Final exam in

Web Security EITF05

Department of Electrical and Information Technology
Lund University

October 19th, 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.

Answer
Attacking the root servers with a DNS amplification attack is one reasonable option. Using a bot net for a large scale attack will be necessary for this project to succeed, and using DNSSEC-enabled DNS servers will also increase the success probability. (3 points)

Problem 2.

Answer
1a: Mallory puts a script on webpage on Server 1.
1b: Alice logs in to Server 2 and obtains a session cookie.
The order of steps 1a and 1b is irrelevant.
2: Alice visits webpage on Server 1.
3: Mallory's script is executed on Alice's computer, sending a request to perform some action on Server 2.

CSRF protection on Server 2:

- Allowing only POST requests

- Requiring session ID to be sent in POST body or GET string as well as in the cookie.
- Check that referrer is as expected
- Make user reauthenticate before certain requests

CSRF protection on user-side:

- signing off

(3 points)

Problem 3.

Answer
A greylisting mailserver will look at (client ip, sender address, recipient address) and temporarily reject the message if the above triplet is previously unused. If recently used, it will accept the message. The spammer can implement a retry.
In nolisting, the first mail server listed in the MX record is non-existing. This can be circumvented by sending to the second mail server if the first one does not respond.
All-in-all, both defense mechanisms can be bypassed by following the protocol. (3 points)

Problem 4.

Answer
In the attack, the adversary injects fake anwers to a query hoping that the querying server will accept the IP in the answer as belonging to the queried name. If it accepts, the server will cache this answer and all subsequent questions will be answered with the wrong IP. Assume that IP_a corresponds to www.a.se but an attacker can poison a DNS cache so that queries to www.a.se instead are answered with IP_b, a computer controlled by the attacker. Then all HTTP requests to www.a.se are sent to IP_b and these can be intercepted by the attacker, read/modified, and then forwarded to IP_a. This could be used e.g., to eavesdrop passwords sent in clear, perform an SSL man-in-the-middle attack if anonymous Diffie-Hellman is used etc. (3 points)

Problem 5.

Answer
`^[0-9]*([02468][048]|[13579][26])$` (3 points)

Problem 6.

Answer
REtJTQ== (3 points)

Problem 7.

Answer
a) A low latency designs means that messages entering a Mix (or a router), leaves soon afterwards with very short delay.
b) The drawback is that the anonymity set is necessarily quite small. Compensation include using several mixes, have a high traffic volume, use synthetic traffic, and taking advantage of the small anonymity set that still exists, mixing packets that arrive within a short time period. (3 points)

Problem 8.

Answer
The same origin policy is implemented in browsers, while PHP scripts are interpreted by the server. (3 points)

Problem 9.

Answer

a) A hash of the DNSKEY.

b) The DS record is used when validating a DNSKEY.

c) The DS record of a DNSKEY is stored at the parent. To validate a DNSKEY, go to the parent and retrieve the corresponding DS record. Check that the hash of the DNSKEY matches the content of the DS record. To check the signature of the DS record, use the parents DNSKEY. To validate this DNSKEY, get the next parants corresponding DS record, and so on. Validation succeeds if a trusted DNSKEY is encountered along the way, typically at the top or root domain.

Problem 10.

Answer
a) `/www`: Everyone except computers from lth.se are allowed.
`/www/dir`: Only computers from lth.se are allowed access.
b) `/www`: Everyone is denied access.
`/www/dir`: Only computers from lth.se are allowed access.
c) They slow down access since the files are checked for each request. It can also be a security problem since users can make changes to the server. The administrator must be careful when deciding what chages are allowed. (3 points)

Problem 11.

Answer
a) It is a temporary public key belonging to A, used by B to encrypt the return message M_2.
b) It adds randomness to the message encrypted by K_1 so that it is not possible to take

the encrypted message part leaving MIX_2 towards MIX_1, encrypt it with K_2 and compare it with the input to MIX_2. Without R_2 it would be possible to track messages sent over MIX_2 (but not MIX_1).
c) Y is given by $R_3(R_4(K_X(R_5, M_2))), A$.

Problem 12.

Answer

a) A string explaining which password the user is expected to enter. Used as salt.

b) Nonce counter, starts at 1 and is incremented by one for every request. Prevents replay attacks.

c) A nonce that the client chooses. Prevents time-memory tradeoff attacks.

d) She can replace the digest authentication header with a basic authentication header. The user will then send username and password in cleartext (Base64-encoded).

Problem 13.

Answer

a) 2^{20} times on average.

b) Exactly once.

c) Recipient's email address is included in the hashed string.

d) Nothing prevents the spammer from constructing one Hashcash header that is valid for all messages, but the mail client on the user-side typically stores previously used headers so that they cannot be used more than once.

Problem 14.

Answer

a) A convenience setting in PHP that automatically declares PHP variables from the corresponding GET/POST request variables.

b) A technique used to avoid SQL-injection.

c) DomainKeys Identified Mail. Associates a domain name to an email – verification that the domain has not been spoofed. Also provides integrity protection.

d) Sender Policy Framework, DNS record that states which mail servers that are allowed to send emails from a given domain.

e) The property that session keys will not be compromised if a private key is leaked at some point in the future.
