentials but the remote computer does not pass the health check, the user and remote computer should be denied network access or have limited access to a quarantine network so that authorized personnel can fix the security deficiencies. Figure 5.1 indicates that the quarantine portion of the enterprise network consists of the policy server and related AR suitability servers. There may also be application servers that do not require the normal security threshold be met. Once an AR has been authenticated and cleared for a certain level of access to the enterprise network, the NAS can enable the AR to interact with resources in the enterprise network. The NAS may mediate every exchange to enforce

a security policy for this AR, or may use other methods to limit the privileges of the AR. Network Access Enforcement Methods Enforcement methods are the actions that are applied to ARs to regulate access to the enterprise network. Many vendors support multiple enforcement methods simultaneously, allowing the customer to tailor the configuration by using one or a combination of methods. The following are common NAC enforcement methods. ■■ IEEE 802.1X: This is a link layer protocol that enforces authorization before a port is assigned an IP address. IEEE 802.1X makes use of the Extensible Authentication Protocol for the authentication process. Sections 5.2 and 5.3 cover the Extensible Authentication Protocol and IEEE 802.1X, respectively. ■■ Virtual local area networks (VLANs): In this approach, the enterprise network, consisting of an interconnected set of LANs, is segmented logically into a number of virtual LANs.1 The NAC system decides to which of the network's VLANs it will direct an AR, based on whether the device needs security remediation, Internet access only, or some level of network access to enterprise resources. VLANs can be created dynamically and VLAN membership, of both enterprise servers and ARs, may overlap. That is, an enterprise server or an AR may belong to more than one VLAN. 1 A VLAN is a logical subgroup within a LAN that is created via software rather than manually moving cables in the wiring closet. It combines user stations and network devices into a single unit regardless of the physical LAN segment they are attached to and allows traffic to flow more efficiently within populations of mutual interest. VLANs are implemented in port-switching hubs and LAN switches. 164 chapter 5 / Network Access Control and Cloud Security ■■ Firewall: A firewall provides a form of NAC by allowing or denying network traffic between an enterprise host and an external user. Firewalls are discussed in Chapter 12. ■■ DHCP management: The Dynamic Host Configuration Protocol (DHCP) is an Internet protocol that enables dynamic allocation of IP addresses to hosts. A DHCP server intercepts DHCP requests and assigns IP addresses instead. Thus, NAC enforcement occurs at the IP layer based on subnet and IP assignment. A DCHP server is easy to install and configure, but is subject to various forms of IP spoofing, providing limited security. There are a number of other enforcement methods available from vendors. The ones in the preceding list are perhaps the most common, and IEEE 802.1X is by far the most commonly implemented solution. 5.2 Extensible Authentication Protocol The Extensible Authentication Protocol (EAP), defined in RFC 3748, acts as a framework for network access and authentication protocols. EAP provides a set of protocol messages that can encapsulate various authentication methods to be used between a client and an authentication server. EAP can operate over a variety of network and link level facilities, including point-to-point links, LANs, and other networks, and can accommodate the authentication needs of the various links and networks. Figure 5.2 illustrates the protocol layers that form the context for EAP. Authentication Methods EAP supports multiple authentication methods. This is what is meant by referring to EAP as extensible. EAP provides a generic transport service for the exchange of authentication information between a client system and an authentication server. The basic EAP transport service is extended by using a specific authentication protocol, or method, that is installed in both the EAP client and the authentication server. Figure 5.2 EAP Layered Context Authentication methods EAP layer Data link layer Extensible Authentication Protocol (EAP) IEEE 802.1X EAP over LAN (EAPOL) EAPTLS EAPTTLS EAPPSK EAPIKEv2 PPP 802.3 Ethernet 802.11 WLAN Other Other 5.2 / Extensible Authentication Protocol 165 Numerous methods have been defined to work over EAP. The following are commonly supported EAP methods: ■■ EAP-TLS (EAP Transport Layer Security): EAP-TLS (RFC 5216) defines how the TLS protocol (described in Chapter 6) can be

encapsulated in EAP messages. EAP-TLS uses the handshake protocol in TLS, not its encryption method. Client and server authenticate each other using digital certificates. Client generates a pre-master secret key by encrypting a random number with the server's public key and sends it to the server. Both client and server use the pre-master to generate the same secret key. ■■ EAP-TTLS (EAP Tunneled TLS): EAP-TTLS is like EAP-TLS, except only the server has a certificate to authenticate itself to the client first. As in EAPTLS, a secure connection (the "tunnel") is established with secret keys, but that connection is used to continue the authentication process by authenticating the client and possibly the server again using any EAP method or legacy method such as PAP (Password Authentication Protocol) and CHAP (Challenge-Handshake Authentication Protocol). EAP-TTLS is defined in RFC 5281. ■■ EAP-GPSK (EAP Generalized Pre-Shared Key): EAP-GPSK, defined in RFC 5433, is an EAP method for mutual authentication and session key derivation using a Pre-Shared Key (PSK). EAP-GPSK specifies an EAP method based on pre-shared keys and employs secret key-based cryptographic algorithms. Hence, this method is efficient in terms of message flows and computational costs, but requires the existence of pre-shared keys between each peer and EAP server. The set up of these pairwise secret keys is part of the peer registration, and thus, must satisfy the system preconditions. It provides a protected communication channel when mutual authentication is successful for both parties to communicate over and is designed for authentication over insecure networks such as IEEE 802.11. EAP-GPSK does not require any public-key cryptography. The EAP method protocol exchange is done in a minimum of four messages. ■■ EAP-IKEv2: It is based on the Internet Key Exchange protocol version 2 (IKEv2), which is described in Chapter 9. It supports mutual authentication and session key establishment using a variety of methods. EAP-TLS is defined in RFC 5106. EAP Exchanges Whatever method is used for authentication, the authentication information and authentication protocol information are carried in EAP messages. RFC 3748 defines the goal of the exchange of EAP messages to be successful authentication. In the context of RFC 3748, successful authentication is an exchange of EAP messages, as a result of which the authenticator decides to allow access by the peer, and the peer decides to use this access. The authenticator's decision typically involves both authentication and authorization aspects; the peer may successfully authenticate to the authenticator, but access may be denied by the authenticator due to policy reasons. 166 chapter 5 / Network Access Control and Cloud Security Figure 5.3 indicates a typical arrangement in which EAP is used. The following components are involved: ■■ EAP peer: Client computer that is attempting to access a network. ■■ EAP authenticator: An access point or NAS that requires EAP authentication prior to granting access to a network. ■■ Authentication server: A server computer that negotiates the use of a specific EAP method with an EAP peer, validates the EAP peer's credentials, and authorizes access to the network. Typically, the authentication server is a Remote Authentication Dial-In User Service (RADIUS) server. The authentication server functions as a backend server that can authenticate peers as a service to a number of EAP authenticators. The EAP authenticator then makes the decision of whether to grant access. This is referred to as the EAP pass-through mode. Less commonly, the authenticator takes over the role of the EAP server; that is, only two parties are involved in the EAP execution. As a first step, a lower-level protocol, such as PPP (point-to-point protocol) or IEEE 802.1X, is used to connect to the EAP authenticator. The software entity in the EAP peer that operates at this level is referred to as the supplicant. EAP messages containing the appropriate information for a chosen EAP method are then exchanged between the EAP peer and the authentication server. EAP messages may

