MP 5: Security in Practice

This project is due on August 2nd, 2017 at 11:59pm. There is only one checkpoint this time, and only one activity. This should be a very short MP.

This is a group project; you SHOULD work in teams of two and if you are in teams of two, you MUST submit one project per team. Please find a partner as soon as possible. If you have trouble forming a team, post to Piazza. The tasks in this MP are designed to be quite easy.

The answers your group submits MUST be entirely your own work, and you are bound by the Student Code. You MAY consult with other students about the conceptualization of the project and the meaning of the questions, but you MUST NOT look at any part of someone else’s solution or collaborate with anyone outside your group. You may consult published references, provided that you appropriately cite them, as you would in an academic paper.

Solutions MUST be submitted electronically in any one of the group member’s svn directory, following the submission checklist given at the end of each checkpoint. Details on the filename and submission guideline is listed at the end of the document.

“If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology.”

– Bruce Schneier
**Introduction**

For this project, you will be investigating the security policies of organizations you have an account with. The purpose is to get a view of your social engineering attack surface, and understand how social engineering attacks might be carried out.

**Objectives:**

- Become familiar with common security practices
- Become comfortable asking about security policies
- Think through the implications of social engineering

**Guidelines**

- You MUST only investigate your accounts
- You MUST be truthful in the course of your investigation
- You MUST NOT impersonate others or otherwise misrepresent yourself
- You MUST NOT lie to anyone in the course of this assignment
- You MUST NOT record any phone conversations
- You MUST NOT violate the law in any way
- You MUST NOT conduct social engineering attacks

All the necessary files to start the project will given under the folder called “mp5” in your SVN directory. We’ve also generated some empty files for you to submit your answers in. You MUST submit your answers in the provided files; we will only grade what’s there!
5.1 Checkpoint 1 (100 points)

5.1.1 Security Audit (75 points)

Choose three organizations that you and/or your partner have some form of account with. This could be an account you use to make payments, access account data, or simply log in to access services (e.g. your bank, your cell provider, Amazon, government organizations, or the university.) Your goal is to research this organization to find out what information is required to make changes to your account or to gain access to account information. By “changes to your account,” we mean things like updating your address or phone number, changing your password, or changing the recovery email address associated with the account. By “account information” we mean things like finding out the account number, account balance, or the email, phone, or address information associated with the account.

Write a brief summary of each of your investigations into the three companies. For all three organizations, you SHOULD try to answer the following questions:

1. What organization did you audit?
2. What information was required to make changes to your account?
3. What information was required to access account information?
4. Are the requirements for gaining account access different online vs. over the phone?
5. Did you make more than one phone call? If so, did you learn anything different in subsequent calls?
6. Is any of the information required to access your account public?
7. Is any of this information something that can’t be changed (e.g. your SSN, birthdate, or mother’s maiden name)?
8. Did you find asking for this information to be awkward or uncomfortable?
9. Do anyone you interacted with during your investigation seem suspicious of you?

What to submit  You should submit your report for each organization.

1. 5.1.1.1.txt
2. 5.1.1.2.txt
3. 5.1.1.3.txt
5.1.2 Extrapolation (25 points)

The investigation you performed in the previous section was done both ethically and lawfully. You were honest, but the “bad guys” would not be constrained in this way. Extrapolate from what you learned in the previous section and write up another brief report. Imagine yourself as a hypothetical attacker and describe any plausible weaknesses that might be exploited to attack these organizations. 

**NOTE:** This section is entirely hypothetical. You MUST NOT carry out any attacks. You SHOULD try to answer the following questions:

1. What more do you think you might learn by lying to or pressuring employees?
2. What kinds of deception or pressure might an attacker try against these organizations?
3. Who might you impersonate to gain further access to information? Would spoofing your phone number help with this impersonation?
4. How much of the information required to gain access to your accounts could an attacker gather from public sources?
5. How much of the information required might have been leaked in a data breach? How might an attacker access that data?
6. Could information or access supplied by one of these organizations be leveraged to attack another organization?
7. Are there any actions you could take to make your accounts safer?

**What to submit**

1. 5.1.2.txt
Checkpoint 1: Submission Checklist

The following blank files for checkpoint 1 has been created in your subversion repository under the directory mp2. Put your solution inside the corresponding file then commit it to subversion. All .hex and .txt files MUST be submitted as ascii plaintext, and any lines in .txt and .hex submissions that begin with ‘#’ will be ignored.

- partners.txt [One netid on each line]
- 5.1.1.1.txt
- 5.1.1.2.txt
- 5.1.1.3.txt
- 5.1.2.txt