CCA (d4364c5f)

2021-8-30 9:46:45

CCA Consent (item 1)

INFORMED CONSENT FOR PARTICIPATION IN RESEARCH ACTIVITIES

Thank you for agreeing to participate in our survey.

Before we start, we'd like for you to read the informed consent information below. Informed consent refers to the voluntary choice of an individual to participate in research based on an accurate and complete understanding of its purposes, procedures, risks, benefits, and alternatives. The survey data will be completely **confidential**. Data from each student, instructor, and institution will be anonymized. If you have any questions before completing this survey, please contact the investigator Dr. Alan Sherman by phone at 410 455-2666, 410 963-4779, or by email at sherman@umbc.edu.

Informed consent:

You must be 18 years or older to participate in this survey.

The purpose of this study is to provide infrastructure for rigorous evidence-based improvement of cybersecurity education by developing the first Cybersecurity Assessment Tools (CATs) targeted at measuring the quality of instruction, which can help universities better prepare the substantial number of cybersecurity professionals needed in America. You are being asked to volunteer because you are in or have completed cybersecurity courses. It will take up to two hours to complete this survey.

We are developing the Cybersecurity Curriculum Assessment (CCA) in hopes of creating a nationally recognized, research-based assessment tool for measuring how well students use adversarial thinking after completing a program of study in cybersecurity. The CCA will help us identify best practices for preparing future cybersecurity professionals. To verify whether the CCA will meet these goals, we are asking you to answer each of the questions on the survey.

There are no known risks involved in completing the survey. There are no tangible benefits for completing the survey, but you will have access to all results and project activities on the web site - http://www.cisa.umbc.edu/cats/index.html.

Participation is entirely voluntary; you may withdraw from participation at any time. If you withdraw from this research study, you will not be penalized in any way for deciding to stop participating.

All data obtained will be confidential. Results from this research will be published in academic conferences and journals, but no personally identifying information will ever be associated with your performance or shared.

This study has been reviewed and approved by the UMBC Institutional Review Board (IRB). A representative of that Board, from the Office for Research Protections and Compliance, is available to discuss the review process or my

rights as a research participant. Contact information of the Office is (410) 455-2737 or compliance@umbc.edu.

If you agree to the terms of this informed consent, please signify your consent by clicking the checkbox "I Consent" below, clicking "Save", and then clicking the "Next" button on the right in order to start the survey. If you'd like to leave the survey at any time, just close your browser tab.

I Consent

CCA Exam Instructions (item 2)

Thank you for taking this draft Cybesecurity Concept Assessment (CCA), which was developed as part of the CATS Project.

Your participation will help us improve the assessment.

Each test item has a scenario and a question (stem). Some questions share a common scenario, but each question should be answered independently. For each question, choose exactly one answer--the single best alternative from among the five given.

After you answer the question, please rate the question and, optionally, provide a comment.

If you believe there is a problem with a test item, report the issue using the report-error button at the side.

An example question is provided below; please answer it to demonstrate that you understand the format of the test.

PLEASE HIT "SAVE" or "SAVE AND GRADE" AFTER EACH QUESTION TO STORE YOUR ANSWER BEFORE HITTING NEXT OR YOUR RESPONSE WILL NOT BE RECORDED.

Question

Choose the correct answer below:

A. Incorrect
B. Incorrect
C. Correct
D. Incorrect
E. Incorrect

PLEASE HIT "SAVE" or "SAVE AND GRADE" AFTER EACH QUESTION TO STORE YOUR ANSWER BEFORE HITTING NEXT OR YOUR RESPONSE WILL NOT BE RECORDED.

demographics (item 3)

This information will be used to help us generate an anonymous report for your instructor. Your personal information will never be directly associated with your performance on the assessment.

School

Professor

Year in School

Freshman

Sophomore

Junior

Senior

Graduate

Press "Grade" to submit. All responses will receive full credit.

CCA Question E1-1 (item 4)

Consider the following protocol in which Alice predicts the outcome of a random coin flip by Bob. Alice and Bob use this protocol to gamble over a secure phone line. Alice and Bob distrust each other and are motivated to cheat.

Desired properties

- RESULT is chosen with uniform distribution from the set {TRUE, FALSE}.
- Neither party can bias the selection of RESULT.
- If Alice and Bob follow the protocol, they should compute the same value of RESULT.
- If Alice or Bob do not follow the protocol, the other should be able to detect this fact.

Assumption

flip_coin() is a function that, using a cryptographically-secure pseudorandom number generator, returns HEADS or TAILS with uniform distribution.

Coin-Flip Protocol

```
Alice                                          Bob
1:  PREDICTION = choose_one_of(HEADS, TAILS)
2:  PREDICTION -------------------------> PREDICTION
3:                                             OUTCOME = flip_coin()
4:  OUTCOME <----------------------------- OUTCOME
5:  RESULT = (PREDICTION equals OUTCOME)       RESULT = (PREDICTION equals OUTCOME)
```

Notation

- `=` denotes the assignment operator
- `equals` denotes the equality comparison
- `---------->` (arrow) denotes sending a message from one party to another

Question. Choose the most significant flaw in the protocol:

A. Messages are neither encrypted nor authenticated.
B. Alice can change her PREDICTION.
C. Bob and Alice might compute different values for RESULT.
D. Bob can choose OUTCOME to be the opposite of Alice's PREDICTION.
E. flip_coin() is a pseudorandom function, not a truly random function.

