Julian Garcia

CSE 489

Two articles on Cybersecurity

1. ***Poly Network hack exposes DeFi flaws, but community comes to the rescue***

   Article Link:

   https://cointelegraph.com/news/poly-network-hack-exposes-defi-flaws-but-community-comes-to-the-rescue

   This article describes a recent hack on a cryptocurrency exchange called Poly Network. $610 million dollars worth of cryptocurrency was stolen by a hacker. What's interesting about this hack is that the hacker essentially returned the funds intentionally, instead of reporting the bug to the developers, he simply exploited it himself. Ironically, his only supposed intention was to expose this flaw so nobody else could exploit it, he chose to expose this flaw by taking advantage of it himself merely because he didn't trust that whoever he sent the bug report to wouldn't exploit it himself, as millions could be made from it. In terms of how the hack was accomplished, the article offered this brief explanation:

   "The hacker bridged fake transaction interactions on one chain to make the system contract on another, transferring ownership rights for the assets' vault to the hacker's public key. Poly Network's developers and auditors didn't notice the vulnerability, allowing for multiple arbitrary user calls via a smart contract that has many privileges."

   To explain some of the jargon, crypto-currency exchanges generally work on a 'contract' system, where the developers establish a system of validation for how funds their users put into the system are exchanged according to the rules of whatever contract they're under. So in theory, there can be contracts given higher privileges than others, which can access funds in the system that aren't supposed to be accessed

without proper context. So, in finding exploits in a crypto-currency's contract system, hackers can essentially gain a key to a vault.

2. ***What Biden's Cybersecurity Executive Order Means for Supply Chain Attacks***

   Article Link:

   https://securityintelligence.com/articles/biden-executive-order-supply-chain-security/

   This article details Supply Chain Attacks, and talks about how Biden's recent executive order affects Supply Chain security. When talking about supply chain activity, the article explains that the term is for the supply chain of Software used by any business/entity or user. Essentially supply chain security is concerned about the security of the software you rely on, which can be of greater concern than your own security, since software that targets a large amount of stakeholders is usually more highly targeted. In terms of how Biden's executive order affects supply chain security, his order essentially establishes a baseline and criteria for what security practices are absolutely necessary of large software suppliers depending on what kind've software they're producing. These guidelines can/will be enforced at the federal level, however whether it is followed by businesses depends entirely on the business, and whether or not they decide the guidelines are worth the cost to follow.

   Exam Questions:

1. What is supply chain security?

   Answer: Supply chain security pertains to the security of the software you rely on that you haven't developed yourself.

2. What system do cryptocurrency exchanges generally rely on to handle their transactions?

   They generally rely on a 'contract' based system.