CS 6823 Network Security
Homework 4

True False Questions

1. 802.11i provides confidentiality for the source and destination MACs (i.e. hardware addresses). True
2. Polymorphic malware can be detected when it executes and is decrypted with signatures based on the decrypted body of the malware present in RAM. False
3. The PGP uses a web-of-trust model to provide a PKI managed by each individual user. True

Short Answer

1. Bitcoin
    a. Describe bitcoin's proof of work. Be specific about the details of the cryptographic functions used and how it adjusts to increasing or decreasing global computation ability of miners.
    For each transaction, a public network of members is tasked to solve a cryptopuzzle using their computing power to vote for the credibility of a transaction. The use of computing power ensures that voting is less likely to be corrupted by one individual. In bitcoin, the previous block hash is used to solve the puzzle for the current transaction (block hash). Once that puzzle is solved it is broadcasted to others on the network, then it is added to the longest blockchain. Bitcoin tries to maintain a 1 block/10 min average, to do so, they adjust the number of 0's in the cryptopuzzle to make it easier or harder for the network to solve.
    b. Describe what the bitcoin blockchain achieves.
    The blockchain achieves integrity for transactions by ensuring that the whole network can check which transactions have occurred or not to prevent false or misused transactions. It is essentially a single repository for all transactions that have occurred, and only one transaction can be added to it at a time.

2. Anonymity/Privacy
    a. Describe two ways that someone can attempt to link the sender and receiver of a stream of messages sent using Tor. Be specific and describe the capabilities required by the attacker and how they would execute their attack.
    Someone can measure the timing of packets in a network, using passive traffic analysis. In this way, when they see the sender has sent a packet and the receiver has received it, they can infer the individuals using the tor network for their communications.
    Another way is through a sybil-type attack, if an attacker has many routers on the network, they can see traffic patterns, and infer users' identities from there.

b. Describe the concept of anonymity and how it differs from message confidentiality.

Anonymity is not being able to identify features known about you as an individual through any form of online presence, whereas message confidentiality is just secrecy of exchanges that can be short term, but others may know information about you.

Research Paper and Questions

https://cseweb.ucsd.edu/~savage/papers/WEIS15.pdf

The underground market proves illustrious for a society connected by the internet. Criminals and non-assuming individuals alike venture into the upregulation realm of goods ranging from pharmaceuticals to human-power and beyond. The concern of these interconnected markets stems from the lack of legislation and control centralized power asserts to the depths of the internet.

Before the internet, counterfeit goods and products had to facilitate every part of their business from advertising to consumers to accepting payment. With the tools of the internet, these processes have become much more specialized, leading to a more robust ecosystem of intermediaries that can provide to different ventures. As stated in the article, this allows for risk transfer between enterprises. If one company is caught, the other can simply claim that they were only doing their job for the following company and so on. This can make it difficult to clamp down on exchange. Additionally, this risk transfer allows for ease of mobility. Organizations can support different trades due to their specificity of work, and therefore, if one of their partners is seized, they can move onto others. Again, making the task of shutting down these connections a large-scale objective.

The services offered range from drug trafficking to media promotion, but as stated by the paper, there seems to be no legal intentions in mind. Services that offer social media likes are quite striking, because they harness compromised media log-ins from active users or bot-users.

Therefore, requiring services from botnet owners or hackers. Further, scams can also claim a physical component, such as with credit card skimmers installed on top of real credit card readers in places like gas stations. This highlights the lengths that individuals will go to sell information for profit.

The objective of profit is central to the research paper because it is what drives all components of these internet markets to continue their precarious work. Specifically, profit centers finance the intermediaries, suggesting that they should be the targets for arrest. Cutting off the sources of income, like banks that offer risky management, makes it difficult for any part of the network to continue. Therefore, that should be a starting point for mitigating this illegal use of the internet. However, beyond this, it is clear that there should be more concern about the lawlessness of the internet and how that will only be magnified with more the needs and interconnectedness of the future.