CCA Question Z6-1 (item 5)

Bob wishes to send a sensitive document D to Alice over a public network. To accomplish this goal, they wish to establish a shared session key k for symmetric encryption.

For asymmetric encryption, Alice has her own secret key s_A and Bob's authenticated public key p_B. Similarly, Bob has his own secret key s_B and Alice's authenticated public key p_A.

The public keys, including Alice's public key p_A and Bob's public key p_B, are posted on a public website. Anyone can download these keys in an authenticated fashion.

To encrypt and decrypt, Alice and Bob use a strong symmetric cipher E and a strong asymmetric cipher R.

Let $E[k,\ D]$ denote symmetric encryption of D with key k, and let $R[s_A,\ D]$ denote asymmetric encryption of D with key s_A. Assume that encrypting with R under a secret key has the effect of creating a signature.

Alice and Bob agree on the following protocol:

1. Alice generates a session key k at random.
2. Alice computes $v = R[s_A,\ (k,t)]$, where t is the current time.
3. Alice sends $c = R[p_B,\ v]$ to Bob.
4. Bob receives c and decrypts c by computing $v = R[s_B,\ c]$.
5. Bob decrypts v by computing $(k,t) = R[p_A,\ v]$. He also verifies the time and signature computed in Step 2.
6. Bob sends $E[k,\ D]$ to Alice.

Question. Choose the most fundamental flaw of this protocol:

A. c is encrypted with a publicly known key.
B. Encryption of v into c with key p_B is redundant.
C. An adversary could pick a random v, send $R[p_B,\ v]$ to Bob, thereby masquerading as Alice.
D. Bob can masquerade as Alice to arbitrary receivers.
E. v should be computed using p_A instead of s_A.

Definitions

masquerade: To pretend to be someone else.

CCA Question Z7-1 (item 6)

Having acquired Alice's username, Eve is trying to break into a sensitive computer system. Alice is an authorized user on the system. The system authenticates Alice by asking for a password. Assume the system runs its authentication routine on a secure computer that Eve cannot compromise.

Consider the following pseudocode that validates the password entered by a user.

```
// Returns: true if password is valid.
//          false if password is invalid.
is_valid_password(username, password)
begin
  stored_password = get_stored_password(username)
  for i = 0 to (length(stored_password) - 1)
    if stored_password[i] != password[i]  // != not equals
      return false
    endif
  endfor
  return true
end
```

Note In the pseudocode, `//` denotes the start of a comment.

Question. Choose the feature of the pseudocode that could most simply enable Eve to discover Alice's password, assuming Eve can make multiple attempts to log in:

A. Terminating the loop at the first non-matching character.
B. Storing passwords in memory as plaintext during execution.
C. Retrieving a potentially non-existent password and reading its bytes.
D. Allowing the upper bound of the loop to be longer than the stored password.
E. Permitting possible overflow and injection attacks through arbitrarily long usernames.

CCA Question C3b-1 (item 7)

Alice is logging on to a server from her laptop. She sends her username and password to the server over the Internet. The server then instructs the security computer to send a challenge to Alice's cell phone, which she responds to via text message. For example, the challenge is the name of Alice's pet, and the response is "Skippy". If the response is valid, the security computer signals the server to accept Alice's log-in request; otherwise, the security computer signals the server to reject the request.

Eve has obtained Alice's username and password and has positioned herself in the middle of Alice's Internet communication with the server. Consequently, Eve can block and inject messages between Alice and the server, but Eve CANNOT read, block, or inject messages between Alice's cell phone and the security computer.

Question. Choose the vulnerability that will most likely allow Eve to log in as Alice:

A. Alice's keystrokes on her laptop are being monitored by malware propagated by Eve.
B. Eve can send messages to Alice that appear to have originated from the server.
C. Alice's firewall is misconfigured, allowing Eve to monitor all communications with the server.
D. The answer to Alice's security challenge is easy to guess.
E. The challenge sent by the security computer does not reference Alice's log-in request.

Definitions

masquerade: To pretend to be someone else.

CCA Question Z5-1 (item 8)

To guard against potential man-in-the-middle attacks on a customer's home computer, a bank requires all remote (i.e., not at the physical bank) transactions to be authenticated by a trusted physically-secure physical device issued by the bank. The device has no clock. The bank verifies a transaction by requesting that the customer transmit the proposed transaction together with a signed token output from the device. To output the token, the customer inserts the device into their home computer and pushes a physical button on the device. The device cryptographically signs the token using a unique secret key physically secured on the device, and outputs the signed token. The bank requires each customer to maintain possession of their device.

Alice logs into the bank's website and fills out a form to transfer $2000 from Account 1 to Account 2. When prompted, she pushes the button on her device to authorize the transaction.

