CYBER SAFE

Bilal Abu-Ghazaleh
Senior Project, Computer Science Yale University 2019
Advisor: Stephen Slade

A. The need for cyber-security

Technology and computers exist all around us. We rely heavily on these machines for a variety of tasks ranging from entertainment to sensitive data storage. These devices are necessary for our academic survival in the 21st century. We spend on average about 5 hours a day connected to the internet and many more hours offline on these devices.[1] We use these devices to communicate with friends and family but also with professors and students. A student is expected to check their email at least a few times a day; it is also the norm to check texts and other forms of instant messaging at least once every few waking hours. We store our assignments, our data for our classes but also our personal, private data on the devices that have become ubiquitous.

Cybercrimes are on the rise globally. It is believed that cybercrime cost the world economy as much as $600 billion in 2017 alone.[2] In the past cybercrimes were committed only by experts in the field. Today, any person with internet access can download a set of tools that would allow him/her to gain unauthorized access to a system. Although technology is everywhere, people seem to remain unaware of the dangers and vulnerabilities that it entails. They refuse to update their software to patch a security flaw, passwords are overwhelmingly weak simply because it is a nuisance to take the necessary precautions.

[1] https://www.telegraph.co.uk/news/2018/08/01/decade-smartphones-now-spend-entire-day-every-week-online/

[2] https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html

B. What is CyberSafe?

CyberSafe is a computer program design to **evaluate**, **eliminate** and **alert** the user of existing security flaws in their computer. CyberSafe is designed and tailored specifically for Apple OS X computers. This is because it is aimed at educating college students of the vulnerabilities that exist in the system and teach them best cyber-security practices. The program performs a security audit of the computer and returns to the user a human readable, simple set of messages and instructions.

C. User Guide

D. How CyberSafe works

1. It checks for remote connections:

That is, the program checks whether any person or software is connected to the user's computer remotely (either using SSH, remote sharing or any other remote connection). The remote connection could potentially allow a malicious user to perform any action the computer owner could. Remote connections such as these would allow a malicious user to access data, passwords (both online and offline) as well as create, delete or modify any existing files and much more. The user has the option of terminating the connection by typing "y".

Technical details: This is first done by identifying the current user's UID. It then runs the bash command "who" to check any active connection, remote or local. It then cross lists the connections with the UID and verifies that they are all legal, local connections. If a remote connection (of any type) is detected, the user is alerted of the IP address origin and given the option to terminate the connection. The connection is terminated using the "kill" command and the PID of the connection.

2. It checks camera monitoring:

This checks all programs currently accessing the computer's camera. It then cross references these programs with a list of allowed programs. If a program is found to be accessing the camera and is not on the list of approved programs, the user is immediately alerted (with the name of the program) and given the option to terminate it. If a malicious program is monitoring and/or recording a user’s camera, this is a serious breach of security and privacy. This check is therefore essential.

Technical details: the bash command “"lsof | grep -e \"VDC\" -e \"AppleCamera\" -e \"iSight\"” is run. Lsof list all processes currently running on the computer. Grep then searches for VDC, AppleCamera and iSight, thereby making the check compatible with all operating systems created in the last 10 years. It then cross lists all the programs currently accessing the camera with the legal programs. It then terminates the unauthorized processes using the “kill” command and PID of all illegal programs, after alerting the user.

3. Encryption check:

The program checks whether encrypting is enabled on the user’s computer and alerts them of the result. If the computer is not encrypted, the user is presented with a set of detailed instructions and a link on how to enable FileVault- Apple’s built in encryption software.

Technical details: the program uses the bash command “fdesetup status” to check the status of the encryption. If it is on, the user is praised. If it is turned off, a user gets a set of instructions that they are recommended to follow.

4. Firewall check:

The program checks whether firewall is enabled on the user’s computer and alerts them of the result. If the Firewall is not turned on, the user is presented with a set of detailed instructions and a link on how to enable Apple’s built in Firewall software.

Technical details: in a similar manner to encryption, the program uses the bash command defaults read “/Library/Preferences/com.apple.alf globalstate” to check the status of the Firewall. If it is on, the user is praised. If it is turned off, a user gets a set of instructions that they are recommended to follow.

5. **Software update check:**

The program check whether the computer software is up to date. New security flaws are discovered on a daily basis and patches for these flaws appear in the security updates. It is therefore good practice to update the software whenever a new version is available. If the software is up to date, the user is praised. If it is not, the user is presented with a set of instructions and a link explaining how to update the software.

Technical details: the bash command “softwareupdate -l” is run and the program checks if an update is needed by using the command “grep -Eo 'Software Update found the following new or updated” on the output of the previous command.

6. DNS check:

The program check whether a DNS server is in use. DNS servers such as google's are important because they offer phishing protection and stronger security against things like DNS poisoning, spoofing and DDoS attacks. It is therefore good practice to use a DNS server. If a DNS server is in use, the user is praised. If it is not, the user is presented with a set of instructions and a link explaining how to set one up.

Technical details: the bash command “networksetup -getdnsservers Wi-Fi” is run and the program checks if a DNS is in use.

7. Password security:

Acknowledgments