include the following fields: ■■ Code: Identifies the Type of EAP message. The codes are Request (1), Response (2), Success (3), and Failure (4). ■■ Identifier: Used to match Responses with Requests. ■■ Length: Indicates the length, in octets, of the EAP message, including the Code, Identifier, Length, and Data fields. Figure 5.3 EAP Protocol Exchanges Method EAP peer/ authenticator EAP layer Lower layer EAP authenticator EAP layer Lower layer Method EAP peer/ authenticator EAP layer Lower layer RADIUS EAP messages EAP messages 802.1X, PPP EAP peer EAP authenticator Authentication server (RADIUS) 5.2 / Extensible Authentication Protocol 167 ■■ Data: Contains information related to authentication. Typically, the Data field consists of a Type subfield, indicating the type of data carried, and a Type-Data field. The Success and Failure messages do not include a Data field. The EAP authentication exchange proceeds as follows. After a lower-level exchange that established the need for an EAP exchange, the authenticator sends a Request to the peer to request an identity, and the peer sends a Response with the identity information. This is followed by a sequence of Requests by the authenticator and Responses by the peer for the exchange of authentication information. The information exchanged and the number of Request–Response exchanges needed depend on the authentication method. The conversation continues until either (1) the authenticator determines that it cannot authenticate the peer and transmits an EAP Failure or (2) the authenticator determines that successful authentication has occurred and transmits an EAP Success. Figure 5.4 gives an example of an EAP exchange. Not shown in the figure is a message or signal sent from the EAP peer to the authenticator using some protocol other than EAP and requesting an EAP exchange to grant network access. One protocol used for this purpose is IEEE 802.1X, discussed in the next section. The first pair of EAP Request and Response messages is of Type identity, in which the authenticator requests the peer's identity, and the peer returns its claimed identity in the Response message. This Response is passed through the authenticator to the authentication server. Subsequent EAP messages are exchanged between the peer and the authentication server. Figure 5.4 EAP Message Flow in Pass-Through Mode EAP peer EAP-Response/Identity EAP-Request/Identity EAP authenticator Authentication server (RADIUS) EAP-Response/Auth EAP-Request/Auth EAP-Response/Auth EAP-Request/Auth EAP-Success/Failure 168 chapter 5 / Network Access Control and Cloud Security Upon receiving the identity Response message from the peer, the server selects an EAP method and sends the first EAP message with a Type field related to an authentication method. If the peer supports and accepts the selected EAP method, it replies with the corresponding Response message of the same type. Otherwise, the peer sends a NAK, and the EAP server either selects another EAP method or aborts the EAP execution with a failure message. The selected EAP method determines the number of Request/Response pairs. During the exchange the appropriate authentication information, including key material, is exchanged. The exchange ends when the server determines that authentication has succeeded or that no further attempt can be made and authentication has failed. 5.3 IEEE 802.1X Port-Based Network Access Control IEEE 802.1X Port-Based Network Access Control was designed to provide access control functions for LANs. Table 5.1 briefly defines key terms used in the IEEE 802.11 standard. The terms supplicant, network access point, and authentication Authenticator An entity at one end of a point-to-point LAN segment that facilities authentication of the entity to the other end of the link. Authentication exchange The two-party conversation between systems performing an authentication process. Authentication process The cryptographic operations and supporting data frames that perform the actual authentication. Authentication server (AS)

An entity that provides an authentication service to an authenticator. This service determines, from the credentials provided by supplicant, whether the supplicant is authorized to access the services provided by the system in which the authenticator resides. Authentication transport The datagram session that actively transfers the authentication exchange between two systems. Bridge port A port of an IEEE 802.1D or 802.1Q bridge. Edge port A bridge port attached to a LAN that has no other bridges attached to it. Network access port A point of attachment of a system to a LAN. It can be a physical port, such as a single LAN MAC attached to a physical LAN segment, or a logical port, for example, an IEEE 802.11 association between a station and an access point. Port access entity (PAE) The protocol entity associated with a port. It can support the protocol functionality associated with the authenticator, the supplicant, or both. Supplicant An entity at one end of a point-to-point LAN segment that seeks to be authenticated by an authenticator attached to the other end of that link. Table 5.1 Terminology Related to IEEE 802.1X 5.3 / IEEE 802.1X Port-Based Network Access Control 169 server correspond to the EAP terms peer, authenticator, and authentication server, respectively. Until the AS authenticates a supplicant (using an authentication protocol), the authenticator only passes control and authentication messages between the supplicant and the AS; the 802.1X control channel is unblocked, but the 802.11 data channel is blocked. Once a supplicant is authenticated and keys are provided, the authenticator can forward data from the supplicant, subject to predefined access control limitations for the supplicant to the network. Under these circumstances, the data channel is unblocked. As indicated in Figure 5.5, 802.1X uses the concepts of controlled and uncontrolled ports. Ports are logical entities defined within the authenticator and refer to physical network connections. Each logical port is mapped to one of these two types of physical ports. An uncontrolled port allows the exchange of protocol data units (PDUs) between the supplicant and the AS, regardless of the authentication state of the supplicant. A controlled port allows the exchange of PDUs between a supplicant and other systems on the network only if the current state of the supplicant authorizes such an exchange. The essential element defined in 802.1X is a protocol known as EAPOL (EAP over LAN). EAPOL operates at the network layers and makes use of an IEEE 802 LAN, such as Ethernet or Wi-Fi, at the link level. EAPOL enables a supplicant to communicate with an authenticator and supports the exchange of EAP packets for authentication. Figure 5.5 802.1X Access Control Supplicant Network access point Uncontrolled port Controlled port Authentication server Network or Internet 170 chapter 5 / Network Access Control and Cloud Security The most common EAPOL packets are listed in Table 5.2. When the supplicant first connects to the LAN, it does not know the MAC address of the authenticator. Actually it doesn't know whether there is an authenticator present at all. By sending an EAPOL-Start packet to a special group-multicast address reserved for IEEE 802.1X authenticators, a supplicant can determine whether an authenticator is present and let it know that the supplicant is ready. In many cases, the authenticator will already be notified that a new device has connected from some hardware notification. For example, a hub knows that a cable is plugged in before the device sends any data. In this case the authenticator may preempt the Start message with its own message. In either case the authenticator sends an EAP-Request Identity message encapsulated in an EAPOL-EAP packet. The EAPOL-EAP is the EAPOL frame type used for transporting EAP packets. The authenticator uses the EAP-Key packet to send cryptographic keys to the supplicant once it has decided to admit it to the network. The EAP-Logoff packet type indicates that the supplicant wishes to be disconnected from the network. The EAPOL packet format includes the following fields: ■■ Protocol version:

