Computer Security – Tutorial Sheet 3
Network & Programming

Shahriar Bijani and David Aspinall

20th February 2012

This is the third problem sheet for the Computer Security course, mainly covering topics in network security and programming securely. Tutorial sheets are provided to help guide your self-study on the course and measure your progress. The process for this tutorial sheet is as follows:

1. Read and try to answer these questions before your Week 8 tutorial.
2. The tutor will discuss some of the answers at the tutorial.
3. After the Week 8 tutorial, write down your answers to all questions.
4. In Week 10, a solution sheet will be issued. To measure your understanding of the material, use the solution sheet to assess your answers.
5. In the Week 11 tutorial, there will be an opportunity to discuss problem points in any of the tutorial questions, to give you personalised feedback on suggested areas to revise before the exam.

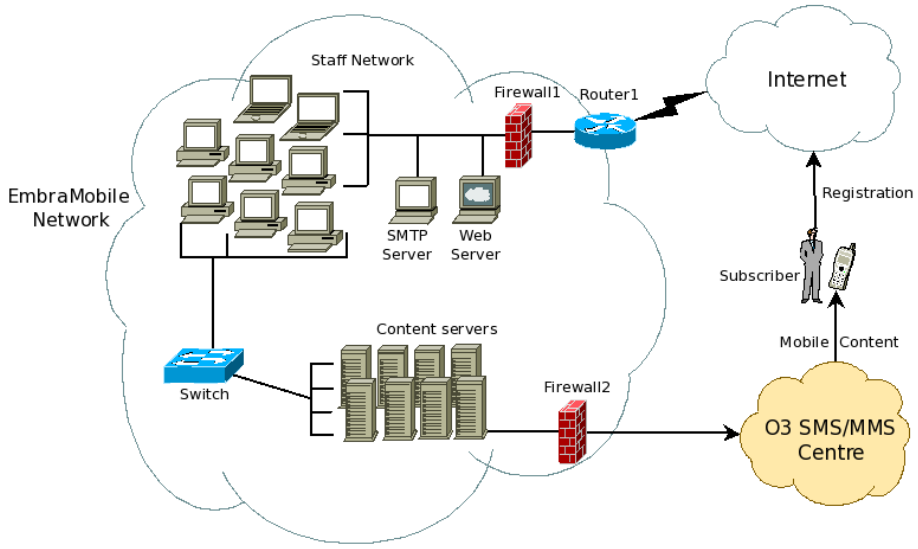
You are free to discuss these questions and their solutions with fellow students also taking the course, and also to discuss in the course forum. Bear in mind that if other people simply tell you the answers directly, you may not learn as much as you would by solving the problems for yourself; also, it may be harder for you assess your progress with the course material.

Question 1: Network Security

EmbraMobile is mobile content provider company in Edinburgh that generates, packages and syndicates text, photo, video, music, games and mobile applications. They provide different information, marketing and entertainment services (e.g. news, ringtones, themes) aimed at over 3 million customers of the O3 mobile network operator. O3 Mobile users can subscribe to EmbraMobile services via its website and receive the requested service on their mobile phone.

Recently, O3 has received a number of complaints from its customers, so has urged EmbraMobile to review their network security, to be able get a security certification. They have two networks: a network of staff machines, which connects staff to the Internet and a network of content servers that is connected to the O3 SMS/MMS centres, shown in the following figure.

EmbraMobile has 30 employees, among which there are 5 IT staff, but currently no dedicated security specialist. Some staff are in charge of content production and aggregation for the content servers. They also access various third-party and partner organisation websites (e.g. new/ multimedia corporation) on the Internet.



You have been asked to perform a security analysis for EmbraMobile. Consider the following steps. In each step, try to be specific (and imaginative!) with respect to the scenario, rather than giving generic answers with little thought.

1. Identify some important assets in the scenario, considering hardware, software and information. In each case, identify the stakeholders (asset owners or other concerned parties) that EmbraMobile should consider when seeking to protect its business, employees, directors and shareholders.

2. Consider the network security aspects of the scenario. For the assets you mentioned, identify whether there are possible threats that target vulnerabilities in the network topology indicated in the diagram. Consider the topology, configuration and the usage scenario, and describe the consequences of at least three threats.

3. For the threats you gave, what countermeasures are available to reduce the associated risks? Consider two distinct security failures, and perhaps consider ways of improving the network topology.

4. It is said that cloud computing could help companies to avoid major new capital expenditures also to reduce ongoing operational expenses. EmbraMobile managers are considering to move some of their operations to the cloud. They believe this might both to improve security and decrease network maintenance cost. The proposal is to migrate the servers to the Amazon EC2 cloud platform located in Ireland.

   (a) Analyse the effects of this migration from security point of view; discuss 3 advantages and disadvantages.

   (b) Describe whether your suggested security improvements will still be applicable, and if not, whether they are mitigated against in some other way, or require another solution.

