Introduction to IT Security
Homework 1

Abraham Murciano

August 27, 2020

1 Current Real World Security Situation

We are to select a week within the past twelve weeks and discuss two cyber attacks or security vulnerabilities which occurred on that week. We shall choose the last week of July 2020.

1.1 Celebrity Twitter Hack

A seventeen year old from Florida by the name Graham Ivan Clark, along with a couple of his friends – Mason John Sheppard, 19, of the United Kingdom, and Nima Fazeli, 22, of Orlando, Florida – succeeded in breaching the accounts of many celebrities on Twitter. They used their ill-obtained access to request bitcoin from the public with the promise of returning double the amount.

They are considered black hat hackers, since their intent was of criminal nature, and had no permission to access their targets' Twitter accounts.

Their motive was to steal money from the general public by exploiting their trust in the integrity of certain famous individuals such as Elon Musk and Barak Obama.

The attack surface they used was an employee who had access to credentials for Twitter's customer service portal. The vulnerability which they targeted was said employee's trust. Clark contacted her and led her to believe that he was a co-worker from the technology department, thus convincing her that it was safe for her to share the secret credentials to the portal.

From there they could attack many different assets. They could access the email addresses and/or phone numbers of many Twitter users, they could steal their usernames and sell them (which they also did), they could also post anything out to the public as if it was posted by any other Twitter user.

All three of the C.I.A. (confidentiality, integrity, and availability) values could have been attacked by this breach.

Confidentiality of the Twitter users could have been attacked since the attackers could have gained access to their email addresses, phone numbers and any other confidential data that twitter stores about its users.

Integrity was attacked, since the hackers posted some tweets which appeared to be written by certain famous people, but were in fact not written by them. Thus causing Twitter to display false information to all of its users.

Availability was also attacked, since the attackers stole the usernames of ten users with unique usernames such as @drug, @w, and @L, and sold them. Therefore the availability of the accounts of these ten people was compromised.

More information on this attack can be found here.

1.2 Vulnerability in IoT Devices

IBM's cyber security team, X-Force Red, recently publicized a vulnerability present in an IoT module used in many different IoT devices which would allow hackers to remotely control all sorts of devices.

X-Force Red are white hat hackers, since they are hired to perform penetration testing on their clients' systems, and their intention is to find and secure vulnerabilities. As their slogan states, "Our mission: Hacking anything to secure everything".

Attack surfaces for this particular attack depend on the device which uses the vulnerable IoT module. Some require physical access whereas some allow for the attack to be performed via a 3G or 4G connection. The attack works by attempting to access a hidden file, which is supposedly restricted by the system. However, X-Force Red found a workaround enabling them to access the company's code which may contain secret information such as passwords. Additionally, they are able to replace the Java code that is running on the module, giving them full remote control over the device.

The vulnerability consisted of a security check whose purpose was to prevent access to hidden files (files that begin with a full stop). The condition checked that the fourth character of the file path (which may look something like this: `a:/.hidden-file`) is a full stop. However an attacker could cause it to try to access a file such as `a://.hidden-file`. This would not be caught by the security check, and then the second slash would be ignored when searching for the file. This would enable anyone to bypass this security check.

As we briefly mentioned above, the threatened assets include:

- The company code's logic, which may in turn contain some sensitive data such as passwords.

- Complete remote control of the vulnerable device. This ranges anywhere from overdosing or underdosing diabetic patients who rely on a vulnerable insulin pump, to interfering with electricity meters causing city-wide power-cuts.

All three of the C.I.A. values could be attacked.

Confidentiality can be compromised by stealing the company's code, as mentioned above, or by stealing any of the user's data that the device may have access to. For example, an insulin pump will have access to the user's insulin levels, which can be used to get a rough idea of the user's eating and exercising habits.

Integrity can also be targeted, since for example an attacker can make an electricity meter report erroneous data to the electric company, causing the user to pay more or less for the electricity they consume.

Availability is also under attack. As we mentioned above, power outages – i.e. unavailability of electricity – can be caused by exploiting this vulnerability.

More information on this vulnerability can be found here.

2 Threat Assessment

Below is a threat assessment which analyses four threats on my personal computer. Some of the fields include a numerical assessment, in which case the range is provided in the form (x, y), where x is the lowest value for that field and y is the highest. For risk priority, each of the four vulnerabilities will be assigned a unique integer, where the lower the number the higher the priority.

1. **Asset** The password manager which is on my computer.

   Threat An attacker who succeeds in controlling my computer remotely or physically can access or take control of any of the accounts whose credentials are stored in the password manager, which would allow them to see all my passwords to these accounts.

   Likelihood (1-5) 3

   Consequence (1-6) 2 – Complete control of all my accounts can be lost, which can lead to identity theft, and even bank robbery.

   Risk Level (4-1) 2

   Risk Priority 1

2. **Asset** My personal computer is always signed in to many online accounts, such as my email or social media applications.

Threat A hacker who gains access to my computer can access or take control of any of these accounts, which would allow them to see lots of my personal information and to falsely communicate with other people via those means in my name.

Likelihood (1-5) 2

Consequence (1-6) 3 – Complete control of these accounts can be lost, which can lead to identity theft.

Risk Level (4-1) 2

Risk Priority 2

3. **Asset** Confidential files which are stored on my computer.

   Threat An individual with malicious intent who gains access to my confidential files can leak them onto the internet or threaten to do so in order to blackmail me.

   Likelihood (1-5) 1

   Consequence (1-6) 1 – The files on my computer aren't confidential enough to warrant giving in to blackmail, nor is it there anything too private that I would not want them available to the public.

   Risk Level (4-1) 4

   Risk Priority 4

4. **Asset** Work files which have not been backed up.

   Threat A hacker can encrypt my files and hold them at ransom.

   Likelihood (1-5) 1

   Consequence (1-6) 2 – Most of the files I work on I back up to cloud services within a couple of days of creating them. So if a hacker did succeed in targeting me with ransomware, there would likely be nothing that I would be willing to pay a ransom for, and the attack would amount to not much more than a nuisance.

   Risk Level (4-1) 3

   Risk Priority 3