version of EAPOL. ■■ Packet type: indicates start, EAP, key, logoff, etc. ■■ Packet body length: If the packet includes a body, this field indicates the body length. ■■ Packet body: The payload for this EAPOL packet. An example is an EAP packet. Figure 5.6 shows an example of exchange using EAPOL. In Chapter 7, we examine the use of EAP and EAPOL in the context of IEEE 802.11 wireless LAN security. 5.4 Cloud Computing There is an increasingly prominent trend in many organizations to move a substantial portion of or even all information technology (IT) operations to an Internetconnected infrastructure known as enterprise cloud computing. This section provides an overview of cloud computing. For a more detailed treatment, see [STAL16b]. Frame Type Definition EAPOL-EAP Contains an encapsulated EAP packet. EAPOL-Start A supplicant can issue this packet instead of waiting for a challenge from the authenticator. EAPOL-Logoff Used to return the state of the port to unauthorized when the supplicant is finished using the network. EAPOL-Key Used to exchange cryptographic keying information. Table 5.2 Common EAPOL Frame Types 5.4 / Cloud Computing 171 Cloud Computing Elements NIST defines cloud computing, in NIST SP 800-145 (The NIST Definition of Cloud Computing), as follows: Figure 5.6 Example Timing Diagram for IEEE 802.1X EAP peer EAPOL-Start EAPOL-EAP (EAP-Request/Identity) EAPOL-EAP (EAP-Response/Identity) EAP authenticator Authentication server (RADIUS) EAPOL-Logo EAPOL-EAP (EAP-Response/Auth) EAPOL-EAP (EAP-Request/Auth) EAPOL-EAP (EAP-Response/Auth) EAPOL-EAP (EAP-Request/Auth) EAPOL-EAP (EAP-Success) Cloud computing: A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models. The definition refers to various models and characteristics, whose relationship is illustrated in Figure 5.7. The essential characteristics of cloud computing include the following: ■■ Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous 172 chapter 5 / Network Access Control and Cloud Security thin or thick client platforms (e.g., mobile phones, laptops, and PDAs) as well as other traditional or cloud-based software services. ■■ Rapid elasticity: Cloud computing gives you the ability to expand and reduce resources according to your specific service requirement. For example, you may need a large number of server resources for the duration of a specific task. You can then release these resources upon completion of the task. ■■ Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. ■■ On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider. Because the service is on demand, the resources are not permanent parts of your IT infrastructure. ■■ Resource pooling: The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a degree of location independence in that the customer Figure 5.7 Cloud Computing Elements Broad Network Access Resource Pooling Rapid Elasticity Essential Characteristics Service Models Deployment Models Measured Service On-Demand Self-

Service Public Private Hybrid Community Software as a Service (SaaS) Platform as a Service (PaaS) Infrastructure as a Service (IaaS) 5.4 / Cloud Computing 173 generally has no control or knowledge of the exact location of the provided resources, but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines. Even private clouds tend to pool resources between different parts of the same organization. NIST defines three service models, which can be viewed as nested service alternatives: ■■ Software as a service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser. Instead of obtaining desktop and server licenses for software products it uses, an enterprise obtains the same functions from the cloud service. SaaS saves the complexity of software installation, maintenance, upgrades, and patches. Examples of services at this level are Gmail, Google's e-mail service, and Salesforce.com, which helps firms keep track of their customers. ■■ Platform as a service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. PaaS often provides middleware-style services such as database and component services for use by applications. In effect, PaaS is an operating system in the cloud. ■■ Infrastructure as a service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. IaaS enables customers to combine basic computing services, such as number crunching and data storage, to build highly adaptable computer systems. NIST defines four deployment models: ■■ Public cloud: The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. The cloud provider is responsible both for the cloud infrastructure and for the control of data and operations within the cloud. ■■ Private cloud: The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise. The cloud provider (CP) is responsible only for the infrastructure and not for the control. ■■ Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise. ■■ Hybrid cloud: The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). 174 chapter 5 / Network Access Control and Cloud Security Figure 5.8 illustrates the typical cloud service context. An enterprise maintains workstations within an enterprise LAN or set of LANs, which are connected by a router through a network or the Internet to the cloud service provider. The cloud service provider maintains a massive collection of servers, which it manages with a variety of network management, redundancy, and security tools. In the figure, the cloud infrastructure is shown as a collection of blade servers, which is a common architecture. Cloud Computing Reference Architecture NIST SP 500-292 (NIST Cloud Computing Reference Architecture) establishes a reference architecture, described as follows: Figure 5.8 Cloud Computing Context Router Servers LAN switch Cloud service provider Network or Internet Router LAN

