1)

a) Set the characters gold or health to a number greater than 9000 by

utilising a buffer overflow. How did you achieve this? Explain using

reference to bytes and ASCII as to what the exact value was that you

achieved.

Setting the name to: stephenabcZZZZZZ gives Gold: 1515870810

b) How could this exploit be prevented?

By limiting the number of characters read in the input stage to 9 chars + '\0' character.

c)Could this exploit be useful for more than just the game? Could it be

used to gain access to a system? If not, why not? If so, where might it

be used?

Yes. This is a typical buffer overflow. It can be used to potentially execute malicious code which can completely compromise the system especially if the game is running with higher permissions that the user currently has.

2)a)Why does the iCubeKinect system use an asymmetric cipher to verify

their DVD games? Would it be possible to use a symmetric cipher

instead?

If a symmetric cipher was used then the key would have to be in all gaming consoles otherwise the game would not be playable. This would essentially give everyone in the world the key defeating the point of using any cryptography or signature. An asymmetric cipher is used so that only they can sign it.

b) What problem exists in the iCubeKinect verification code? How could you make the machine execute any arbitrary DVD?

The code is only hashing 52 bytes, 'metadata' and 'content\_hash'. Malicious code could be put in the metadata, then using a birthday attack assuming thousands of available certificates the 'content\_hash' is changed as a nonce until the MD5 matches one of the valid MD5's then its RSA signature can be copied, making it valid.

c)How would you fix it? Would the security vulnerability be made less serious by using either a stronger hashing scheme (such as SHA-512) or a different asymmetric cipher?

No, SHA-512 or a different cipher would not change the security. It can be fixed by hashing the key-id at the front. ie) char \*cert\_hash=MD5(cert.key\_id + cert.metadata + cert.content\_hash); This would prevent a birthday attack assuming that the key\_id is unique.

1.3)

a)

b) No? Java has stack protection??? Check

c)Imagine you were exploiting a program that was running with escalated

privileges (i.e. could read sensitive files, modify other users settings and

so on) is it possible to obtain a BASH shell using buffer overflows? Be sure to explain what shellcode is and how the shellcode is executed.

Call system() or some other C function?

Look here: <http://www.phrack.com/issues.html?issue=49&id=14>

2)

a) Show how it is possible to log in as any user by performing an SQL injection attack on the username/password login page.

username = ….

password = a' OR 1==1 –

b)The website has been clued in on their major security problem and pre-

vented the previous attack. Is it possible to use the status query to work

out the password of one of the administrators Bobby?