Question. Choose the most significant security limitation of the device in this context: The device...

A. is incapable of producing a timestamp.
B. lacks a display to show Alice the details of the transaction being authorized.
C. cannot verify who pushed the button.
D. communicates with Alice's home computer through an unencrypted channel.
E. signs the token with its own secret key, not with Alice's secret key.

CCA Question Z4-2 (item 9)

A security company is considering two possible designs for its physically-secure authentication dongle to authenticate authorized users to access a variety of online banking sites. The dongle is manufactured with tamper-resistant and tamper-responding technologies. In each of the following designs, to authenticate a user, the server issues a unique challenge. The user replies with output from the dongle, and the server verifies the user's reply.

Design A. Using a symmetric-key block cipher in output feedback mode (to generate a pseudorandom stream of bits from an initial secret seed unique to each dongle), the dongle outputs a sequence of pseudorandom passwords. To output a password valid for two minutes, the user presses a physical button on the authentication dongle.

Design B. Using a public-key cryptosystem capable of producing digital signatures, the dongle implements two functions: initial pairing, and subsequent authentication. During initial pairing, the dongle generates a (public key, private key)-pair and transmits the public key to the banking server. Initial pairing takes place at a physical bank. During subsequent authentication, the dongle responds to a challenge from the banking server by signing the challenge using the dongle's secret key.

Question. Choose the most significant vulnerability common to both designs:

A. Man-in-the-middle attacks.
B. Replay attacks.
C. Authentication dongles can be compromised during production.
D. Clock synchronization attacks exploiting drift in clocks between dongle and server.
E. The underlying cryptography is vulnerable to quantum computers.

CCA Question E3-1 (item 10)

Alice sends a plaintext message m to Bob as follows. Adversary Eve controls the network and is able to read and modify all messages sent over the network.

Alice sends *MSG* to Bob where *MSG* is the four-tuple:

MSG = <
("Bob", "Alice"*),*
$R[p_B, k]$,
$E[k, m]$,
$R[s_A, (E[k, m], \textit{"Alice"})]$
>.

Notation

- m = a plaintext message
- p_A = public key of Alice
- s_A = secret key of Alice
- p_B = public key of Bob
- s_B = secret key of Bob
- p_E = public key of Eve
- s_E = secret key of Eve
- *"Alice"* = a string identifying Alice
- *"Bob"* = a string identifying Bob
- k = a session key randomly generated by Alice
- $E[k, m]$ = symmetric encryption of a message m under key k.
- $R[k, m]$ = asymmetric encryption of a message m under key k.

Assumptions

- Alice, Bob, and Eve know each other's public keys.
- Alice, Bob, and Eve can see all of the messages in the network.
- The encryption functions are immune to cryptanalysis.
- $R[k, m]$ can be used to perform signatures.

Question. Choose the best answer describing how Eve can most seriously exploit Alice's transmission while minimizing the likelihood of detection:

A. Decrypt k, because it is encrypted using the publicly-known value p_B.
B. Replace message m with an alternate message m_2.
C. Replace the first component of *MSG* with $R[p_A, k_2]$.
D. Recompute and replace the first and fourth components using *"Eve"* for *"Alice"* and s_E for s_A.
E. Masquerade as Bob to Alice by intercepting *MSG* and replying to it.

Definitions

masquerade: To pretend to be someone else.

CCA Question S2-1 (item 11)

Jo is a system administrator in charge of a network of computers in remote locations that must perform tasks at the start of every hour. The computers synchronize their times once a day using a network link and perform a task provided to them by a central server. Recently, one computer began consistently finishing its tasks late, and network monitoring shows unusual new traffic flows originating from that computer. Upon logging into the affected computer, however, Jo finds that it seems fine. She lists the running processes, but nothing seems to explain the observed behaviors.

Question. Choose the adversary's action that best explains the observed behaviors of the affected computer:

A. Tampered with the time-synchronization process.
B. Virtualized the operating system and software.
C. Caused the network interface card to drop packets.
D. Performed a denial-of-service attack against the central server.
E. Ran malicious user-level processes.

CCA Question K1-1 (item 12)

A military communication system uses three 256-bit symmetric keys. Each key is chosen randomly with uniform distribution over the set of all such keys. The communicants share a long-term key Y, changed once a year and distributed by a trusted courier.

Each message is encrypted with a message key K, changed for each message. Each message key is encrypted with a daily key D, changed at 6am each day. The keys K and D are sent as part of each message transmission, as explained below.

For Alice to send a message x to Bob, she computes and transmits the triple

$< E[K,x],\ K$ XOR $D,\ E[Y,D] >$,

where E is a trusted block cipher, and $E[K,x]$ denotes the encryption of message x using key K, and XOR denotes exclusive-OR.

Question. Choose the most serious weakness of this system:

A. The same encryption function is used to encrypt x and D.
B. Key Y is used for too long a period of time.
C. A chosen-message attack reveals the long-term key.
D. Compromise of any message key reveals the daily key.
E. The system fails to protect the integrity of messages.

CCA Question E2-1 (item 13)

ACME University recently introduced a system through which students submit assignments electronically. Students upload assignments through a web form, which writes the assignments to a common directory assigned to the relevant course and instructor.

