Examination Paper

Spring Session 2012

Part A

1) Three types of malware are _____ , _____ and _____.

Part A

1) Three types of malware are viruses , Trojan horses and Worms. These malwares are categorized based on the way the malwares are activated and propagated. Virus propagates by manual transferring of infected files; worm propagates using only network connection; and Trojan horses disguised as legitimate software to gain access to the computers, once activated, Trojan horse can enable cyber-criminals to spy on the victim, steal sensitive data, and gain backdoor access to the system.

Part A

2) Lamport's one-time password scheme relies on using hash functions that are one-way and collision resistant. One-way means the hash function takes in any input and produces a hash digest, and there is no way one can from the hash digest obtain the input. Collision resistant means there is no possibility (very small possibility) that a hash function can produce the same hash digest from two different input.

Part A

3) Each row of the authorization table of Sandhu & Samarti contains access triplet (Subject, Object, Action). It is also known as the capabilities which is from the point of view of the subject's action on the various objects.

Part A

4) A least upper bound for a lattice implies Domination, in other words, there exists at least one level that dominates the rest.

Part A

5) Data perturbation can be used in statistical database to change the values in the database such that the statistical information is accurate, but the inferential data is inaccurate to provide protection against inference attack.

Part A

6) Spear phishing differs from general phishing in that Spear phishing is targeting a specific person while general phishing is targeting all the people and expecting some to be fooled.

Part A

7) Firewalls are assumed to be trusted and invulnerable. There are two other main assumptions, access to the firewall should be through firewall and only authorized traffic should be allowed through the firewall.

Part A

8) Syncookies provide protection against connection based denial of service by not dropping connection when the SYN queue fills up until the server receives a “correct” ACK from the client. At this time, the server can reconstruct the SYN queue entry and then connection proceeds as usual.

Part A

9) The two primary bases for intrusion detection agents are Host based and Network base.

SIM-2016-S3-CSCI262-S8a, Slide 32 or textbook
Computer Security: Principle and Practice, 3ed ed, William Stallings, Lawrie Brown, 2015, Pearson Education Limited, page 293.

Part A

10) The purpose of sanitization in the context of auditing is to remove any information for which there is a user who is not allowed to see that information.

Part A

11) In multilevel access control every subject and object is given clearances and classification or sensitivity and access is determined by a set of rules, for example, Bell-La Padula rules.

Part A

12) Treating programs as data until verified provides protection against malware because if a program is treated as data, it would not be executed and the virus will not take effect.

Part A

13) Persistent and non-persistent XSS differ in that

in persistent XSS, data provided by Web client stays (is stored) on the server, while in non-persistent XSS, the data provided by a web client is used immediately, usually without proper sanitisation by server-site scripts to generate result for the user.

Part A

14) One major role of a honeypot is to divert attackers from a critical system, and/or collect information about the attacker's activities.

Part A

15) A master password is typically used to protect sensitive information such as other passwords and certificates.

Part A

16) Units are relevant in digital forensics and logging because if the 'unit' is missing, it is not possible to assess the extend of the impact of the attack. For example, if the log registered "there were 100 blocks were downloaded at 9:30." This information is not very useful. 100 bytes blocks or 100 Kbytes blocks or something else. Also, at 9:30 am or pm?

Part B – Question 1 …1

1) Briefly explain the three basic components in an access control triplet. Describe how these triplets relate to an ACM. Give an example of an ACM, and the two related representations based on it, to illustrate your answer.

