LETTERKENNY INSTITUTE OF TECHNOLOGY

ASSIGNMENT COVER SHEET

Lecturer’s Name: Danny Mc Fadden

Assessment Title: is modern security thwarting our ability to carry out forensics on mobile devices

Work to be submitted to: Danny Mc Fadden

Date for submission of work: 18/05/2022

Place and time for submitting work: online for 11:59 on the 18/05/20222

To be completed by the Student

Student’s Name: Stephen Duffy

Class: CSDF 2nd year

Subject/Module: Advanced digital forensics 2

Word Count (where applicable): 1364

I confirm that the work submitted has been produced solely through my own efforts.

Student’s signature: Stephen Duffy Date: 18 – 05 - 2022

|  |
| --- |
| **Notes:**  **Penalties:** The total marks available for an assessment is reduced by 15% for work submitted up to one week late. The total marks available are reduced by 30% for work up to two weeks late. Assessment work received more than two weeks late will receive a mark of zero. [Incidents of alleged plagiarism and cheating are dealt with in accordance with the Institute’s Assessment Regulations.]  **Plagiarism:** Presenting the ideas etc. of someone else without proper acknowledgement (see section L1 paragraph 8).  **Cheating:** The use of unauthorised material in a test, exam etc., unauthorised access to test matter, unauthorised collusion, dishonest behaviour in respect of assessments, and deliberate plagiarism (see section L1 paragraph 8).  **Continuous Assessment:** For students repeating an examination, marks awarded for continuous assessment, shall normally be carried forward from the original examination to the repeat examination. |
|  |

**Is modern security thwarting our ability to carry out forensics on mobile devices?**

How modern devices are encrypted

What is encryption? Encryption is taking information such as plaintext, intelligible numbers, sound, and images and encoding it in a way that it can’t be deciphered by an average person, ideally only authorized people and parties who encrypted or have access too can decipher the ciphered text back to its original form of information.

In modern technology today smart phones are encrypted when the data stored on the device is encoded. Today, AES is the most widely used encryption method used for mobile phone/app encryption, WIFI security and most VPNS to date. Although there is other methods that are not as popular such as RSA (Rivest Shamir aldermen), Triple DES (Data encryption standard) and Twofish.

The passcode needed to access the mobile device on its home screen is more than oftenly used to lock and unlock encrypted phones. Some phones, particularly later/the newest iPhones, additionally have a secure computer chip with a hardware key.

When it comes to encrypting your device If you don’t have a newer android or iPhone you will have to manually encrypt it yourself via the settings on the mobile device, although if you are in possession of a more up to date android or iPhone it will more than likely be encrypted by default and you don’t have to worry about your information not being encoded although this cannot be said for cheap phones that you may pick up from your local store as they are normally not encrypted in any shape or form.

What Security is used?

The security used to encrypt your device is as mentioned before AES, AES stands for Advanced Encryption Standard, it is an algorithm that was created by the US national institute off standards and technology in 2001 for the purpose of protecting your information or any information stored on a mobile device so that it cannot be accessed by any unauthorized users that may try to gain access. The algorithm uses a symmetric block cipher algorithm using difference block sizes to cipher your information by converting them into blocks of keys and joining them together to construct the ciphered text.

How is security implemented?

Mobile device security is implemented in many different ways such as optional/default encoding encryption, passwords, face recognition, VPNs, AVs, Your operating system, and fingerprint scanners.

All these methods were implemented in their own way to fight against their own battles. Each security method has its own use. Security methods such as face recognition, passwords, and fingerprint scanners were implemented to stop unauthorized people around you or maybe someone who has stolen your device and is trying to gain access to stop them from doing so.

Passwords are the most common type of security that is implemented as you are normally prompted in entering a password for the first time that you turn on your new phone, it’s a simple method that can be easily remembered and effective in it’s use of security as with this method, data is converted into encrypted code that can only be accessed by authorised users.

Who has the ability to decrypt?

When it comes down to who has the ability to full decrypt a device it normally only comes down to the authorised user who originally decrypted their device using their security method such as facial recognition or even a password but also the company that made the device and encryption method that is used on it.

Although unless under extreme terms you will be the only person who will have the ability to decrypt your information.

When you lock your phone after using it, it encrypts all the contents of the device, even if someone tried to pull all of your information or data off the phone it would just be plain ciphered text that is basically gibberish and would be completely unable to be read unless you knew how to uncypher the text which very little people have access/the knowledge to do so.

Deciphering all this data would require a key that only appears when your phone is unlocked with a password, Mobile Phones now provide many layers of protection as well as separate encryption keys for different degrees of sensitive data. Many keys are associated with device unlocking, but the most sensitive require further authentication.

The operating system and some specific hardware are in charge of handling all of those keys as well as the capacity to handle all of the administration permissions for that, so you don't have to worry about it.

Associated vulnerabilities with mobile security

When it comes down the mobile security vulnerabilities there is 4 different types to be aware of such as network vulnerabilities, operating system vulnerabilities, human vulnerabilities and process vulnerabilities, examples of these may be unencrypted data on a network, hidden bugs that were discord in the operating system, human vulnerabilities such as lacking knowledge and being a target of phishing attacks or connecting to an unsecure public network or maybe even a fault in the encryption of the device itself.

A great example of the fault of an encryption of a device would be the Samsung galaxy incident back in early 2021. According to Tel Aviv university research paper 100 million android devices suffered from a serious encryption flaw due to Samsung’s attempt of implementing a portion of the android trusted execution environment which led to almost 100 million devices being vulnerable to initialization vector reuse attacks, this was caused by an issue using keys that could allow attackers to replace the ivs into key parameters and replace them with their own instead of a random one that Is normally generated by their Keymaster TA using an IV (initialization vector) since Keymaster was on all Samsung devices and now can have their randomly generated key replaced, hackers/attackers could spoof keys and now decrypt this supposedly secure information and now gain access illicitly to any Samsung device of their choosing due to this seriously overlooked situation which took several several months to receive a patch and fix these devices only if they were kept updated leaving them extremely vulnerable for those long months and even now if they didn’t keep their devices up to date.

The main reason this was such a problem was that if an attacker made a successful IV attack on the Samsung device or even multiple, they could gain root access to the device and install any malware or malicious software off there choosing and give it administrative/root permission and run it on the device with no way to defend it as it is on a android kernel level which is the root of the android OS

Website References:

<https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption>

<https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture8.pdf>

<https://www.techrepublic.com/article/100-million-samsung-phones-affected-by-encryption-weakness>