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

Cloud Security, CLS

22nd – 26th April 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, 11th June 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 July 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.

Cloud security course assignment

April 2013

Read the following scenario and then answer the questions based on the scenario.

A financial institution ***FI*** has a well-established private Cloud infrastructure. FI starts to suffer from financial losses and has been advised that their losses are a result of both malicious insiders and using an old risk management application. FI has approached a well-established company, ***BI***, specialized in business intelligence. BI also has a public Cloud infrastructure and claims that they could address FI's problems.

BI has a risk management product which is a highly complex multi-tier application. This product has high licence costs, and would require an expensive infrastructure to function. The design of this product offers high resiliency, scalability, and reliability properties, which are fundamental requirements to FI. Security is also a key requirement for FI. BI offers the possibility of hosting the risk management application at BI's Cloud infrastructure with reduced costs on a "per usage" basis. This could be either in the form of Software as a Service (SaaS) or Platform as a Service (PaaS). Alternatively, BI could fully deploy and integrate its products within FI's infrastructure.

BI has a good reputation and is used by many financial institutes and government agencies. FI thought it could reduce its operational costs by outsourcing not only the risk management application but also all their applications to BI using a combinations of Infrastructure as a Service (IaaS), PaaS and/or SaaS. FI approached you as an expert in Cloud computing seeking your advice of how to proceed. They asked for a detailed report to cover the following main points:

a) Which Cloud deployment type should FI consider: stay private, move to BI's public Cloud, or switch to community or hybrid? Your answer should consider security threats, mitigations, and other pertinent issues arising out of the different deployment models.
b) Assuming FI decided to outsource all its applications to BI's public Cloud. Which Cloud service should FI consider: IaaS, PaaS and/or SaaS? Please structure your answer to identify the pros and cons of each service in terms of security threats, mitigations, and additional challenges arising from these different services.
c) Assume that FI decided to outsource only the risk management application to BI as PaaS. Discuss what FI and BI need to do to provide sufficient assurance that the application is managed as requested.
d) Discuss the relation between provenance and self-managed services and how they possibly could address the security threats and challenges identified in points a & b.

Guidance

Aim for a concise answer. It would be surprising if your final submission were more than fifteen pages long – excluding illustrative images – it might be somewhat shorter. Be sure, however, to answer thoroughly and (where appropriate) realistically.

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, nor to quote at length from them. Do not reproduce large amounts of material from elsewhere. Keep in mind the assessment criteria: the objective is to test your own understanding, not someone else's. 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.

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, and use 11pt font or larger.**

Assessment Criteria

The assignment is intended to measure the extent to which you:

- can explain Cloud architecture, properties, management services, and security challenges;
- understand security risks associated with different Cloud deployment models, and what could be done to address such risks;
- can relate theoretical understanding of ideals with the realistic trade-offs and challenges of designing and deploying a realistic cloud-based system for a nominated application domain.