The three basic components of access control triplets are (S, O, A) where

- S: a set of subjects
- O: a set of objects
- A: an access control matrix, A[S, O] with entries a(s,o)

Part B – Question 1 …2

- A triplet describes the state and state transitions of an access control matrix (ACM).
- The following is one example of an access control matrix

Part B – Question 1 …3

Subject: Alice Bob Chris Dan

Object: Fence Wall Barrel Bob

Actions: Jump Climb Paint Roll push

Control Access Matrix:

Object / Subject	Fence	Wall	Barrel	Bob
Alice	Jump	Climb		
Bob	Paint	Paint	Roll	
Chris		Climb	Climb	
Dan			Paint	Push

Access Control List:

Fence: (Alice, jump), (Bob, paint)
Wall: (Alice, climb), (Bob, paint), (Chris, climb)
Barrel: (Bob, roll), (Chris, climb), (Dan, paint)
Bob: (Dan, push)

Capability List:

Alice: (Fence, jump), (Wall, climb)
Bob: (Fence, paint), (Wall, paint), (Barrel, roll)
Chris: (Wall, climb), (Barrel, Climb)
Dan: (Barrel, paint), (Bob, push)

Part B – Question 2 …1

2) Describe three distinct types of attacks against password systems. Briefly discuss appropriate countermeasures against one of those types of attacks.

Part B – Question 2 …2

- The three distinct attacks are dictionary attack, brute-force attack and hybrid attack. A dictionary attack uses a “dictionary” of all known words and try to find the password. Brute-force attack is trying all the possible combination of the password until it is correct. Hybrid attack is combination of brute-force and dictionary attack where we use dictionary as the basis but take variants on each of the words tested. We can protect against dictionary attack if we use words that are not commonly found in the dictionary or random words. Alternatively, use salt and regularly change the password.

Part b – Question 3 …1

3) Consider a BLP lattice system with multilevel classifications $C = \{X, Y\}$ and multilateral categories $K = \{A, B\}$. Sketch a diagram to illustrate the relationship between the security levels in this system. Explain, with reference to your diagram, the concept of partial ordering. State the BLP rule and give an example, based on your diagram, to explain each aspect of it.

Please refer to the sample solution included in the Tutorial slides.

Part B – Question 4 …1

4) Describe the relevance of the Principle of Least Privilege in the context of Buffer Overflows. You will need to briefly explain the Principle and the possible relevant effects of Buffer Overflows, but not the details of Buffer Overflows themselves.

Part B – Question 4 …2

- Principle of least privilege in the context of buffer overflow is that we limit the access an attacker can have hence even if he identify a way to launch a buffer overflow attack. Effect of buffer overflow would be that the attacker may install a malicious code and then input the address of the code to the return address of the program, hence when the actual program returns, it actually runs the malicious code.

Part B – Question 5 …1

5) Briefly explain the difference between logging and auditing. Describe two specific considerations when determining what should be logged and audited, and explain how they may influence your decisions.

Part B – Question 5 …2

- Logging is recording of events or statistics to provide information of the system use, misuse and performance. Auditing is the analysis of the log events provided by logging and to provide the information of the system in a more readable and understandable manner. The two considerations are, we need to consider how the attempts that violate the security policies can be made and we need to consider how to detect those attempts. This may influence my decision as there is no point of detecting a problem if we do not know the indicating effect.

Part B – Question 6 …1

6) Garfinkel stated … “Something you had once, something you’ve…, or something ….”. Complete the quote and explain the significance of it, in particular of this version.

Something you had once, something you have **forgotten**, or something **you once were**.

“Something you have, something you know, or something you are”

Part B – Question 7 … 1

7) Describe two general “good practices in coding”. For each of these explain why they are appropriate and give an example of what could go wrong if that practice is not followed.

The two general “good practices in coding” are:

- Never store secret in code
- Set default to deny instead of default to allow.

Part C – Question 1 …1

1) One of the client puzzles we considered contained the statement $h(C, Ns, Nc, Y) = 000 \ldots 000X$.
   a. Describe each of the components in the expression above.
   b. How much work is required to "solve" the puzzle, in the context of this statement?
   c. What is the purpose of such a puzzle?
   d. Describe how we could modify this to generate sub-puzzles.
   e. What advantage do we obtain by using many sub-puzzles rather than just one single large puzzle?

Part C – Question 1 …2

$$h(C, Ns, Nc, Y) = 000 \ldots 000X.$$

a) Describe each of the components in the expression above.

