THE UNIVERSITY OF AUCKLAND

FIRST SEMESTER, 2002
Campus: City

COMPUTER SCIENCE

Software Security

(Time allowed: TWO hours)

NOTE: Attempt **ALL** questions in the 12-page script book provided. Total possible: **100 marks.**

1. The Computer System Statute 2000 of our University has the following provision:

> "... 'System' means any computer ... controlled or operated by the University ... A student ... may not ... use the System to display, to transmit or to make available for transmission through computer networks, any work or publication, including files containing any text, image, sound or multimedia, that: ... has been composed knowingly so as to appear to have been produced by another person."

Which (if any) of Pfleeger's four security threats, and what legal or ethical right, are controlled by this clause? Can you foresee any difficulties in the enforcement of this provision? Explain your answers briefly, in approximately 75 words. **[15 marks]**

2. In an application of the D'Agents technology, a user can send software agents to search a distributed database to discover documents matching their query. The agents may travel to different database servers, "fork" additional agents, and send messages back to the user. Each server maintains a list of users whose agents, if digitally signed, should be allowed to execute. Each server also maintains a list of other servers that can be trusted to handle agents correctly. Consider the following list of security goals:

   a. Servers should not run agents for unauthorised users;

   b. Servers should run agents for authorised users; and

   c. Servers should not make unauthorised changes to agents, and servers should not make unauthorised agents (or copies of agents) bearing a user's signature.

Give an appropriate one-word name for each goal, and indicate the extent to which it is addressed by the digital-signature technology of D'Agents.

Your answer should have three parts, each of approximately 25 words. In each part you should discuss one of these goals. **[15 marks]**

3. Sander and Tschudin's 1998 paper "Towards Mobile Cryptography" contains the following claim and explanation:

> "We ... present a way how an agent might securely perform a cryptographic primitive, digital signing, in an untrusted execution environment ... [A] rational function [is] the quotient of two polynomials ... birational permutation schemes s [map rational functions] K^n [onto rational functions] K^n ... Let s be a rational function used by Alice to produce the digital signature $s(m)$ of an arbitrary message m ... [where] m [is] the result of a rational function f applied to some input data x ... Ways to contruct birational functions s that are easy to invert have been described by Shamir in the second part of [Shamir, 1993]. However, the [digital signature] schemes resulting from these constructions have been successfully attacked by Coppersmith, Stern and Vaudenay [Coppersmith, 1993]. So there is a need to find new constructions for secure birational functions to put our ideas to work. We expect that other ways to construct secure birational maps can be found ..."

Write a brief comment (approximately 50 words), discussing security techniques that could be employed to defend the digital-signature function of a software agent, when it is running on an untrusted host.

To receive full credit, your comment must make critical and appreciative use of the information in the excerpt above, and from at least one other required reading in COMPSCI 725. **[10 marks]**

4. Consider a simple digital rights management (DRM) transaction, in which a user is allowed to view an online document after they have supplied an email address.

In approximately 50 words, briefly discuss two legally-recognised rights that are controlled by this DRM transaction.

For full credit, your answer should

- name these two rights,
- identify the original owner(s) of these rights,
- indicate to whom these rights are being transferred or extended during this DRM transaction,
- briefly describe a possible "bad surprise" (an unexpected and unwanted outcome) for the user, and
- briefly describe a possible bad surprise for the author of the document. **[10 marks]**

5. A local bank is concerned about the security of its home-banking webservice.

In the bank's current system, a user at their home PC downloads a client Java applet from the bank's website. This applet communicates with the bank's webserver using SSL, in which the authenticity of the bank's webserver is verified with a public-key certificate issued by VeriSign. The bank's webserver authenticates the customer by asking them, through the applet interface, to use the keyboard of their PC to enter their bank account (a 9-digit number) and 4-digit PIN.

The bank has already issued smart cards to all of its customers, for use as debit cards and credit cards. The bank is now considering whether it would be a good idea, or not, to give a STR100 smart-card reader (see attached datasheet) to its most security-conscious customers. These customers would be given assistance, if necessary, to properly attach the smart-card reader to an unused serial port on their PC, and to configure their web-browser to run a second-generation (smart-card) remote-banking Java applet.

The bank is concerned that a highly skilled attacker might find a way to make fraudulent transactions involving many different customer accounts, by remotely "hacking" their PC. If these transactions were cleverly chosen, significant losses would be incurred before the fraud could be stopped by the bank's traditional security systems.

Identify and briefly explain some of the security vulnerabilities that may be present in the current system and in the proposed second-generation system. Your answer should consist of approximately 75 words.

You will receive full credit if your answer makes understandable, accurate and relevant references to *three* required readings in COMPSCI 725. You need not make precise bibliographic citations to receive full credit. **[15 marks]**

6. Chang et al. propose a scheme for tamperproofing, in which "guards" compute a checksum over a piece of program code to verify its integrity. Horne et al. describe a similar scheme, in which "testers" compute and verify a chained linear hash function.

Briefly describe how a skilled attacker might tamper with a program that may contain testers or guards. To obtain full credit, your answer should identify *two* significant problems that the attacker must face, and suggest a reasonable way for the attacker to handle each of these problems.