Question 2: Security Breach

A document giving the next 5-years marketing plans of XGame, an enterprise computer game company, is illegally published on the Internet. The immediate financial loss for XGame is estimated to be more than £100,000 due to the need to reschedule and adjust marketing plans; the company cannot be sure about additional knock-on effects from competitors learning some of their strategy.

The company want to investigate how the breach occurred and ask you to investigate the possible attacks that might have happened.

The encrypted PDF file is saved in a secure file server, in which all important files are encrypted by AES. The file server resides in the marketing department and only a few managers have access to it via the company intranet. All of the servers and machines have Window operating systems and are managed by Active Directory. Five months ago, a chief marketing manager sent the encrypted document to a consulting firm that has Non Disclosure Agreement (NDA) with XGame. The NDA also says that the file has to be removed from all the machines of the consulting firm after 2 months.

1. Using an *attack tree* to structure your answer, provide an analysis of the possible ways that this threat may have happened.

   Recall that a simple attack tree is an AND-OR tree whose leaf nodes are labelled with Possible or Impossible. See the article by Bruce Schneier in Dr Dobb's Journal for examples.

   Label the nodes in the tree with Possible or Impossible, using your background knowledge and making assumptions about the specific scenario. You do not have to draw the tree graphically, but be careful to indicate the tree structure in your answer and label nodes as AND or OR. To explain the tree, give brief descriptions for the nodes.

2. Identify two likely attack routes among paths in your tree which end with possible nodes. Explain why you believe these are the most likely to have lead to the security breach.

Question 3: Secure Programming

A group of talented graduates has recently developed a general purpose online store application for SMEs. They used Java and the MySQL database for their online store. Unfortunately none of them took a Computer Security course, so they have not thought much about the security of their code. You can see some parts of their Java source code on the following pages.

1. Find and describe 5 or 6 programming vulnerabilities in this code.

2. Explain how to exploit the vulnerabilities and what an attacker can do in case of success.

3. Give a suggestion for how to fix each security flaw.

To help with this question, you might like to consult references on secure programming mentioned in the lectures, including the Oracle/CERT secure coding guidelines available at `https://www.securecoding.cert.org`.

```
1
2  import java.unit.Random;
3  import java.sql.*;
4  ...
5
6  class DBConnect {
7    Connection conn=null;
8    ...
9    private String Connect() {
10     try{
11            String url = "jdbc:mysql://129.23.45.77:3306/mydb";
12            Class.forName ("com.mysql.jdbc.Driver");
13            conn = DriverManager.getConnection (url);
14      String res = "Database connection established";
15           return res;
16     }  catch(SQLException ex) {...}
17   }
18  }
19 ...
20
21 class UserManagement {
22   private void loginCheck (String username,
23               String passwordHash) throws IOException {
24     bool loginSuccessful = checkCredentialsValidity(username,
         passwordHash);
25     if (loginSuccessful) {
26       logger.severe("User login succeeded for: " + username);
27       /* the user is directed to her/his own pages */ ...
28     } else {
29       logger.severe("User login failed for: " + username);
30       /* restricted access to public pages */ ...
31     }
32   }
33
34  /* A method that helps to generate a password for a new user or reset
       the password of an existing user*/
35  private void resetPassword (String  newPass){
36     Random  number = new random(123L);
37     Character c;
38     newPass = null;
39     for (int i = 0; i < 9; i++) {
40       // Generate another random integer in the range of [0, 255]
41       int n = number.nextInt(256);
42       c = (char) n;
43       newPass = newPass +  c.toString() ;
44     }
45  }
46
47 }
48 ...
49
50 class Purchase {
51
52   private Data pDate;
53
54   public  Purchase(){
55     pDate = new Date();
56   }
57
58   public Date getDate() {
59     return pDate;
60   }
```

```
 ...
 /* create an XML query from the user request.
 outStream = query for the database, quantity = The user specifies the
     quantity of an item available for purchase */
 private void createXMLQuery (BufferedOutputStream outStream,
                              String quantity) throws IOException {
  ...
  String xmlString;
    xmlString = "<item>\n<description>Widget</description>\n" +
                "<price>500.0</price>\n" +
                "<quantity>" + quantity + "</quantity></item>";
  outStream.write(xmlString.getBytes());
  outStream.flush();
 }

  public void checkAllInventories() {
    for (int i=1; i<= DepartmentNum, i++) {
      Inventory in = new Inventory();
      in.checkInventory(i);
    }
  }

}
...

public class Inventory {
  static Vector vector = new Vector();

  public void checkInventory(int count) {
    for (int n = 0; n < count; n++) {
      vector.add(Integer.toString(n));
    }
    // ckeck any mismatch in the inventory list
    checkMismatch();
    ...
    for (int n = count - 1; n > 0; n--) { // Free the memory
      vector.removeElementAt(n);
    }
  }

}
```