The files in the directory can be accessed only through the system. Through a separate web form, instructors can access and grade assignments in the submission directory. The system writes grades to a grade file that resides in the submission directory alongside the submitted assignments. The system authenticates all users.

Consider the following listing of the submission directory:

```
rw- www  assignment1.txt
rw- www  grades.txt
rw- www  JohnAssig1.doc
rw- www  MikeSmith1.docx
rw- www  SallyAssn1.pdf
```

Notes

- txt, doc, docx, and pdf are document file types.

- `www` is the name of the account under which the web server runs.
- `rw- www` means the `www` account has read and write (but not execute) privileges for the given file.

Alice is teaching a course at ACME University. After finishing her latest round of grading, she discovers that all of the assignment grades have been changed to perfect scores.

Question. Choose the action that best describes how an adversary could most easily change these grades:

A. Compromise Alice's faculty credentials and modify the grades through the web form.
B. Exploit the lax permissions of the course assignment directory using a command line shell.
C. Execute an injection attack in the web form to gain privileged access to the system machine.
D. Embed malware in an assignment, compromising the system.
E. Construct an assignment file with the same name as the grade file and submit it.

CCA Question A4-1 (item 14)

An enterprise with highly sensitive data needs to be able to retrieve information from the Internet. To support this requirement while protecting its sensitive data, the enterprise partitions its internal computer network into three segments: Public, Quarantine, and Private. In this system, data can flow ONLY from Internet to Public, Public to Internet, Public to Quarantine, and from Quarantine to Private.

Question. While respecting the design specifications, choose the protocol that can be used to transfer a file from Public through Quarantine to Private:

A. A reliable protocol that expects a handshake between the sender and receiver for file transfer.
B. A streaming connectionless protocol using redundant paths that depends on message ordering between the sender and receiver for file transfers.
C. A connectionless protocol that does not depend on acknowledgments between the sender and receiver for file transfer.
D. A protocol that encrypts the transferred file, using a key established by a key-agreement protocol between sender and receiver.
E. A protocol that relies on authenticated tunneling through a configured firewall.

CCA Question A4-2 (item 15)

An enterprise with highly sensitive data needs to be able to retrieve information from the Internet. To support this requirement while protecting its sensitive data, the enterprise partitions its internal computer network into three segments: Public, Quarantine, and Private. In this system, data can flow ONLY from Internet to Public, Public to Internet, Public to Quarantine, and from Quarantine to Private.

Question. As an operator of this system, choose the following workspace configuration that best supports secure use of the network. In each configuration, the operator must interact with each terminal to move data from Public to Private.

A. There is one terminal that dynamically switches between Public, Quarantine, and Private.
B. Private has two terminals, one that communicates with Quarantine and Private; the other communicates with Public and Private.
C. Quarantine has two terminals, one that communicates with Public and Quarantine; the other communicates with Private and Quarantine.
D. Each segment has a unique terminal: one terminal communicates with Public, one terminal communicates with Quarantine, and one terminal communicates with Private.
E. There are four terminals, one communicates with Public, one communicates with Quarantine, one communicates with Private, and one communicates with a service that manages network traffic between the segments.

CCA Question Z4-1 (item 16)

A security company is considering two possible designs for its physically-secure authentication dongle to authenticate authorized users to access a variety of online banking sites. The dongle is manufactured with tamper-resistant and tamper-responding technologies. In each of the following designs, to authenticate a user, the server issues a unique challenge. The user replies with output from the dongle, and the server verifies the user's reply.

Design A. Using a symmetric-key block cipher in output feedback mode (to generate a pseudorandom stream of bits from an initial secret seed unique to each dongle), the dongle outputs a sequence of pseudorandom passwords. To output a password valid for two minutes, the user presses a physical button on the authentication dongle.

Design B. Using a public-key cryptosystem capable of producing digital signatures, the dongle implements two functions: initial pairing, and subsequent authentication. During initial pairing, the dongle generates a (public key, private key)-pair and transmits the public key to the banking server. Initial pairing takes place at a physical bank. During subsequent authentication, the dongle responds to a challenge from the banking server by signing the challenge using the dongle's secret key.

Question. Choose the most significant way in which Design B improves Design A:

A. It mitigates the threat of man-in-the-middle attacks.
B. It uses truly random bits rather than pseudorandom bits.
C. Passwords can be valid for longer than two minutes.
D. The server does not store any secret cryptographic variables.
E. There is no physical button.

CCA Question D1-1 (item 17)

Consider how each of the following five cipher systems establishes a session key. Each system uses a secure block cipher. In various ways, each system uses a trusted source of physical randomness (TSPR).

System A generates a 128-bit key by hashing 4096 bits from a TSPR using a cryptographically-secure hash function.

System B generates a 256-bit key at random using a TSPR.

System C generates a 512-bit key using bits output from a trusted public beacon of random bits generated by a TSPR based on quantum physics.

System D generates a 1024-bit key from the output of a cryptographically-secure pseudorandom number generator using a 128-bit seed taken from a TSPR.