switch Enterprise (Cloud user) The NIST cloud computing reference architecture focuses on the requirements of “what” cloud services provide, not a “how to” design solution and implementation. The reference architecture is intended to facilitate the understanding of the operational intricacies in cloud computing. It does not represent the system architecture of a specific cloud computing system; instead it is a tool for describing, discussing, and developing a system-specific architecture using a common framework of reference. 5.4 / Cloud Computing 175 NIST developed the reference architecture with the following objectives in mind: ■■ to illustrate and understand the various cloud services in the context of an overall cloud computing conceptual model ■■ to provide a technical reference for consumers to understand, discuss, categorize, and compare cloud services ■■ to facilitate the analysis of candidate standards for security, interoperability, and portability and reference implementations The reference architecture, depicted in Figure 5.9, defines five major actors in terms of the roles and responsibilities: ■■ Cloud consumer: A person or organization that maintains a business relationship with, and uses service from, cloud providers. ■■ Cloud provider: A person, organization, or entity responsible for making a service available to interested parties. ■■ Cloud auditor: A party that can conduct independent assessment of cloud services, information system operations, performance, and security of the cloud implementation. ■■ Cloud broker: An entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between CPs and cloud consumers. ■■ Cloud carrier: An intermediary that provides connectivity and transport of cloud services from CPs to cloud consumers. The roles of the cloud consumer and provider have already been discussed. To summarize, a cloud provider can provide one or more of the cloud services to meet IT and business requirements of cloud consumers. For each of the three service Figure 5.9 NIST Cloud Computing Reference Architecture Cloud consumer Cloud auditor Service intermediation Service aggregation Service arbitrage Cloud broker Cloud provider Security audit Performance audit Privacy impact audit SaaS Service layer Service orchestration Cloud service management PaaS Hardware Physical resource layer Facility Resource abstraction and control layer IaaS Business support Provisioning/ conguration Portability/ interoperability Security Privacy Cloud carrier 176 chapter 5 / Network Access Control and Cloud Security models (SaaS, PaaS, IaaS), the CP provides the storage and processing facilities needed to support that service model, together with a cloud interface for cloud service consumers. For SaaS, the CP deploys, configures, maintains, and updates the operation of the software applications on a cloud infrastructure so that the services are provisioned at the expected service levels to cloud consumers. The consumers of SaaS can be organizations that provide their members with access to software applications, end users who directly use software applications, or software application administrators who configure applications for end users. For PaaS, the CP manages the computing infrastructure for the platform and runs the cloud software that provides the components of the platform, such as runtime software execution stack, databases, and other middleware components. Cloud consumers of PaaS can employ the tools and execution resources provided by CPs to develop, test, deploy, and manage the applications hosted in a cloud environment. For IaaS, the CP acquires the physical computing resources underlying the service, including the servers, networks, storage, and hosting infrastructure. The IaaS cloud consumer in turn uses these computing resources, such as a virtual computer, for their fundamental computing needs. The cloud carrier is a networking facility that provides connectivity and transport of cloud services between cloud consumers and CPs. Typically, a CP will set up service level agreements (SLAs) with

a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers, and may require the cloud carrier to provide dedicated and secure connections between cloud consumers and CPs. A cloud broker is useful when cloud services are too complex for a cloud consumer to easily manage. Three areas of support can be offered by a cloud broker: ■■ Service intermediation: These are value-added services, such as identity management, performance reporting, and enhanced security. ■■ Service aggregation: The broker combines multiple cloud services to meet consumer needs not specifically addressed by a single CP, or to optimize performance or minimize cost. ■■ Service arbitrage: This is similar to service aggregation except that the services being aggregated are not fixed. Service arbitrage means a broker has the flexibility to choose services from multiple agencies. The cloud broker, for example, can use a credit-scoring service to measure and select an agency with the best score. A cloud auditor can evaluate the services provided by a CP in terms of security controls, privacy impact, performance, and so on. The auditor is an independent entity that can assure that the CP conforms to a set of standards. 5.5 Cloud Security Risks and Countermeasures In general terms, security controls in cloud computing are similar to the security controls in any IT environment. However, because of the operational models and technologies used to enable cloud service, cloud computing may present risks that are specific to the cloud environment. The essential concept in this regard is that the enterprise loses a substantial amount of control over resources, services, and applications but must maintain accountability for security and privacy policies. 5.5 / Cloud Security Risks and Countermeasures 177 The Cloud Security Alliance [CSA10] lists the following as the top cloudspecific security threats, together with suggested countermeasures: ■■ Abuse and nefarious use of cloud computing: For many CPs, it is relatively easy to register and begin using cloud services, some even offering free limited trial periods. This enables attackers to get inside the cloud to conduct various attacks, such as spamming, malicious code attacks, and denial of service. PaaS providers have traditionally suffered most from this kind of attacks; however, recent evidence shows that hackers have begun to target IaaS vendors as well. The burden is on the CP to protect against such attacks, but cloud service clients must monitor activity with respect to their data and resources to detect any malicious behavior. Countermeasures include (1) stricter initial registration and validation processes; (2) enhanced credit card fraud monitoring and coordination; (3) comprehensive introspection of customer network traffic; and (4) monitoring public blacklists for one's own network blocks. ■■ Insecure interfaces and APIs: CPs expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. The security and availability of general cloud services are dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy. Countermeasures include (1) analyzing the security model of CP interfaces; (2) ensuring that strong authentication and access controls are implemented in concert with encrypted transmission; and (3) understanding the dependency chain associated with the API. ■■ Malicious insiders: Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and, in doing so, confers an unprecedented level of trust onto the CP. One grave concern is the risk of malicious insider activity. Cloud architectures necessitate certain roles that are extremely high risk. Examples include CP system administrators and managed security service providers. Countermeasures include the following: (1) enforce strict supply chain management and conduct a comprehensive supplier assessment; (2)

