| | | |
|---|---|---|
| outside attack | risk | system resource |
| passive attack | security attack | threat agent |
| prevent | security mechanism | traffic analysis |
| privacy | security policy | unauthorized disclosure |
| psychological acceptability | security service | usurpation |
| replay | separation of privilege | vulnerabilities |
| repudiation | system integrity | |

## Review Questions

**1.1** What is meant by the CIA triad?.

**1.2** What is the difference between data integrity and system integrity?

**1.3** List and briefly define the kinds of threat consequences and the types of threat actions which cause these consequences.

**1.4** List and briefly define the fundamental security design principles.

**1.5** What is a security policy? What are the actions involved when implementing a security policy?

**1.6** Differentiate between a network attack surface and a software attack surface.

## Problems

**1.1** Consider a student information system (SIS) in which students provide a university student number (USN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of the importance of the requirement.

**1.2** Repeat Problem 1.1 for a network routing system that routes data packets through a network based on the IP address provided by the sender.

**1.3** Consider a desktop publishing system used to produce documents for various organizations.

- **a.** Give an example of a type of publication for which confidentiality of the stored data is the most important requirement.
- **b.** Give an example of a type of publication in which data integrity is the most important requirement.
- **c.** Give an example in which system availability is the most important requirement.

**1.4** For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers.

- **a.** An organization managing public information on its Web server.
- **b.** A law enforcement organization managing extremely sensitive investigative information.
- **c.** A financial organization managing routine administrative information (not privacy-related information).
- **d.** An information system used for large acquisitions in a contracting organization contains both sensitive, pre-solicitation phase contract information and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.
- **e.** A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.

**1.5** Consider the following general code for allowing access to a resource:

```
DWORD dwRet = IsAccessAllowed(...);
if (dwRet == ERROR_ACCESS_DENIED) {
// Security check failed.
// Inform user that access is denied.
} else {
// Security check OK.
}
```

**a.** Explain the security flaw in this program.
**b.** Rewrite the code to avoid the flaw.

*Hint*: Consider the design principle of fail-safe defaults.

**1.6** Develop an attack tree for gaining access to the contents of a physical safe.

**1.7** Consider a company whose operations are housed in two buildings on the same property: one building is headquarters, the other building contains network and computer services. The property is physically protected by a fence around the perimeter. The only entrance to the property is through a guarded front gate. The local networks are split between the Headquarters' LAN and the Network Services' LAN. Internet users connect to the Web server through a firewall. Dial-up users get access to a particular server on the Network Services' LAN. Develop an attack tree in which the root node represents disclosure of proprietary secrets. Include physical, social engineering, and technical attacks. The tree may contain both AND and OR nodes. Develop a tree that has at least 15 leaf nodes.

**1.8** Read all of the classic papers cited in the Recommended Reading document at http://williamstallings.com/ComputerSecurity/ Compose a 500–1000 word paper (or 8–12 slide presentation) that summarizes the key concepts that emerge from these papers, emphasizing concepts that are common to most or all of the papers.

| | | |
|---|---|---|
| encryption | preimage resistant | second preimage resistant |
| hash function | private key | secret key |
| keystream | pseudorandom number | secure hash algorithm (SHA) |
| message authentication | public key | secure hash function |
| message authentication code (MAC) | public-key certificate | strong collision resistant |
| modes of operation | public-key encryption | symmetric encryption |
| one-way hash function | random number | triple DES |
| plaintext | RSA | weak collision resistant |

## Review Questions

**2.1** How is cryptanalysis different from brute-force attack?
**2.2** List and briefly explain the different approaches to attacking a symmetric encryption scheme.
**2.3** What are the two principal requirements for the secure use of symmetric encryption?
**2.4** List the two important aspects of data authentication.
**2.5** What is one-way hash function?
**2.6** Briefly describe the three schemes illustrated in Figure 2.3.
**2.7** What properties must a hash function have to be useful for message authentication?
**2.8** What are the principal ingredients of a public-key cryptosystem?
**2.9** List and briefly define three uses of a public-key cryptosystem.
**2.10** What advantage might elliptic curve cryptography (ECC) have over RSA?
**2.11** Do digital signatures provide confidentiality?
**2.12** What is a public-key certificate?
**2.13** What are three different ways in which random numbers are used in cryptography?

