## Instructions

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

Your participation will help us improve the assessment. You have 50 minutes to answer 25 questions.

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.

We also invite you to answer an additional seven optional questions in 22 minutes in the auxillary exam.

## Informed consent

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

The purpose of this study is to provide infrastructure for rigorous evidence-based improvement of cyber security education by developing the first Cyber Security Assessment Tools (CATs) targeted at measuring the quality of instruction, which can help universities better prepare the substantial number of cyber security professionals needed in America. You are being asked to volunteer because you are in or have completed a cybersecurity course. It will take up to 60 minutes to complete this survey.

We are developing the Cybersecurity Concept Inventory (CCI) in hopes of creating a nationally recognized, research-based assessment tool for measuring how well students use adversarial thinking after a first course in cybersecurity. The CCI will help us identify best practices for preparing future cybersecurity professionals. To verify whether the CCI 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 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.

## Demographics

This information will be anonymous from the user.

### School

### Professor

### Year in School

- ○ Freshman
- ○ Sophomore
- ○ Junior
- ○ Senior
- ○ Graduate

## Question 1

*Scenario A1. A company delivers packages to customers using drones. The company's command center controls the drones by exchanging messages with them. The company's command center authenticates each message with a keyed message authentication code (MAC), using a key that is known by the command center and installed in each drone at initialization. The command center stores this key encrypted in a database.*

Choose the post promising action for a malicious adversary to masquerade as the command center:

- Jam the command center’s signals and replace them.
- Capture a drone and extract its secret key.
- Exploit a vulnerability in the command center's firewall to access the database that contains the authentication key.
- Bribe an employee to give you the proprietary source code of the drone.
- Try to find messages with MACs that collide with the MACs of legitimate messages.

**Definitions:**

to masquerade: To pretend to be someone else.

## Question 2

*Scenario A2. Alice wants to send a file to Bob over an Internet connection.*

Alice sends to Bob the file and a tag. The tag is the output of a message authentication code applied to the file and a key known only by Alice and Bob. Charlie is a malicious actor monitoring the connection between Alice and Bob.

Choose the action by Charlie that this tag mitigates:

- Pretend to be Alice by resending the file and the tag.
- Collude with Bob to forge a file sent by Alice.
- Recover the file contents.
- Change bits of the file in transit.
- Prevent Alice from completing the file transfer.

## Question 3

*Scenario A2. Alice wants to send a file to Bob over an Internet connection.*

Bob receives a file digitally signed with Alice's private (signature) key, using a secure digital signature algorithm. The file specifies an electronic order to purchase a large number of shares for a new public offering. Contrary to expectation, the value of the stock plummets. Following this incident, Alice denies having signed the purchase order, pointing out that Charlie has been caught forging her signature.

Choose the most likely explanation for how Charlie forged Alice's signature:

- Copied Alice's digital signature from an older electronic purchase order.
- Mathematically analyzed Alice's signature to deduce her private key.
- Changed bits in Alice's signature to sign another electronic document.
- Received Alice's private key from Alice.
- Created a new document producing the same digital signature.

## Question 4

*Scenario A3. 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.*

Choose the best defense to protect against possible security problems suggested by this error:

- Implement the system in a more secure programming language.
- Sanitize input at the server side.
- More thoroughly test the software before deploying it.
- Encrypt and authenticate all messages between the client and the server.
- Require all characters input by the user to be from a restricted set of characters.

## Question 5

*Scenario A4. 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 should flow only from Public to Quarantine, and from Quarantine to Private.*

Choose the most important security objective for this system:

- Maintain integrity of sensitive data.
- Detect intrusions.
- Block malicious traffic with a firewall.
- Restrict access to only trusted users.
- Prevent data exfiltration.

**Definitions:**

quarantine: A place of isolation in which potentially infectious items are placed and checked.

