THE UNIVERSITY OF AUCKLAND

SECOND SEMESTER, 2013
Campus: City

COMPUTER SCIENCE
Software Security
(Time allowed: 20 minutes)

NOTE: Attempt **ALL** questions in the 12-page script book provided, using approximately **25** words to answer each 5-mark question, **50** words to answer each 10-mark question, and approximately **75** words to answer each 15-mark question. Total possible: **100 marks.**

This is an ungraded sample exam. Please do not put your name on your answer sheet.

A. As discussed recently in a lecture, Boaz Barak distinguishes systems with "well-defined security" from those that have "fuzzy security". A system with fuzzy security is composed of "fuzzily specified components". A system with well-defined security has "rigorously specified components", and these components are accompanied by "security proofs [which] can be validated by anyone" that are based on "assumptions [which] can be checked for validity by anyone".

1. Pick any article on the required-reading list for CompSci 725. Identify some secure system that is analysed or attacked in this article. Determine whether this analysis or attack is on a security property that is well-defined. Discuss briefly. To receive full marks, your answer must name (or very briefly describe) ***one* article**, ***one* secure system**, ***one* security analysis or attack**, and ***one* security property**, and it must explain **why** you consider this security property to be "fuzzy" or "well-defined". ***[15 marks]***

Sample answer #1:

In the article "An Evaluation of the Effectiveness of Extended Validation Against Picture-in-Picture Phishing Attacks", C. Jackson et. all [2007] from Stanford University describes an experiment conducted to evaluate the effectiveness of extended validation in Internet Explorer 7 for picture-in-picture phishing attacks. The secure system works in Internet Explorer web browser, where the address bar is green when a legitimate site is accessed and turns red when the target site matches the blacklist of phishing sites. In the experiment, the described secure system works fine in terms of distinguishing phishing sites from legitimate sites. However, the usability of the system wasn't very satisfying.

Assessment of #1: The article is very clearly identified (**+3 marks**). An approximate title or a brief summary of the content would have been sufficient for full marks, e.g. "In the required reading on the effectiveness of extended validation certificates". The secure system is not clearly named or described: its boundaries are unclear (**+ 1 mark**). I had expected most students to identify the IE7 web browser as the secure system; some students might add the user of the browser to this system. This answer tells me that the "secure system works in [the] Internet Explorer web browser", but I cannot determine which components of the browser are part of this system. Perhaps some (or all?) of the EV-certificate-handling components, and some (or all?) of the GUI components involved in displaying the address bar of the browser. The security attack is named in the title: it is a "picture-in-picture phishing attack" (**+3 marks**). The student has not named or described a security property (**+ 0 marks)**. The student has not indicated why they consider this system to have fuzzy or well-defined security (**+ 0 marks**). Summative assessment: **7/15 marks**.

Sample answer #2:

Article: An extended validation certificate user study on Picture in Picture Phishing attacks by Jackson et al 2007.

Secure system: banking web page requesting login information

Security attack: Phishing attack – picture in picture

Security property: Ownership of the website or access to the information entered

Fuzzy - no definite components owned in the banking website. The login area could be compromised or the entire webpage.

Assessment of #2: The article is very clearly identified (**+3 marks**). The secure system is described (**+ 3 marks**); the description is somewhat vague, but that is part of the fuzziness of the security model in this article as noted later in this student's answer. The student has introduced an additional limitation into the security model of the article, which considered phishing attacks on any website with a secure login; but this is a very minor inaccuracy especially since the article's experimentation was on two financial websites, PayPal and Bank of the West. The security attack is named (**+3 marks**). The student has described two security properties (authenticity of the banking website and confidentiality of the user's banking information) (**+ 3 marks)**. The student has asserted that there is fuzziness in the security model for this system because the system being analysed does not have "definite components". I agree: the authors have left it to the reader to define an appropriate set of boundaries for some system which is designed to allow its users to securely enter their login credentials. Summative assessment: **15/15 marks**.

Sample answer #3:

The article I am choosing is "Alise in Warning land". The article describes the effectiveness of pop up window warnings.

Assessment of #3: The student has identified and briefly described an article on the required reading list (**+3 marks**). The student has not identified a secure system, a security analysis or attack, a security property, or a reason why this system has fuzzy or well-defined security. Summative assessment: **3/15 marks**.

Sample answer #4:

Article – "A Data Reachability Model for Elucidating Privacy & Security Risks Related to the Use of Online Social Networks". Author – Creese, Nurse, … 2012.

In this article the authors have discussed about a Data Reachability Matrix which is used to guess private details about the user of the social network.

For eg: - based on the online friends a user has his age and gender can be guessed OR Based on the community a user joins on the social network his employer can be guessed with some accuracy.

The authors have defined terms like "data points" and "target information". The data points include the details which can be used to reach the target information.

In the example stated above the details about online friends will be the data points which can be used to reach or derive the target information which is the age and gender of the user in this case.

The authors have also used accuracy and the ease to define how easily and how accurately these details can be obtained about any user.

However the Data Reachability Matrix used is vague and incomplete since the author's have not specified details about the blue boxes which they have used in the matrix. These blue boxes consist of numbers and letters. They have just said the numbers represent inferences for which published evidence could be found & letters are just based on knowledge above the field & several rounds of brainstorming.

Boaz Barak has explained the difference between "well defined security" and "fuzzy security". But he has also said well defined components are not good enough for good security.

Assessment of #4: The student has identified and summarised an article on the required reading list (**+3 marks**). The student has not identified a secure system, a security analysis or attack, a security property, nor a reason why this system has fuzzy or well-defined security. Some of this information can be found in their summary, but the student has not demonstrated an ability to analyse this technical information as required in order to answer this question. However the student has supplied some marginally-relevant additional information from my lecture slides on Boaz's argument (**+1 mark**). Summative assessment: **4/15 marks**.

Sample answer #5:

There is a paper in the reading list talks about the security feature of hotspots of iphone and in my opinion this is a example of fuzzy security. In which, the validation function only require good enough security, i.e. in a certain time limit it is not easy to be break. Although it provides a certain level protection and has the Authentication and Authorisation mechanism, the protection function is not strong as metioned in this article.

Assessment of #5: The student has adequately identified an article on the required reading list (**+3 marks**). I had some difficulty determining what secure system the student had in mind, when writing their answer, finally deciding that it must be either "hotspots of iphone" or "iphone". Both are reasonable targets for a security analysis, but the ambiguity precludes an award of full marks (**+2 marks**). The student has not clearly identified a security analysis or attack; however their answer discusses a "validation function… [which] is not easy to … break" (**+2 marks**). The student has correctly identified two relevant security properties, Authentication and Authorisation, of a hotspot (**+3 marks**); I note that these are also security properties of an iphone, but the security analysis of this article was not focussed on its authentication and authorisation properties. The student has done a very nice job of arguing that this article defined and analysed a fuzzy form of authentication and authorisation (**+3 marks**). Summative assessment: **13/15 marks.**

B. A system with Mandatory Access Control (MAC) does not allow a user to delegate, to others, the access rights for resources owned by that user.

2. Describe the primary data structure used in a typical realisation of MAC, and explain how this data structure controls what each user can and cannot do. ***[5 marks]***

C. (Other questions). ***[80 marks]***