THE UNIVERSITY OF AUCKLAND

SECOND SEMESTER, 2014
Campus: City

COMPUTER SCIENCE

Software Security

(Time Allowed: 20 minutes)

Sample answers and marking notes

NOTE:

- This is an *ungraded* sample exam. Please do not put your name on your answer sheet.
- As a rough guide: if you budget your time so that you are spending about 1 minute per mark, and if you produce about 5 well-chosen words per minute, you would receive full marks on this examination.
- I'd advise you to read through *all* questions on any examination or test, before starting to write.
- I believe you will be allowed a short time to read an examination at our University, before you are allowed to start writing.

1. The following questions refer to the following quotation from Landwehr et al., "A taxonomy of program security flaws". All occurrences of the word "validation" have been italicised.

   … *Validation* flaws may be likened to a lazy gatekeeper: one who fails to check all the credentials of a traveler seeking to pass through a gate. They occur when a program fails to check that the parameters supplied or returned to it conform to its assumptions about them, or when these checks are misplaced, so they are ineffectual. These assumptions may include the number of parameters provided, the type of each, the location or maximum length of a buffer, or the access permissions on a file. We lump together cases of incomplete *validation* (where some but not all parameters are checked) and inconsistent *validation* (where different interface routines to a common data structure fail to apply the same set of checks)…

   … An identification/authentication flaw is one that permits a protected operation to be invoked without sufficiently checking the identity and authority of the invoking agent. These flaws could perhaps be counted as *validation* flaws, since presumably some routine is failing to validate authorizations properly. However, a sufficiently large number of cases have occurred in which checking the identity and authority of the

user initiating an operation has in fact been neglected to keep this as a separate category…

					Count	Case ID's
Genesis	Intentional	Malicious	Trojan Horse	Non-Replicating	2	PC1 PC3
				Replicating (virus)	7	U1,PC2,PC4, MA1,MA2,CA1, AT1
			Trapdoor		(2)	(U1)(U10)
			Logic/Time Bomb		1	I8
		Non-Malicious	Covert Channel	Storage	1	DT1
				Timing	2	I9,D2
			Other		5	I7,B1,U3, U6,U10
	Inadvertent	Validation Error (Incomplete / Inconsistent)			10	I4,I5,MT1,MU2, MU4,MU8,U7, U11,U12,U13
		Domain Error (Including Object Re-use, Residuals, and Exposed Representation Errors)			7	I3,I6,MT2, MT3,MU3, UN1,D1
		Serialization/aliasing (Including TOCTTOU Errors)			2	I1,I2
		Identification/Authentication Inadequate			5	MU1,U2, U4,U5,U14
		Boundary Condition Violation (Including Resource Exhaustion and Violable Constraint Errors)			4	MT4,MU5, MU6,U9
		Other Exploitable Logic Error			4	MU7,MU9, U8,IN1

Figure 1. Security flaw taxonomy: Flaws by Genesis. Parenthesized entries indicate secondary assignments.

a. **[5 marks]** Briefly describe a program security flaw that is a validation error in Landwehr's taxonomy. To receive full marks you must discuss a validation flaw that was described in a required reading for this course, or was mentioned in a lecture or student presentation in this course.

1. A validation error in Landwehr's taxonomy is that it does not consider the case of credentials provide by the user in the LogIn process, i.e. it consider uppercase and lowercase same (ABC | abc -> abc) but in practical life they are different.

   The major security breakdown happen when system grant access of a account without checking proper credentials, specialy in case of password.

   Some times system give you access of the file by just considering your identify without checking your authentication, which is a major security fault.

   0 marks. This student has discussed an Identification / Authorization Inadequate flaw.

2. A program security flaw that is validation error means a program fails to check the parameters supplied or returned to it conform to the assumptions about them.

1 mark. This student has correctly copied a phrase, from the quoted passage, which describes one type of Validation flaw. (The other type of validation flaw mentioned in this passage was a misplaced check of a parameter which was ineffective.) This student's answer didn't describe any example of a validation flaw.

3. Bank error giving obscene amounts of money when misplacing a comma. A simple bank teller should not be able to authorize upwards of $10M. The program should have validated the numbers given by the bank teller are same. The banking program did not validate all of the restrictions of the user.

   5 marks. This student has recalled some details of the discussion of "a bank teller doing a Roturua" in lecture, and has correctly classified this as a validation flaw.