## Question 6

*Scenario A4. 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 should flow only from Public to Quarantine, and from Quarantine to Private.*

Choose the most effective method to prevent unwanted data flows:

- Authenticate all data flows.
- Restrict access to authorized users only.
- Encrypt all data flows.
- Use only one-way physical connections between the segments.
- Install software firewalls between the segments.

**Definitions:**

quarantine: A place of isolation in which potentially infectious items are placed and checked.

## Question 7

*Scenario A4. 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 should flow only from Public to Quarantine, and from Quarantine to Private.*

A malicious file was discovered on the Private segment. Choose the most likely cause of this failure:

- A user on Public visited a malicious website.
- The malicious file was not identified as bad in quarantine.
- The system administrator failed to update software on Private.
- A former employee who knew the network architecture created the file.
- A firewall in front of Private was misconfigured.

**Definitions:**

quarantine: A place of isolation in which potentially infectious items are placed and checked.

## Question 8

*Scenario B1. A bank offers online banking services. To connect to these services from her home computer, the user searches for the bank's name and follows the first link returned by the search. She logs into the website by entering her username and password. She then performs several banking transactions.*

Alice logged on to the bank's website to make a payment of one thousand dollars to Bob. The next day, she discovers that an additional one thousand dollars were transferred to Bob's account. Bob had intercepted the encrypted traffic between Alice and the bank's website.

Choose the mostly likely explanation for how Bob used the intercepted traffic to transfer the additional one thousand dollars:

- Hijacked Alice's connection by extracting session data.
- Decrypted the traffic to discover the login credentials.
- Sent a copy of the encrypted traffic to the bank's website.
- Reverse engineered the banking protocol.
- Tricked the bank's online customer service.

## Question 9

*Scenario B1. A bank offers online banking services. To connect to these services from her home computer, the user searches for the bank's name and follows the first link returned by the search. She logs into the website by entering her username and password. She then performs several banking transactions.*

Mary logged onto the bank's website and requested a transfer of two thousand dollars. Subsequently, she discovered that, instead, ten thousand dollars were transferred. A criminal was able to modify the transaction amount by modifying the traffic.

Choose the vulnerability that most likely explains this event:

- The transmitted data was not protected by an error-correcting code.
- The data format was publicly revealed.
- The protocol lacked two-factor authentication.
- The transaction was not protected by a signed hash.
- The bank's firewall was configured incorrectly.

## Question 10

*Scenario B2. While Mary is traveling she decides to do some shopping online. She connects from a computer in a hotel business office that uses a wired network.*

A fellow hotel guest wants to steal Mary's credit card information. The hotel's IT staff monitors machines in the business office using anti-malware and network intrusion-detection software.

Choose the attack that is least likely to be detected by the IT staff:

- Perform a man-in-the-middle attack on the hotel's local network to masquerade as the online shopping service.
- Establish screen sharing with Mary's machine from another machine in the business office.
- Plant a key-stroke logging device between Mary's keyboard and machine.
- Monitor traffic on the hotel's local network to observe packets sent by Mary's machine.
- Insert a USB drive into the machine that automatically installs custom software.

**Definitions:**

masquerade: To pretend to be someone else.

## Question 11

*Scenario B2. While Mary is traveling she decides to do some shopping online. She connects from a computer in a hotel business office that uses a wired network.*

The hotel manager is concerned that for the past year, many hotel guests have reported credit card thefts after visiting the business center. Repeated attempts to solve this problem, such as reimaging machines, purchasing new software and hardware, and encrypting network traffic have all failed.
Choose the most likely explanation for these attacks:

- The purchased hardware includes backdoors implemented by the manufacturer.
- Hotel guests frequently visit dubious websites from machines in the business center.
- Attackers have defeated the security of protocols protecting guest-to-server communications.
- Attackers are monitoring traffic on the business center's local network.
- A member of the IT staff is involved in the thefts.

## Question 12

*Scenario B3. A soft drink company electronically stores the secret formula for its popular drink on a computer that is disconnected from all networks. A competitor wants to the learn the secret formula.*

Choose the action that is LEAST useful at preventing the competitor from learning this formula.