specify human resource requirements as part of legal contract; (3) require transparency into overall information security and management practices, as well as compliance reporting; and (4) determine security breach notification processes. ■■ Shared technology issues: IaaS vendors deliver their services in a scalable way by sharing infrastructure. Often, the underlying components that make up this infrastructure (CPU caches, GPUs, etc.) were not designed to offer strong isolation properties for a multi-tenant architecture. CPs typically approach this risk by the use of isolated virtual machines for individual clients. This approach is still vulnerable to attack, by both insiders and outsiders, and so can only be a part of an overall security strategy. Countermeasures include the following: (1) implement security best practices for installation/configuration; (2) monitor environment for unauthorized changes/activity; (3) promote strong authentication and access control 178 chapter 5 / Network Access Control and Cloud Security for administrative access and operations; (4) enforce SLAs for patching and vulnerability remediation; and (5) conduct vulnerability scanning and configuration audits. ■■ Data loss or leakage: For many clients, the most devastating impact from a security breach is the loss or leakage of data. We address this issue in the next subsection. Countermeasures include the following: (1) implement strong API access control; (2) encrypt and protect integrity of data in transit; (3) analyze data protection at both design and run time; and (4) implement strong key generation, storage and management, and destruction practices. ■■ Account or service hijacking: Account or service hijacking, usually with stolen credentials, remains a top threat. With stolen credentials, attackers can often access critical areas of deployed cloud computing services, allowing them to compromise the confidentiality, integrity, and availability of those services. Countermeasures include the following: (1) prohibit the sharing of account credentials between users and services; (2) leverage strong two-factor authentication techniques where possible; (3) employ proactive monitoring to detect unauthorized activity; and (4) understand CP security policies and SLAs. ■■ Unknown risk profile: In using cloud infrastructures, the client necessarily cedes control to the CP on a number of issues that may affect security. Thus the client must pay attention to and clearly define the roles and responsibilities involved for managing risks. For example, employees may deploy applications and data resources at the CP without observing the normal policies and procedures for privacy, security, and oversight. Countermeasures include (1) disclosure of applicable logs and data; (2) partial/full disclosure of infrastructure details (e.g., patch levels and firewalls); and (3) monitoring and alerting on necessary information. Similar lists have been developed by the European Network and Information Security Agency [ENIS09] and NIST [JANS11]. 5.6 Data Protection in the Cloud As can be seen from the previous section, there are numerous aspects to cloud security and numerous approaches to providing cloud security measures. A further example is seen in the NIST guidelines for cloud security, specified in SP-800-14 and listed in Table 5.3. Thus, the topic of cloud security is well beyond the scope of this chapter. In this section, we focus on one specific element of cloud security. There are many ways to compromise data. Deletion or alteration of records without a backup of the original content is an obvious example. Unlinking a record from a larger context may render it unrecoverable, as can storage on unreliable media. Loss of an encoding key may result in effective destruction. Finally, unauthorized parties must be prevented from gaining access to sensitive data. 5.6 / Data Protection in the Cloud 179 Governance Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. Put in place audit

mechanisms and tools to ensure organizational practices are followed throughout the system life cycle. Compliance Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, records management, and electronic discovery requirements. Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements. Ensure that the cloud provider's electronic discovery capabilities and processes do not compromise the privacy or security of data and applications. Trust Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time. Establish clear, exclusive ownership rights over data. Institute a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the life cycle of the system. Continuously monitor the security state of the information system to support ongoing risk management decisions. Architecture Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system life cycle and across all system components. Identity and access management Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization. Software isolation Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization. Data protection Evaluate the suitability of the cloud provider's data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data. Take into consideration the risk of collating organizational data with those of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value. Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider. Availability Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization's continuity and contingency planning requirements. Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstituted in a timely and organized manner. Incident response Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization. Table 5.3 NIST Guidelines on Security and Privacy Issues and Recommendations 180 chapter 5 / Network Access Control and Cloud Security Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident. Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment. Table 5.3 Continued The threat of data compromise increases in the cloud, due to the number of and interactions between risks and challenges that are either unique to the cloud or more dangerous because of the architectural or operational characteristics of the cloud environment. Database environments used in cloud computing can vary significantly. Some providers support a multi-instance model, which provides a unique DBMS running on a virtual machine instance for each cloud subscriber. This gives the

subscriber complete control over role definition, user authorization, and other administrative tasks related to security. Other providers support a multi-tenant model, which provides a predefined environment for the cloud subscriber that is shared with other tenants, typically through tagging data with a subscriber identifier. Tagging gives the appearance of exclusive use of the instance, but relies on the CP to establish and maintain a sound secure database environment. Data must be secured while at rest, in transit, and in use, and access to the data must be controlled. The client can employ encryption to protect data in transit, though this involves key management responsibilities for the CP. The client can enforce access control techniques but, again, the CP is involved to some extent depending on the service model used. For data at rest, the ideal security measure is for the client to encrypt the database and only store encrypted data in the cloud, with the CP having no access to the encryption key. So long as the key remains secure, the CP has no ability to read the data, although corruption and other denial-of-service attacks remain a risk. A straightforward solution to the security problem in this context is to encrypt the entire database and not provide the encryption/decryption keys to the service provider. This solution by itself is inflexible. The user has little ability to access individual data items based on searches or indexing on key parameters, but rather would have to download entire tables from the database, decrypt the tables, and work with the results. To provide more flexibility, it must be possible to work with the database in its encrypted form. An example of such an approach, depicted in Figure 5.10, is reported in [DAMI05] and [DAMI03]. A similar approach is described in [HACI02]. Four entities are involved: ■■ Data owner: An organization that produces data to be made available for controlled release, either within the organization or to external users. ■■ User: Human entity that presents requests (queries) to the system. The user could be an employee of the organization who is granted access to the database via the server, or a user external to the organization who, after authentication, is granted access. ■■ Client: Frontend that transforms user queries into queries on the encrypted data stored on the server. 5.6 / Data Protection in the Cloud 181 ■■ Server: An organization that receives the encrypted data from a data owner and makes them available for distribution to clients. The server could in fact be owned by the data owner but, more typically, is a facility owned and maintained by an external provider. For our discussion, the server is a cloud server. Before continuing this discussion, we need to define some database terms. In relational database parlance, the basic building block is a relation, which is a flat table. Rows are referred to as tuples, and columns are referred to as attributes. A primary key is defined to be a portion of a row used to uniquely identify a row in a table; the primary key consists of one or more column names.2 For example, in an employee table, the employee ID is sufficient to uniquely identify a row in a particular table. Let us first examine the simplest possible arrangement based on this scenario. Suppose that each individual item in the database is encrypted separately, all using the same encryption key. The encrypted database is stored at the server, but the server does not have the encryption key. Thus, the data are secure at the server. Even if someone were able to hack into the server's system, all he or she would have access to is encrypted data. The client system does have a copy of the encryption key. A user at the client can retrieve a record from the database with the following sequence: 1. The user issues a query for fields from one or more records with a specific value of the primary key. 2 Note that a primary key has nothing to do with cryptographic keys. A primary key in a database is a means of indexing into the database. Figure 5.10 An Encryption Scheme for a Cloud-Based Database Query processor 1. Original query Metadata 4. Plaintext result 2. Transformed query 3. Encrypted result Client User Data owner Cloud server Encrypt/ Decrypt Query executor

