Homework 2
This homework is focused on helping you familiarize yourself with practical security tools.

Overview

- **Due Date:** Nov 20, 2015, 5pm (but note that some things need to be done at least 3 days before the deadline)
- **Group or Individual:** Individual
- **How to Submit:** Submit to Catalyst. Submit one PDF.

Background

The purpose of this homework assignment is to give you some practical experience with and awareness of some consumer-focused security systems.

Questions

**Question 1: Send an encrypted email**

For this task, the goal is to give you experience with sending encrypted emails. To successfully complete this task, you will need to set up your email client and send/receive an encrypted email to/from the TAs.

Setup information

Setting up your email client to send encrypted emails is a bit complicated, and the following link is helpful if you don’t want to follow the recommended setup below or you know what you are doing.

[How to Encrypt Your Email and Keep Your Conversations Private](#)

Recommended setup

We found that using Mailvelope extension for the browser is easiest since you will be able to
1. Get Mailvelope, which works with Chrome or Firefox. The rest of this guide assumes you are using Chrome.

2. Once installed, you should see a icon on the top right corner of the browser, click on it then click ‘Options’

3. Generate a key for yourself
   - Name: Your name
   - Email: Your @uw.edu email
   - Password: Optional but recommended password to secure your key

4. Import Adrian’s public key here by pasting the contents into Mailvelope (Options -> Import Keys)

5. You are now set up! Go to your email page, hit Compose and you should see . Click on it to start composing an encrypted email, click ‘encrypt’ when you are done.

6. You will see a dialog box that allows you to choose who you want to encrypt the email for. Make sure to click “Add” and my key is in the “Encrypt for: ” field! Note that you can “Encrypt for: “ you and me.

7. Using your UW mail account, send an email to the TAs in this format

   To: adrsham@cs.washington.edu
   Subject: [Homework 2] Encrypted email
   Content: <your UW Net ID> (so we know who you are)
   Attachment: <your public key> (Select your key from ‘Display Keys’ on the Mailvelope site, and export the public key only. Download <yourkey>_pub.asc and attach it.)

   Once you are OK with the contents, hit encrypt, select the correct key for the recipient and transfer the encrypted contents.

   Note: In order for the TAs to send you an encrypted email, you will need to attach your public key with your email.
If you don’t want to use your main email account, you can use this with a throw away email address inside a virtual machine.

Once the TAs receive this email, a secret reply will be sent back to you. Submit the content of this email to your writeup.

Note that since this will be a manual process, it is **important** that you start early on this (i.e. the TAs might not reply in time if you send them an email right before the due date). *Please email the TAs at least 48 hours before the deadline.*

**Deliverables**

1. [4 points] Secret value provided by the TA
2. Answers to short answer questions
   a. [2 points] Does this process involve the use of symmetric or asymmetric encryption or both?
   b. [2 points] We recommended a browser extension for ease of use, but what are the security risks of enabling this browser extension? (hint: what permissions did the extension ask for during install?)
   c. [2 points] Besides encryption, what else can we do to secure our email communications?

**Question 2: Two factor authentication**

This task involves setting up and making use of two factor authentication, with the goal of exposing you to what it is like to enable two factor authentication

**CAUTION:** Before enabling two factor authentication, please understand that you may lock yourself out of your account if you lose your second factor and don’t have backups. It is important to get backup codes and enable fallback options, such as sending codes to your phone. If you’d like, you can do this whole process with a new, throw-away account, but you’d need to be willing to log-in daily for this exercise (see below).

**Task**

Pick an account you login to at least **once** daily, and look into enabling two factor authentication. Since there are many services now that provide two factor, you may choose which service you want to use from the link below, pick a service that is green.

- [List of sites with two factor authentication (Green)](#)
A good example of a service with 2 factor is Gmail, called 2-step Verification. Here you can specify
- The primary way you receive codes (Google Authenticator App or SMS)
- A backup phone number that Google can call/text if you lose your primary phone
- Backup codes that can be downloaded and saved for use to login if the above fails

Deliverables

After at least three days of using a service with 2FA, answer these questions.

A. [1 points] For which service did you enable 2 factor authentication?
B. [1 point] What was the primary way you received codes?
C. [1 point] What were the backup options if you lost your primary option?
D. [2 points] Do you like this feature or not, and why?
E. [2 points] What is the benefit of using something like Google Authenticator vs SMS?
F. [2 points] Read this wikipedia article, and explain in a few sentences how you think Google Authenticator works.
G. [2 points] If you are the ISP of a country (you have control over all network traffic) and want to get into the account of a user with 2FA (and you have their password), what could you try to do?

Question 3: Certificates

The goal of this task is to give you a better understanding of Certificate Authorities (CA) and certificates.

Take a look at the CAs certificates that your computer trusts.
- Mac: Spotlight search ‘Keychain Access’
- Windows: Control Panel -> Search ‘Internet Options’ -> Content -> Certificates

Deliverables

A. [2 points] How many root CA certificates does your computer have?
B. [2 points] What is something that you found interesting from looking at the root CA certificates?
C. [2 points] Go to google.com using your favorite browser, and find a way to look at the certificates for google.com
   ○ List the chain of certificates your browser sees
D. [2 points] What is a possible risk of trusting a CA?
Question 4: Ad-blockers

Experiment with an anti-tracking browser add-on, such as Ghostery, Lightbeam, or Privacy Badger. Pick three websites (e.g., www.cnn.com, www.facebook.com, and www.weather.com -- though you may pick any sites), visit them with the add-on installed, and report on what you find.

Deliverables

- [3 points] How many trackers are on each site?
- [2 points] Can you think of ways to improve the add-on you tried?
- [2 points] Does anything surprise you?