CUEH - Semester 2, ALL Task 1

January 2016

1 Authentication

This word comes up a lot in security. How do we know a person is who they say they are? How do we know a command is coming from a trusted source?

There are a wide range of solutions to these kidns of problems and each have their own characteristics.

This week, your group is testing the security of an implementation of hash-based message authentication codes (HMAC). The implementation is open and can be found here: `http://pastebin.com/giLsCWpn`

2 CUEH_HMAC_1

This is version one of the implementation.

The intended use is for verification of messages from clients to a server. For example, a mobile app allowing users to control their home lighting system.

To prevent unauthorised users from controlling the system, the app and the server share a secret key. When the client sends a message, it sends the plain text message, plus a digest made from a hash of the message combined with a secret key.

When the server recieves a message, it can take the message portion, hash it when combined with the secret and see if it matches the digest sent along with the message.

3 Your Task

You must explore the protocol and determine if it is fit for purpose.

Be aware thatthere might be more than one problem.

You should show a proof-of-concept attack if possible.

Answers should include soem notes on how to rectify problems.

4 Competition

In adition to the report you will produce, the first group to send me a message with a correct HMAC code that is produced by exploiting the protocol will be declared "the winners". There may be a (small, probably edible) prize.

In one use of the system, the following messages have been recorded:

```
25193|power up gigamatrix server
21084|install toaster updates
25136|realign singularity polishing buffers
14382|enhance undulation
23900|detatch porpoise
```

By email to csx239@coventry.ac.uk, your task is to send a new instruction that will be verified by the secret key.