THE UNIVERSITY OF AUCKLAND

SECOND SEMESTER, 2012
Campus: City

COMPUTER SCIENCE
Software Security
(Time allowed: TWO hours)

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, which should take you about 25 minutes to complete.
Sample answers from students are shown in blue.
Instructor's comments are shown in green.

A. Zhou *et al.*, in "Taming Information-Stealing Smartphone Applications (on Android)" proposed an architecture for privacy protection. Their prototype included a method for protecting contacts which used the flowchart of their Figure 3 (reproduced below). Their explanation of this figure included the following sentences: "The dotted line in Figure 3 encloses those components that also exist in the original Android. The rest [of the] components (outside the dotted area) show the additional components we added for the privacy mode support in Android."

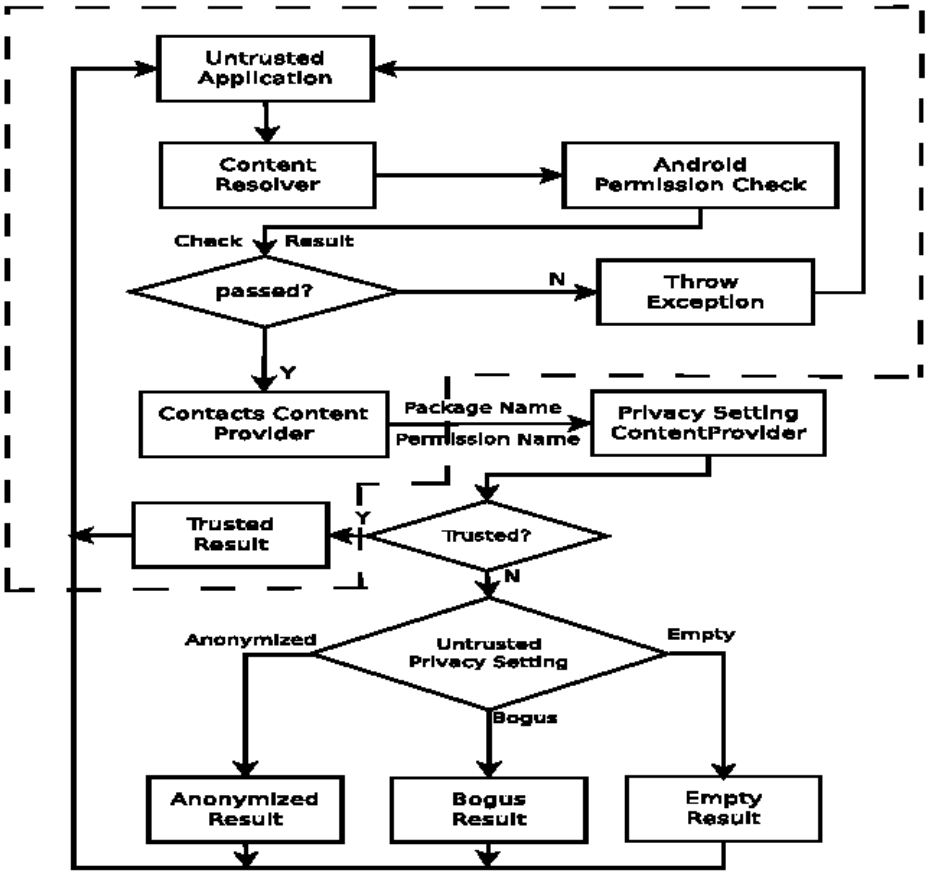

Fig. 3. Protecting Contacts in TISSA

In another required reading for this course, Bellamy-McIntyre *et al.* explained a modelling technique called "form storyboarding". Figures 1 and 2 of this article are reproduced below.