- Encrypt the sensitive data.
- Change passwords frequently.
- Require two people to access the data.
- Perform thorough background checks on all employees.
- Protect the facility with guards and fences.

## Question 13

*Scenario B4. To comply with the terms of a nuclear test ban treaty, Country A would like to implant a seismic sensor under Country B's soil to monitor underground weapons testing. Country A fears that B will try to falsify the signals of the sensor, and Country B fears that A will try to exfiltrate spy information embedded in the seismic data. Neither party trusts the other.*
*Requirements of the system are:*

1. *Country A wants assurance that the seismic data it receives came from its sensor and were not modified.*
2. *Country B wants to be able to monitor the signals transmitted from the sensor in real time. It also wants assurance that the signals were not modified.*
3. *The design should be fair to both parties.*

A device is placed in a deep, narrow hole underground in Country B and certain cryptographic keys are distributed to the device, Country A, and Country B. The device comprises a seismic sensor and cryptographic hardware for processing its signals before they are broadcast to a satellite.

To best satisfy the system requirements, choose what type of cipher the device should apply to each message:

- Symmetric cipher separately applying two keys, one known only by A and the device, and one known only by B and the device.
- Symmetric cipher applying a key known by A, B, and the device.
- Asymmetric cipher (public-key cryptography) applying a private key known only by the device. The corresponding public key is known by A, B, and the device.
- Asymmetric cipher (public-key cryptography) applying a private key known only by the device and A, with the corresponding public key known by A, B, and the device.
- Asymmetric cipher (public-key cryptography) applying a public key known by A, B, and the device. The corresponding private key is known only by the device.

## Question 14

*Scenario B4. To comply with the terms of a nuclear test ban treaty, Country A would like to implant a seismic sensor under Country B's soil to monitor underground weapons testing. Country A fears that B will try to falsify the signals of the sensor, and Country B fears that A will try to exfiltrate spy information embedded in the seismic data. Neither party trusts the other.*
*Requirements of the system are:*

1. *Country A wants assurance that the seismic data it receives came from its sensor and were not modified.*
2. *Country B wants to be able to monitor the signals transmitted from the sensor in real time. It also wants assurance that the signals were not modified.*
3. *The design should be fair to both parties.*

Data are chunked into messages, each with a unique sequential message number.

Choose the security goal that is supported by including unique message numbers:

- Protect against replay attacks.
- Prevent any messages from producing equal hash values.
- Facilitate the retransmission of lost or garbled messages: the recipient can specify by message number which messages need to be retransmitted.
- Protect against man-in-the-middle attacks.
- Provide ordering information necessary to verify authenticity of the message.

## Question 15

*Scenario B4. To comply with the terms of a nuclear test ban treaty, Country A would like to implant a seismic sensor under Country B's soil to monitor underground weapons testing. Country A fears that B will try to falsify the signals of the sensor, and Country B fears that A will try to exfiltrate spy information embedded in the seismic data. Neither party trusts the other.*
*Requirements of the system are:*

1. *Country A wants assurance that the seismic data it receives came from its sensor and were not modified.*
2. *Country B wants to be able to monitor the signals transmitted from the sensor in real time. It also wants assurance that the signals were not modified.*
3. *The design should be fair to both parties.*

Consider a design in which the device applies a keyed cryptographic hash function to each message using a key distributed only to the device, Country A, and Country B.

To enable both countries to authenticate each message and satisfy all system requirements, choose what the device should output:

- The message together with a hash of the following: message and current time.
- The key together with a hash of the message.
- The message together with a hash of the message.
- A hash of the message.
- This design cannot satisfy the system requirements.