Your answer should have three parts, each of approximately 25 words. In the first part, you should sketch a complete tampering attack, and identify two significant problems. The second and third parts should each discuss one of the significant problems you identified in the first part of your answer. **[15 marks]**

7. Craver et al. describe a Single Watermarked Image Counterfeit Original (SWICO) attack as follows:

> Alice watermarks image I to get $\hat{I}$, which she makes public. Bob computes an image $\hat{I}'$ and watermark S', such that watermarking $\hat{I}'$ with S' yields $\hat{I}$.

The pair of functions $(D(), E())$ is called a watermarking scheme. In the strongest form of a SWICO attack, Bob uses Alice's watermarking scheme.

A distinction can be made between "public" and "private" watermarking schemes. A scheme is called "public" if $D()$ is a boolean function of a possibly-watermarked image J and a watermark S. If $D()$ has a second image parameter, a reference image (usually the unwatermarked image), then the scheme is called "private" – because the watermarker does *not* reveal her reference image to the public.

Alice and Bob do not publish their watermarks S and S'. However, they must reveal their watermark and reference image, if required, to a trusted third party (such as a judge or expert arbitrator) during any ownership dispute.

Bob's strong SWICO attack is successful against a public watermarking scheme, if $D(\hat{I}, S') = True$ and $E(\hat{I}', S') = \hat{I}$. Note that these facts are just as convincing to the third party as Alice's ownership claim of $D(\hat{I}, S) = True$ and $E(I, S) = \hat{I}$.

Consider three technologies for software watermarks:

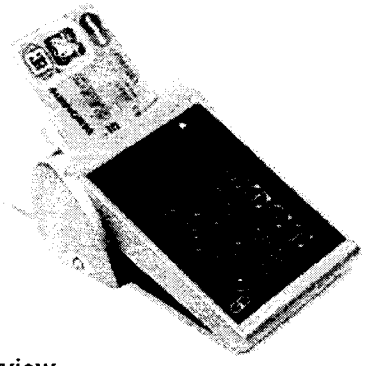
a. Easter Eggs;

b. The static code watermark described by Stern et al, embedded by swapping small groups of instructions, and detected by finding many small groups of instructions in the order defined by a watermark S;

c. Dynamic data structure watermarks.

If we extend the definition of a public watermark scheme by using "software or image" to replace "image" in the definitions above, which of these software watermark technologies can be used as public watermark schemes? Of the resulting public watermark schemes (if any), which are susceptible to a strong SWICO attack?

Your answer should have three parts, each of approximately 35 words. In each part you should discuss one of the three technologies for software watermarks listed above. For full credit, your answer must clearly define the functions $D()$, $E()$ and their parameters for each technology; argue whether or not a public scheme is possible for each technology; and argue (if a public scheme is possible for each technology) whether or not Bob can feasibly mount a strong SWICO attack against that scheme. **[20 marks]**



SCM MICROSYSTEMS

STR100

High security Smart Card Reader for Internet banking

Overview

SCM Microsystems' STR100 is a programmable terminal for the PC, designed specifically to provide a high level of security for online web transactions.

Combining Smart Card technology with a user's PIN code, the STR100 is ideal for home banking and other applications requiring secure data exchange.

With its on-board memory, STR100 can be used as a secure method of downloading applications. The STR100 also offers RSA functionality for added security.

The STR100 can be fully customized for the OEM:

- Choice of color
- Printed logo
- Individually packaged

The SCM Microsystems Advantage

Why choose SCM Microsystems? It's simple:

- Over 11 years experience in ASIC development
- Over 50 patents
- Global top tier OEM customer base
- Industry endorsed Smart OS™ middleware
- Direct relationships with the leading Smart Card manufacturers

STR100 Benefits

- Windows Plug and Play compatible
- High security, cost effective solution
- Serial port connectivity
- Tamper evident and tamper proof design
- Tested and compliant with all major smart cards on the market
- Fully OEM branded – choice of color, printed logo, individually packaged (subject to quantity)

Drivers

Microsoft PC/SC drivers
STR100 is available for Windows 95, 98, Millennium, NT4 and 2000 operating systems.

Technical data

PC connection	• RS232, 115200 b/s, PnP Support
Smart Card Interface (Electric)	• Standard ISO 7816 1/3 chip card interface • 5V Microprocessor card support (T=1, T=0) • 5V memory card on demand • Current compliant with ISO : 60 mA max
Smart card Interface (Mechanic)	• 6 contacts • Certified for 100,000 insertions • EMV 3.11 compliant • Supports embossed smart card
User interface	• Display: 1 LED, LCD 2x16 characters • Keypad: 4x4 with customizable keys
Memory	• 320 Kbytes of flash • 128 Kbytes of SRAM
Security features	• RSA 1024 available • Tamper evidence (casing)
Cable/Power	• Cable: 2 meter long, DB9 and PS/2 connector for power supply • Colors of connector (RS-232 and keyboard pass through) compliant with PC 99 recommendations
Dimension	• LWH 140 x 100 x 60 (mm)
Operating temperature	• 0° to 60° Celsius
OS	• SCM SmartOS™

Regulatory Agency approvals

The STR100 passed FCC, UL and CE testing

EMV approval

The STR100 has been designed to pass EMV Level 1 approval (in progress)

HBCI – Home banking in Germany

The STR100 is compliant with HBCI (ZKA-Germany)