CS 4235 / CS 8803IIS Homework 4

Assigned: 9 March 2011
Due: 16 March 2011, 5:00pm Atlanta time. Students submitting solutions after that time but by 5:00pm Atlanta time on 18 March will have their scores scaled by 0.8. No solutions will be accepted after 5:00pm on 18 March.
Teaming: Work individually.

Solutions should be typewritten and submitted as a PDF file on T-Square. Be sure to include your name and GTID number on your submission. Scores will be posted on T-Square.

Although you may use outside sources for information, you:

- **must not** copy-and-paste text or figures from those sources, and
- **must** cite the sources. A citation should provide sufficient information for myself or anyone else to find the source that you used.

You do not need to cite the textbook or any course materials. If you are unsure whether or not you are using outside material appropriately, please ask me rather than guessing.

This homework has one written part worth 100 points. Please solve the following problems.

Written exercises

1. (20 points) Intrusion detection systems (IDSes) may generate false positives, or alerts when no attack is underway, and have false negatives, or missed attacks. The rate of false positives and negatives is the ratio of errors per some number of events. For an IDS, we can measure counts of the following:

   - A_T: True alerts (attacks that were detected).
   - A_F: False alerts (no attack underway, but the IDS generated a false positive).
   - N_T: True negatives (no attack underway, no alert).
   - N_F: False negatives (attack underway, but the IDS missed it and failed to alert).

   Answer the following:

   (a) Use these four symbols to give a mathematical formula for the false positive rate. Explain the rationale behind your formula.

   (b) Use the symbols to give a formula for the false negative rate. Explain your rationale.

2. (40 points) A group of photography enthusiasts have created a website called *Cameras In Action*. Their php-enabled web server (http://cia.us) hosts a file (/ops.php) with the following PHP code:

```
<?
$mysql = mysql_connect("localhost", "admin", "myvoiceismypassword");
mysql_select_db("cia", $mysql);

/* Set a cookie & add a user if they don't exist. */
if ($_COOKIE[‘name’] == ‘’) {
  setcookie(‘name’, $name, time()+86400); // one day
  setcookie(‘address’, $address, time()+86400);
  setcookie(‘uid’, $uid, time()+86400);
  $q1 = "INSERT INTO who (‘uid’, ‘name’) VALUES ($uid, ‘$name’);
         INSERT INTO where (‘uid’, ‘address’) VALUES ($uid, ‘$address’)";
  mysql_query($q1, $mysql);
}

/* Print the user's name as supplied from input. */
echo "Hello ".$name;

/* Print the user's name as extracted from the database. */
$q2 = "SELECT name FROM who WHERE uid=$uid";
$result = mysql_query($q2, $mysql);
if (mysql_num_rows($result) > 0) {
  while ($row = mysql_fetch_row($result)) {
    for ($i = 0; $i < count($row); $i++) {
      echo $row[i];
    }
  }
}
?>
```

A browser will request the page via GET requests of the form:

```
GET http://cia.us/ops.php?name=AAA&address=BBB&uid=###
```

The php server communicates with a MySQL database. The database `cia` contains two tables called `who` and `where`. Each table has two columns. The table `who` has a column `uid` containing a numeric user ID, and a column `name` containing the string name of the photographer having that user ID. The table `where` has a column `uid` of the same numeric IDs, and a column `address` containing the address of the photographer with each user ID.

Answer the following questions:

(a) Write a value for `$name` that will cause the server to delete the entire table `who`.

(b) Write a value for `$uid` that will cause the server to return the entire list of user IDs and names stored in the table `who`.

(c) Write a value for `$uid` that will cause the server to return all photographers' names and addresses.

(d) A competitor, *Features, Shorts, and B-movies*, believes that motion pictures will reign supreme over still photography and has created their own site (http://fsb.ru). The FSB wants to acquire the identities of the CIA's photographers. Write a value for `$name` that will cause the name and address of the user loading the page to be sent to http://fsb.ru.

(e) Explain how the CIA should alter the code of ops.php to prevent each of these attacks.

3. (20 points) To help detect attacks, system administrators may record an audit log of the network traffic passing to and from their enterprise's network.

   (a) Suppose that the log records only network headers listing source and destination IP addresses and ports. How could this audit log compromise the privacy of computer users in the enterprise?

   (b) Suppose that the log additionally records packet payloads. What additional privacy problems might arise?

4. (20 points) The Wright et al. reading demonstrates that eavesdroppers can extract useful information from encrypted network traffic flows even without the ability to break the cryptography.

   (a) Their work was done in the context of Voice-over-IP. Suggest another scenario other than voice communication in which a network eavesdropper gains knowledge about the possible content of an encrypted traffic flow without crypto attacks.

   (b) What features does your scenario share with the VoIP scenario? How does this lead to information disclosure? Suggest a possible change to the network communication to complicate the eavesdropping attack.