## Problems

**2.1** Typically, in practice, the length of the message is greater than the block size of the encryption algorithm. The simplest approach to handle such encryption is known as electronic codebook (ECB) mode. Explain this mode. Mention a scenario where it cannot be applied. Explain briefly why it is not a secure mode of encryption.

**2.2** This problem uses a real-world example of a symmetric cipher, from an old U.S. Special Forces manual (public domain). The document, filename *Special Forces.pdf*, is available at box.com/CompSec4e.

**a.** Using the two keys (memory words) *cryptographic* and *network security*, encrypt the following message:

> Be at the third pillar from the left outside the lyceum theatre tonight at seven. If you are distrustful bring two friends.

Make reasonable assumptions about how to treat redundant letters and excess letters in the memory words and how to treat spaces and punctuation. Indicate what your assumptions are.
*Note*: The message is from the Sherlock Holmes novel *The Sign of Four*.

**b.** Decrypt the ciphertext. Show your work.

**c.** Comment on when it would be appropriate to use this technique and what its advantages are.

**2.3** Consider a very simple symmetric block encryption algorithm, in which 64-bits blocks of plaintext are encrypted using a 128-bit key. Encryption is defined as

$$C = (P \oplus K_0) \boxplus K_1$$

where $C$ = ciphertext; $K$ = secret key; $K_0$ = leftmost 64 bits of $K$; $K_1$ = rightmost 64 bits of $K$, $\oplus$ = bitwise exclusive or; and $\boxplus$ is addition mod $2^{64}$.

**a.** Show the decryption equation. That is, show the equation for $P$ as a function of $C$, $K_1$ and $K_2$.

**b.** Suppose an adversary has access to two sets of plaintexts and their corresponding ciphertexts and wishes to determine $K$. We have the two equations:

$$C = (P \oplus K_0) \boxplus K_1; C' = (P' \oplus K_0) \boxplus K_1$$

First, derive an equation in one unknown (e.g., $K_0$). Is it possible to proceed further to solve for $K_0$?

**2.4** Perhaps the simplest "serious" symmetric block encryption algorithm is the Tiny Encryption Algorithm (TEA). TEA operates on 64-bit blocks of plaintext using a 128-bit key. The plaintext is divided into two 32-bit blocks ($L_0$, $R_0$), and the key is divided into four 32-bit blocks ($K_0$, $K_1$, $K_2$, $K_3$). Encryption involves repeated application of a pair of rounds, defined as follows for rounds $i$ and $i + 1$:

$$\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} \boxplus \mathrm{F}(R_{i-1}, K_0, K_1, \delta_i) \\ L_{i+1} &= R_i \\ R_{i+1} &= L_i \boxplus \mathrm{F}(R_i, K_2, K_3, \delta_{i+1}) \end{aligned}$$

where F is defined as

$$\mathrm{F}(M, K_j, K_k, \delta_i) = ((\mathrm{M} \ll 4) \boxplus K_j) \oplus ((\mathrm{M} \gg 5) \boxplus K_k) \oplus (\mathrm{M} + \delta_i)$$

and where the logical shift of $x$ by $y$ bits is denoted by $x \ll y$; the logical right shift $x$ by $y$ bits is denoted by $x \gg y$; and $\delta_i$ is a sequence of predetermined constants.

**a.** Comment on the significance and benefit of using the sequence of constants.

**b.** Illustrate the operation of TEA using a block diagram or flow chart type of depiction.

**c.** If only one pair of rounds is used, then the ciphertext consists of the 64-bit block ($L_2$, $R_2$). For this case, express the decryption algorithm in terms of equations.

**d.** Repeat part (c) using an illustration similar to that used for part (b).

**2.5** In this problem, we will compare the security services that are provided by digital signatures (DS) and message authentication codes (MAC). We assume Oscar is able to observe all messages sent from Alice to Bob and vice versa. Oscar has no knowledge of any keys but the public one in case of DS. State whether and how (i) DS and (ii) MAC protect against each attack. The value auth(x) is computed with a DS or a MAC algorithm, respectively.

**a.** (Message integrity) Alice sends a message x = "Transfer $1000 to Mark" in the clear and also sends auth(x) to Bob. Oscar intercepts the message and replaces "Mark" with "Oscar." Will Bob detect this?