System E generates a 2048-bit key by computing the exclusive-OR (XOR) of three 2048-bit sequences of contiguous characters chosen at random from a publicly-declared English text (e.g., first edition of Encyclopedia Britannica) using a TSPR.

Question. Choose the cipher system below that offers the greatest assurance against an adversary who attempts to determine the session key:

A. System A, because its session key has 4096 bits of entropy.
B. System B, because its session key has 256 bits of entropy.
C. System C, because its session key has 512 bits of entropy.
D. System D, because its session key has 1024 bits of entropy.
E. System E, because its session key has 2048 bits of entropy.

Definitions

beacon: A source that broadcasts a stream of bits.

contiguous characters: Adjacent characters; characters next to each other.

entropy: Uncertainty, measured in bits.

CCA Question A3-2 (item 18)

When a user Mike O'Brien registered a new account for an online shopping site, he was required to provide his username, address, first and last name, and a password. Immediately after Mike submitted his request, you—as the security engineer—observe a database input error message in the logs.

In the following database code,

- + means string concatenation.
- ; delimits a query string
- ' (single quote) delimits the string.
- * matches any column in the database table. In the database described below, * will retrieve NAME,ADDRESS,DOB for any record that matches the query (i.e., username)
- = is the assignment operator

Consider the database structure below:

```
USER_INFORMATION =>
                  NAME,
                  ADDRESS,
                  DOB
```

Also, observe the database code below:

```
Func GenerateAndExecuteQuery(username){

    query = "SELECT * FROM USER_INFORMATION WHERE USERNAME = '"
        + username
        + "';"

    execute(query)
}
```

Question. Choose the best way to improve the security of the database code above:

A. Pass *username* into a pre-compiled database query.
B. Sanitize input at the server side.
C. Require all characters input for *username* to be from a restricted set of characters.
D. Encrypt *query* before sending it to the database.
E. Validate that *username* is a non-null string and exists in the database.

CCA Question D2-1 (item 19)

A state issues a restricted number of permits for hunting certain trophy animals. The state issues the allotted number of permits, one per application, following a random ordering of all valid applications received by the posted deadline. Before the deadline, the state publicly posts all software used in the process. Many citizens highly desire these permits, and the state seeks a process that is fair and will be accepted by the citizens.

Consider the following two designs for determining the random ordering:

Design A. A trusted out-of-state auditing firm selects the ordering using the output from a known cryptographically-secure pseudorandom number generator. The seed for this generator is the 256-bit output from a cryptographically-secure hash function applied to the concatenation of 1000 random bits harvested from the firm's operating system.

Design B. The state selects the ordering using the output from a known cryptographically-secure pseudorandom number generator. The seed for this generator is the 256-bit output from a cryptographically-secure hash function applied to the concatenation of all of the winning numbers drawn at the first state lottery after the posted deadline (assume that there are at least 100 such numbers).

Consider the following potential properties of the state's system:

I. A corrupt insider (an employee of the state or at the auditing firm) cannot influence the ordering.
II. A malicious outsider cannot influence the ordering by penetrating the computer system than runs the software.
III. Any malicious influence of the ordering could be detected by the public.

Question. Choose the design that the state should use:

A. Design A, because it satisfies Properties I and II.
B. Design A, because it satisfies Property III, even though it does not satisfy Properties I and II.
C. Design A, because it places trust in an impartial auditing firm located outside the state.
D. Design B, because it satisfies Properties I and II.
E. Design B, because it satisfies Property III, even though it does not satisfy Properties I and II.

Definitions

concatenate: To join or link.

CCA Question T5-1 (item 20)

You are a security engineer at AcmeCorp. AcmeCorp uses certificates for server and user identity on the enterprise network, which has over a billion nodes. All network actions on this network typically fail (never succeed) one out of every 10 million actions. To operate on this network, a node must have a valid certificate. You have concerns about how certificates are distributed and revoked.

Question. Choose the method that best minimizes the damage a compromised certificate can cause on the enterprise network:

A. Install a whitelist on each node, that is periodically updated, containing allowed certificates which are checked on every request.
B. Use certificates that expire after a few days.
C. Cache certificates in an offline storage medium for easy replication.
D. Use a trusted third party to verify all certificate requests and exchanges.
E. Allow certificates to be used only over the corporate VPN (virtual private network).

CCA Question M1-1 (item 21)

Let E denote a secure length-preserving symmetric block cipher that encrypts 256-bit blocks under the control of a 128-bit key. The key is known only by the sender and receiver. Let X be any message whose length in bits is a multiple of 128. Encrypt the message X as follows.

First divide X into n 128-bit chunks $X = (y_1, y_2, ..., y_n)$.

Second, construct the 256-bit blocks $B_i = (h(y_i), y_i)$, for $i = 1,2,...,n$, where h is a trusted cryptographic hash function that produces a 128-bit output.

Third, separately encrypt the blocks to produce the ciphertext $C = (E[k, B_1], E[k, B_2], ..., E[k, B_n])$, where $E[k, B]$ denotes the encryption of block B using key k.

