COMP307 Assignment 1

Encryption/Decryption

September 5, 2018 Written by: Kevin Ma (#300867968) | Ostap Hamarnyk (#300836326)

1. Pick a secret message with minimum 5 words between 10 and 20 characters long (don’t show it here).
2. Use the link: http://inventwithpython.com/cipherwheel/ to encrypt the message (rotate the outer wheel and note the number where the outer letter A (with a dot) lands. Write down the encrypted message using that fixed position of the wheel going from outer circle to inner circle.

**Encrypted Message**

*EJ PDA BQPQNA E SWJP PK XA W OAYQNEPU OLAYEWHEOP*

**Key**

*22*

1. Pick a “Decryption Partner” (for him/her you will be his/her “Encryption Partner”).

**Decrypted Message**

*IN THE FUTURE I WANT TO BE A SECURITY SPECIALIST*

1. Repeat the above exercises with Caesar cipher with your partner. (5)

**Encrypted Message**

*QFMDHCUFODVM WG O JSFM RWTTWQIZH HCDWQ HC AOGHSF*

**Shift Amount**

*14*

**Decrypted Message**

*CRYPTOGRAPHY IS A VERY DIFFICULT TOPIC TO MASTER*

1. Research and list at least four good Software security best practices and their related threats. Each practice must be accompanied by a short (one or two sentences) explanation.

Defining a good security strategy is the challenge that every modern organization faces, and it is crucial to follow best practices when it comes to software security. If any of those rules are ignored or misunderstood it may negatively affect the business. Here we will list some common threats and their related software security best practices:

**Threat #1:** Security Misconfiguration

**Best Practice:**

* Attackers usually use automation (bots, scripts etc.) to detect open ports, security misconfiguration etc. It is always a good practice to automate daily security tasks to run analysis on firewall changes as well as security configuration. Otherwise, manual techniques might not be able to detect an attack and react accordingly.

**Threat #2:** Exploitation of known vulnerabilities

**Best Practice:**

* If software or systems use old or outdated software, users with malicious intent can break into the system and cause damage to the system by abusing known vulnerabilities. To circumvent this, one could employ the software security best practice of keeping their systems up to date and patched with the newest updates.

**Threat #3:** Privilege Escalation

**Best Practice:**

* It is crucial to ensure that privileges given to both individuals and systems are the minimum required to perform the job. If user require some extra functionality he/she should submit a request to specific group of people who can verify that application and install it securely on user's machine.

**Threat #4:** Security Breach

**Best Practice:**

* One of the most common security best practices is to implement proper network segmentation. Once the security breach happens, the attacker won't have access to sensitive data and other important configuration settings to move forward. Also, it is quite helpful to develop an Incident Report plan to mitigate the attacks with minimum losses.