UNIVERSITY OF OXFORD
SOFTWARE ENGINEERING PROGRAMME

Wolfson Building, Parks Road, Oxford OX1 3QD, UK
Tel +44(0)1865 283525 Fax +44(0)1865 283531
info@softeng.ox.ac.uk www.softeng.ox.ac.uk

Part-time postgraduate study in software engineering

Security Principles, SPR

21st – 25th January 2013
ASSIGNMENT

The purpose of this assignment is to test the extent to which you have achieved the learning objectives of the course. As such, your answer must be substantially your own original work. Where material has been quoted, reproduced, or co-authored, you should take care to identify the extent of that material, and the source or co-author.

Your answers to the questions on this assignment should be submitted to:

Software Engineering Programme
Department of Computer Science
Wolfson Building
Parks Road
Oxford OX1 3QD

Alternatively, you may submit using the Software Engineering Programme website — `www.softeng.ox.ac.uk` — following the submission guidelines. The deadline for submission is 12 noon on Tuesday, 12th March 2013. If you have not already returned a signed assignment acceptance form, you must do so before the deadline, or your work may not be considered. We hope to have results and comments available during the week commencing Monday, 22nd April 2013.

ANY QUERIES OR REQUESTS FOR CLARIFICATION REGARDING THIS ASSIGNMENT SHOULD, IN THE FIRST INSTANCE, BE DIRECTED TO THE PROGRAMME OFFICE WITHIN THE NEXT TWO WEEKS.

Software Engineering Programme

Software and Systems Security

SPR: Security Principles

Assignment January 2013

DigiPound

In this assignment, your task is to design digital money using the cryptographic methods introduced in the lecture. The digital money is called *DigiPound*, and the properties of DigiPound should be similar to physical, real-world cash. In particular, the transactions of DigiPounds should fulfil the following requirements: (R1) users should not be able to generate DigiPounds arbitrarily; (R2) users can only spend the amount of DigiPounds available to them; (R3) users are prevented from spending the same DigiPound twice. Furthermore, there is a trusted-third party called *DigiPound Bank*. The role of the DigiPound Bank is to provide a public-key infrastructure (PKI), offer exchange between real money and DigiPounds, and to verify that the requirements of DigiPounds are fulfilled. However, due to scalability problems, the DigiPound Bank cannot be used as a mediator for the DigiPound transactions. This means that the DigiPounds are exchanged directly between the DigiPound users. The DigiPound Bank can only be used to verify the validity and to keep the record of the spent DigiPounds.

1. Describe the main security requirements, threats, and potential vulnerabilities of the DigiPound system.

2. The electronic representation of a DigiPound might involve unique IDs, timestamps, hashes, encryption, signatures, and/or message authentication codes. Propose a possible design for the DigiPound. Justify your design choices in detail and explain how the aforementioned requirements (R1-R3) can be fulfilled.

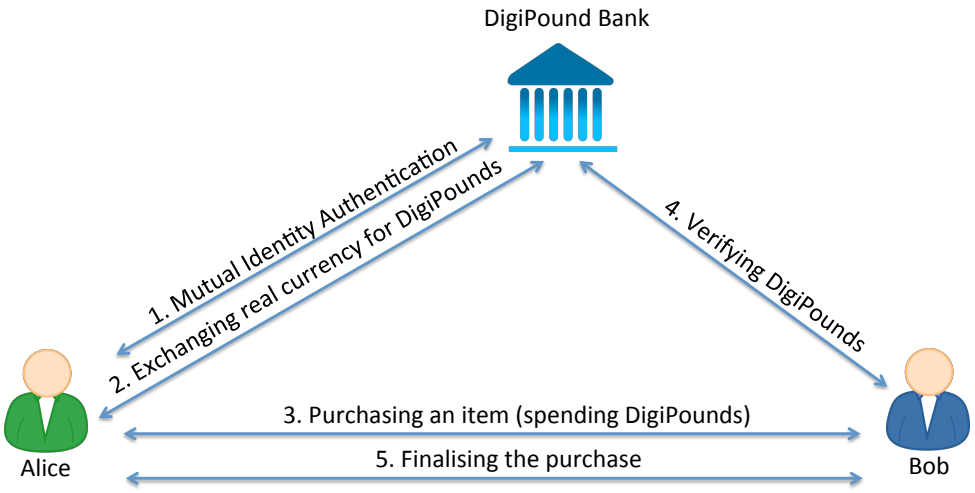

Figure 1: DigiPound Scenario

Assume that Alice and Bob are legitimate users of the DigiPound system (having their accounts and Digital Certificates issued by a DigiPound Bank). Figure 1 depicts the communication between Alice, Bob, and a DigiPound Bank in a typical purchase scenario in which Alice buys an item from Bob.