Notation

- $E[k, B]$ = encryption of block B under key k
- $h(y)$ = hash of chunk y
- X = a message
- y_i = the i^{th} chunk of X
- n = the number of chunks in X
- B_i = the i^{th} block
- C = ciphertext

Question. Choose the application that is best supported by this method to encrypt message X:

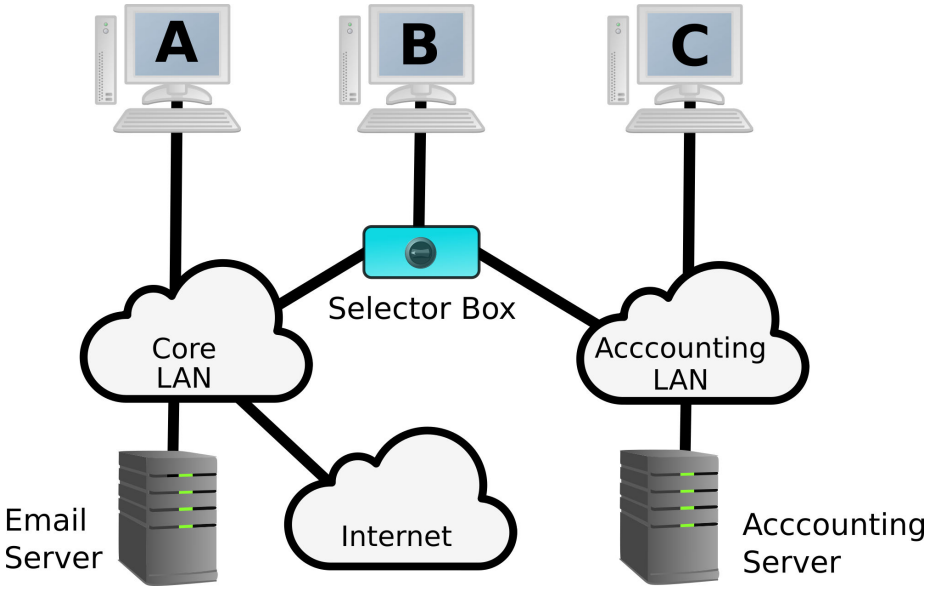
A. protect a randomly-chosen key of length exactly 128 bits by encrypting it (X is a key).
B. provide strong confidentiality of long messages with high speed by encrypting multiple blocks in parallel.
C. provide authentication for messages if the first block consists of the sender's name followed by random padding.
D. detect any modification of messages.
E. limit error propagation across blocks caused by bit-insertion errors in the ciphertext, because each such error would be restricted to the block in which it appears.

Definitions

bit-insertion error: When an extra bit is inserted into a sequence of bits.

CCA Question S1-1 (item 22)

A company has two internal Local Area Networks (LANs): a core LAN connected to an email server and the Internet, and an accounting LAN connected to the corporate accounting server (which is not connected to the Internet). Each desktop computer has one network interface card. Some computers are connected to only one of the networks (e.g., computers A and C). A computer that requires access to both LANs (e.g., computer B) is connected to a selector box with a toggle switch that physically connects the computer to exactly one LAN at a time.



Question. Choose the action that this design best prevents:

A. Emailing accounting data.
B. Infecting the accounting LAN with malware.
C. Computer A communicating with computer B.
D. User of Computer B accessing the accounting LAN without authorization.
E. Employees accessing the accounting server from home.

CCA Question Z5-2 (item 23)

To guard against potential man-in-the-middle attacks on a customer's home computer, a bank requires all remote (i.e., not at the physical bank) transactions to be authenticated by a trusted physically-secure physical device issued by the bank. The device has no clock. The bank verifies a transaction by requesting that the customer transmit the proposed transaction together with a token output from the device. To output the token, the customer inserts the device into their home computer and pushes a physical button on the device. The device cryptographically signs the token using a unique secret key physically secured on the device. The bank requires each customer to maintain possession of their device.

The bank adds a trusted GPS receiver to the device to enable the device to report its physical location assuredly. Specifically, the device includes GPS coordinates in each token. These GPS coordinates cannot be spoofed. Bank policy requires all transactions to be conducted within an authorized physical location (e.g., near the client's home).

Accused of a crime in New York (200 miles north of her home in Maryland), Alice provides the following alibi: a token generated from Alice's device shows that, at the time of the crime, she conducted a banking transaction from her home in Maryland.

Question. Choose the strength of this alibi:

A. Very weak. Somebody else could have pressed the button.
B. Weak. A bank employee may have colluded with Alice.
C. Neither weak nor strong. Alice's device could be defective.
D. Strong. To authorize a transaction, the device must be plugged into a computer near Alice's home.
E. Very Strong. The GPS coordinates of the device cannot be forged.

CCA Question H2-1 (item 24)

Consider the following log of corporate user activity. The corporation issues each employee a work PC and a smartphone.

