Final exam in

Web Security EITF05

Department of Electrical and Information Technology
Lund University

Oct 20, 2010, 14-19

- You may answer in either Swedish or English.
- If any data is lacking, make (and state) reasonable assumptions.
- Use legible hand writing. If your answers cannot be read, you will receive zero points on that problem.
- Grading is done as follows.
  Grade 3 = 20–29 points,
  Grade 4 = 30–39 points,
  Grade 5 = 40–50 points.

Good luck!

Paul & Martin

Problem 1. Explain the terms *safe method* and *idempotent method* in the context of HTTP. Are GET and POST safe methods? Are they idempotent methods? (3 points)

Problem 2. Give the Base64 encoding of the word "ACES".

HINT: Decimal representation of ASCII characters is given by:

A = 65, B = 66, ... , Z = 90, a = 97, b = 98, ... , z = 122

The Base64 alphabet is:

0 = A, ... , 25 = Z, 26 = a, ... , 51 = z, 52 = 0, 53 = 1, ... , 61 = 9, 62 = +, 63 = /

(3 points)

Problem 3. User tracking is used by many websites for different reasons. Explain and compare user tracking with first and third party cookies. (3 points)

Problem 4. In this problem we will make a toy example of the disclosure attack on a Chaum Mix. Assume that we know (or can guess with high probability) in which output set a message from Alice is sent. In the communication system there are in total $N = 26$ users, labeled A, B, C, ..., Y, Z. We know that Alice has $m = 4$ communication partners among the users. The Mix outputs $n = 5$ messages at each time and we know that exactly one of these is sent from Alice. In the first part of the attack we collect m mutually disjoint sets:

(A,M,P,G,J), (B,Q,R,F,I), (C,N,E,S,T), (D,H,K,L,O)

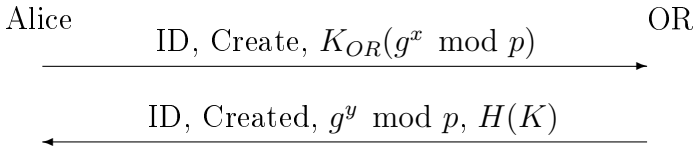
In the second part of the attack we use new sets in order to reveal the m communication partners of Alice. Complete the second part of the attack if the collected output destinations are:

(F,B,K,V,M)	(R,I,U,B,V)	(G,D,X,L,T)	(Y,N,Q,M,D)
(C,J,F,O,Z)	(Q,C,E,Z,U)	(R,S,H,A,L)	(F,T,P,A,W)

(3 points)

Problem 5. Write a regular expression that checks if a string is a base64 encoding of a SHA-256 hash. (3 points)

Problem 6. Consider the key negotiation with the first Tor node as presented below.



Assume that we record *all* transactions between Alice and the OR during some time period. Much later, the private key of the OR is disclosed. Is it then possible to use this key to decrypt the recorded traffic? Motivate your answer clearly. (3 points)

Problem 7. In Hashcash, the string

`ver:bits:date:resource:[ext]:rand:counter`

is hashed using SHA-1. However, not all such strings are valid Hashcash strings. Explain how a valid Hashcash string is computed. Why is an email containing a Hashcash header most likely legitimate? (3 points)

Problem 8. Consider the following piece of (edited) PHP code.

```
$uname = $_POST['username'];
$pass = $_POST['passwd'];

$db = mysqli_connect();

...[some hidden code]...

/* bind parameters and result, execute and fetch parameters */
mysqli_stmt_bind_param($stmt, "ss", $uname, $pass);
mysqli_stmt_execute($stmt);
mysqli_stmt_bind_result($stmt, $u_name, $u_pass, $u_email);
mysqli_stmt_fetch($stmt);

if ($u_name) {
  /* user is authenticated */
  session_regenerate_id();
  ...
```

a) Which technique is used to prevent SQL-injection? Give one other way to prevent this type of attack.

b) Explain, without writing code, how the database connection call can be made without parameters.

c) What is the purpose of `session_regenerate_id()`?

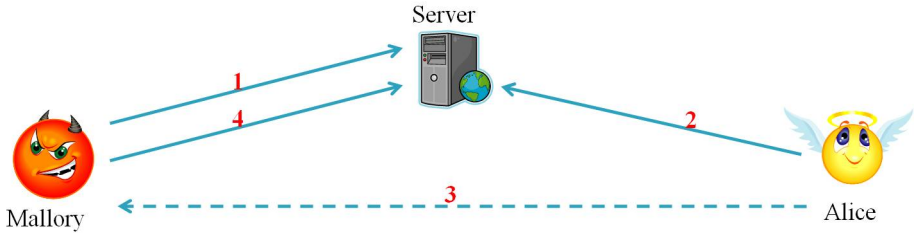
(3 points)

Problem 9. Although it would have been technically possible, DNSSEC was not designed to use digital certificates. How are keys verified in DNSSEC? In what way is the trust model in DNSSEC similar to that of digital certificates? (3 points)

Problem 10. Early versions of the BIND DNS server used sequential transaction IDs when making queries, i.e., if the transaction ID in one query was x, the transaction ID used for the next query was $x + 1$ etc. Describe how you would mount a DNS cache poisoning attack in this situation. (3 points)

Problem 11. Explain how an XSS attack works. You may use the picture below for references. Also, state where the following script fits in and what it can be used for.

```
<script>
document.body.innerHTML=
  '<iframe src="http://www.server.com"
  width="100%"
  height="100%"
  frameborder="0" />';
</script>
```



(5 points)

Problem 12. Consider the Digest Authentication (1999) protocol with *qop*=*auth* given below.

$$md5(md5(A1) : nonce : nc : cnonce : qop : md5(A2))$$
$$A1 : \quad username : realm : password$$
$$A2 : \quad method : URI$$

a) What purposes do the *realm* and *cnonce* parameters serve?

b) If you are a man-in-the-middle that can alter messages, how would you rank the following options from best to worst. Motivate your answer.

1) Replace the entire Digest Authentication header with a Basic Authentication header.
2) Replace all server-provided items and perform a TMTO attack on the remaining information.
3) Perform a dictionary attack on md5(A1).

(5 points)

Problem 13. A DKIM signature header of an email is given below.

```
DKIM-Signature:
v=1;
a=rsa-sha256;
c=simple/relaxed;
d=gmail.com;
s=gamma;
h=received:message-id:date:from:to:subject:mime-version:content-type;
bh=9gicsZnlcLK7yYh6VIrgyAMMRZiWsSbWqSPIhc78RRk=;
b=k4ofvpHPkaQmvuSoGVhRrnCsPK+JEuv9
  KUrZO7aiypvf/6Y1N2iIatvLvdzwOnZX
  /W6Kxyx6Z4Ybuk8Dqk/vNTIE7Jpy+GQU
  UHFvM0NFtmZo1CbGRvo8DdHnXRBB/qWw
  lV+Z6wxw/mq7lNuJknVprOAaTLws5mwc
  Z+AWL8KwHg0=
```

a) What is a "Selector"?

b) How many bits are in the RSA signature?

c) Which parts of the email are integrity protected?

d) How does the client obtain the public key?

e) How does one know that the public key belongs to the signer?

(5 points)

Problem 14. Explain briefly the following terms

a) SPF record

b) NSEC record

c) register_globals

d) URL encoding

e) .htaccess

(5 points)
