

Digital Security

SEM2

SID:1626142

**MOD003264**

**Submitted: May 2017**

Contents

[Question 1 3](#_Toc511902620)

[1.1 Outline what cybercrime is and its cost to society, using real world examples and figures 3](#_Toc511902621)

[1.2 Describe the Act and how it safeguards digital security 3](#_Toc511902622)

[1.3 Describe the consequences of breaking the Act 3](#_Toc511902623)

[1.4 Provide real world examples of misuse of the Act 4](#_Toc511902624)

[Question 2 4](#_Toc511902625)

[2.1 Outline the risks of handling this sort of sensitive data 4](#_Toc511902626)

[2.2 explains how a security model, such as CIA, can infer trust in data handling 4](#_Toc511902627)

[2.3 use examples to compare and contrast symmetric encryption with asymmetric encryption 5](#_Toc511902628)

[2.4 recommend and justify an encryption algorithm for transferring student assignment reports to an examiner over the internet 5](#_Toc511902629)

[2.5 consider the longer term impact of increasing computing power on encryption 6](#_Toc511902630)

[Question 3 6](#_Toc511902631)

[3.1 Explain why complex code can be vulnerable to attack 6](#_Toc511902632)

[3.2 Describe OWASP, with relevance to secure coding 6](#_Toc511902633)

[3.3 using the OWASP Top 10, identifies *three*different attacks that hospital software applications might be vulnerable to; outlining why these vulnerabilities might exist, the potential impact upon the hospital and mitigation techniques to prevent an attack occurring 7](#_Toc511902634)

[References 8](#_Toc511902635)

# Question 1

## 1.1 Outline what cybercrime is and its cost to society, using real world examples and figures

Cybercrime has started since computers and the internet have been invented. As soon as people discovered that they could steal other people’s bank details and invade their personal life, they found ways to breach this “security”. In addition to this, it is found to be a massive problem nowadays, with a horrifying number of $600 billion loss a year, it certainly should be a big concern, states Gross (2018).



Although this problem remains, there isn’t a lot that authorities can do to tackle this problem with huge impact, due to its nature being the users fault. As far as authorities are concerned, all they can do is warn users on how to be safe around the internet. Norton Security Online (unk) describes that this can be broken down into two categories, damaging and exploiting.

## 1.2 Describe the Act and how it safeguards digital security

According to the legislation.gov.uk (1990) the act of Computer Misuse offences incorporates some subcategories such as the unauthorised access to computer material and unauthorised access with intent to commit or facilitate commission of further offences.  
The computer misuse act has been around since 1990 to “threat”, and James (2015) eagerly writes that it imposes authority to those who want to break the law in some way and hopefully prevent people from hacking. BBC (2014) implies that this laws provide security and protection towards the users.

Furthermore, we know that criminals without authorization will be prosecuted if restricted material is accessed or modified in any way. On the other hand, even though the law prosecutes computer misuse and hacking, there are people who are authorized to hack, such as penetration testers, for the benefit of controlling and putting down such hackers. That is one of the ways it safeguards digital security.

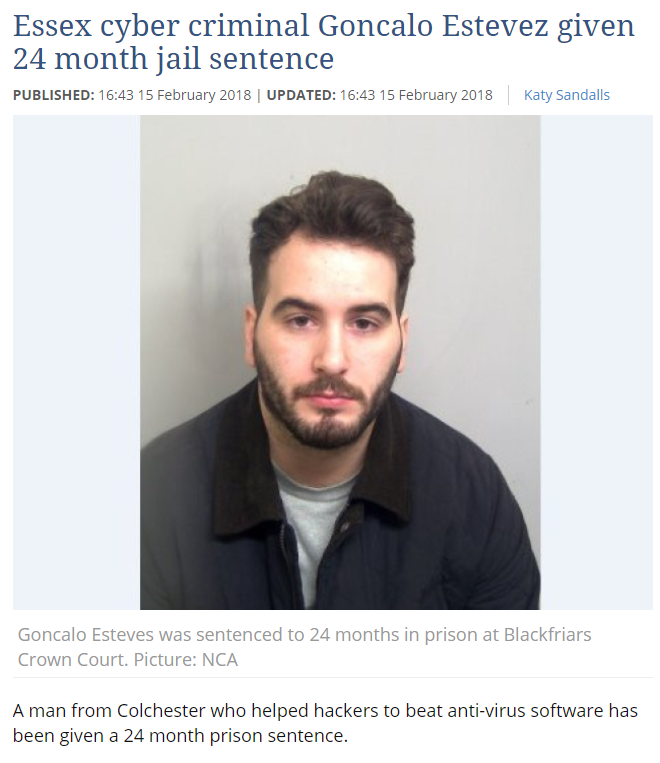
## 1.3 Describe the consequences of breaking the Act

Some of the offences and punishment will be on a table below, which were cited by legislation.gov.uk (1990):

|  |  |
| --- | --- |
| The offences | The punishment |
| Unauthorised access to a computer | 2 years of prison + and a fine up to 5000 pounds. |
| Unauthorised access to a computer in order to commit another offence | 10 years of prison & unlimited fine. |
| Unauthorised modification to the contents of a computer, or providing the tools in order to do so | 10 years of prison & unlimited fine. |

## 1.4 Provide real world examples of misuse of the Act

In this real world example given by Sandalls (2018) is a family friend of mine that happened not so long ago. Goncalo Estevez was young hacker from Colchester, who developed a software that would “sharpen the knives” of hackers, by testing if the hacking system they developed would beat anti-virus software or not. He was running a website called reFUD.me which is where he operated his “business” of selling that software. It was discovered that Goncalo made 32000 pounds off 800 paypal transactions, which indicates that he sold his software for around 40 pounds. Goncalo Estevez was known as KillaMuvz.