4. Validation error in Landwehr's taxonomy means a system might have the case of incomplete validation or inconsistent validation. An example of security flaw that is a validation error would be say in a RBAC system, during the authentication phase, it only requires the user to enter username and password. If the offender managed to get on hold to the user's iafr (?), that means the attacker can login as the user, this is a validation error because the system should have ask more than just username and password, it should ask things like birthdate, secret pin code, or secret question and answer.
   - Username, password
   - No checking (?) ip, mac address, login location
   - System update, might alter the process of validation

   0 marks. This answer starts with a lengthy description of an Identification / Authorization Inadequate flaw. The last two bullet points suggest that the student may have also been thinking about a couple of other flaws. If this student had crossed out all but the third bullet point in their answer, they would have received 2 mark because it sounds like a (very incomplete) description of the second type of validation flaw identified in the quoted passage from Landwehr et al. (1994).

b. **[5 marks]** Briefly describe a program security flaw that would be classified as "Identification / Authentication Inadequate" in Landwehr's taxonomy. To receive full marks you must discuss a flaw that was described in a required reading for this course, or was mentioned in a lecture or student presentation in this course.

1. Identification/Authentication Inadequate is one that permits a protected operation to be invoked without sufficiently checking the identity and authority of the invoking agent.
   0 marks. This answer directly quotes a sentence from the question.

2. A program security flaw that would be classed as Identification/Authentication Inadequate in Landwehr's taxonomy is that it assumes that the validated user have access right to access the sensitive information. An example demonstrate this flaw is that the system grant access to CEO of the company to access all the sensitive information of finance and HR dept. Being higher in level will not give you access of all the dept.

2 marks. This student has worked creatively with the definition but did not demonstrate any knowledge of what was taught in this course.

3. Capturing a message from A->B, then either repeating or modifying the message and sending it to B again as a new message, i.e. M->B. B does not ID/Auth the sender of the message appropriately.

   5 marks. This student has accurately classified a flaw that was discussed in this course..

c. **[5 marks]** As indicated in Figure 1 (above) and as discussed in the quoted text, Landwehr et al. decided to introduce a "Identification / Authentication Inadequate" category – even though such flaws could "perhaps be counted as validation flaws." Identify *one* advantage or *one* disadvantage of this decision, and discuss this advantage or disadvantage briefly. To receive full marks, your discussion must refer to the declared goal of Landwehr et al.: "… we are fundamentally concerned with the problems of building and operating systems that can enforce security policies".

1. To secure a building, we lock the doors. But locking the door would not stop the intruder/theif to break into the house. There can many other issues that can be considered in case of security like moral, economic, legal, and difficulty. The moral value of society which says that robbery is bad can stop a person from breaking into a house. The legal jurisdiction which has strong laws and punishment for robbery can also prevent the theif from doing so. The difficult levels to break int house also stops the theif.

   1 marks. This is an accurate analysis of an example of real-world security from the Lampson reading, in the context of the "soft security" framework taught in this course. Possibly the student misunderstood my question, so I'd award a mark even though their answer is not responding to the question being asked.

2. The major disadvantage of such decision is that in a system if the user have required credentials they can access complete resources and information files of a different user. That's a very big problem as it is a major loophole in privacy of the user's personal data. An example to demonstrate this is that in a hospital system environment there are three major types of user like doctor (prof), nurse and student. So if a user is a student have an access of the system, if can access all the resources of the environment, like notes and slides & reading shared by the prof by they are not allowed to check the upcoming assignment and marks of other user. This problem/flaw is not a validation flaw as it is out of scope of validation but as there is a breakage in the security.

   4 marks. This student misunderstands the question, but they are responding to a closely-related question by discussing an identification/authorisation flaw which is clearly not a validation flaw. I'd say the existence of such flaws is an important *advantage* of Landwehr's definitions of these categories (not a disadvantage); it

wasn't identified in the Landwehr article; and it shows strong understanding of the topic area despite a misunderstanding of my question so I'm awarding high marks.

3. One advantage – easier to break it down and plan, build and test for. Validation errors can be spotted much quicker as they would generally throw some error or alert, but ID/Auth can go unnoticed for a long time as it's more difficult to detect someone who has the authentication but was not authenticated. Since ID/Auth is much harder to detect, it must not be treated the same as Validation error. For the interests of planning, building and testing a secure operating system (OS), ID/Auth should be treated separately as it would be detected/found in a different manner from Validation. Treating them the same may result in non-detection, for a long period of time.

   5 marks. This is an excellent analysis, going deeper than I would expect for a 5-mark question.