Seunghyuk Baek

Sbaek44@vt.edu

ECE5480 HW1

1. In your own words, describe and distinguish between vulnerability, threat, and control.

- Vulnerability: A weak point of a system that can be exploited by an attacker
- Threat: A scenario or circumstance that may cause harm to a system. An attacker exploits vulnerability to cause threat
- Control: Any methods that cause reduction of vulnerability

2. Find one real-world example of a cybersecurity attack that happened AFTER 1 January 2018 and that violated at least one of the cybersecurity principles CIA. This attack must be an attack against some element of an IOT system. In your own words, state:

A. Name of the attack

- DNS hijacking

B. Date of the attack

- Aug 10, 2018

C. Description of the attack

- Hackers infiltrated end-users' modem or router and changed its DNS server to malicious DNS server which redirects end-users to fake banking sites.

D. CIA principle violated

- Confidentiality: A hacker could alter DNS server of the uses' router without permission
- Integrity: DNS server information was altered.

E. What was the vulnerability the attack exploited?

- The device couldn't differentiate authorized url to remote access its configuration from unauthorized url.

F. What system or who was attacked?

- The Brazilian end-users using DLink DSL modem routers.

G. Attack citation

"https://www.scmagazine.com/home/network-security/brazilian-banking-customers-targeted-by-iot-dns-hijacking-attacks/"

3. Write a technical summary

Introduction

"Learning Internet-of-Things Security" Hands-On" by Kolias , Constantinos., et al (https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=919708). This case study journal is to demonstrate the possible IoT security bleaching of simple smart systems made with off-the shelf products. The authors mention vulnerabilities of each samples system and possible harm to users.

Description

The goal of this paper is to demonstrate possible security attacks on network systems containing IoT devices. By experimenting with simple systems built with off-the shelf devices. The journal diagnoses vulnerabilities of each system and analyze the main cause of their vulnerabilities. In addition, possible harm to an end user also described for each system. To begin with, personal identifiable information leakage was evaluated with iBeacon. This example follows a scenario that location data and UUID of a person's smartphone or other smart devices always broadcast the location and UUID to other devices. This example can be a convenient method for smart light bulb which may react to a user's present in an office room by turning light on with personalized light strength. However, since the receiver detect a user via Wi-Fi medium, an attacker can execute DoS attack to interrupt light bulb's function. Also, exposed location can cause leakage of user privacy. The next system contains a physical sensor to detect certain change in surrounding environment. Sometimes, these sensors can give data to potential criminals. For example, change in temperature of a house can indicate whether the householder is at home or not. The vulnerability of such system can be caused by poorly designed UI application or limitation of IoT devices. In most case, IoT devices possess less processing and storage power than traditional computer such as desktop or laptop. This leads to minimalized security which is the vulnerable point for an attacker. The last system that the authors built was an automated device connected to cloud service. In the sample system, a user's fitness smart device detects the user's sleep pattern and prepare food before he or she awakes in the morning. Since a cooker or fitness device lacks proper UI and database, cloud is used to control and configure the system. In this case, the researchers used UPnP devices, which makes sense since such devices will be used by only one owner or not considered as the device that contains sensitive privacy. However, UPnP devices will allow insecure connection to any anonymous which increase vulnerability. In addition, connecting a device to a cloud service increase the surface of the system making even more vulnerable to threat.

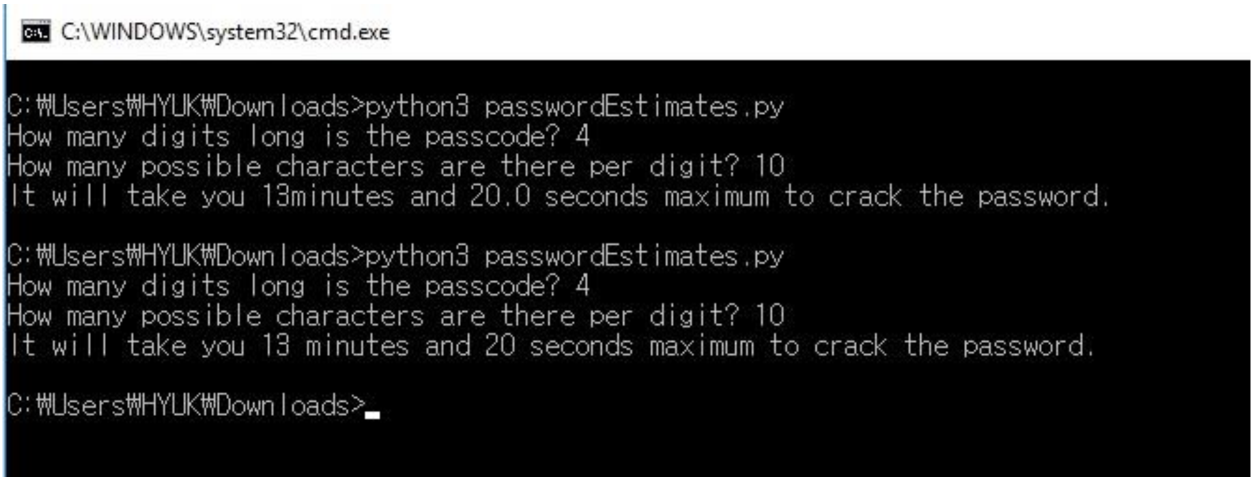
Analysis

This journal states possible vulnerabilities and treats of simple computer network systems with IoT device involved. By using off-the shelf devices the authors clearly presented that IoT security is the main concern not only for IT companies but also for end-users. Most IoT devices nowadays have very limited capability compare to desktop computers. This hinders IoT service providers to fortify barrier against malicious attacks. Privacy information of end users has been main attack point for hackers for long time. However, increase of smart home devices expanded vulnerable point of our life.

Conclusion

Smart device or IoT is growing rapidly even at this moment. However, it seems lack of security base due to the limitation of processing power of the devices. Also, there is no standard protocol that gives extended security coverage to all of these IoT devices.

4. How many minutes would it take, maximum, to crack a 4 digit passcode if each digit could be one of ten possible numeric digits (eg 0-9)?



```
C:₩Users₩HYUK₩Downloads>python3 passwordEstimates.py
How many digits long is the passcode? 4
How many possible characters are there per digit? 10
It will take you 13minutes and 20.0 seconds maximum to crack the password.

C:₩Users₩HYUK₩Downloads>python3 passwordEstimates.py
How many digits long is the passcode? 4
How many possible characters are there per digit? 10
It will take you 13 minutes and 20 seconds maximum to crack the password.

C:₩Users₩HYUK₩Downloads>_
```

```
def numberPossiblePasswords(numDigits, numPossiblePerDigit):
 numPasswords = numPossiblePerDigit**numDigits
 return numPasswords

def maxSecondsToCrack(numPossiblePasswords, secPerAttempt):
 time = numPossiblePasswords*secPerAttempt
 return time
nd = int(input("How many digits long is the passcode? "))
nc = int(input("How many possible characters are there per digit? "))
secondsPerAttempt = .08
npp = numberPossiblePasswords(nd, nc)
totalSeconds = maxSecondsToCrack(npp, secondsPerAttempt)
```

```
  print("It will take you " + str(int(totalSeconds/60)) + " minutes and "+ str(int(totalSeconds % 60)) + " seconds maximum to crack the password.")
```