CS5430 – System Security Spring 2018

Assignment 1

Due: February 26, 2018

Problem 1: Threats and Harms

You've been hired as a Security Engineer at Secure Systems Inc. and are consulting on the design of three different systems. You're tasked with analyzing the types of threats and harms each system must protect against. Each system is described in adequate detail required to answer this question below. Do be thorough, but this question is not looking for super long answers. Remember that this question is solely asking you to perform a **threat and harm analysis**, and is **not asking** how to secure the information described or how an attack could take place.

Part A

Secure Systems would like to implement a peer to peer messenger system. Users are identified by 'screen names,' in other words a unique username. This username is not public - a user can only discover other users through another medium. Users create an account by registering with Secure Systems using only a username and password (thus a single user could have many accounts). Chat logs are available to the user, but no other information is stored on this system.

Part B

In addition to the messenger, Secure Systems would like to expand the above system to include a more detailed profile of the user. This new system almost resembles a social media website. Registration now requires an email address, and users can now locate each other through a search function provided by the system - thus their 'screen name' is now their actual name. Users can make their profile as detailed as they'd like, such as adding in who their family members are, adding their birthday, posting status updates, and uploading photos or videos.

Part C

Seeing the recent rise in interest in cryptocurrencies, Secure Systems has decided they'd like to build their own digital asset exchange. However, due to legal constraints, this system must hold a significant amount of information on the users in order to properly process tax documents. Users are required to register with an email address, cell phone, and government issued ID. Thus every account is reliably tied to a single user. In addition,

in order to make purchases users can link their credit/debit cards, or even a bank account. The digital assets are stored securely in a distributed manner in cold storage (i.e., an offline storage for digital assets, such as a USB drive in a safe deposit box).

Problem 2: Harms and Countermeasures

With the advent of smart homes, many new security considerations come into play now that users are able to control functions of their house remotely. For this question we will consider a system with the following capabilities and included countermeasures.

- Users have a single application running on their smart phone that acts as a control panel for the house. This application has been linked to a secret key tied to the house that cannot be duplicated remotely.
- The application communicates solely with a receiver inside the house.
- Users authenticate both by unlocking their phone and knowledge of a 4 digit pin generated by the application.
- The user is capable of unlocking the front and back doors of the house along with the garage, all three of which are monitored by a small unnoticeable security camera. The user cannot access other entrances.
- The user has access to security feeds on the monitored entrances mentioned above only through the control panel in the house.

For each capability, identify what a potential harm the included countermeasure is protecting against (if applicable). This question is asking for a really short answer (1-2 sentences).

Problem 3: Vulnerabilities

In this question you will be familiarizing yourself with the FindBugs program. The following instructions serve as a guide for setting up FindBugs.

- Ensure Java is already installed in your machine. Java 8 is strongly recommended. As far as we know, earlier versions should work, but Java 9 likely will not.
- Download and unzip Findbugs 3.0.1 (http://findbugs.sourceforge.net/downloads.html). Also download gradesystem.zip from CMS. This is part of the source code of a course project from a previous semester. Please do not redistribute this code.
- Follow instructions in Quick Start to launch the FindBugs GUI.

  (http://findbugs.sourceforge.net/manual/running.html)

- In the FindBugs GUI, choose File->New Project. Give the project a name of your choice. Add to the "Classpath for Analysis" the gradesystem.zip file you downloaded in the previous part of the lab. Add to "Source Directories" the same gradesystem.zip file. Run the analysis.
- Use the View menu to view only Scary bugs. Then only the Scariest bugs. Then All Bug Ranks.
- Experiment with viewing bugs in different ways using the "Group Bugs By" interface. Drag-and-drop the different bug attributes ("Bug Kind", "Category", etc.) to see how bugs can be sorted in various ways. Attributes before symbol "<->" are considered for the "Group Bugs By" operation, while attributes after "<->" are ignored.

Now, answer the following questions after familiarizing yourself with FindBugs.

1. How many bugs of Troubling or worse rank exist in the Security category?
2. Examine the rank 12, Correctness bug, where field logDisplay in method Client_Second.connectClient is deemed to be unwritten. Did the analysis miss an initialization of this field? Or did the programmer fail to initialize it? What is the potential problem that results from this bug? How should this bug be fixed?
3. Examine any of the security bugs identified by the analysis in ConnectionClass.java. What is a potential harm that results from this bug and how can this harm be caused? Hint: read about SQL injection.