The Guardian (2017) reports that a hacker by the name of Adam Mudd, was only 16 when he developed a hacking program called Titanium Stresser. This program would perform a DDoS attack against an IP Address. It was reported that there was more than 112.000 registered users on Mudd’s program, who then have hacked about 666.000 IP addresses. Throughout his “hacking career” Adam has earned around 386.000 pounds from selling the program to cybercriminals around the globe.   
In the end, Adam was sentenced to 2 years of prison.



# Question 2

## 2.1 Outline the risks of handling this sort of sensitive data

Beaver (2015) has witnessed so many careless handling of data, and that most often will lead to a security breach. A survey managed by “The State of Data-Centric Security” has found that about 57% of IT professionals don’t understand where sensitive data is located. This being said, there is a lot of risks when it comes to handling sensitive data such which should always be considered.

## 2.2 explains how a security model, such as CIA, can infer trust in data handling

CIA, which stands for Central Intelligence Agency, is “…responsible for assisting the President and the US government in making decisions relating to national security.” CIA (2007). Assuming this, in order to provide security and to help make decisions in terms of whether someone goes to prison or not through analysing their case, CIA needs access to privacy.  
Through proving in court that someone is guilty, we trust that CIA uses that information only for proving whether someone is guilty or not.



## 2.3 use examples to compare and contrast symmetric encryption with asymmetric encryption

|  |  |
| --- | --- |
| Symmetric encryption | Asymmetric Encryption |
| When people receive a message, that message needs a single key to be shared | **In order to decrypt and encrypt, there needs to be a public and a private key when communicating** |
| This is an old technique | **This is a new technique** |
| This isn’t as useful as asymmetric | **It was introduced to “…complement the inherent problem of the need to share the key.” SSL2BUY (2017)** |
| Is shorter than asymmetric to apply | **Takes longer to apply** |
| Key Algorithms are AES, Blowfish, DES, Triple DES, Serpent and Twofish | **Key algorithms are RSA and DSA** |

## 2.4 recommend and justify an encryption algorithm for transferring student assignment reports to an examiner over the internet

The asymmetric encryption should be used for the school in terms of making sure the assignment reports are safe. There are a couple reasons that will be explained:

* It’s a popular encryption used wide over the internet



* Takes 2 keys to decrypt the message which makes security stronger
* Even though asymmetric takes longer to process, it shouldn’t matter given the fact that security should be priority over quick access. And in this example, quick access isn’t priority
* Asymmetric is the latest encryption algorithm, making it more fit to take on more recent hacker programs
* This allows to share the public key with someone else, whilst being safe at the same time as there are 2 keys.

## 2.5 consider the longer term impact of increasing computing power on encryption

Kaspersky (2013) affirms that encryption is essential to keep basic protection on their sensitive data.   
Some of the long term impacts that increasing computing power on encryption can provide are:

* Computer power would need more energy which, in the long term it will end up costing more money.
* Hiring more technicians to provide service when it comes to increasing the computing power on encryption, once again, can mean costing more money.
* Applications could take longer to answer, which means users can be led to frustration.
* Increase in computer power would allow the calculations of more complex algorithms possible, which then would lead to longer time for a brute force attack on a piece of data

# Question 3

## 3.1 Explain why complex code can be vulnerable to attack

Complex code as a lot of problems, and as hard as it is to believe, it definitely is more vulnerable to attacks. It is fact that the more lines a code possesses, the harder it is to debug, and therefore it has more security bugs, says McCabe (unk).  
In addition to this, it also has more interactions, which again, leads to more security bugs.   
Another problem that complex code has is that the longer the code, the harder it is to test it, which leads to untested portions of the code, which then can lead to insecurity and easy breaching.  
Finally, complex code is harder to design, configure, implement and use securely, which leads it to harder for users to understand it.

## 3.2 Describe OWASP, with relevance to secure coding

OWASP stands for Open Web Application Security Project, which is a “…organization focused on improving the security of software.” OWASP (2018).

