Final exam in

Web Security EITF05

Department of Electrical and Information Technology
Lund University

October 19$^{\text{th}}$, 2011, 14.00-19.00

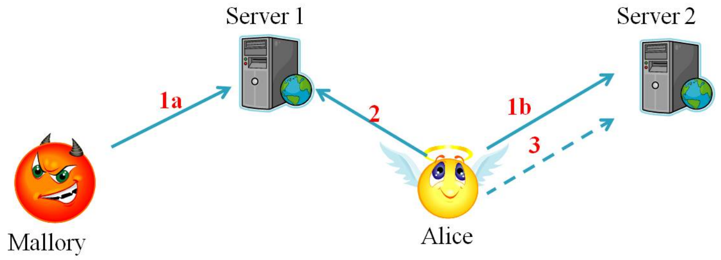
- You may answer in either Swedish or English.
- If any data is lacking, make (and state) reasonable assumptions.
- Use legible hand writing. If your answers cannot be read, you will receive zero points on that problem.
- Grading is done as follows.
  Grade 3 = 20–29 points,
  Grade 4 = 30–39 points,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

Good luck!

Martin, Paul & Christopher

Problem 1. You are an evil attacker that aims at bringing down the entire Internet. What should you reasonably direct your efforts towards, and which attack method should you select? Briefly explain how your selected attack method works and what you can do to maximize the success probability of your attack. (3 points)

Problem 2. Explain how a CSRF attack works. Also, name at least one countermeasure. You may refer to the picture below.



(3 points)

Problem 3. How can spammers bypass greylisting and nolisting? (3 points)

Problem 4. Explain how a DNS cache poisoning attack can realize a man-in-the-middle attack. (3 points)

Problem 5. Give a regular expression that checks if an input is a number and that the number is divisible by 4.
Hint: You may assume that the number has at least two digits. (3 points)

Problem 6. Give the Base64 encoding of the word "DKIM".

Hint: Decimal representation of ASCII characters is given by:

$$\text{A} = 65, \text{B} = 66, \ldots, \text{Z} = 90, \text{a} = 97, \text{b} = 98, \ldots, \text{z} = 122$$

The Base64 alphabet is:

$$0 = \text{A}, \ldots, 25 = \text{Z}, 26 = \text{a}, \ldots, 51 = \text{z}, 52 = 0, 53 = 1, \ldots, 61 = 9, 62 = +, 63 = /$$

(3 points)

Problem 7. Tor is a so called low-latency design for anonymous communication.

a) What is meant by this?

b) What drawbacks do low-latency designs have and how are they compensated?

(3 points)

Problem 8. In a remote file inclusion attack, the adversary tricks the PHP script to read a remote file and interpret its content. However, according to the same-origin policy one origin cannot read resources in other origins. Why doesn't the remote file inclusion attack violate the same-origin policy? (3 points)

Problem 9. Several new DNS records are used for DNSSEC, one of them is the DS record.

a) What is in a DNS DS record?

b) When is the information used?

c) How is the information used? (3 points)

Problem 10. Access to directories on a web server can be defined in the *httpd.conf* file and in a *.htaccess* file.

a) Determine who has access to the directories `/www` and `/www/dir` when the following directive is given in *httpd.conf* file and *.htaccess* files located in the directories:

```
httpd.conf
<Directory /www>
    AllowOverride None
    Order Deny,Allow
    Deny from lth.se
</Directory>
```

```
httpd.conf
<Directory /www/dir>
    AllowOverride All
    Order Deny,Allow
    Deny from all
</Directory>
```

```
.htaccess in /www
Allow from all
```

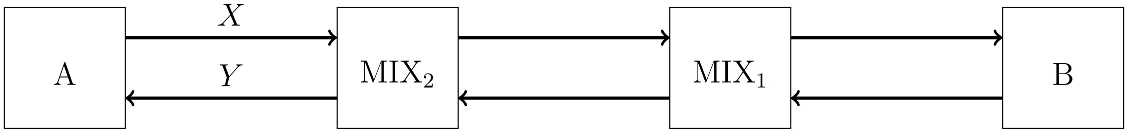
```
.htaccess in /www/dir
Allow from lth.se
```

b) How is access to the two directories affected if all `Order` directives are changed to `Order Allow,Deny`?

c) Give one reason why `.htaccess` files should not be used if not absolutely needed.

(3 points)

Problem 11. Consider anonymous emails using two Chaum mixes, MIX_1 and MIX_2. Alice with address A sends a message M_1 to Bob with address B, including an untraceable return address. Bob replies to Alice with the message M_2.



The keys K_1 and K_2 are the public keys of MIX_1 and MIX_2 respectively. The item X prepared by Alice and sent to MIX_2 is constructed as

$$X : K_2(R_2, K_1(R_1, K_B(R_0, M_1, \underbrace{K_1(R_4, K_2(R_3, A))}_{\text{Untraceable return address}}, K_X), B))$$

a) What is K_X and what is it used for?

b) What is the purpose of R_2?

c) Determine the item Y. (5 points)

Problem 12. Digest authentication (RFC2617) calculates the digest according to

$$\text{MD5}(\ \text{MD5}(A1) : \textit{nonce} : \textit{nc} : \textit{cnonce} : \textit{qop} : \text{MD5}(A2)\ ),$$

with

$$\begin{aligned} A1 &= \textit{username} : \textit{realm} : \textit{password}, \\ A2 &= \begin{cases} \textit{method} : URI & \text{if } \textit{qop} = \textit{auth}, \\ \textit{method} : URI : \text{MD5}(\textit{entity-body}) & \text{if } \textit{qop} = \textit{auth-int}. \end{cases} \end{aligned}$$

a) Explain the usage and purpose of the *realm* parameter.

b) Explain the usage and purpose of the *nc* parameter?

c) Explain the usage and purpose of the *cnonce* parameter?

d) For digest authentication to work as intended, the end-user must be *aware* that the server requires digest authentication for specific pages. How can a man-in-the-middle extract username and password from an unaware user? (5 points)

Problem 13. Consider a Hashcash solution in which a string

$$ver : bits : date : resource : rand : counter$$

is hashed using SHA-1, where

ver is version number (currently 1),
bits indicates how costly the function is for sender,
date gives current date,
resource is recipients email address,
rand is a random number (separates different senders).

A spammer wants to send 1000 messages $M_1, \ldots, M_{1000}$ to each and every recipient on his very large mailing list, and he plans on including a Hashcash header with each mail.

a) How many calls to SHA-1 does it take to *generate* a Hashcash header with $bits = 20$? Exactly or on average?

b) How many calls to SHA-1 does it take to *verify* a Hashcash header with $bits = 20$? Exactly or on average?

c) What prevents the spammer from using the same Hashcash header when sending the message M_1 to *all* recipients on his mailing list?

d) What prevents the spammer from using the same Hashcash header when sending all messages $M_1, \ldots, M_{1000}$ to *one* specific recipient? (5 points)

Problem 14. Briefly explain the following terms.

a) register_globals

b) Prepared statement

c) DKIM

d) SPF

e) Perfect forward secrecy (5 points)
