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.

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)".

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.

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.