Metadata Metadata Encrypted database Database 182 chapter 5 / Network Access Control and Cloud Security 2. The query processor at the client encrypts the primary key, modifies the query accordingly, and transmits the query to the server. 3. The server processes the query using the encrypted value of the primary key and returns the appropriate record or records. 4. The query processor decrypts the data and returns the results. This method is certainly straightforward but is quite limited. For example, suppose the Employee table contains a salary attribute and the user wishes to retrieve all records for salaries less than $70K. There is no obvious way to do this, because the attribute value for salary in each record is encrypted. The set of encrypted values does not preserve the ordering of values in the original attribute. There are a number of ways to extend the functionality of this approach. For example, an unencrypted index value can be associated with a given attribute and the table can be partitioned based on these index values, enabling a user to retrieve a certain portion of the table. The details of such schemes are beyond our scope. See [STAL15] for more detail. 5.7 Cloud Security as a Service The term Security as a Service (SecaaS) has generally meant a package of security services offered by a service provider that offloads much of the security responsibility from an enterprise to the security service provider. Among the services typically provided are authentication, antivirus, antimalware/-spyware, intrusion detection, and security event management. In the context of cloud computing, cloud security as a service, designated SecaaS, is a segment of the SaaS offering of a CP. The Cloud Security Alliance defines SecaaS as the provision of security applications and services via the cloud either to cloud-based infrastructure and software or from the cloud to the customers' on-premise systems [CSA11b]. The Cloud Security Alliance has identified the following SecaaS categories of service: ■■ Identity and access management ■■ Data loss prevention ■■ Web security ■■ E-mail security ■■ Security assessments ■■ Intrusion management ■■ Security information and event management ■■ Encryption ■■ Business continuity and disaster recovery ■■ Network security In this section, we examine these categories with a focus on security of the cloud-based infrastructure and services (Figure 5.11). 5.7 / Cloud Security as a Service 183 Identity and access management (IAM) includes people, processes, and systems that are used to manage access to enterprise resources by assuring that the identity of an entity is verified, and then granting the correct level of access based on this assured identity. One aspect of identity management is identity provisioning, which has to do with providing access to identified users and subsequently deprovisioning, or deny access, to users when the client enterprise designates such users as no longer having access to enterprise resources in the cloud. Another aspect of identity management is for the cloud to participate in the federated identity management scheme (see Chapter 4) used by the client enterprise. Among other requirements, the cloud service provider (CSP) must be able to exchange identity attributes with the enterprise's chosen identity provider. The access management portion of IAM involves authentication and access control services. For example, the CSP must be able to authenticate users in a trustworthy manner. The access control requirements in SPI environments include establishing trusted user profile and policy information, using it to control access within the cloud service, and doing this in an auditable way. Data loss prevention (DLP) is the monitoring, protecting, and verifying the security of data at rest, in motion, and in use. Much of DLP can be implemented Figure 5.11 Elements of Cloud Security as a Service Cloud service clients and adversaries Identity and access management Network security Data loss prevention Web security Intrusion management Encryption Email security Security assessments Security information and event management Business continuity and disaster recovery 184 chapter 5 / Network

Access Control and Cloud Security by the cloud client, such as discussed in Section 5.6. The CSP can also provide DLP services, such as implementing rules about what functions can be performed on data in various contexts. Web security is real-time protection offered either on premise through software/appliance installation or via the cloud by proxying or redirecting Web traffic to the CP. This provides an added layer of protection on top of things like antiviruses to prevent malware from entering the enterprise via activities such as Web browsing. In addition to protecting against malware, a cloud-based Web security service might include usage policy enforcement, data backup, traffic control, and Web access control. A CSP may provide a Web-based e-mail service, for which security measures are needed. E-mail security provides control over inbound and outbound e-mail, protecting the organization from phishing, malicious attachments, enforcing corporate polices such as acceptable use and spam prevention. The CSP may also incorporate digital signatures on all e-mail clients and provide optional e-mail encryption. Security assessments are third-part audits of cloud services. While this service is outside the province of the CSP, the CSP can provide tools and access points to facilitate various assessment activities. Intrusion management encompasses intrusion detection, prevention, and response. The core of this service is the implementation of intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) at entry points to the cloud and on servers in the cloud. An IDS is a set of automated tools designed to detect unauthorized access to a host system. We discuss this in Chapter 11. An IPS incorporates IDS functionality but also includes mechanisms designed to block traffic from intruders. Security information and event management (SIEM) aggregates (via push or pull mechanisms) log and event data from virtual and real networks, applications, and systems. This information is then correlated and analyzed to provide real-time reporting and alerting on information/events that may require intervention or other type of response. The CSP typically provides an integrated service that can put together information from a variety of sources both within the cloud and within the client enterprise network. Encryption is a pervasive service that can be provided for data at rest in the cloud, e-mail traffic, client-specific network management information, and identity information. Encryption services provided by the CSP involve a range of complex issues, including key management, how to implement virtual private network (VPN) services in the cloud, application encryption, and data content access. Business continuity and disaster recovery comprise measures and mechanisms to ensure operational resiliency in the event of any service interruptions. This is an area where the CSP, because of economies of scale, can offer obvious benefits to a cloud service client [WOOD10]. The CSP can provide backup at multiple locations, with reliable failover and disaster recovery facilities. This service must include a flexible infrastructure, redundancy of functions and hardware, monitored operations, geographically distributed data centers, and network survivability. Network security consists of security services that allocate access, distribute, monitor, and protect the underlying resource services. Services include perimeter and server firewalls and denial-of-service protection. Many of the other services 5.8 / Addressing Cloud Computing Security Concerns 185 listed in this section, including intrusion management, identity and access management, data loss protection, and Web security, also contribute to the network security service. 5.8 Addressing Cloud Computing Security Concerns Numerous documents have been developed to guide businesses thinking about the security issues associated with cloud computing. In addition to SP 800-144, which provides overall guidance, NIST has issued SP 800-146 (Cloud Computing Synopsis and Recommendations, May 2012). NIST's recommendations systematically consider each of

