**CS42600 Spring 2019 Midterm 1 Solutions**, February 12, 2019
*Prof. Chris Clifton*

**Turn Off Your Cell Phone.** Use of any electronic device during the test is prohibited. As previously noted, you are allowed notes: Up to two sheets of 8.5x11 or A4 paper, single-sided (or one sheet double-sided).

Time will be tight. If you spend more than the recommended time on any question, **go on to the next one**. If you can't answer it in the recommended time, you are either giving too much detail or the question is material you don't know well. You can skip one or two parts and still demonstrate what I believe to be an A-level understanding of the material.

Note: It is okay to abbreviate in your answers, as long as the abbreviations are unambiguous and reasonably obvious.

In all cases, it is important that you give some idea of how you derived the answer, not simply give an answer. Setting up the solution correctly, even if you don't carry out the calculations to get the final answer, is good for nearly full credit.

# 1 Privilege Escalation (6 minutes, 5 points)

A. What is a privilege escalation attack?

**A privilege escalation attack is one that allows an authorized user or process to obtain privileges to which they are not authorized.**

B. Give an example of how a privilege escalation exploit could occur. (This doesn't have to be an exploit that would work in a real system, just an illustrative example.)

**Calling a system function that operates at a higher level of privilege to perform a specific operation, then using some other attack (e.g., buffer overflow to enable running arbitrary code) to use those privileges for something other than the intended operation.**

C. Name two types of vulnerabilities that must exist to enable the example security violation you describe above. If you feel there is only one vulnerability, describe why that one vulnerability being exploited would be sufficient to enable a privilege escalation attack.

**Violation of principle of least privilege (system function has authority to do more than the specific operation); memory vulnerability to allow code execution.**

*Scoring: 1 for reasonable description; 1 for example that is privilege escalation, 1 for reasonably complete example; 1 each for "Least Privilege" and something else that fits attack. At least one should be that the attack target is overprivileged - simply "becoming root" doesn't explain why there exists an entity in the system that has authority to do/access everything (doesn't this seem foolish?)*

# 2 Buffer Overflow (6 minutes, 4 points)

Briefly describe two methods of preventing buffer overflow attacks. For each, give one or two sentences about how to implement the method, and one or two sentences describing why it prevents buffer overflow attacks.

A.

**Only allow execution from certain areas of memory, and disallow applications to write to those areas of memory (a hardware fix.) Doesn't prevent buffer overflow, but prevents execution of any data written by the exploiting a buffer vulnerability.**

B.

**Use a memory-safe language/compiler that does not allow data to be written outside of allocated memory. Prevents the writing of data into space that it shouldn't be.**

*Scoring: 1 each for method (need not be the above), 1 for description of why it works.*

# 3 Insider Threat (7 minutes, 5 points)

We divided insider threat into three types: "Moles", "Disgruntled", and "Opportunists".

- Describe two security approaches/principles that are effective against all three types of insider threat.

  **Complete mediation, Principle of Least Privilege**

- Describe a security approach/principle that works against one or two of these threat types, but not against all of them. Describe why it works against some but not all.

  **Auditing behavior. Can catch mole, may deter opportunist, but likely works too late to prevent attack by disgruntled employee.** Many said background checks only work against moles. While I did credit this with good reasoning, I will mention that background checks can include psychological profiling (is this person likely to seek revenge if unhappy?) and financial checks, often recurring (does this person need money that would lead them to be an opportunist?)

*Scoring: 2 for principles; 1 for principle, 1 for reasons why it works, 1 for why it doesn't work.* There really weren't right or wrong answers here, as much as right or wrong reasoning. Almost any approach could work against any type of attacker if done correctly, but wouldn't help if done incorrectly - the key is to think carefully about what you are trying to accomplish.

# 4 Heartbleed (6 minutes, 5 points)

The OpenSSL Heartbleed attack worked by an attacker sending a string and the size of that string; the victim stored the string in memory and returned the string up to the reported size. If the reported size is greater than the string length, whatever happened to be in memory after the string was returned.

A. Does Heartbleed violate Confidentiality, Integrity, or Availability?

   **Confidentiality**

B. Buffer overflow attacks typically overwrite beyond the end of a buffer, and use this to cause a program to execute something it isn't supposed to. Is this what Heartbleed does?

   **No. Heartbleed doesn't overwrite data.**

C. One method for preventing buffer overflow attacks is to prevent execution from data areas of memory. Does this protect against Heartbleed? Explain why or why not.

