THE UNIVERSITY OF AUCKLAND

SEMESTER TWO, 2017
Campus: City

COMPUTER SCIENCE

COMPSCI 725 Practice Exam

(Time allowed: TWO hours)

NOTE: Do not write your name on your answer sheet.

The required readings for this course are listed on the back side of this question sheet.

1. (10 marks) Recall Lampson's 'restrict' strategy: "let the bad guys in, but keep them from doing damage."

Could this strategy be used to defend the password MiTM threat identified by Gelernter (2017)? Explain briefly. To receive full marks, you must identify the "bad guys", the secured area that the "bad guys" are allowed to enter, the "damage" which could be prevented, and a way in which this preventable damage could be prevented.

- Marking rubric: 4 marks for relevant information from Gelertner 2017. 2 marks for identifying some bad guys and a restricted area. 4 marks for discussing how a 'restrict' defense could prevent some particular form of damage from a PRMitM attack.

- Sample answer #1, with emphasis added to key phrases. *In the PRMitM attack, there is an attacker that tricks the victim to provide their email and response to a series of security questions using a malicious website and then the attacker initiates a pasword reset process at the email service provider of the victim.* The password reset process will require the attacker to answer a few challenges such as answers to security questions. To bypass these challenge, the attacker can simply forward the challenges to the victim via a malicious website and again forward their response back to the password reset process. This way *the bad guy is the attacker who forwards the challenges to the victim* and then back to the email service provider. In my opinion the 'restrict' strategy cannot be used to defend against the PRMitM because all users are allowed to reset their passwords and login, there is no way to differentiate between the attacker and a legitimate user trying to reset their password. Therefore, by restricting legitimate users, it can lead to usability issues or can affect other features that are offered by the service provider. Instead, the 'exclude' strategy should be used, where the service providers should do everything in their power to keep the bad guys out. The *consequence of the attack include the attacker being able to take over the victim's account for a particular service.* Taking over a social media account can lead to large implications.

  Assessment: 10 marks. Shows strong knowledge of Gelertner (2017), with a well-reasoned explanation for the inapplicability of the 'restrict' defense for an attack which leads to a loss of control of an account. Not mentioned in Gelertner (2017) is the possibility of granting a user (or their attacker!) only a restricted-authority access to a service if the password has been changed recently. As noted by the student in their answer, any such restriction could be considered a usability fault; however a loss of usability may be acceptable (for at least some stakeholders) if it significantly improves security. See e.g. `http://steamcommunity.com/discussions/forum/1/558749191451989915/`: "Steam and their RIDICULOUS restrictions rules!!!", Crash Test, 4 March 2014: "... If you reset your password, you will be restricted from trading and the Community Market for 5 days..." I'm awarding full marks to this student because they were well on the way to discovering this defense, and because I don't expect any student to complete a deep or creative analysis before answering a 10-mark question.

- Sample answer #2. Attack description: Attacker wants the victim to register for a service (e.g. with email address) and asks for the answer to a secret question (e.g. first pet, name of mother, ...). This combination of information is then used to reset the password for another service the victim is using. The restrict strategy applied on this attack would mean the attacker (bad guy's) are still able to replay the information to the second service but restrict the damage i.e. victim looses control of his account. One way to prevent the damage would be a second factor authentication in which the victim receives a link to a password reset website on another communication channel (e.g. SMS, email, phone call, app) and authenticates not only by knowing a secret, but also by possessing a SIM-card/specific phone/...

  Assessment: 9 marks. This is an accurate and adequate description of the basic PRMitM threat described in Gelertner (2017). The student outlines what is (arguably) a 'restrict' defense, because it is allowing the attacker to enter a secured area (a state in the password-reset protocol in which a second authenticator must be provided before the password will actually be reset). I awarded only 9/10 marks, because I'm not sure the student realises that Gelertner (2017) focussed its attention on four subcases of the basic attack. Each of the subcases incorporate the defense outlined by the student in a particular way: through a CAPTCHA, a security question, a code to a mobile phone, or a reset link to an email address.

- Sample answer #3. 1) Restrict strategy is to allow *bugs* in, but make them from doing any damage. *Restrict strategy is sandboxing. Sandboxing requires access control on the resource.* 2) The PRMitM attack is an attack mode where an vicim tries to download a resource form a website. The website asks the victim to register using Google or Facebook account to become a member. During the registration process, the website becomes a man-in-the-middle and performs the password reset process in order to take over the victim's account. 3a) In the PRMiTM attack, the *"bad guys is the malicious website"* since the purpose is trying to take over the user account. 3b) By applying the restrict strategy, the "bad guy" is only able to communicate with the user, which means the information the user provided for registering an account. Any attempt to use this information for other purpose cannot be allowed. 3c) Since the information provided by the victim is restrict, the malicious website cannot utilize such information.

  Assessment: 6 marks. Gelertner: 4/4, very nicely described (although the target of the attack isn't limited to Google and Facebook accounts). Damage & prevention by restriction: 1/4, because the student describes a desired outcome of a restriction rather than a plausible way in which it could be implemented (except perhaps through an exclusion, after identifying the bad guys). Bad guys and secured area: 1/2, although the student has identified an agent of the bad guys (a bug or a website), rather than some person or some group of people which could be punished.