**b.** (Replay) Alice sends a message x = "Transfer $1000 to Oscar" in the clear and also sends auth(x) to Bob. Oscar observes the message and signature and sends them 100 times to Bob. Will Bob detect this?

**c.** (Sender authentication with cheating third party) Oscar claims that he sent some message x with a valid auth(x) to Bob but Alice claims the same. Can Bob clear the question in either case?

**d.** (Authentication with Bob cheating) Bob claims that he received a message x with a valid signature auth(x) from Alice (e.g., "Transfer $1000 from Alice to Bob") but Alice claims she has never sent it. Can Alice clear this question in either case?

**2.6** Suppose *H(M)* is a cryptographic hash function that maps a message of an arbitrary bit length on to an *n*-bit hash value. Briefly explain the primary security requirements of the hash function *H*. Assume that *H* outputs 16-bit hash values. How many random messages would be required to find two different messages $M$ and $M'$ such that $H(M) = H(M')$.

**2.7** This problem introduces a hash function similar in spirit to SHA that operates on letters instead of binary data. It is called the *toy tetragraph hash* (tth).[8] Given a message consisting of a sequence of letters, tth produces a hash value consisting of four letters. First, tth divides the message into blocks of 16 letters, ignoring spaces, punctuation, and capitalization. If the message length is not divisible by 16, it is padded out with nulls. A four-number running total is maintained that starts out with the value (0, 0, 0, 0); this is input to a function, known as a *compression function*, for processing the first block. The compression function consists of two rounds. **Round 1:** Get the next block of text and arrange it as a row-wise $4 \times 4$ block of text and convert it to numbers (A = 0, B = 1), for example, for the block ABCDEFGHIJKLMNOP, we have

| | | | |
|---|---|---|---|
| A | B | C | D |
| E | F | G | H |
| I | J | K | L |
| M | N | O | P |

| | | | |
|---|---|---|---|
| 0 | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 |
| 8 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 |

Then, add each column mod 26 and add the result to the running total, mod 26. In this example, the running total is (24, 2, 6, 10). **Round 2:** Using the matrix from round 1, rotate the first row left by 1, second row left by 2, third row left by 3, and reverse the order of the fourth row. In our example,

| | | | |
|---|---|---|---|
| B | C | D | A |
| G | H | E | F |
| L | I | J | K |
| P | O | N | M |

| | | | |
|---|---|---|---|
| 1 | 2 | 3 | 0 |
| 6 | 7 | 4 | 5 |
| 11 | 8 | 9 | 10 |
| 15 | 14 | 13 | 12 |

Now, add each column mod 26 and add the result to the running total. The new running total is (5, 7, 9, 11). This running total is now the input into the first round of the compression function for the next block of text. After the final block is processed, convert the final running total to letters. For example, if the message is ABCDEFGHIJKLMNOP, then the hash is FHJL.

**a.** Draw figures of the overall tth logic and the compression function logic.

**b.** Calculate the hash function for the 48-letter message "I leave twenty million dollars to my friendly cousin Bill."

**c.** To demonstrate the weakness of tth, find a 48-letter block that produces the same hash as that just derived. *Hint*: Use lots of As.

**2.8** Prior to the discovery of any specific public-key schemes, such as RSA, an existence proof was developed whose purpose was to demonstrate that public-key encryption is possible in theory. Consider the functions $f_1(x_1) = z_1; f_2(x_2, y_2) = z_2; f_3(x_3, y_3) = z_3$, where all values are integers with $1 \leq x_i, y_i, z_i \leq N$. Function $f_1$ can be represented by a vector **M1** of length $N$, in which the $k$th entry is the value of $f_1(k)$. Similarly,

[8] I thank William K. Mason and The American Cryptogram Association for providing this example.

4.2 **a.** Explain, with an appropriate example, how protection domains provide flexibility.
**b.** How is the concept of protection domains related to operating systems? Explain by quoting an example from the UNIX operating system.

4.3 The VAX/VMS operating system makes use of four processor access modes to facilitate the protection and sharing of system resources among processes. The access mode determines:

- **Instruction execution privileges:** What instructions the processor may execute
- **Memory access privileges:** Which locations in virtual memory the current instruction may access

The four modes are as follows:

- **Kernel:** Executes the kernel of the VMS operating system, which includes memory management, interrupt handling, and I/O operations
- **Executive:** Executes many of the operating system service calls, including file and record (disk and tape) management routines
- **Supervisor:** Executes other operating system services, such as responses to user commands
- **User:** Executes user programs, plus utilities such as compilers, editors, linkers, and debuggers

A process executing in a less-privileged mode often needs to call a procedure that executes in a more-privileged mode; for example, a user program requires an operating system service. This call is achieved by using a change-mode (CHM) instruction, which causes an interrupt that transfers control to a routine at the new access mode. A return is made by executing the REI (return from exception or interrupt) instruction.

