COMPSCI 725

THE UNIVERSITY OF AUCKLAND

SECOND SEMESTER, 2009
Campus: City

COMPUTER SCIENCE

Software Security

(Time allowed: TWO hours)

NOTE:

- Attempt ALL questions, 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.
- This exam has 4 questions for a total of 100 marks.
- Write your answers in the script book provided. Put the question number clearly next to your answer. Leave a gap of several lines between each answer.
- Draw a diagonal line through any work you do not want marked. Please do not use correcting fluid.

1. Consider the following quotation from Radhakrishnan and Solworth, in "NetAuth: Supporting User-Based Network Services".

> UBNS is not the only way to partition a service into multiple processes. Another complementary way is privilege separation [29] in which an application is partitioned into two processes, one privileged and one unprivileged. ... We do not describe the authorization part of netAuth in this paper for two reasons. First, there is not sufficient space. Second, the authentication mechanism can be used with any authorization model. For example, even POSIX authorization, privilege separation, and VMs could be combined to provide a reasonable base for UBNS. The most value for authorization is gained when privileges are based both on the executable and the user of the process, increasing the value of privilege separation. Such separation is essential to allow multiple privilege separated services to run on the same OS.

(a) Discuss the UBNS authentication mechanism in the context of an access control system, as defined in Lampsons article on "Computer Security in the Real World". To receive full marks, you must use the following words accurately in your answer: subject, object, guard, authentication, authorisation. (10)

(b) In their article on "Capability Based Financial Instruments", Miller et al. use a Granovetter diagram to illustrate Alice sending a message about Carol to Bob. Draw one or more Granovetter diagrams to illustrate how a UBNS service a) accepts a connection, b) performs user authentication to identify the user requesting the service, c) creates a new process and d) changes the ownership of the process to the authenticated user. Discuss your diagram briefly. To receive full marks, your discussion should include the words "privilege separation", and your diagrams should include the following principals: the user (U), the UBNS service (S), the child process (C), the message (M) containing the connection request, and the external system (E) which sent message M. (15)

(c) Barth et al., in their article on cross-site request forgery, discuss a defensive technique. "To use secret validation tokens to protect against login CSRF, the site must first create a pre-session, implement token-based CSRF protection, and then transition to a real session after successful authentication." Compare and contrast this technique with UBNS. (5)

(d) Miller et al. plan to extend their netAuth system, using the DisCFS mechanism, to “extend the set of users on the fly by adding their public keys to allow anonymous access (assuming authorization allows it for a service) thus combining the best of authenticated and public services”. If all three elements of Lampsons “gold standard” for implementing security are included in this extended netAuth system, could it provide “Accountable Privacy” as defined in the article by Burmeister et al.? Discuss briefly. (10)

2. Consider the article by Duflot on “CPU Bugs, CPU Backdoors and Consequences of Security”. Also consider the article by Garcia et al. on “Dismantling MIFARE Classic”, and the article by Jelacity and Bilicky on the automated detection of botnets.

   (a) Discuss the ethical issues raised by the content of these three articles, from the perspective of Tomlinson as expressed in his “Rudimentary Treatise on the Construction of Locks”. To receive full marks, your answer must refer to specific information disclosed in the Duflot, Garcia, and Jelacity articles. (15)

   (b) Discuss the ethical issues raised by the content of the articles by Duflot, Garcia et al., and Jelacity et al. from the perspective of the “elite circle that includes programmers, graphic designers and many others” described in the article by Rosner entitled “Steal this software”. (5)

3. Consider the Source Code Author Profiles (SCAP) discussed in the article by Frantzescou et al. in the context of the static k-gram based birthmark (SKB) discussed in the article by Bai et al. Also consider the following paragraphs from Anderson and Peticolas, in “On the Limits of Steganography”.

> There is a critical distinction between passive wardens, who monitor traffic and signal to some process outside the system if unauthorized traffic is detected, and active wardens, who try to remove all possible covert messages from traffic that passes through their hands. In classical systems, the wardens could be either active or passive; while in marking systems, we are usually concerned with active wardens such as software pirates.
>
> Consider the marking of executable code. Software birthmarks, as mentioned above, have been used to prove the authorship of code in court. They were more or less automatically generated when system software was hand assembled, but they must be produced more deliberately now that most

> code is compiled. One technique is to deliberately mangle the object code: the automatic, random replacement of code fragments with equivalent ones is used by Intel to customize security code.
>
> One can imagine a contest between software authors and pirates to see who can mangle code most thoroughly without [affecting] its performance too much. If the author has the better mangler, then some of the information he adds will be left untouched by the pirate; but if the pirates code mangler is aware of all the equivalences exploited by the authors, he may be able to block the stego channel completely. In general, if an active wardens model of the communication is as good as the communicating parties model, and the covertext information separates cleanly from the usable redundancy, then he can replace the latter with noise.

(a) Do any of the assertions by Anderson and Peticolas, in the paragraphs above, imply that SCAP is ineffective at determining the authorship of decompiled code obtained from viruses and worms? Discuss briefly. (5)

(b) Compare and contrast SCAP with SKB. To receive full marks, you should discuss the calculations made when comparing two programs, the (presumed) behaviour of the adversary, and one other significant difference or similarity. (15)

(c) Briefly describe the dynamic k-gram based birthmark (DKB), then discuss its applicability to the problem of authorship analysis as defined by Frantzeskou et al. (10)

(d) In “An Empirical Study of Real-world Polymorphic Code Injection Attacks”, Polychronakis et al. “... used a binary code clustering method to group the unique payloads with similar code from all captured attacks into corresponding payload types. ... we first extract any obvious embedded strings using regular expressions, and disassemble the remaining code to derive a corresponding instruction sequence. We then group the payloads using agglomerative hierarchical clustering, with the relative edit distance over the compared instruction sequences as the distance metric.” Would SCAP have been an appropriate tool for Polychronakis et al. to use, when clustering this malware? Discuss briefly. (5)

4. Consider the article by Jelasity and Bilicki on P2P botnet detection, in the context of the article by Bettini et al. on location-based privacy, and also in the context of the article by Kreibach et al. on spamcraft.

   (a) Would the anonymisation technique described by Bettini et al. be considered a P2P botnet by Jelasity and Bilicki? Explain briefly. (5)