## Question 16

*Scenario B4. To comply with the terms of a nuclear test ban treaty, Country A would like to implant a seismic sensor under Country B's soil to monitor underground weapons testing. Country A fears that B will try to falsify the signals of the sensor, and Country B fears that A will try to exfiltrate spy information embedded in the seismic data. Neither party trusts the other.*
*Requirements of the system are:*

1. *Country A wants assurance that the seismic data it receives came from its sensor and were not modified.*
2. *Country B wants to be able to monitor the signals transmitted from the sensor in real time. It also wants assurance that the signals were not modified.*
3. *The design should be fair to both parties.*

The cryptographic hardware encrypts with a widely-deployed symmetric cipher with key k known by Country A, Country B, and the device.

Choose the the most serious limitation of this authentication strategy:

- Symmetric ciphers provide confidentiality, not authentication.
- Anyone who knows k can forge a message.
- It is difficult to distribute a new key k.
- Using encryption makes it more difficult to recover from transmission errors.
- If a party misplaces k, they cannot authenticate any message.

## Question 17

*Scenario C1. Bob's manager Alice is traveling abroad to give a sales presentation about an important new product. Bob receives an email with the following message: "Bob, I just arrived and the airline lost my luggage. Would you please send me the technical specifications? Thanks, Alice."*

Upon receiving Alice's message, choose what action Bob should take:

- Check that the source address in the received email exactly matches Alice's corporate e-mail.
- Ask Alice via email for the address of her hotel, and then send the specifications by courier.
- Send the encrypted specifications to Alice via email and then text her the decryption key.
- Verify that Alice sent the email requesting the technical specifications.
- Reply to Alice's email, attaching the specifications together with a cryptographic hash.

**Definitions:**

courier: A special-purpose messenger.

## Question 18

*Scenario C2. A security company is designing a precinct voting system to enable members of the military to vote in their hometown elections by casting a ballot at their overseas military base. The system must provide, among other properties, voter authentication, ballot confidentiality, integrity of marked ballots, and assured operations. When a voter checks in, a pollworker records the voter's name on the voter check-in list and verifies each of the following:*

1. *The voter's appearance resembles the image on an acceptable photo identification card.*
2. *The voter's name is on the voter registration list.*

Identify the primary purpose of checking if the voter's name is on the voter registration list:

- Be able to verify later that the person cast a ballot.
- Prevent criminals from casting votes on behalf of deceased people.
- Determine whether the person is eligible to vote at this location.
- Ensure that the person votes only once.
- Verify the person is who they claim to be.

**Definitions:**

precinct voting: Voting that takes place in an enclosed area which is supervised and provides a considerable degree of security and ballot privacy.

## Question 19

*Scenario C3a. Alice logs into a server by sending her username, password, and a timestamp to the server over the Internet. Eve listens to the communications.*

Eve wishes to log into Alice's account at a later time. Choose the modification to the login protocol that best deters Eve from later logging in to Alice’s account:

- Instead of sending the username, password, and timestamp over the Internet, send them in a text message from Alice's smartphone.
- In a second step, prompt Alice for additional personal information, such as her mother's maiden name.
- Replace the username and password pair with Alice's fingerprint.
- Encrypt the username, password, and timestamp.
- Include a use-once, randomly generated value to prevent replay attacks.

## Question 20

*Scenario C3b. Alice is logging onto 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 answers using a text message. For example, the challenge is the name of Alice's pet, and the response is "Skippy". Upon deeming the response valid, the security computer signals the server to accept Alice's login request.*

Eve has obtained Alice's username and password and has positioned herself in the middle of Alice's Internet communication with the server. While this allows Eve to block and inject messages between Alice and the server, Eve is not able to do the same between Alice's cell phone and the security computer.

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

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

**Definitions:**

masquerade: To pretend to be someone else.

## Question 21

*Scenario C4. Alice runs a top-secret government facility where she has hidden a USB stick, with critical information, under a floor tile in her workspace. The facility is secured by guards, 24/7 surveillance, fences, electronically locked doors, sensors, alarms, and windows that cannot be opened. To gain entrance to the facility, all employees must present a cryptographically hardened ID card to guards at a security checkpoint. All of the computer networks in the facility use state-of-the-art computer security practices and are actively monitored.*

Alice hires Mark (an independent penetration tester) to exfiltrate the data on the USB stick hidden in her workspace.