**a.** A number of operating systems have two modes: kernel and user. What are the advantages and disadvantages of providing four modes instead of two?
**b.** Can you make a case for even more than four modes?

4.4 The VMS scheme discussed in the preceding problem is often referred to as a ring protection structure, as illustrated in Figure 4.15. Indeed, the simple kernel/user scheme is a two-ring structure. A disadvantage of a ring-structured access control system is that it violates the principle of least privilege. For example if we wish to have an object accessible in ring $X$ but not ring $Y$, this requires that $X < Y$. Under this arrangement all objects accessible in ring $X$ are also accessible in ring $Y$.

**a.** Explain in more detail what the problem is and why least privilege is violated.
**b.** Suggest a way that a ring-structured operating system can deal with this problem.

4.5 UNIX treats file directories in the same fashion as files; that is, both are defined by the same type of data structure, called an inode. As with files, directories include a nine-bit protection string. If care is not taken, this can create access control problems. For example, consider a file with protection mode 644 (octal) contained in a directory with protection mode 730. How might the file be compromised in this case?

4.6 In the traditional UNIX file access model, which we describe in Section 4.4, UNIX systems provide a default setting for newly created files and directories, which the owner may later change. The default is typically full access for the owner combined with one of the following: no access for group and other, read/execute access for group and none for other, or read/execute access for both group and other. Briefly discuss the advantages and disadvantages of each of these cases, including an example of a type of organization where each would be appropriate.

4.7 Consider user accounts on a system with a Web server configured to provide access to user Web areas. In general, this uses a standard directory name, such as 'public_html,' in a user's home directory. This acts as their user Web area if it exists. However, to allow the Web server to access the pages in this directory, it must have at least search (execute) access to the user's home directory, read/execute access to the Web directory, and read access to any webpages in it. Consider the interaction of this requirement

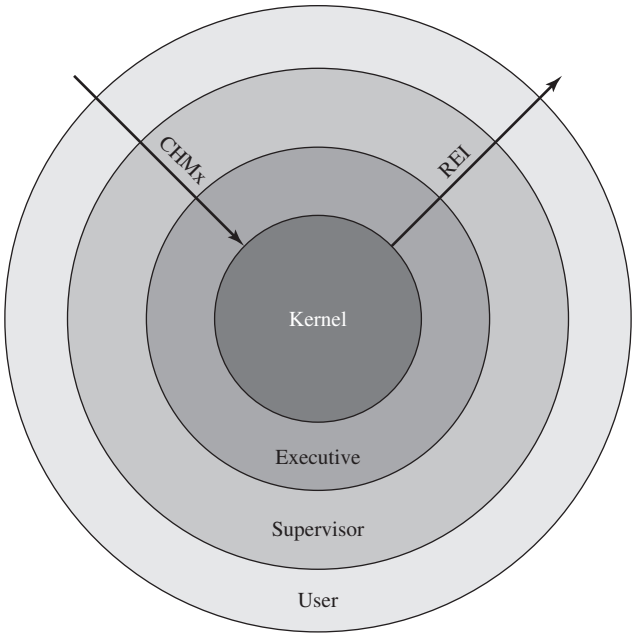


**Figure 4.15 VAX/VMS Access Modes**

with the cases you discussed for the preceding problem. What consequences does this requirement have? Note a Web server typically executes as a special user, and in a group that is not shared with most users on the system. Are there some circumstances when running such a Web service is simply not appropriate? Explain.

**4.8** Assume an application requires access control policies based on the applicant's age and the type of funding to be provided. Using an ABAC approach, write policy rules for each of the following scenarios:

**a.** If the applicant's age is more than 35, only "Research Grants (RG)" can be provided.

**b.** If the applicant's age is less than or equal to 35, both "RG and Travel Grants (TG)" can be provided.

**4.9** Assume a system with $K$ subject attributes, $M$ object attributes and Range () denotes the range of possible values that each attribute can take. What are the number of roles and permissions required for an RBAC model? What is the problem with this approach if additional attributes are added?

