Weaver
Fall 2019

CS 161
Computer Security

Discussion 12

Miscellaneous Topics

Question 1 ***Worm Spread***

(a) In class we have seen that typical network worms propagate using scanning. Can you think of other ways to spread a worm?

(b) Bitcoin (and most other cryptocurrencies) use a peer-to-peer gossip network to communicate. In a gossip network, each node has a list of peers. Whenever the node receives a message, it "gossips" the message to all of its peers. This process repeats recursively until the message reaches the entire network–typically within seconds. Why would a memory safety bug in the Bitcoin client's networking code be so deadly?

(c) The typical virus exploits a benign application to execute its own (malicious) code. Exploiting real world applications is getting tougher every year because of the mitigations for buffer overflows that we discussed. Can you think of a way that a virus would not require an exploit to achieve code execution?

Question 2 ***Botnet C&C***

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 C&C. 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 C&C scheme.

(c) How well will this detection method for Twitter work?

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

Question 3 *Censorship and Anonymity*

(a) You are a resident of the country of Censorshipistan (a former *Eastern Block* state). You suspect that your country is employing an *on-path* censorship device to block content deemed objectionable by the ruling party. How might you detect that you are being censored?

(b) After determining that you are indeed being censored, you decide to evade the censorship using the Tor anonymity software.[1] How might the government of Censorshipistan detect your Tor usage, and block it?

Question 4 *Trusting Trust*

The title of the Ken Thompson talk that Nick mentioned in class was "Reflections on Trusting Trust."

(a) Think of your daily computer usage, and list down the corporations that you *have* to trust to keep your private data private. Remember that trust is transitive: if you trust EvilCorp, you also have to trust corporations that EvilCorp relies on.

[1] https://www.torproject.org/