- h: a cryptographic hash function (e.g., MD5 or SHA)
- C: the client identity
- N_s: the server's nonce
- N_c: the client's nonce
- Y: the solution of the puzzle
- $000 \ldots 000$: the k first bits of the hash value; must be zero. The reasonable values of k lie between 0 and 64.
- X: the rest of the hash value; may be anything

Part C – Question 1 ...3

b) How much work is required to “solve” the puzzle, in the context of this statement?

The cost of solving the puzzle depends exponentially on the required number of k of zero bits in the beginning of the hash. If $k = 0$, no work is required. If $k = 64$, then in the worst case, it would be 2^k. In such a puzzle, the reasonable values of k lie between 0 and 64.

Part C – Question 1 …4

c) What is the purpose of such a puzzle?

The purpose of such a puzzle is to ensure that the client should always commit its resources to the authentication protocol first and the server should be able to verify the client commitment before allocating its own resources.

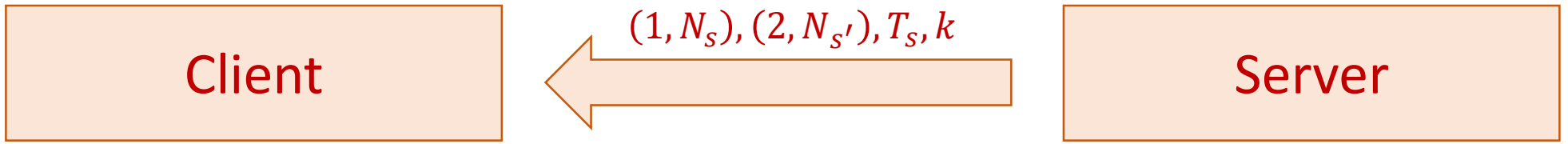
Part C – Question 1 …5

d) Describe how we could modify this to generate sub-puzzles.

The modification can be done as follow:

The Server:

- Server determines k.
- Server generates two nonce - $N_s \; and \; N_{s'}$, and a timestamp T_s.
- Server sends the two puzzles with sequence number - $(1, N_s) \; and \; (2, N_{s'})$, the timestamp T_s and the puzzle difficulty level k to client.



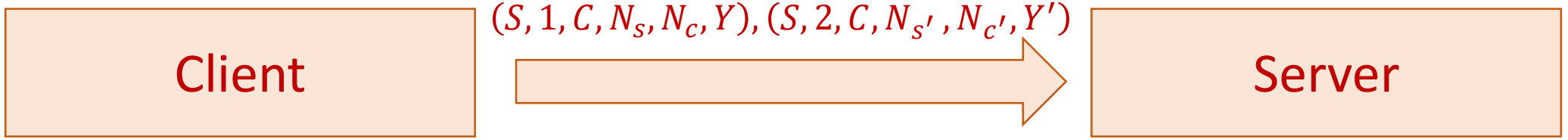
Part C – Question 1 …6

The Client:

- Client receive the puzzles and commits its resources into solving the puzzle.
- Client verifies the timestamp T_s.
- Client generates two nonce $N_c \; and \; N_{c'}$
- Client finds Y such that $h(1, C, N_s, N_c, Y) = 000 \ldots 000X$, where $000 \ldots 000$ denotes $k \; 0's$, and X can be any value.
- Client finds the second solution Y' such that $h(2, C, N_{s'}, N_{c'}, Y') = 000 \ldots 000X$, where $000 \ldots 000$ denotes $k \; 0's$, and X can be any value.

Part C – Question 1 …7

- Client sends the solutions (solved puzzles) $(S, 1, C, N_s, N_c, Y)\ and\ (S, 2, C, N_{s'}, N_{c'}, Y')$ to server.



Part C – Question 1 …8

The Server:

- verifies that $N_s \; and \; N_{s'}$ are recent.
- checks that $C, N_s, N_{s'}, N_c, and \; N_{c'}$ have not been used before.
- checks if there are $k \; 0's$ in each solution, that is, the server checks if $h(1, C, N_s, N_c, Y) = 000 \ldots 000X$ and $h(2, C, N_{s'}, N_{c'}, Y') = 000 \ldots 000X$ are correct.
- If they do, the server commits the resources, stores $(C, N_s, N_{s'}, N_c, N_{c'})$ and sends $(S, C, N_c, N_{c'})$ to the client.
- The operation can now continue.