the major types of cloud services consumed by businesses including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS). While security issues vary somewhat depending on the type of cloud service, there are multiple NIST recommendations that are independent of service type. Not surprisingly, NIST recommends selecting cloud providers that support strong encryption, have appropriate redundancy mechanisms in place, employ authentication mechanisms, and offer subscribers sufficient visibility about mechanisms used to protect subscribers from other subscribers and the provider. SP 800-146 also lists the overall security controls that are relevant in a cloud computing environment and that must be assigned to the different cloud actors. These are shown in Table 5.4. As more businesses incorporate cloud services into their enterprise network infrastructures, cloud computing security will persist as an important issue. Examples of cloud computing security failures have the potential to have a chilling effect on business interest in cloud services and this is inspiring service providers to be serious about incorporating security mechanisms that will allay concerns of potential subscribers. Some service providers have moved their operations to Tier 4 data centers to address user concerns about availability and redundancy. Because so many businesses remain reluctant to embrace cloud computing in a big way, cloud service providers will have to continue to work hard to convince potential customers that computing support for core business processes and mission critical applications can be moved safely and securely to the cloud. Technical Operational Management Access Control Audit and Accountability Identification and Authentication System and Communication Protection Awareness and Training Configuration and Management Contingency Planning Incident Response Maintenance Media Protection Physical and Environmental Protection Personnel Security System and Information Integrity Certification, Accreditation, and Security Assessment Planning Risk Assessment System and Services Acquisition Table 5.4 Control Functions and Classes 186 chapter 5 / Network Access Control and Cloud Security Key Terms access requestor (AR) authentication server cloud cloud auditor cloud broker cloud carrier cloud computing cloud consumer cloud provider community cloud Dynamic Host Configuration Protocol (DHCP) EAP authenticator EAP-GPSK EAP-IKEv2 EAP over LAN (EAPOL) EAP method EAP pass-through mode EAP peer EAP-TLS EAP-TTLS Extensible Authentication Protocol (EAP) firewall IEEE 802.1X media gateway Network Access Control (NAC) Network Access Server (NAS) Platform as a Service (PaaS) policy server private cloud public cloud Remote Access Server (RAS) Security as a Service (SecaaS) Software as a Service (SaaS) supplicant Virtual Local Area Network (VLAN) 5.9 Key Terms, Review Questions, and Problems Review Questions 5.1 Provide a brief definition of network access control. 5.2 What is an EAP? 5.3 List and briefly define four EAP authentication methods. 5.4 What is DHCP? How useful is it to help achieve security of IP addresses? 5.5 Why is EAPOL an essential element of IEEE 802.1X? 5.6 What are the essential characteristics of cloud computing? 5.7 List and briefly define the deployment models of cloud computing. 5.8 What is the cloud computing reference architecture? 5.9 Describe some of the main cloud-specific security threats. Problems 5.1 Investigate the network access control scheme used at your school or place of employment. Draw a diagram and describe the principal components. 5.2 Figure 5.3 suggests that EAP can be described in the context of a four-layer model. Indicate the functions and formats of each of the four layers. You may need to refer to RFC 3748. 5.3 List some commonly used cloud-based data services. Explore and compare these services based on their use of encryption, flexibility, efficiency, speed, and ease of use. Study security breaches on these services in recent past. What changes were made by the

services after these attacks? 187 6.1 Web Security Considerations Web Security Threats Web Traffic Security Approaches 6.2 Transport Layer Security TLS Architecture TLS Record Protocol Change Cipher Spec Protocol Alert Protocol Handshake Protocol Cryptographic Computations Heartbeat Protocol SSL/TLS Attacks TLSv1.3 6.3 HTTPS Connection Initiation Connection Closure 6.4 Secure Shell (SSH) Transport Layer Protocol User Authentication Protocol Connection Protocol 6.5 Key Terms, Review Questions, and Problems Chapter Transport-Level Security 188 chapter 6 / Transport-Level Security Virtually all businesses, most government agencies, and many individuals now have Web sites. The number of individuals and companies with Internet access is expanding rapidly and all of these have graphical Web browsers. As a result, businesses are enthusiastic about setting up facilities on the Web for electronic commerce. But the reality is that the Internet and the Web are extremely vulnerable to compromises of various sorts. As businesses wake up to this reality, the demand for secure Web services grows. The topic of Web security is a broad one and can easily fill a book. In this chapter, we begin with a discussion of the general requirements for Web security and then focus on three standardized schemes that are becoming increasingly important as part of Web commerce and that focus on security at the transport layer: SSL/TLS, HTTPS, and SSH. 6.1 Web Security Considerations The World Wide Web is fundamentally a client/server application running over the Internet and TCP/IP intranets. As such, the security tools and approaches discussed so far in this book are relevant to the issue of Web security. However, the following characteristics of Web usage suggest the need for tailored security tools: ■■ Although Web browsers are very easy to use, Web servers are relatively easy to configure and manage, and Web content is increasingly easy to develop, the underlying software is extraordinarily complex. This complex software may hide many potential security flaws. The short history of the Web is filled with examples of new and upgraded systems, properly installed, that are vulnerable to a variety of security attacks. ■■ A Web server can be exploited as a launching pad into the corporation's or agency's entire computer complex. Once the Web server is subverted, an attacker may be able to gain access to data and systems not part of the Web itself but connected to the server at the local site. Learning Objectives After studying this chapter, you should be able to: ◆ Summarize Web security threats and Web traffic security approaches. ◆ Present an overview of Transport Layer Security (TLS). ◆ Understand the differences between Secure Sockets Layer and Transport Layer Security. ◆ Compare the pseudorandom function used in Transport Layer Security with those discussed earlier in the book. ◆ Present an overview of HTTPS (HTTP over SSL). ◆ Present an overview of Secure Shell (SSH). 6.1 / Web Security Considerations 189 ■■ Casual and untrained (in security matters) users are common clients for Webbased services. Such users are not necessarily aware of the security risks that exist and do not have the tools or knowledge to take effective countermeasures. Web Security Threats Table 6.1 provides a summary of the types of security threats faced when using the Web. One way to group these threats is in terms of passive and active attacks. Passive attacks include eavesdropping on network traffic between browser and server and gaining access to information on a Web site that is supposed to be restricted. Active attacks include impersonating another user, altering messages in transit between client and server, and altering information on a Web site. Another way to classify Web security threats is in terms of the location of the threat: Web server, Web browser, and network traffic between browser and server. Issues of server and browser security fall into the category of computer system security; Part Six of this book addresses the issue of system security in general but is also applicable to Web system security. Issues of traffic security