- Sample answer #4. Yes, the restrict strategy can be used to defend the password Man In the Middle threat. *In order to restrict the threat, we must identify the bad guys.*

There are various ways to exploit this threat. Following are the scenarios. 1) When you try to reset the password using the secured channel that the website provides, the website usually requests for a personal identifier such as email or the username. Once the username is provided, the website sends the reset password link to the registered user. In this scenario, the *mail account can be hacked* by *the hackers who are the bad guys.* 2) When you reset the password using one time password, the message carriers can be exploited to steal the one time password. There can also be arbiterate [arbitrary?] attacks on the users who never invoked the password reset. This can be interpreted by different users of different backgrounds. For e.g. an advanced user will not fall for the bait but novice users might turn up their confidential details that can be exploited.

Assessment: 6 marks. Gelertner: 4/4 marks. Damage & its prevention by restriction: 1/4 marks. Bad guys & the secured area: 1/2 marks. This student has accurately identified two of the cases considered in Gelertner (2017), although their discussion of the second case is almost incomprehensible. My best guess of their intended meaning is that they're describing two subcases of their second case: an eavesdropping exploit on "the message carriers", and the identity-confusion exploit discussed in Gelertner (2017). This student shows a poor understanding of the 'restrict' defense, by asserting that it is necessary to "identify the bad guys" in order to restrict the threat. This student indicates that an advanced user could prevent the attack, but any such prevention would be an 'exclude' defense (in which the user is serving as a guard in an access-control system that prevents an attacker's request for a password-reset from being actioned).

- Sample answer #5. PRMitM defences focus on getting the user attention about the reset password process by including the full details of the received message, purpose, a warning not to use the code to other websites. They also recommend to send a link instead of a code so the user would notice if the attacker website asks to copy the link into its page. Bad guys: The users that will be fooled by the attackers. Secured area: The message that includes the code/link which will be used to reset the password. Damage: damage would happen if the fooled user gave the attacker the code/link. The restrict strategy could be used after defining the above.

  Assessment: 4 marks. Gelernter 3/4, because the student included irrelevant detail about two of the authors' proposed defences (both of which used an exclusion strategy), without including the directly-relevant information of the basic threat (or one of its subcases). Damage & prevention by restriction: 0/4. Bad guys & the secured area: 1/2. I'm awarding a mark for the identification of a "secured area" even though a one-time link or code is a credential which allows a single access to a secured area; I rarely award half-marks.

- Sample answer #6. Lampson define 'restrict' as allowing the 'bad guys' in but *exclude the person from the area or the environment where he could do harm.* Now the 'bad guy' could the person who acts as the MiTM (man-in-the-middle) which try to harm by steal the password. By allowing the 'bad guys' into the system and steal the password is not a good ideas. Apply 'restrict' is good because we cannot not apply 'exclude' by stop all people out of it.

Assessment: 2 marks. The student shows no knowledge of Gelertner (2017), and incorrectly asserts that an 'exclude' defence is infeasible for a PRMitM threat. However they do a nice job of describing, in their own words, a restrictive sandbox which offers controlled access to higher-security resources. As described in Lampson: " Sandboxing typically involves access control on resources to define the holes in the sandbox."

- Sample answer #7. Yes restrict strategy would be define to protect every one who is using the system, or a system which provinding [providing? provisioning?] the services to any industry. The password polrecy [policy?] should be secure and sign [?] be every user who uses the system even the administrator of the system should have restricted access to use the system. The bad guys or intruders can access the system by many ways by trying to identified the password by common passwords like 123456 or by date of birth of the person who own the user account or by matching hint by first name last name also every one should not use the dictionary words of famous word while selecting the password. The password policy should be unique or must be strong.

  Assessment: 0 marks. This answer is mostly irrelevant to the question asked.

The following articles were on the assigned reading list this semester. They are listed in order of discussion.

Lampson (2004)	Computer security in the real world
McReynolds (2017)	Toys that listen: A study of parents, children, and internet-connected toys
Guri (2016)	SPEAKE(a)R: Turn speakers to microphones for fun and profit
Mehrnezhad (2017)	Stealing PINs via mobile sensors: Actual risk versus user perception
Gelernter (2017)	The password reset MitM attack
Wu (2017)	Automated inference on criminality using face images
Yampolskiy (2016)	Artificial intelligence safety and cybersecurity: A timeline of AI failures
Brown (2017)	Finding and preventing bugs in JavaScript bindings
Liang (2016)	An empirical validation of malicious insider characteristics
Twyman (2015)	Robustness of multiple indicators in automated screening systems for deception detection
Baki (2017)	Scaling and effectiveness of email masquerade attacks: Exploiting natural language generation
Doty (2013)	Privacy Design patterns and anti-patterns: Patterns misapplied and unintended consequences
Jia (2016)	The 'web/local boundary' is fuzzy: A security study of Chrome's process-based sandboxing
Walker (2012)	Contract cheating: a new challenge for academic honesty?