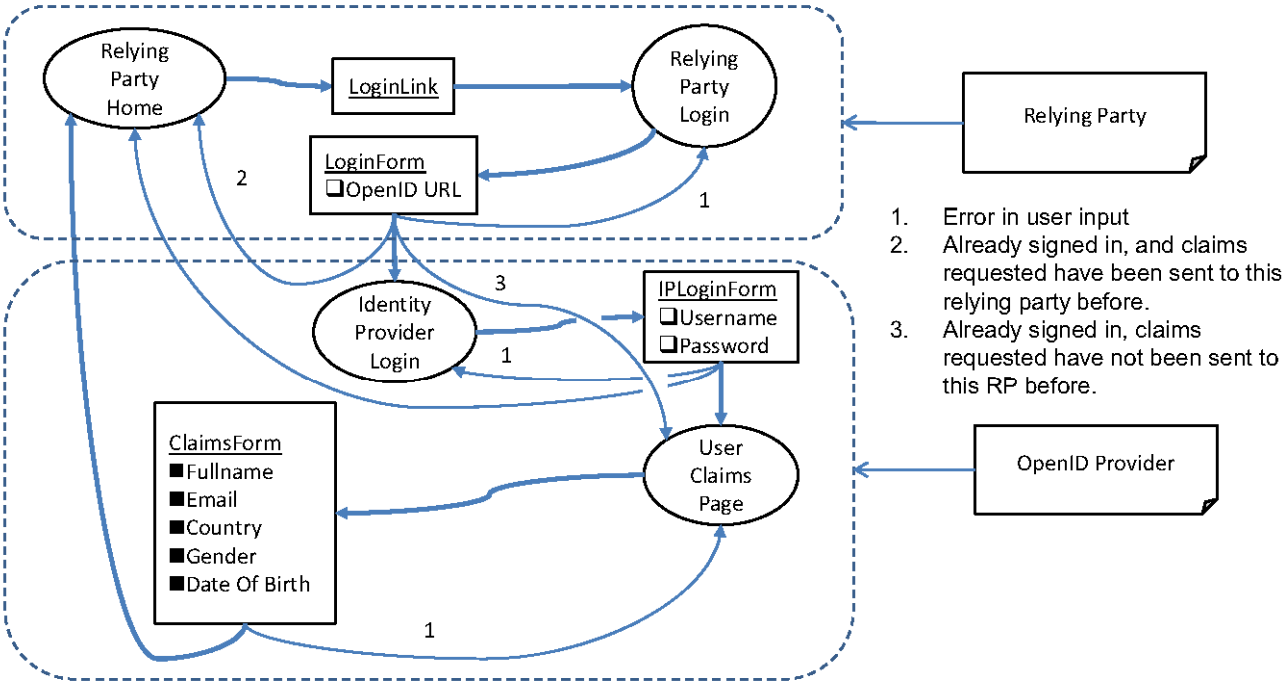

Figure 1. OpenID from the user perspective.

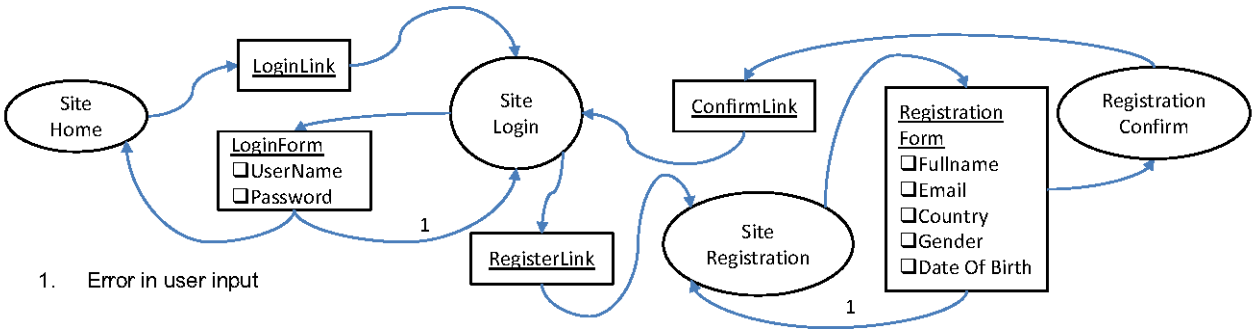

Figure 2. Site-centric authentication with account registration.

1. Consider the problem of drawing a form storyboard for the contact-protection prototype of Zhou *et al.* Would the information in Figure 3 be more helpful for drawing a storyboard from the user's perspective or from the system's perspective? Explain your answer briefly. To receive full credit, your explanation must be accompanied by a fragment of a storyboard diagram for Zhou's prototype. You should not attempt to draw a complete storyboard diagram.

(15 marks)

Student A: Figure 3 would be more helpful in creating a storyboard from the system's perspective because the figure is based mostly on the technical background rather than the interface or page flow as for figure 1 and figure 2.