Choose the strategy that best avoids detection while effectively exfiltrating the data:

- Compromise the facility's network and add Mark as an authorized guest.
- Convince an authorized employee to remove the USB stick and give it to Mark.
- Unlock electronically-locked doors using malware.
- Climb over the perimeter fence at night and sneak into Alice's workspace.
- Fabricate a fake ID to fool the guards at the security checkpoint.

**Definitions:**

24/7: Twenty-four hours a day, seven days a week.

## Question 22

*Scenario C4. Alice runs a top-secret government facility where she has hidden a USB stick, with critical information, under a floor tile in her workspace. The facility is secured by guards, 24/7 surveillance, fences, electronically locked doors, sensors, alarms, and windows that cannot be opened. To gain entrance to the facility, all employees must present a cryptographically hardened ID card to guards at a security checkpoint. All of the computer networks in the facility use state-of-the-art computer security practices and are actively monitored.*

Alice's workspace is protected by an electronically-locked door featuring a tamper-resistant fingerprint scanner. To unlock the door, the electronic door lock scans a fingerprint and checks it against an encrypted fingerprint stored in a database. The encryption keys are secret. Additionally, the door is monitored continuously by a camera whose output is observed by a security guard.

Choose the action that best exploits this system:

- Try many possible fingerprints using a device that quickly outputs randomly-chosen fingerprints to the scanner.
- Use a screwdriver or other physical tools to expose the electronics of the lock to unlock the door by gaining access to the lock control wire or physical door latch.
- In the database, replace Alice's encrypted fingerprint with the attacker's encrypted fingerprint.
- Lift fingerprints from objects touched by Alice to recreate her fingerprint.
- Retrieve Alice's fingerprint by decrypting the encrypted copy stored in the database.

**Definitions:**

24/7: Twenty-four hours a day, seven days a week.

## Question 23

*Scenario D1. A law firm stores sensitive client records in a database on their local network.*

Choose the action that is the MOST likely to prevent an opposing law firm from reading the records:

- Require fingerprint scans to access the law offices.
- Disconnect their local network from the Internet
- Use only trusted vendor software.
- Protect the network with a state-of-the-art firewall and intrusion-detection system.
- Secure the law offices 24/7 with strong locks and security cameras.

**Definitions:**

24/7: Twenty-four hours a day, seven days a week.

## Question 24

*Scenario T1: Mike is a penetration tester performing a penetration test of ACME Corporation, a leading producer of automobiles. Mike has been given a wired connection to ACME's local area network (LAN).*

Choose the node that Mike should first compromise to have the highest likelihood of success in remaining undetected and understanding how ACME Corporation operates:

- Server containing data about automobile prototypes.
- Database storing human resources information.
- Firewall between ACME's LAN and the Internet.
- Server that stores logs of network connections for the LAN.
- Server responsible for authenticating all users on the LAN.

## Question 25

*Scenario Z2. Bob wishes to send a sensitive document D to Alice. 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 sA and Bob's authenticated public key pB. Similarly, Bob has his own secret key sB and Alice's authenticated public key pA. 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(sA, D) denote asymmetric encryption of D with key sA.*

Alice and Bob agree on the following protocol:

1. Alice generates a session key k at random.
2. Alice sends c = R(sA, k) to Bob.
3. Bob receives c and decrypts c by computing k = R(pA, c).
4. Bob sends E(k, D) to Alice.

where
pA = Alice's public key,
sA = Alice's secret key,
pB = Bob's public key, and
sB = Bob's secret key.

Choose the most fundamental flaw of this protocol:

- A passive eavesdropper can read the document D.
- Bob cannot decrypt c.
- An adversary can modify bits of c in transit.
- It is computationally expensive to compute several encryptions/decryptions.
- The session key k is not authenticated by Alice.

**Definitions:**

masquerade: To pretend to be someone else.