Day	Time	User	Action	Device	Data Volume [kilobytes]
May 21	20:22:28	Bob	Local login	Work PC #5	0 UP / 0 DOWN
May 21	20:23:01	Bob	Connection to local server	Work PC #5	6,702 UP / 244,328 DOWN
May 21	20:25:12	Bob	Access to acmeshare.com	Work PC #5	122,164 UP / 3,456 DOWN
May 21	20:26:35	Bob	USB drive connected	Work PC #5	122,164 UP / 0 DOWN
May 22	08:28:12	Alice	Connection to remote host	Work PC #5	122,164 UP / 2,378 DOWN
May 22	08:32:12	Charlie	VPN login to network	Smartphone #9	2,490 UP / 4,566 DOWN
May 22	08:38:55	Charlie	Access to acmeshare.com	Smartphone #9	1,792 UP / 125,620 DOWN

Notes

- acmeshare.com is a fictional, free file-sharing service.
- UP and DOWN data transfer volumes are given from the perspective of the device specified in the device column and reflect application content only (i.e., not network acknowledgments). For example, in Line 2, User Bob transferred 6,702 kilobytes from Work PC #5 to the local server, and User Bob transferred 244,328 kilobytes from the local server to that PC.

Question. Choose the most serious malicious activity possibly suggested by this log:

A. Bob, Alice, and Charlie cooperated to exfiltrate data.
B. Alice sent corporate secrets to some unspecified remote host.
C. Bob connected a USB drive and wrote sensitive data to it from his corporate work PC.
D. Charlie and Bob shared a malicious file via acmeshare.com.
E. A malicious party installed a rootkit on Bob's work PC, giving the party easy continued unauthorized access to the PC.

Definitions

rootkit: A tool that hides itself and typically provides unauthorized root-level access to a computer.

CCA Question T2-1 (item 25)

There is a collection of nodes distributed across all 24 UTC time zones. Daily network traffic shows that nodes in time zones UTC+6, UTC+7, and UTC+8 have increased activity during the four-hour window starting at midnight and ending at 4am, in the UTC+6 time zone.

Question. Choose the most likely cause for the increase in network activity on nodes in time zones UTC+6, UTC+7, and UTC+8:

A. The nodes in time zones UTC+6, UTC+7, and UTC+8 are honeypots to attract malicious actors.
B. The infrastructure team runs remote daily backups from midnight to 8am in the UTC+6 time zone.
C. The adversary's standard workday begins at 9am in the UTC-3 time zone.
D. Because the nodes in time zones UTC+6, UTC+7, and UTC+8 have multiple network interface cards, they can process more network activity.
E. The nodes in time zones UTC+6, UTC+7, and UTC+8 are used for disaster recovery and stress testing.

Definitions

UTC: Universal Time Coordinated is a way of specifying time zones. For example, UTC+0 is the time at Greenwich, England, and UTC+2 is the time at a time zone two hours ahead of Greenwich.

CCA Question H1-1 (item 26)

A security-solutions software company hosts a website from which users download software. The company replicates the website on multiple servers throughout the world. For each downloadable file, the website lists a hash digest of the file produced by a cryptographically-secure hash function. All communications between users and the website take place over authenticated connections that protect confidentiality and integrity. News stories report that the company's websites were recently compromised, resulting in malicious files and corrupted listed hash values.

Victor downloads some software. When hashing his downloaded file (using the same cryptographically-secure hash function), Victor's digest matches the digest given on the vendor's website.

Question. Choose the most plausible reason why the file might nevertheless be malicious:

A. An intermediate router between the server and Victor modified the downloaded bits to insert malicious code.
B. Hackers changed only domain names referenced in the software, so the hash remained the same.
C. A company employee inserted malicious code into the software that Victor downloaded and updated the digest on the website accordingly.
D. During a recent system update, Victor unknowingly installed a malicious hash function, which when it recognizes certain malicious files, returns the correct hash value without computing the hash.
E. An adversary found a malicious file whose digest collided with the digest of the valid file.

CCA Question Y1-1 (item 27)

There is a software module that enables users to modify firewall rules for their corporate computers. Users enter the rules through a web interface.

Consider the following code snippet, which reads and executes firewall rules entered by users.

```
1. processRecord(inputBuffer){
2.     while(readNextCharacter(inputBuffer) != new_line ){        // != not equals
3.          append(recordToProcess, currentCharacter(inputBuffer))
4.     }
5.     if validate(recordToProcess[0..999]) {
6.          executeRecord(recordToProcess)
7.     }
8. }
```