**4.10** For the NIST RBAC standard, we can define the general role hierarchy as follows:

RH $\subseteq$ ROLES $\times$ ROLES is a partial order on ROLES called the inheritance relation, written as $\geq$, where $r_1 \geq r_2$ only if all permissions of $r_2$ are also permissions of $r_1$, and all users of $r_1$ are also users of $r_2$. Define the set *authorized_permissions*($r_i$) to be the set of all permissions associated with role $r_i$. Define the set *authorized_users*($r_i$) to be the set of all users assigned to role $r_i$. Finally, node $r_1$ is represented as an immediate descendant of $r_2$ by $r_1 \gg r_2$, if $r_1 \geq r_2$, but no role in the role hierarchy lies between $r_1$ and $r_2$.

**a.** Using the preceding definitions, as needed, provide a formal definition of the general role hierarchy.

**b.** Provide a formal definition of a limited role hierarchy.

**23.3** Consider the details of the X.509 certificate shown below.

**a.** Identify the key elements in this certificate, including the owner's name and public key, its validity dates, the name of the CA that signed it, and the type and value of signature.

**b.** State whether this is a CA or end-user certificate, and why.

**c.** Indicate whether the certificate is valid or not, and why.

**d.** State whether there are any other obvious problems with the algorithms used in this certificate.

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 3c:50:33:c2:f8:e7:5c:ca:07:c2:4e:83:f2:e8:0e:4f
    Signature Algorithm: md5WithRSAEncryption
    Issuer: O=VeriSign, Inc.,
           OU=VeriSign Trust Network,
           CN=VeriSign Class 1 CA Individual Persona Not Validated
    Validity
      Not Before: Jan 13 00:00:00 2000 GMT
      Not After : Mar 13 23:59:59 2000 GMT
    Subject: O=VeriSign, Inc.,
           OU=VeriSign Trust Network,
           OU=Persona Not Validated,
          OU=Digital ID Class 1 - Netscape
          CN=John Doe/Email=john.doe@adfa.edu.au
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (512 bit)
        Modulus (512 bit):
            00:98:f2:89:c4:48:e1:3b:2c:c5:d1:48:67:80:53:
            d8:eb:4d:4f:ac:31:a9:fd:11:68:94:ba:44:d8:48:
            46:0d:fc:5c:6d:89:47:3f:9f:d0:c0:6d:3e:9a:8e:
            ec:82:21:48:9b:b9:78:cf:aa:09:61:92:f6:d1:cf:
            45:ca:ea:8f:df
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:FALSE
      X509v3 Certificate Policies:
        Policy: 2.16.840.1.113733.1.7.1.1
          CPS: https://www.verisign.com/CPS
      X509v3 CRL Distribution Points:
        URI:http://crl.verisign.com/class1.crl
```

```
Signature Algorithm: md5WithRSAEncryption
  5a:71:77:c2:ce:82:26:02:45:41:a5:11:68:d6:99:f0:4c:ce:
  7a:ce:80:44:f4:a3:1a:72:43:e9:dc:e1:1a:9b:ec:64:f7:ff:
  21:f2:29:89:d6:61:e5:39:bd:04:e7:e5:3d:7b:14:46:d6:eb:
  8e:37:b0:cb:ed:38:35:81:1f:40:57:57:58:a5:c0:64:ef:55:
  59:c0:79:75:7a:54:47:6a:37:b2:6c:23:6b:57:4d:62:2f:94:
  d3:aa:69:9d:3d:64:43:61:a7:a3:e0:b8:09:ac:94:9b:23:38:
  e8:1b:0f:e5:1b:6e:e2:fa:32:86:f0:c4:0b:ed:89:d9:16:e4:
  a7:77
```

**23.4** Using your Web browser, visit any secure Web site (i.e., one whose URL starts with "https"). Examine the details of the X.509 certificate used by that site. This is usually accessible by selecting the padlock symbol. Answer the same questions as for Problem 23.3.

**23.5** Now access the "Trust Store" (list of certificates) used by your Web browser. This is usually accessed via its Preference settings. Access the list of Certificate Authority certificates used by the browser. Pick one, examine the details of its X.509 certificate, and answer the same questions as for Problem 23.3.