The student's diagram shows an "Application Home" in an oval, which produces a "Contact Login" form (in a rectangle). The diagram includes a note on the Contact Login form: "Not from a user's perspective therefore challenging to create a storyboard."
This is an excellent response, demonstrating a very strong understanding of form storyboarding and at least a good understanding of the TISSA architecture. The student notes, correctly, that the flowchart of Figure 3 does not show any interactions with the user. 15/15

Note: there are two places in which the flowchart in Figure 3 implies a user interaction. When an exception is thrown (due to insufficient privilege), this would (presumably!) result in the application giving some visible signal to the user and (we might hope!) offering the user some chance to remedy the situation. Also, the Privacy Setting Content Provider must have some interaction with the user to discover their privacy preferences. Because neither of these interactions were explicit in the flowchart, I can't fault a student for not drawing them into their storyboard; and this is one of the reasons I asked only for a fragment of a storyboard diagram. This was a very difficult question and I'm pleased that someone was able to get full marks on it!

Student B: Drawing the form storyboard from the system's perspective would be more useful from the developer's point of view. The user's perspective deals more with the 'outside' part of security, like there are blackbox areas where processing is hidden. From adeveloper's point of view, what we want to know is how security is handled in that blackbox areas as this gives a more concrete & specific processes for the development of security.

The student's diagram shows an "untrusted application" (in an oval) which produces a "Content resolver" form (in a rectangle) which is consumed by an "Android permissions" form (in a rectangle). (? – I don't understand how a Content resolver" can be a form, nor do I understand how a form can consume another form) The Android permissions form is consumed by an "Application rejected" process (in an oval), which produces no user-visible output. The Android permissions form is also consumed (?) by a "Contacts content provider" form (in a rectangle). Other forms and processes on the student's diagram have labels taken from the other elements in Zhou's flowchart.

The student's diagram is not a form storyboard diagram, as defined in the Bellamy-McIntyre article. Their written comments do not answer the question. However these comments do make sense, and they do make a valid point about what sort of information would be "helpful" to a technically-oriented security developer. So the answer is tangentially responsive to the question, so I am awarding a small number of marks: 3/15.

Note: if you're unable to answer a question completely, it is much better to answer part of the question rather than not writing anything. At the very least you should try to demonstrate that you understand the underlying conceptual material, which in this case is flowcharts, form storyboards, and Zhou's TISSA method. The form storyboard modelling technique was highlighted, in appreciative comments, by two of the three oral presentations on the Bellamy-McIntyre article.

Student C: From the systems perspective. This is because Fig. 3 displays a view of the underlying Architecture for the system developed by Zhou et al. This is apparent because of the input & outputs seen in the componenets which are neither provided by user input or seen by users. For example, the input (request for a resource) & output (the content provider or an exception) are abstractions of the underlying system and not the presentation layer. See the below diagram.

The student's diagram shows a "Content Resolver" form (in a rectangle) being consumed by an "Android Permission Check" form (in a rectangle), which is consumed (?) by a "Passed?" entity (in a diamond) which produces a "Contacts Content Provider" form (in a rectangle), which is consumed by a "Throw Exception" form (in a rectangle). The student's diagram is identical to a fragment of Figure 3, in which (for some reason – perhaps this is just a transcription error on the part of the student) the "N" arrow from the "Passed?" decision-point in the flowchart of Figure 3 has its tail at the "Contacts Content Provider" rectangle in the student's diagram.

I am unable to interpret the student's diagram as a form storyboard. The system elements drawn in rectangles are not forms; some or all of these elements might be drawn as ovals (to indicate server-side actions) but I don't see any way to "correct" a small mistake in this student's diagram so that it is composed solely of ovals

and rectangles in a bipartite graph (that is, into a diagram in which every rectangular form is produced and consumed by an oval action).

This student's written answer indicates that they have a good understanding of the goal of form storyboarding: that it is intended to model the interactions of a user with a system. The student correctly characterises Figure 3 as displaying a "view of the underlying architecture" of TISSA. Accordingly I'm awarding somewhat more than passing marks to this answer, even though this student did not draw even a small fragment of a form storyboard for TISSA. 8/15

2. Briefly characterise the privacy protection afforded by Zhou's prototype, using terminology from Lampson's article on "Computer Security in the Real World". To receive full credit, your characterisation must use all of the relevant terms from the following list: specification, implementation, correctness; secrecy, integrity, availability, accountability; isolate, exclude, restrict, recover, punish. **(10 marks)**

Student D: Zhou's prototype tries to protect the secrecy of of my contact list, so that no untrusted application is able to access the full list. This happens by restricting the access to the list based on the level of trust of a certain application (the list is isolated from the applications, access is only possible through an implementation of this prototype acting like a 'guard'.