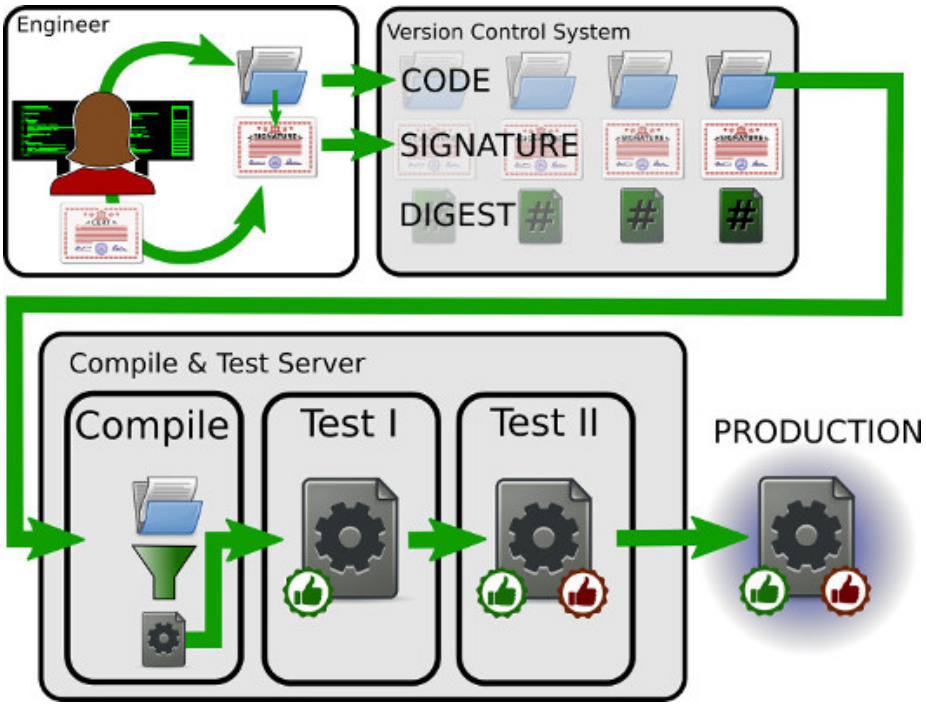
Note // denotes the start of a comment.

Question. Choose the most significant potential vulnerability involving Line 6:

A. A malicious user intercepts and modifies the user-supplied record.
B. The program does not terminate, because new_line is never encountered.
C. inputBuffer could overflow.
D. User-entered code could be executed.
E. Multiple records could be inserted at the same time.

CCA Question T1-1 (item 28)

As a member of the Blue Team (defense) at a software company, you have been tasked with improving the code-deployment pipeline for the software engineering team. This pipeline involves a trusted version-control system, a trusted server including its hardware and operating system (but not necessarily all of its software). All communications through the pipeline occur over secure channels. The pipeline comprises five steps:



1. A trusted engineer digitally signs and commits source code to the version-control system, which computes and stores a cryptographic hash digest of the committed code.
2. The pipeline system transfers the source code along with its digest from the version-control system to a company server.
3. The pipeline system compiles the source code on the server, producing a binary file.
4. On the same server, the pipeline system runs a pre-specified functional test suite against the binary file.
5. If functional testing succeeds, the pipeline system executes the non-functional test suite against the binary file.
6. If functional and non-functional testing succeed, the pipeline system releases the binary file to production.

Question. Choose the modification to the code deployment pipeline that would

most increase the likelihood that the released binary was compiled from the committed source code:

A. In Step 1, verify the digital signature of the committed code on the version control system.
B. In Step 2, verify the digest of the transferred code on the company server.
C. In Step 3, use a trusted compiler.
D. In Step 4, also perform static code analysis.
E. In Step 5, include a more rigorous Quality Assurance test environment.

Definitions

functional testing: Checks whether the code satisfies the input-output specifications. Example: The absolute value function will not return a negative value.

non-functional testing: Checks whether the code satisfies the operational requirements of the system. Example: The system must respond to requests from multiple geographic locations.

CCA Demographics (item 29)

Demographics Questions

Identifying information (e.g., your email address and school) will not be associated with demographics.

All fields are optional.

1. Identify your degree program (or the closest match):

A. Cybersecurty
B. Computer Science
C. Computer Information Systems / IS / MIS / IT
D. Computer Engineering
E. Information Assurance
F. Business
G. Decline to state
H. Other (enter below)

2. Identify your type of cybersecurity program (or the closest match):

Major

Minor

Track / Concentration

Certificate

Decline to state

Other (enter below)

3. Identify your degree objective (or closest match):

Associates

Bachelors

Masters

PhD or equivalent

Decline to state

None

Other (enter below)

4. How many classes have you taken that highlighted cybersecurity?

Choose one

0

1

2

3

4

5

6

7

8

9

10+

Decline to state

5. Please briefly describe your career goals:

6. Please select any cybersecurity certifications that you have:

CCNA (Cisco)

CCNP (Cisco)

CEH (EC-Council)

CISM (ISACA)

CISSP (ISC^2)

GSEC (SANS GIAC)

OSCP (Offensive Security)

Security+ (CompTIA)

Decline to state

None

Other (enter below)

7. Age:

Choose one

18-25 26-35 36-45 46-55 56+

Decline to state

8. Ethnicity: East Asian (e.g., Chinese, Japanese, Korean, Taiwanese) Southeast Asian (e.g., Cambodian, Vietnamese, Hmong, Filipino) South Asian (e.g., Indian, Pakistani, Nepalese, Sri Lankan) Other Asian Black / African Caucasian / White Hispanic / Latinx Native American Pacific Islander

Decline to state

Other (enter below)

9. Gender: Female Male Non-binary

Decline to state

Prefer to self-describe below

Click "Save only" if you want to go back to any question, or click "Save & Grade" if you are finished with the test.