NetID: iv447
UniversityID: N17385760

HomeWork 4:

True False questions :

1. Bitcoin is still resilient to malicious miners even when over 50% of the computational work is provided by malicious miners. **False**

2. Transport level encryption of SMTP via TSL would provide confidentiality from a passive man-in-the-middle network attacker that can eavesdrop on messages between the SMTP client and server. **True**

3. Tor provides sender-receiver anonymity against a non-global network eavesdrop attacker. **True**

Short Answers :

1. Web Server Application Security

1. Describe the differences between first and second order Cross Site Scripting (XSS) attack and provide an example of what each type of attack can achieve. [10 points]

Answer : Scripting languages make web pages more dynamic. Cross site scripting (XSS) is when attacker injects malicious code on client side with intentions to run malicious script on legitimate web sites and web applications. There different order of cross site scripting.

First order or Type 1 XSS : This is also known as reflected or non-persistent vulnerability. When the data provided by the client is immediately used by the scripts on the server to generate results which are displayed back to the users. In reflected XSS user is tricked into visiting an honest website (via phishing email, link in banner ad, comment in a blog etc). When the user visits the malicious site bug in the website causes it to echo to the user's browser an arbitrary attack script. This malicious script can manipulate website contents (DOM) to show the bogus information, might request

for sensitive data, control form fields on web site page and linked pages and cause user's browser to attack other website.

- Second order or Type 2 XSS : This is also known as Persistent or stored XSS Vulnerability. In this type of attack user-provided data is stored on the web server and later on displayed to the users without being encoded using HTML entities. This type of attack can be found on social networking sites and message boards where user can post comment in HTML formatted message so that other people can see their messages.

2. Describe two different types of defenses to XSS attacks. [10 points]

Answer : Defenses against XSS attacks :

1. Any user input and client-side data must be preprocessed before it is used inside HTML.

2. We should remove/encode HTML special characters.

   For this following things can be done :

- Use a good escaping library such as Microsoft's AntiXSS , OWASP ESAPI (Enterprise Security API)
- In PHP, htmlspecialchars(string) can be used to replace all special character with their HTML codes For example ***"*** becomes &quot, ***&*** becomes &amp.
- In ASP.NET, server.HtmlEncode(String) can be used.

2. Bitcoin

1. 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. [10 points]

Answer : Mining is the process of adding transaction records to Bitcoin's public ledger of past transactions. A proof of work is a piece of data which is difficult to produce but easy for others to verify. Bitcoin's proof of work is based on certain protocols. These protocol for proof of work are relative to a given challenge string. The

person trying to engage in protocol will try to come up with a corresponding proof that is tied to this challenge string. It has very specific mathematical properties in relation to the challenge string. Cryptographic algorithm that can be applied to the concatenation of challenge and proof string is SHA-256 or equivalent crypotgraphic function. Mining a block is difficult because SHA-256 hash of a block's header must be lower than or equal to the target so that the block can be accepted by the network. The simplified version of the problem for explanation purpose : Block hash must be started with certain number of zeroes. Many attempts has to be made using brute force. That is effectively lots of proof strings will have to be generated trying lot of many possibilities until you find the string you want.

2. Describe what the Bitcoin block chain achieves. [5 points]

Answer: A blockchain is continuously growing list of all records (blocks), which are linked to each other using secured cryptography. Each block contains the cryptographic hash of previous block, a timestamp and transaction data. A block chain is digitized, decentralized, public ledger of all cryptocurrency transactions. It's the main technological innovation for bitcoin. Because block chain is decentralized, it's not regulated by central authority. Based on bitcoin protocol the database is shared among different nodes which are participating in the system. Upon joining the network each system receives a copy of blockchain, which had records attached to it of all the previous transactions. Blockchain has matured into a core technology in financial IT. Blockchain based application can be used to solve problems that used to be extremely time consuming and costly.

Research Paper Summary :

Spamalytics: An Empirical Analysis of Spam Marketing Conversion

This paper throws light on spam marketing conversion i.e the probability that an unsolicited email will ultimately elicit a sale. In this paper the authors have presented methods for measuring the conversion rate of spams. They used parasitic infiltration for an existing botnet infrastructure. Spam-based marketing is curious beast. Instead of implementing many anti-spam technologies, the spammers are in profit. Clearly many people are tricked into buying the stuff that spammers spread, but how many, how often and how much is the question.

There are no indirect method to measure the spam conversion rate. So in this experiment, the authors have created their own website and marketed it via spam and then record the number of sales they obtain by spamming. The application makes use of existing botnet. Using this methodology, they documented three spam campaigns compromising over 469 million emails. Through this they wanted to know, how many spam got delivered, how many got filtered and most important how many clicked on it and got tricked by the spam. The measurements were carried on using storm botnet and its spamming agents. Storm is peer to peer botnet that propagates via the spam. Storm communicates using TCP and UDP based overnet protocol. Overnet protocol : there are four basic messages to facilitate basic functioning of overnet : Connect, Search, Publicize and Publish. There are three primary classes for storm botnet : Master servers, Proxy bots and Worker bots. Worker bots make request and upon receiving orders, sends spam as requested, proxy bots works as medium between master server and worker bots and finally master servers provide commands to workers and receive their status reports.

Methodology for the experiment : Worker bots request spam task through the proxies, proxies forward spam workload responses from master servers. Workers send the spam and return delivery reports. This approach is based on botnet infiltration which insinuates spam in to botnet's "command and control" (C&C) network. This experiment is based on rewriting C&C protocol. Runtime C&C rewriter consist of two components.
A custom Click-based network element redirects potential C&C traffic to a fixed IP address and port, where a user-space proxy server which is implemented in python will accepts incoming connections for impersonating the proxy bots. To evaluate the results of spam delivery along e-mail delivery, researchers established test e-mail accounts and arranged for worker bots to send spam to these accounts. After this these accounts were periodically polled for the received messages along with the timestamp.

The authors created their own site of pharmaceutical company and postcard self propagation site and use this these campaigns to measure spam conversion rate. In their results they found that only a fraction of span got filtered through the spam filter to the user and a tiny fraction of spams made users to actually buy something. They also calculated the time-to-click distribution access to pharmaceutical site in order to demonstrate the latency between the spam that were sent out and users who clicked on the spam links on average in a single day. The statistics turned out to be surprising low, the conversion rate was around 0.00001% after 26 days and after sending 350 million e-mail messages. The revenue generated by this was around $2,731.88.

The paper is well rounded, authors have explained their methodology and results in very concrete way. Lot of emails were filtered out by spam filter or were not delivered. These factors can be ruled out conversion rate can be measured again, they may get high conversion rates for spams, if more users are exposed to spams.