fall into the category of network security and are addressed in this chapter. Web Traffic Security Approaches A number of approaches to providing Web security are possible. The various approaches that have been considered are similar in the services they provide and, to some extent, in the mechanisms that they use, but they differ with respect to their scope of applicability and their relative location within the TCP/IP protocol stack. Threats Consequences Countermeasures Integrity • Modification of user data • Trojan horse browser • Modification of memory • Modification of message traffic in transit • Loss of information • Compromise of machine • Vulnerability to all other threats Cryptographic checksums Confidentiality • Eavesdropping on the net • Theft of info from server • Theft of data from client • Info about network configuration • Info about which client talks to server • Loss of information • Loss of privacy Encryption, Web proxies Denial of Service • Killing of user threads • Flooding machine with bogus requests • Filling up disk or memory • Isolating machine by DNS attacks • Disruptive • Annoying • Prevent user from getting work done Difficult to prevent Authentication • Impersonation of legitimate users • Data forgery • Misrepresentation of user • Belief that false information is valid Cryptographic techniques Table 6.1 A Comparison of Threats on the Web 190 chapter 6 / Transport-Level Security Figure 6.1 illustrates this difference. One way to provide Web security is to use IP security (IPsec) (Figure 6.1a). The advantage of using IPsec is that it is transparent to end users and applications and provides a general-purpose solution. Furthermore, IPsec includes a filtering capability so that only selected traffic need incur the overhead of IPsec processing. Another relatively general-purpose solution is to implement security just above TCP (Figure 6.1b). The foremost example of this approach is the Secure Sockets Layer (SSL) and the follow-on Internet standard known as Transport Layer Security (TLS). At this level, there are two implementation choices. For full generality, SSL (or TLS) could be provided as part of the underlying protocol suite and therefore be transparent to applications. Alternatively, TLS can be embedded in specific packages. For example, virtually all browsers come equipped with TLS, and most Web servers have implemented the protocol. Application-specific security services are embedded within the particular application. Figure 6.1c shows examples of this architecture. The advantage of this approach is that the service can be tailored to the specific needs of a given application. 6.2 Transport Layer Security One of the most widely used security services is Transport Layer Security (TSL); the current version is Version 1.2, defined in RFC 5246. TLS is an Internet standard that evolved from a commercial protocol known as Secure Sockets Layer (SSL). Although SSL implementations are still around, it has been deprecated by IETF and is disabled by most corporations offering TLS software. TLS is a generalpurpose service implemented as a set of protocols that rely on TCP. At this level, there are two implementation choices. For full generality, TLS could be provided as part of the underlying protocol suite and therefore be transparent to applications. Alternatively, TLS can be embedded in specific packages. For example, most browsers come equipped with TLS, and most Web servers have implemented the protocol. TLS Architecture TLS is designed to make use of TCP to provide a reliable end-to-end secure service. TLS is not a single protocol but rather two layers of protocols, as illustrated in Figure 6.2. Figure 6.1 Relative Location of Security Facilities in the TCP/IP Protocol Stack HTTP SMTP TCP IP/IPSec (a) Network level FTP HTTP SMTP TCP SSL or TLS IP (b) Transport level FTP IP S/MIME Kerberos HTTP UDP SMTP (c) Application level TCP 6.2 / Transport Layer Security 191 The TLS Record Protocol provides basic security services to various higherlayer protocols. In particular, the Hypertext Transfer Protocol (HTTP), which provides the transfer service for Web client/server interaction, can operate on top of TLS. Three higher-

layer protocols are defined as part of TLS: the Handshake Protocol; the Change Cipher Spec Protocol; and the Alert Protocol. These TLSspecific protocols are used in the management of TLS exchanges and are examined later in this section. A fourth protocol, the Heartbeat Protocol, is defined in a separate RFC and is also discussed subsequently in this section. Two important TLS concepts are the TLS session and the TLS connection, which are defined in the specification as follows: ■■ Connection: A connection is a transport (in the OSI layering model definition) that provides a suitable type of service. For TLS, such connections are peer-topeer relationships. The connections are transient. Every connection is associated with one session. ■■ Session: A TLS session is an association between a client and a server. Sessions are created by the Handshake Protocol. Sessions define a set of cryptographic security parameters, which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection. Between any pair of parties (applications such as HTTP on client and server), there may be multiple secure connections. In theory, there may also be multiple simultaneous sessions between parties, but this feature is not used in practice. There are a number of states associated with each session. Once a session is established, there is a current operating state for both read and write (i.e., receive and send). In addition, during the Handshake Protocol, pending read and write states are created. Upon successful conclusion of the Handshake Protocol, the pending states become the current states. A session state is defined by the following parameters: ■■ Session identifier: An arbitrary byte sequence chosen by the server to identify an active or resumable session state. ■■ Peer certificate: An X509.v3 certificate of the peer. This element of the state may be null. Figure 6.2 TLS Protocol Stack IP TCP Record protocol Handshake protocol Change cipher spec protocol Alert protocol HTTP Heartbeat protocol 192 chapter 6 / Transport-Level Security ■■ Compression method: The algorithm used to compress data prior to encryption. ■■ Cipher spec: Specifies the bulk data encryption algorithm (such as null, AES, etc.) and a hash algorithm (such as MD5 or SHA-1) used for MAC calculation. It also defines cryptographic attributes such as the hash_size. ■■ Master secret: 48-byte secret shared between the client and server. ■■ Is resumable: A flag indicating whether the session can be used to initiate new connections. A connection state is defined by the following parameters: ■■ Server and client random: Byte sequences that are chosen by the server and client for each connection. ■■ Server write MAC secret: The secret key used in MAC operations on data sent by the server. ■■ Client write MAC secret: The symmetric key used in MAC operations on data sent by the client. ■■ Server write key: The symmetric encryption key for data encrypted by the server and decrypted by the client. ■■ Client write key: The symmetric encryption key for data encrypted by the client and decrypted by the server. ■■ Initialization vectors: When a block cipher in CBC mode is used, an initialization vector (IV) is maintained for each key. This field is first initialized by the TLS Handshake Protocol. Thereafter, the final ciphertext block from each record is preserved for use as the IV with the following record. ■■ Sequence numbers: Each party maintains separate sequence numbers for transmitted and received messages for each connection. When a party sends or receives a “change cipher spec message,” the appropriate sequence number is set to zero. Sequence numbers may not exceed 264 - 1. TLS Record Protocol The TLS Record Protocol provides two services for TLS connections: ■■ Confidentiality: The Handshake Protocol defines a shared secret key that is used for conventional encryption of TLS payloads. ■■ Message Integrity: The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC). Figure 6.3 indicates the overall operation of the TLS Record Protocol. The Record