Computer Security - Tutorial Sheet 3: Network & Programming Security

School of Informatics

27th February 2014

This is the third problem sheet for the Computer Security course, 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 7 tutorial.
2. The tutor will discuss some of the answers at the tutorial.
3. After the Week 7 tutorial, write down your answers to all questions.
4. In Week 9, 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 9 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.

Part A: Network Security

A security company *GBHarry* has been severely embarrassed by hacks on its web site that exploited flaws in commodity web applications, including a content management system and blogging software. GBHarry is considering deploying a *Web Application Firewall* (WAF) to help protect its web site in future.

A WAF is a specialised kind of firewall designed to protect web sites from attack. It is deployed between a server running a web application and the Internet-facing router or firewall. Features of a WAF can include support for:

protocols : parsing HTTP and HTML to validate and restrict them.

attack detection : rejecting bad patterns or only accepting good ones.

security : providing additional layers without modifying the web application.

response : either inside the WAF, via the router, or via the web application.

Answer the questions below, based on the above outline or by doing some additional investigation into currently available WAF products.[1]

[1]For links, visit the OWASP site here: `https://www.owasp.org/index.php/Web_Application_Firewall`

1. Suggest two ways that the HTTP protocol could be usefully restricted in the WAF and give two reasons why the WAF may be a better place than the web server.

2. Before running attack detection methods, *input normalisation* may be performed by the WAF. Explain why it might be useful for it to do this, and what it could do.

3. As suggested, WAF attack detection methods can be based on *negative* or *positive* security policies. Compare the two, giving an advantage and disadvantage of each and mentioning similar trade-offs elsewhere.

4. Suggest a response mechanism the WAF might employ in each of the three places suggested (via router, internally, and via application) and, in each case, an attack which would be best dealt by each.

5. Besides the feature categories given above, there are other highly desirable kinds of feature GBHarry (or any user) would probably expect from a WAF. Describe two of these with examples of the functionality you would want.

6. GBHarry finds some of the technical features of the WAF quite convincing, but has some reservations (*other* than the purchase price of the tool and hardware). Suggest what some of these other concerns with deploying a WAF might be, and suggest how GBHarry could make the decision whether to deploy a WAF.

Part B: 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. Identify 5 security issues as described in the lecture. Can you find another vulnerability?

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.

```
1
  import java.unit.Random;
3 import java.sql.*;
  ...
5
  class DBConnect {
7   Connection conn=null;
    ...
9   private String Connect() {
      try{
11            String url = "jdbc:mysql://129.23.45.77:3306/mydb";
```

```
            Class.forName ("com.mysql.jdbc.Driver");
            conn = DriverManager.getConnection (url);
      String res = "Database connection established";
           return res;
     }  catch(SQLException ex) {...}
   }
  }
...

class UserManagement {
  private void loginCheck (String username,
              String passwordHash) throws IOException {
    bool loginSuccessful = checkCredentialsValidity(username,
        passwordHash);
    if (loginSuccessful) {
      logger.severe("User login succeeded for: " + username);
      /* the user is directed to her/his own pages */ ...
    } else {
      logger.severe("User login failed for: " + username);
      /* restricted access to public pages */ ...
    }
   }

  /* A method that helps to generate a password for a new user
   or reset the password of an existing user*/
  private void resetPassword (String  newPass){
    Random  number = new random(123L);
    Character c;
    newPass = null;
    for (int i = 0; i < 9; i++) {
      // Generate another random integer in the range of [0, 255]
      int n = number.nextInt(256);
      c = (char) n;
      newPass = newPass +  c.toString() ;
    }
  }

}
...

class Purchase {

  private Data pDate;

  public  Purchase(){
    pDate = new Date();
  }

  public Date getDate() {
    return pDate;
  }
 ...
 /* 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);
      }
    }

}
```

Part C: Access Control

Edinburgh University Informatics wants to have a combined discussion forum for the two courses *Computer Security* and *Computability and Intractability*. It should be used by the students, all tutors and the examiners. To ensure that no confidential information about the assignments and exercises is leaked different security levels are needed:

- **Students** can write and read with each other in their own threads, but should never be allowed to see the confidential information in the tutor- or examiner-threads before the exam. Since Students know nothing confidential, they are allowed to post suggestions that might be considered in the assignments or the exams to the teaching-staff.
- **Tutors** are allowed to follow the student-threads to adept the tutorials, but since they know the answers for the assignments they are not allowed to write there. They do have their own threads where they can discuss important questions to prepare for the tutorials.
- **Examiners** are allowed to read everything to see how everybody is doing, but can not write except in their own threads, to minimize the risk of leakage.

Some students, tutors and examiners are involved with both lectures, some with only one and others are involved with none of those two.
Furthermore assume we do have one discussion for each of the following topics concerning the lecture Computer Security:

- (students) Question about Exercise 1.2
- (tutors) Clarification about last tutorial
- (examiners) Exam question ideas

1. This kind of security hierarchy can be represented in a lattice:
   (a) Use the construction discussed in the lecture (see Gollman) to write down the security levels and the security lattice for this particular problem.
   (b) To evaluate Computer Security an independent observer is assigned to watch the corresponding threads of the students and the tutors. On which security layer should this observer be set up?
   (c) The results of the student-evaluation of both curses are collected. It is necessary to post a two important results to the tutors of Computer Security and the examiners of Computability and Intractability. Which security clearance is necessary and sufficient to make both posts.
   (d) Dorothy E. Denning postulated the need for a security lattice by establishing 4 axioms about security levels. Her 2nd axiom states "The can flow relation $\leq$ is a partial order on the security classes" Explain the meaning and the need for this axiom in a security structure.
2. Write down the permission matrix for the three threads mentioned above and the Computer Security student Bob, the tutor Luke and the examiner David. Assume none of the tree subjects are involved in Computability and Intractability.

One of the student threads "Problem-Thread" get very controversial about a method presented in the lecture and Luke (a tutor) as well as Dave (an examiner) have to interfere. The Bell-LaPadula model allows them to temporary adjust their security level to be allowed to answer to this thread.

3. Write down the whole BLP-state for this situation. Is the transition made here secure?

Daniel Franzen and David Aspinall