3. The first step is a mutual authentication between Alice and a DigiPound Bank, which verifies the possession of the valid public and private keys. Select a suitable security protocol for this task from those we studied in the lectures, or design one which meets the requirements.

4. Next, we need a protocol which allows DigiPounds to be transferred from one party to another. Alice uses this protocol to receive DigiPounds from the bank (after she has paid real money for them) and also uses it to send DigiPounds to Bob during a purchase transaction. Design a protocol which achieves this securely. Your protocol will probably use the authentication from question (3) in its initial steps. Make your protocol as efficient as possible.

5. In the fourth step, Bob verifies the received DigiPounds with the DigiPound Bank and if the DigiPounds are valid, he finalises the purchase by signing the bill that includes the transferred DigiPounds and sends it to Alice. Your task is to design a protocol that Bob can use to verify that the received DigiPounds are valid.

   [Optional:] Typically, Alice has lots of spare compute cycles available, whereas Bob's server is operating close to capacity. Can you optimize the protocols so that they take account of this asymmetry?

6. In the third step, Bob agrees to sell an item to Alice by signing the purchase request. Alice receives the signed purchase request and transfers the DigiPounds to Bob. Bob verifies with the bank, and then finalizes the purchase.

   If your protocols are good, Marvin, an attacker, may not be able to mount a protocol-based attack against this scheme, but in a realistic deployment, things may still go wrong. You may want to consider Alice and Bob's computers or smartphones, the network, their own behaviour (or lack of attention), tricks, compromise of some or all of the Bank's functions, collusion between two of the parties, or other known or anticipated forms of attack. One such form of attack is a man-in-the-middle, in this attack a malicious user Marvin attempts a Man-In-The-Middle attack with the goal to intercept the DigiPound transfer and to steal the DigiPounds intended for Bob. You should describe how this might work, but you should describe other possible attacks also.

Guidance

You should attempt all of the questions. Present protocols using the notation we had in class wherever possible, and state any extra assumptions or notation you use. Question 6 will require a substantially longer answer than the other questions, and might draw on many features of the course.

A long answer is not necessary: although there are several questions, it would be surprising if your final submission were more than twenty pages long; it might be somewhat shorter. Be sure, however, to answer *thoroughly* and (where appropriate) *realistically*.
The questions are progressively more-and-more open-ended. Answers which pursue the loose ends are of course those more likely to gain distinction-level grades. The questions are *not* all equally weighted.

Any discussion of the security of real/realistic systems is likely to be covered in depth on a range of web sites. You are not expected to show a thorough knowledge of these, and you should certainly not make extensive quotes from web sites or books. Of course, if you do refer to external sources of information, you must make clear *what* you have referred to, *and* the extent of any quote or re-use of ideas. Do keep in mind the assessment criteria: the purpose of the assignment is for you to demonstrate your *own* understanding of the issues.

Please structure your answer so that there is a *cover sheet,* which contains *only* your name, the subject and date, and a note of the total number of pages. Do not put any answer material on the cover sheet; begin your answer on a fresh page. Avoid putting your name on any page except the cover page. *Do* number the pages.

Assessment Criteria

Within each question, the assessment is intended to judge:

- the extent to which you can understand and explain the main themes in, and parameters of, information systems security and cryptographic protocols;
- your understanding of the available major classes of solutions, including their capabilities, strengths, and weaknesses;
- whether you are able to apply suitable evaluation techniques to the consideration of unfamiliar scenarios and solutions;
- your appraisal of how present developments and future trends may affect the viability and security of particular technologies. Appropriate application of the principles taught in the course will offer an excellent means of demonstrating the relevant capabilities.