Part C – Question 1 …9

e) What advantage do we obtain by using many sub-puzzles rather than just one single large puzzle?

If we use a single big puzzle instead of sub puzzles, then the difficulty level is hard to adjust. This is because one bit of change in *k* could require a much longer time to solve the puzzle. Using sub puzzles we can fine tune the difficulty level.

Part C – Question 2 ..1

2) These questions relate to intrusion detection systems:
   a. Explain the difference between masqueraders and misfeasors.
   b. Explain the difference between anomaly detection and misuse based detection. Give an example to help illustrate each.
   c. Explain what Unified Threat Management Systems are. Given an advantage and a disadvantage of using one.

Part C – Question 2 ..2

a. Masqueraders are those illegitimate users who are trying to imitate legitimate users while misfeasor are those authorized user who misuse their power.

What is clandestine in the context of IDS?
Clandestine refers to someone who try to avoid the intrusion detection or auditing system.

Part C – Question 2 ..3

b. Anomaly detection refers to detection where observed behaviour differs from a typical behaviour of a user while misuse based detection refers to detection where observed behaviour indicates an attempt to inappropriately use resources.

An example of anomaly detection: A particular user, let's say user A logs in only on week days, but suddenly user A logs in on Sunday mid-night for three different occasions.

An example of misuse based detection: A user trying to access resources that he or she is not authorized to.

Part C – Question 2 ..4

c. Unified Threat Management System is a system where different threat management services like anti-virus, firewall, intrusion prevention, intrusion detection etc. features unified together.

Advantage of UTM:

- UTM provides unified and consistent protection.
- Simplifies the management and maintenance, since it's effectively a single device/software element from a single provider.

Disadvantage of UTM:

- It may be a bottleneck in terms of processing and bandwidth
- There is a single point of failure.

Part C – Question 3 …1

3) These questions relate to malware and problematic code:
   a. Describe how virus and worm propagation differs.
   b. Describe the difference between direct action and memory residence.

Part C – Question 3 …2

a. Virus propagates on the manual transfer of virus infected files while worm propagates using network connection.
b. Viruses install themselves into the memory of the host computer when the original virus program is executed. Even when the original virus program is closed, new object can still be infected without having to run anything else. These are called memory residence. Direct action viruses are only active when an infected object is active.

Part C – Question 3 …2

c. Consider the following piece of code and answer the subsequent questions. Assume x is a private key w-bits long. The $function\ modexp(s[k], y, n)$ involves determining the result of raising $s[k]$ to the power of y, and taking $mod\ n$ of the result.

```
s[0] = 1;
for ( k=0; k<w; k++) {
     if ( x[k] == 1)
          R[k] = modexp(s[k], y, n);
     else
          R[k] =  s[k];
     s[k+1] = R[k]*R[k] mod n
}
return R[w-1];
```

i. What attack is the code vulnerable to?
ii. Explain how you would carry out such an attack.
iii. Explain how you could protect against such an attack.

Part C – Question 3 …2

i. Buffer Overflow attack
ii. By using value of n that is greater than w, the attacker can overflow the buffer.
iii. Apply defensive programming to ensure n is <= w.

Part C – Question 4 …1

4) Explain briefly what potential problem and domain each of the statements or code fragments is associated with, and what a likely effect would be. The syntax may not be precise.
   a. For k while for k
   b. strcpy (variable, “Polymorphic”);
   c. int N; cin << N; new char[N];
   d. system(user_input);

Part C – Question 5 …1

5) The following questions cover a range of topics:
   a. One major component of access control representations is the grouping together of entities. Explain why this is done and give examples illustrating two significant but distinct types of grouping that are possible.
   b. Explain what salting is, where we use it, and why we use it.
   c. Would Biba or BLP be more appropriate for protecting a file system against unauthorized modification of data? Justify your answer.