   **No. Heartbleed simply retrieves data (an immediate confidentiality violation), it does not require executing any code other than the existing OpenSSL code.**

*Scoring: 1 for Confidentiality, 2: 1 for "No", 3: 1 for "No", 1 for explanation, 2 if explanation specifically notes Heartbleed does not require execution of non-standard code.*

# 5 Training (5 minutes, 2 points)

The NIST security training standard distinguishes between "Security awareness" and "Security training". Describe one distinction between the two.

**Awareness seeks to build general security understanding (e.g., avoiding phishing attacks); training is targeted to specific job tasks (e.g., what data can and cannot be disclosed under FERPA) and often requires evaluating the result of the training (e.g., passing a test.)**

*Scoring: 2 for a clear distinction, 1 for showing some understanding of the difference.*

# 6 Keylogging (9 minutes, 5 points)

A keylogging device captures whatever is typed, which could include passwords, and make this available to an attacker.

A. Is this a physical security threat or personnel security threat?

**Physical security**

B. Describe a user training approach that could help mitigate keylogging device attacks.

**Train users to look for unusual devices.**

C. Describe a way to mitigate attacks by keylogging device that does not involve user retraining.

**Physically securing devices so a keylogger cannot be installed.**

*Scoring: 1 for "Physical"; 1 for a method that helps against keylogging and 1 if it is purely user training; 1 for a method that helps against keylogging and 1 if it does not change the way a user operates. (E.g. 2-factor authentication would be 1 point, since the user has to be trained to use it.)*

# 7 One-time Pad (6 minutes, 3 points)

One-time pads provide information-theoretically secure ("perfect") secrecy. But we almost never use it. Briefly explain why one-time pad is infeasible in practice.

**Distributing the keys can become very impractical when large amounts of data need to be securely transferred. No key can ever be reused, and the key must be the same length as the message. These two factors make it infeasible in practice to distribute enough keys of appropriate sizes.** Note that if we didn't have both problems, one-time pad could be feasible. If the key was shorter than the message, we could send the next key as part of the previous message.

*Scoring: 1 for showing understanding of 1-time pad, 1 long key, 1 for no reuse, 1 for describing why reuse bad (max 3).*

# 8 Replay Attacks (8 minutes, 5 points)

Replay attacks provide a means of bypassing authentication mechanisms, even if the authentication credentials are encrypted.

A. Describe briefly how a replay attack occurs.

**Adversary listens on channel and records authentication packets. Adversary then authenticates using same packets, even if adversary cannot understand them.**

B. Name or briefly describe two measures to prevent replay attacks.

**Challenge/response and sequence numbers.**

C. For **one** of the measures you list in part 2, briefly describe *why* it prevents a replay attack.

**Challenge/response works by Alice choosing a random $r$ and sending it (encrypted) to Bob. Bob computes $f(r)$ and sends back to Alice. Attacker trying to authenticate as Bob will receive $r'$ from Alice, responding by replaying $f(r)$ gives incorrect value.**

*Scoring: 1 for description showing understanding of attack, 1 each for naming types, 1 for description of prevention mechanism, 1 for proof sketch/discussion of why prevention breaks replay attack. Note that you may get partial points, e.g., if you describe something other than a replay attack, you could get some points in parts B and C for proper answers to the attack you do describe.*

## 9 Hashing to Encrypt (3 minutes, 2 points)

Suppose we let $C = H(M)$, where $M$ is the message, and $C$ is the ciphertext, and $H$ is a one-way hash function. Is $C$ a good encryption of $M$? Briefly explain why or why not.

**No, cryptographic hash functions should be one-way functions. An encryption scheme needs to be reversible (given the key), otherwise the receiving party could never decrypt it!**

*Scoring: 1 for showing some understanding of hash function, 1 for "unable to decrypt" or "deterministic encryption reveals if same message sent twice".*

## 10 Stream and Block Ciphers (10 minutes, 3 points)

- Briefly explain the difference between a stream cipher and a block cipher.

  **Stream ciphers encrypt part of the data before sending; block ciphers encrypt the entire data at once.**

- Give a reason to use a block cipher rather than a stream cipher.

  **Generally block ciphers have better security, because of better diffusion.**

- Give a reason to use a stream cipher rather than a block cipher.

  **Performance: We don't have to wait to have all the data before starting to encrypt.**

*Scoring: 1 for showing understanding of difference, 1 each for an appropriate reason to use one over the other.*

## 11 Public Key Infrastructure (6 minute, 2 points)

Does Public Key Infrastructure (PKI) use symmetric or asymmetric encryption? Briefly explain your answer.

**Asymmetric encryption. Information is encrypted under a person's public key, and decrypted under a private key that only the recipient has access to. These two keys must differ so that only the receiving individual can decrypt, but anyone can encrypt a message to them with their public key.**

*Scoring: asymmetric (1 point), must be two keys (1 point)*