INFORMATION SECURITY

What is actually the purpose of encrypting the values in a cookie?

Ask Question

I was researching on internet security. When I reached at

3

But an encryption can be easily decrypted by someone who can tamper the cookies. Considering the fact that if we have tampered the cookie, then whether it is encrypted or not, it is possible to access the session corresponding to that cookie. Then what is actually the purpose of encrypting the cookie?

encryption cookies tampering

asked Sep 15 '14 at 7:37

Anandu M Das
871 12 24 43

Can you explain the following bit? "...encryption can be easily decrypted by someone who can tamper the cookies." I'm not sure why you believe this, and I think there may be an assumption that is missing from the question, or perhaps different wording might be clearer. – Xander Sep 15 '14 at 13:43

What i meant is, if someone is able to tamper the cookies then he can see the encrypted values inside the cookie. (Obviously he can perform anything on cookie only if he can tamper the cookie) Now if he can identify the encryption used, then it is easy for him to decrypt the same. I don't think identifying the type of encryption might be a big deal. – Anandu M Das Sep 15 '14 at 13:59

I think you may be confusing "encrypting" with "encoding." As @Mark mentioned in his answer, a user who has an encrypted value cannot, in fact, decrypt it without the key, even if he knows everything else about how it was encrypted. – Xander Sep 15 '14 at 14:50

As I mention in a similar thread security.stackexchange.com/questions/113415/… Considering that each implementation of encryption is a potential failure, since it is so often done badly even by experts. I'd consider twice all decisions that lead me to have so sensitive information in cookies that I'd have to encrypt them. –

Home

Questions

Unanswered

2 Answers

9 ✓

If the encryption key is stored on the server, then only the server can decrypt the cookie, and only the server can make predictable changes to the cookie. An attacker can make changes to the cyphertext of the cookie, but they cannot know in advance what effect those changes will have. If the cookie additionally includes a message authentication code or other anti-tampering measure, then an attacker cannot make changes to an encrypted cookie without invalidating it.

Encrypting the cookie also keeps the user and others on the same computer from being able to see what information is being stored. This permits the server to associate sensitive information with a user (eg. "log me in automatically" information), without needing to track the session server-side.

Cookie encryption does nothing to keep cookie-stealing attacks from being used to impersonate a user; to defend against that, other measures are needed.

answered Sep 15 '14 at 7:58

Mark
31.9k 9 71 120

Perhaps with the addition that when you steal cookies to impersonate someone, it is very helpful to be able to manipulate the cookie or the session information. Encryption helps there. So it does 'something'. – Simply G. Feb 12 '16 at 7:01

For impersonation prevention, what are some things you could do? – Shawn Aug 30 '18 at 15:55

stackoverflow.com/questions/12233406/… – Mark Aug 30 '18 at 22:18

0

Cookies can be used for a variety of reasons. At the simplest level it might contain a random number that advises the site that you are the same person that visited previously, either for tracking purposes or to provide enhanced functionality such as user preferences. Such cookies do not need to be encrypted.

Encrypted cookies are used when you want to persist something client side that do you do not want changed and/or seen by a user. For example on the completion of an authentication process you will set an encrypted cookie containing details of the user to be presented with each subsequent request. This is what provides the appearance of a 'logged on session' when in fact the browser is making a series of otherwise unrelated atomic requests. In most large web sites this authenticated session management is handled by front end infrastructure services that hide this complexity from the application developer.

The cookie can also be used to contain current application state, which is useful if you application runs across multiple geographic sites and the user is expected to return to a another site before you have had a chance to replicate data there.

As to your last point, if you tamper with encrypted data you either cause the server side application to fail, or fail validation of the encrypted data.

answered Sep 15 '14 at 12:35

DodgyG33za
745 3 6