Final exam in

Web Security EITF05

Department of Electrical and Information Technology
Lund University

October 22nd, 2013, 8.00-13.00

- 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!

Paul & Martin

Problem 1. Compare the contents and usage of the MX and SPF records of a DNS server. (3 points)

Problem 2. Briefly explain how JavaScript comes into play in

a) AJAX,
b) DNS rebinding attacks,
c) HTTP response splitting attacks. (3 points)

Problem 3. Why is it typically a good idea to have random session IDs stored in e.g., cookies? Describe an attack that could work if the session ID is not random. (3 points)

Problem 4. DMARC encapsulates and adds funtionality to both DKIM and SPF.

a) What it the purpose of DKIM?
b) Why is DMARC better than DKIM and SPF put together.
c) How does alignment work with DKIM and SPF? (3 points)

Problem 5. Digest authentication (RFC2617) calculates the digest according to

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

with

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

A client request may resemble

```
GET /dir/index.html HTTP/1.0
Host: localhost
Authorization: Digest username="Mufasa",
                      realm="testrealm@host.com",
                      nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
                      uri="/dir/index.html",
                      qop=auth,
                      nc=00000001,
                      cnonce="0a4f113b",
                      response="6629fae49393a05397450978507c4ef1",
                      opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

a) Explain the usage and purpose of the MD5(*entity-body*) part?
b) Explain the usage and purpose of the *cnonce* parameter?
c) Why is Basic Digest Authentication insecure? (3 points)

Problem 6. Give a regular expression that checks if an input is an email address of a subdomain to either one of the three top-level domains `com`, `se` or `nu`. Assume that the email address only contains alphanumerical characters, where applicable. (3 points)

Problem 7. Two engineers walk into the Base64 Bar. Engineer A orders "QkVFUg==" and engineer B orders "Sk9MVA==". Who gets to drive the car on the way home?

Hint 1: Only one of the engineers drinks alcoholic beverages.
Hint 2: 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 8. Explain how Content Security Policy (CSP) is used to prevent XSS attacks. Where is the policy enforced? (2 + 1 points)

Problem 9. One possible php.ini setting is:

```
allow_url_include = 1
```

Describe the attack that requires this setting. What other conditions must be met for the attack to be possible? (3 points)

Problem 10. Consider the Domain Name System Security Extensions (DNSSEC).

a) What is the purpose of the NSEC record?
b) Do DNSSEC signatures need to be recalculated between requests from different users? Motivate your answer.
c) Explain one serious negative effect of employing DNSSEC. (3 points)

Problem 11. Password cracking using TMTO/Rainbow tables.

a) Explain how the chains of a TMTO/Rainbow table (choose one) are traversed when inverting a hashed password. Make sure that you mention the terms *start point, end point* and *reduction function*.
b) Compare the password cracking efficiency in the three cases of using
   i) no salt,
   ii) a unique salt for the entire site,
   iii) a unique salt per user. (2 + 3 points)

Problem 12. 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.

A spammer plans on including a Hashcash header with each mail she sends.

a) How is a *valid* Hashcash header with $bits = 30$ constructed?
b) How many calls to SHA-1 does it take to *generate* a Hashcash header with $bits = 30$? Exactly or on average?
c) How many calls to SHA-1 does it take to *verify* a Hashcash header with $bits = 30$? Exactly or on average?
d) Why are Hashcash headers with $bits = 80$ and $bits = 1$ impractical?
e) What is the purpose of the *rand* parameter? (5 points)

Hint: If x is a randomly chosen input and $h = \text{SHA-1}(x)$ is the corresponding 160-bit hash, then every bit position in h has value 0 or 1 with probability $\frac{1}{2}$.

Problem 13. A DNS cache poisoning attack can be very valuable if it is successful.

a) Explain how a DNS cache poisoning attack works.
b) How should DNS queries be constructed in order to minimize the success probability of the attack?
c) How would the attack be affected if queries were sent using TCP instead of UDP?

(5 points)

Problem 14. Briefly explain the following terms.

a) Greylisting
b) DS record
c) Same-origin policy
d) SMTP
e) DNS rebinding (5 points)