Part C – Question 5 …2

a. One major component of access control representations is the grouping together of entities. Explain why this is done and give examples illustrating two significant but distinct types of grouping that are possible.

Grouping is where the user are place into a group. Permission granted to a group will allow the users of that group to enact that right.

Two distinct grouping may be “Employee” and “Non-Employee”.

Part C – Question 5 …3

b. Explain what salting is, where we use it, and why we use it.

The “Salt” is a value randomly generated. It is used in hashing where instead of only the password is hashed, the password is combined with the salt and then hashed. The salt it stored somewhere too. This is used so that the adversary have many combination to try the password with many salts and delays the adversary from finding the correct password hash.

Part C – Question 5 …4

c. Would Biba or BLP be more appropriate for protecting a file system against unauthorized modification of data? Justify your answer.

Biba is more appropriate as it is an integrity based access control model. The policy of Biba is “No write up, No Read Down”. Hence a subject of a low level cannot modify “write” to an object of higher level.

Part C – Question 6 …1

6) The following questions cover a range of topics:
   a. CWE/SANS classify the top problems into three categories: Insecure interaction between components, risky resource management and porous defences. Name and briefly describe an example from each of these categories.
   b. Explain what buffers, buffer overflows and shell coding are. Use an example to illustrate how they are related.
   c. What is the aim of inference, in the context of statistical databases?

Part C – Question 6 …2

a. Examples:
   - Insecure Interaction with components
     - Injection, XSS etc.
   - Risky Resource Management
     - Buffer overflow, limited pathname restriction, uncontrolled format string
   - Porous Defences
     - Missing or incorrect authentication or authorization, no encryption

Part C – Question 6 …3

b. Explain what buffers, buffer overflows and shell coding are. Use an example to illustrate how they are related.

In computing, a buffer is a memory location where data is stored. Buffer overflow is an effect where data is not limited by bounds of its allocated memory and overflows to other memory location. Shell coding is insertion of own code into the buffer.

How buffer, buffer overflow and shell code are related is best described using the following example. A buffer stores data but if an inefficient function such as strcpy() is used, the function does not check for bound and it may overflow into other memory location. If the return address of the program is found, an adversary may insert his/her malicious code in place of the return address and when the program hits to the return address, the malicious code is executed.

Part C – Question 6 ...4

c. What is the aim of inference, in the context of statistical databases?

The aim of inference is to derive sensitive data from non-sensitive data such as aggregated data. By doing a sequence of aggregated queries it is possible to find the value of the sensitive data.

Part C – Question 7 …1

7) The following questions cover a range of topics:
   a. How do two-channel and two-factor authentication differ?
   b. Describe a typical phishing process.
   c. Explain one example to illustrate the role of sandbox environments in the security of mobile code or in the detection of malware.
   d. Briefly describe how the three primary components of a virus are related.

Part C – Question 7 …2

a. How do two-channel and two-factor authentication differ?

In two factor authentication, the authentication system uses password/pin and a device (token system) which is able to produce one time password. In two-channel authentication, two different channels are used; one channel is from the client to the server and the second channel is from server to client using a different channel e.g. telephone etc. to give targeted authentication

Part C – Question 7 …3

b. Describe a typical phishing process.

A typical phishing process involves deception where the user is fooled into believing that there are issue with his account and enter his account details to fix the issue but is actually stored and collected by the phisher to cause harm.

Part C – Question 7 …4

c. Explain one example to illustrate the role of sandbox environments in the security of mobile code or in the detection of malware.

Sandbox plays an import role as if a software is suspected to be a malware and it is a malware, the vector of damage caused by the infection is limited to that vector and it cannot affect the main environment keeping the main environment safe.

Part C – Question 7 …5

d. Briefly describe how the three primary components of a virus are related.

The three components of a virus are infection vector, payload and trigger. The infection vector is the structure of the virus allowing it to duplicate, payload is what the virus does beside spreading and trigger is the condition which the virus has to meet to activate the payload.