Basically the androids system only checks the permission granted to the application whereas this framework also specifies a check based on 'privacy settings' the user made.

The advantage is, that an untrusted application still can have access to certain (relevant but anonymised) information, wheas secret information might be excluded. This guarantees on one hand the integrity of the users contact list but on the other hand the application still has correct results which it can deal with (otherwise it maybe has to cancel the ongoing operation due to missing information).

Student D correctly used the following terms from the list provided in the question: secrecy, restrict. They also correctly used the term "guard". Their use of the term "excluded" had a grammatical error as noted below, but I am accepting it for full credit because I don't expect students to have error-free grammar, especially under examination conditions!

The student apparently knows the meaning of "integrity". Their answer correctly identified a problematic situation whenever TISSA produces an "Empty Result" (as shown in the bottom-right corner of Figure 3). I was disappointed that the student referred to this as "missing information"; and that the student didn't discuss the difficulties caused by the loss of integrity (from the untrusted application's perspective) whenever TISSA produces a Bogus Result or an Anonymized Result.

This student incorrectly used the term "isolate". Note: in Lampson's taxonomy of defensive strategies, if the contact list were isolated, then no application would have access to it! Lampson notes that this "coarse-grained strategy provides the best security, but it keeps users from sharing information or services. This is impractical for all but a few applications." This term could have been used correctly if the student had said that the privacy settings are isolated from the applications. Only the Privacy Setting Manager can change these settings, and this is not an application.

The student did not use the term "availability", even though a thrown exception (from Android) or an "Empty Result" (from TISSA) are restrictions on the availability of a resource because of a lack of permission (Android) or trust (TISSA).

The student did not use the terms "specification", "implementation", or "correctness", even though all of these are important considerations in TISSA.

The student did not use the term "restrict", even though TISSA is providing restricted access to a contact list, through its introduction of Anonymised and Empty values.

Note on grammar: in a defensive structure where "x excludes y from z", it is "y" that is being excluded. The grammatical distinction is between the active and passive voice. When it stated in the passive voice, this

defensive strategy is "y is excluded by x from z". In the TISSA architecture, x = TISSA, y = an untrusted application, and z = sensitive information from the contacts list.

Overall: this student showed good understanding of TISSA, by correctly characterising it as a guard, and by describing the "privacy settings" as being under direct control of the user. Neither of these are explicit in Figure 3 or the question. The student showed an adequate understanding of Lampson's defensive strategies. They neglected to discuss TISSA from the three aspects of specification, implementation, and correctness. 8/15.

Student E: The implementation of the prototype aims to protect contacts that are seeking permission of the usage of the android smartphone. The plugin isolates the permission seeking from the rest of the phone.

This answer is a very inaccurate description of TISSA. Its usage of "implementation" is only marginally correct; in Lampson's framework, a prototype is an implementation, but a prototype is not an adequate specification for a security design. Its usage of "isolate" is incorrect, because some portion of the 'rest of the phone' must be able to access the TISSA portion. Furthermore, TISSA is not a plugin. This answer gives me no confidence that the student who wrote it has any understanding of the technical material presented in the required readings by Lampson and Zhou et al., so I will not award any marks for it. 0/15

Student F: Zhous prototype implementation include further checks the privacy settings of the Contact Content provider to restrict untrusted packages/permissions. If untrusted Zhou is able to isolate the user from the correct result response. This means that that an application will always have a result available to prevent the program crashing. Therefore it would be able to recover all though the results are not what might expected. On the other hand if we see that the package and permissions are correct we can return the correct value to the application maintaining its integrity.

This response has so many grammatical errors that I'm not completely confident I'm interpreting it in the way intended by the student. I'd strongly encourage this student to take the DELNA assessment, if they haven't done so already, and to take advantage of the English Language Support offered by our University to its postgraduate students.

The student uses the terms "implementation", "isolate", "available", "recover", "correct", "integrity". Their usage of "implementation", "isolate", "recover", and "correct" do not follow the (specialised) meanings given to these terms by Lampson. This student is using these terms, in their more general meanings, to broadly characterise the TISSA architecture. This characterisation is mostly correct. It is not completely correct, because TISSA can return an "Empty Result", and because TISSA might cause an untrusted application (which this student calls a "program") to "crash" by returning an Anonymized or Bogus result. I'd say this answer shows an adequate understanding of TISSA (6/8), and an inadequate understanding of Lampson's article (0/7), so it's somewhat less than "half right": 6/15.

(Other questions). **[75 marks]**
