Jonathon Scott

CPE 321 - 02

Introduction to Computer Security

Professor Phillip Nico

Lab 1

April 14, 2017

System Description and Environment

The computer system that I'm going to use audit is my personal MacBook. I carry the laptop with me wherever I go, it has a dedicated space within my backpack. I used to complete coursework as a computer science student by connecting wirelessly to the unix servers. Other primary uses include YouTube, Gmail, and Google Drive. I am the primary user of the device, other people only use the device under my supervision. The computer is typically exposed to indoor room temperature environments, but occasionally it is used outdoors.

Specifications
Model: MacBook Air (11-inch, Mid 2013)
Operating System: El Capitan version 10.11.2
Processor: 1.3 GHz Intel Core i5
Memory: 4 GB 1600 MHz DDR3
Graphics: Intel HD Graphics 5000 1536 MB

Security Audit

Threat #1	Data sent over a wireless network could be intercepted.
Goals Violated	Confidentiality: Confidential banking, personally identifiable, and account login information could be exposed.
Vulnerabilities	Networks permit a large number of connections, difficult to regulate the flow of data.
Controls	General: Only connect to known, password protected wireless networks.

Threat #2	Computer could be stolen and course work lost.
Goals Violated	Confidentiality: Personally identifiable information could be exposed to the thief. Availability: The primary tool for completing coursework would no longer be available and mobile. In progress project data would be lost.
Vulnerabilities	Laptops are small, lightweight, and expensive. Prime targets for a thief
Controls	General: When not in use, laptop is kept inside backpack on person at all times. When sleeping, backpack is in locked apartment and inside bedroom with owner.

	Confidentiality: The laptop is password protected using a passphrase not derivative of any part of the owner’s personal data (i.e. date of birth, initials, or address) Availability: Coursework is often completed using Google Drive and associated applications or external servers. This work would still be available should the laptop no longer be physically present.

Threat #3	Hardware could malfunction.
Goals Violated	Availability: Depending upon the malfunction, the laptop may be reduced to an unusable state in need of repairs. Integrity: Depending upon the malfunction, the laptop could still appear to be functional but instead merely appear to be so and incorrectly storing data. The malfunction may or may not be apparent to the user, but the validity of an operation performed would be subject to question.
Vulnerabilities	Hardware is made of physical components and is thus responsive to the environment in which the device is being used.
Controls	Availability: Laptop is kept in a laptop case with a foam cushion to protect it from minor impacts. Majority of use is done indoors at room temperature, unexposed to weather (particularly rain and wind).

Threat #4	Social media & email accounts could be compromised.
Goals Violated	Availability: Compromised accounts could have their passwords changed and would be unavailable to the original owner. Integrity: The thief could impersonate the owner and distribute messages to contacts. Content and views that the owner would not condone could be distributed. Confidentiality: Personal information of contacts would be exposed to the thief.
Vulnerabilities	For convenience, the laptop has been set to save login information for commonly visited sites (i.e. Facebook, Google calendar, Gmail).
Controls	General: Owner is aware of the laptop’s location at all times, it never leaves his side (as far as he knows). Confidentiality: Passwords are habitually changed every three months.

Threat #5	On board camera could record while owner is unaware
Goals Violated	Confidentiality: The owner could be watched while under the assumption of privacy.
Vulnerabilities	The laptop has a video camera.
Controls	

Threat #6	Someone could look over the user's shoulder while the user is unaware.
Goals Violated	Confidentiality: Any activities the user completes would be witnessed by the observer, including the viewing of any personally identifiable or confidential information. Coursework covered under a non-collaboration agreement could be unintentionally shared and result in academic dishonesty.
Vulnerabilities	Computer screens are bright and tend to draw eyes towards them. Humans are curious.
Controls	Confidentiality: When choosing a location to work, preference is given to locations where people cannot be behind the user (a corner or wall within five feet the user's back) . The brightness of the screen could be turned down to reduce its visible distance.

Threat #7	The laptop could be dropped from a height that causes damage the screen or hardware.
Goals Violated	Availability: A laptop with a broken screen is unusable.
Vulnerabilities	I watch netflix while in bed with the laptop. The laptop could be pushed off the bed while tossing and turning at night.
Controls	General: When sleep is near, I close the laptop and set it on a dresser underneath my bed.

Risk Evaluation

The use of the computer system is of a medium risk, with confidentiality as the most common goal being violated. In general, the control measures are minimal, but the only reason the use of the system is not high risk is because that which is being protect, a single individual's information and work, would not warrant extensive security precautions. There is most certainly room for improvement.

Several security precautions have been circumvented for the sake of convenience and other threats have weak or no controls to manage the risk of the vulnerability. For example, when the camera is not being used, it could be physically covered with tape in order to prevent it from recording. The proximity of the device to the owner is a good physical precaution but runs the risk of human error (not paying attention to the laptop in public or the entire backpack being stolen). The completion of coursework through third parties increases the availability of any data that may be lost, but also puts faith on unexamined computer systems that could have unexamined security implications. In order to further reduce the risk of using this machine, I should invest in purchasing a more rigid case to protect the laptop from weather and gravity and use an external hard drive for backups. Additionally, I should logout of accounts when ending a session and I should not permit other people to use my device.