According to the OWASP (2010) Secure Coding Practices Checklist, some of the input validation should:

* Conduct data validation on a trusted system
* Input rejection should be a result of validation failures
* Validate data length
* Validate data range
* Validate for expected data types

Moreover, the output encoding of the secure coding practice checklist is to:

* “Conduct all encoding on a trusted system”
* “Utilize a standard, tested routine for each type of outbound encoding”

Finally, some general coding practices should be:

* Everyone should be using tested code rather than using unmanaged code
* Restricting the users that access the code, to alter existing code or generate new one
* You must avoid all calculation errors, which involves understanding your programming language, the representation and the interaction with numeric calculation

## 3.3 using the OWASP Top 10, identifies *three*different attacks that hospital software applications might be vulnerable to; outlining why these vulnerabilities might exist, the potential impact upon the hospital and mitigation techniques to prevent an attack occurring

The following table will be filled in with the help of OWASP (2018) document.

|  |  |  |  |
| --- | --- | --- | --- |
| Type of attacks hospital software is vulnerable to | Why these vulnerabilities exist | Potential impact upon the hospital | Mitigation to prevent attacks |
| Injection | When the data that the user provides, which might not be validated, filtered or decontaminated by the application | Hospital might lose data, or data might get corrupted, even disclosure to unauthorised parties.  Also loss of accountability or denial of access. | The main option to mitigate this would be to use a safe API, which offers an interface that is parameterized. |
| Broken Authentication | Some of the permits would have default, weak or typically used passwords such as “123qweasdyxc, Password, admin/admin, etc”. | Stealing money, social security fraud, disclosing highly sensitive information or identity theft. | Implement strong passwords, align password lengths. When shipping or deploying, never use default credentials, especially for admin users. |
| Broken Access Control | CORS is misconfigured which allows unauthorized API access.  In addition, lack of automated detection and effective testing by developers | Similar to injection and broken authentication, the disclosure of sensitive information, or unauthorised access to certain information.  Also loss of records. | Deny by default, implement access control mechanisms.  Log access control failures with alerts to admins and JWT tokens should be invalidated on server after logout. |

# References

BBC, 2014. *How to prevent computer misuse.* [Online]   
Available at: http://www.bbc.co.uk/schools/gcsebitesize/ict/legal/1dataandcomputermisuserev2.shtml  
[Accessed 18 4 2018].

Beaver, K., 2015. *The Mishandling of Sensitive Data: Do You Really Know What You Don’t Know?.* [Online]   
Available at: https://securityintelligence.com/the-mishandling-of-sensitive-data-do-you-really-know-what-you-dont-know/  
[Accessed 18 4 2018].

CIA, 2007. *What We Do.* [Online]   
Available at: https://www.cia.gov/about-cia/todays-cia/what-we-do  
[Accessed 18 4 2018].

Gross, G., 2018. *The Cost of Cybercrime.* [Online]   
Available at: https://www.internetsociety.org/blog/2018/02/the-cost-of-cybercrime/  
[Accessed 09 04 2018].

James, S., 2015. *Can legislation stop cybercrime?.* [Online]   
Available at: https://www.computerweekly.com/opinion/Can-legislation-stop-cyber-crime  
[Accessed 18 4 2018].

Kaspersky, 2013. *Encryption: Five Major Benefits.* [Online]   
Available at: http://newsroom.kaspersky.eu/fr-be/news/news-article/article/encryption-five-major-benefits-2/?no\_cache=1&cHash=830e0de35b70a99fff12b2ab05405eae  
[Accessed 18 4 2018].

Legislation.gov.uk, 1990. *Computer Misuse Act 1990.* [Online]   
Available at: https://www.legislation.gov.uk/ukpga/1990/18/contents  
[Accessed 18 4 2018].

McCabe, unk. *More complex equals less secure.* [Online]   
Available at: http://www.mccabe.com/pdf/More%20Complex%20Equals%20Less%20Secure-McCabe.pdf  
[Accessed 18 4 2018].

Norton Security Online, Unknown. *What is Cybercrime?.* [Online]   
Available at: https://www.nortonsecurityonline.com/security-center/cybercrime.html  
[Accessed 09 04 2018].

OWASP, 2010. *Secure Coding Practices - Quick Reference Guide.* [Online]   
Available at: https://www.owasp.org/images/0/08/OWASP\_SCP\_Quick\_Reference\_Guide\_v2.pdf  
[Accessed 18 4 2018].

OWASP, 2017. *OWASP Top 10 Application Security Risks - 2017.* [Online]   
Available at: https://www.owasp.org/index.php/Category:OWASP\_Top\_Ten\_Project  
[Accessed 19 4 2018].

OWASP, 2018. *Welcome to OWASP.* [Online]   
Available at: https://www.owasp.org/index.php/Main\_Page  
[Accessed 18 4 2018].

Sandalls, K., 2018. *Essex cyber criminal Goncalo Estevez given 24 month jail sentence.* [Online]   
Available at: http://www.eadt.co.uk/news/essex-cyber-criminal-goncalo-estevez-given-24-month-jail-sentence-1-5396620  
[Accessed 18 4 2018].

SSL2BUY, 2017. *Symmetric vs. Asymmetric Encryption – What are differences?.* [Online]   
Available at: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences  
[Accessed 18 4 2018].

The Guardian, 2017. *Teenage hacker jailed for masterminding attacks on Sony and Microsoft.* [Online]   
Available at: https://www.theguardian.com/technology/2017/apr/25/teenage-hacker-adam-mudd-jailed-masterminding-attacks-sony-microsoft  
[Accessed 18 4 2018].