Question 1 ***Worm Spread*** **(15 min)**

(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 ***Abusing Network Monitoring*** **(10 min)**

(a) What does "NOBUS" mean? Give an example from lecture of an instance where the NSA had NOBUS. What are some examples of where the NSA does not have NOBUS?

(b) Recall that network traffic is often encrypted. Much of the "monitoring" intelligence agencies use is similar to installing NIDS. Given this, how can recording TLS communication still be useful to intelligence agencies?

(c) What is "cookie linking," and what's its purpose? Be as specific as you can.

Question 3 ***Ransomware*** **(10 min)**

In lecture we discussed *ransomware*, in which the malware holds a computer system or data on it hostage by demanding a ransom for its restoration.

(a) Describe how symmetric encryption could be used for this purpose.

(b) Describe how asymmetric encryption could be used for this purpose.

(c) What other types of threats (apart from deleting or encrypting data) can you imagine a virus making to extract payment?

Question 4 ***Trusting Trust*** **(5 min)**

We highly suggest reading article, "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.