COM-301 Computer Security
Exercise 12:
Malware and Privacy

December 18, 2023

Malware

1. Consider the use of Twitter for botnet command-and-control. Assume a simplified version of Twitter that works as follows: (1) users register accounts, which requires solving a CAPTCHA; (2) once registered, users can post (many) short messages, termed tweets; (3) user A can follow user B so that A receives copies of B's tweets; (4) user B can tell when user A has decided to follow user B; (5) from the Twitter home page, anyone can view a small random sample (0.1%) of recent tweets

   (a) Sketch how a botmaster could structure a botnet to make use of Twitter for CC. Be clear in what actions the different parties (individual bots, botmaster) take. Assume that there is no worry of defensive countermeasures.

   (b) Briefly describe a method that Twitter could use to detect botnets using this CC scheme.

   (c) Briefly discuss a revised design that the botmaster could employ to resist this detection by Twitter.

   Solution:

   (a) Option 1: the botmaster registers two Twitter accounts, A and B solving two CAPTCHAS by hand. Account A is used to send commands, and B for receiving commands. The bot malware includes within it the credentials for the B account. New bots then access the B account to read the tweets sent by the A account, which encode the instructions to the bots.

Option 2: Create a new account per bot, they follow each other to follow commands. How would you solve all CAPTCHAs? for example, use Amazon Turk, or hire a CAPTCHA solving service from the underground economy.

Option 3: The botmaster registers a single account and use it to generate thousands of identical tweets for each command they want to send. The bots sample the home page and find the command there. The number of Tweets inserted by the botmaster have to be enough to appear in the sample.

(b) Option 1: Twitter could look for access to the same account from many different IP addresses.

Option 2: Twitter could look for accounts whose followers all only follow that account.

Option 3: Twitter could remove duplicate messages from a same account.

(c) Option 1: cannot be solved, bots do have different IP addresses. Choose one of the other methods.

Option 2: The botmaster could have the bots follow some other randomly selected users in order to look more normal.

Option 3: The botmaster could add some minor variation to their repeated tweets so that Twitter doesn't view them as identical.

2. Agree or disagree and justify. "A pure tree CC structure with the hacker as root (level 0), CC servers in level 1, and bots in level 2 is as robust against takedown as the hybrid structure in which each bot is connected to one CC, and CC servers are connected in a P2P fashion (as seen in slide 35)".

Solution:
Agree. They are equally robust. The security team still needs to take down the CC servers one by one.

Privacy

1. Let us assume you are a service provider designing a new recommendation system for best restaurants in campus. Assume a simplified environment in which there are three actors: the students using the application, the restaurant owners, and the service provider serving the application.

Compare the following configurations in terms of privacy (i.e., privacy risks with respect to other entities in the system) from the point of view of the students.

CONFIG A: The application gathers the recommendations from the students and then: lets other students see each others' recommendations, and lets the restaurants see the student recommendations so that they can offer discounts to students that give good ratings.

CONFIG B: The application gathers the recommendations from the students and then: lets other students and the restaurant owners see the average rating for a restaurant.

CONFIG C: The student's application computes a ranking of the restaurants and uses advanced cryptography to send this ranking to the service provider. This cryptography enables the service provider to compute a global ranking without seeing each individual student opinion. The restaurant owners receive the global rating.

Solution:
First, think that having access to the ratings reveals when and where a student has had lunch. Depending on the type of restaurant this may reveal further information. For instance the student is vegan, the religious orientation of the student (e.g., restaurants with no pork, restaurants offering kosher food), the health condition of the student (restaurant specialized in food without gluten), etc.

CONFIG A: This configuration is very bad for privacy. In this configuration, other students, restaurant and service provider see all the recommendations and ratings.
CONFIG B: This configuration is better, but the service providers still sees all the data. Others only see aggregates.
CONFIG C: Best option, only the student herself gets access to her own ratings.

2. Agree or disagree and justify

   (a) The privacy of employees out of their work place (i.e. Facebook, Twitter) is relevant when designing a company's access control mechanisms.

   (b) The privacy of ministers' children is not relevant for National Security.

   (c) The privacy of professors is relevant for students' safety in their homes.

   Solution:

   (a) Agree: how private are the employees may define which access control methods are secure or not. For instance, if they have photos online,

facial recognition may be weak; if they publish all their information in social networks security questions may be irrelevant; etc.

(b) Disagree: it is very important, as they are very juicy targets if enemies or terrorists want to put pressure on the ministers.

(c) Disagree: professors and student homes are totally uncorrelated.