University of Glasgow

Friday, 28 April 2017
9.30 am – 11.30 am
(Duration: 2 hours)

DEGREES OF MSc, MSci, MEng, BEng, BSc,MA and MA (Social Sciences)

Cyber Security Fundamentals (M)

(Answer All Questions)

This examination paper is worth a total of 60 marks

The use of a calculator is not permitted in this examination

INSTRUCTIONS TO INVIGILATORS

Please collect all exam question papers and exam answer scripts and retain for school to collect. Candidates must not remove exam question papers.

1. Two possible algorithms for steganography using digital images are the LSB algorithm and the BPCS algorithm. You can assume a 24 bit uncompressed image is the cover object for the purpose of your answers.

Compare and contrast the BCPS algorithm with the LSB algorithm in particular their use of bit manipulation.

[5]

Identify the steps the BPCS algorithm uses to achieve a higher capacity without compromising the stegoimage in the way a LSB algorithm using the four least significant bits would. In particular explain how the complexity calculation works.

[5]

2. A web application has been built which includes a page called delete.php located at http://www.coolsite.com/delete.php which deletes the account of a user who is currently logged in. You want to attempt a Cross Site Request Forgery attack which results in a user who is currently logged in having their account deleted.

(a) Giving sample HTML code where appropriate, explain the steps you would take to complete the attack in this scenario. In particular identify any conditions which must be true for the attack to work.

[5]

(b) Present the steps you would take if you were the owner of coolsite.com and wished to make your site robust to such attacks using challenge tokens. In particular explain how they can be implemented, and how they help mitigate a Cross Site Request Forgery attack.

[5]

3. You are at a coffee shop with a friend; they are using the free Wi-Fi which the coffee shop offers to its customers by providing the password when they purchase a beverage. Your friend is using the connection to access a website which they have an account for using a username and password, but the website does not use SSL. You know your friend uses the same password on multiple sites. You assert that this is a poor decision from a security point of view.

(a) Defend this position by describing a vulnerability the network is open to and provide an example of software which could be used to exploit this vulnerability as well as a brief indication of the possible impact of the attack.

[5]

(b) Your friend now agrees that this is problematic but still wishes to use the Wi-Fi. Describe a security mechanism they could use which could allow them to access the website more securely on any public network such as that provided by the coffee shop.

[5]

4. You overhear a colleague discussing the AES and they describe it as thus:

It's a symmetric key encryption where the key size is 56 and comprises an exclusive OR operation with the key followed by a minimum of 10 rounds of substitution and transposition.

You are aware this is incorrect.

(a) Critique this description by identifying the errors

[4]

(b) Correct each of the errors identified in a)

[4]

(c) After explaining this, your colleague claims that it doesn't matter, because everyone should just use public key encryption. Justify why this may not always be an appropriate choice.

[2]

(d) Write in Java a method which performs AES encryption on a `String s` given a `SecretKey key` using Electronic Code Book mode and PKCS5Padding. You can assume you do not need to deal with catching any exceptions. Pseudo code is acceptable so long as you can demonstrate you know and understand the appropriate engines and methods from the Java security packages.

[5]

(e) Your boss has decided you know more about cryptography, and has asked you to explain how the Diffe-Hellman algorithm works and why it is needed for symmetric encryption but not asymmetric.

[5]

5. In 2014 the Heartbleed bug was identified as a serious vulnerability in OpenSSL. Briefly summarise the security failure or failures which led to the Heartbleed bug, how the vulnerability could be exploited in an attack and what (if anything) could have prevented the incident highlighting how you think it would achieve this.

[10]