Jie Liang CSE300

Professor Suver Nov 17th 2016

HTTP Flood attack in Cloud Computing

In the past few years, cloud computing has transformed the way storing data in people's mind. It uses the internet infrastructure to provide path between cloud providers and users for transferring data. The development and use of cloud computing has already been a huge impact on society. Dropbox, Google, Amazon, and other numerous companies have devoted their resources into cloud computing in order to provide better service. However, with such convenience, we must need to think about security. Otherwise, the data integrity will be violated or the data will fall into the wrong hands, and both will cause serious consequences. This paper introduces a potential security issues regarding to HTTP Flood of DDoS attack, which will threat the data security in cloud computing.

There's already some researches on security in cloud computing. Zhang, Cheng, and Boutaba revealed the potential problems are caused by the characteristics of cloud computing, but failed to relate the problems to other aspects of cloud computing. It makes their arguments narrow-minded since there are a lot more factors can be contributed to data security in cloud computing. In Subashini and Kavitha's study, they emphasized on the potential data leakage when users are trying to transfer their data to the cloud, which brings an innovative perspective so that people realize data can not only be corrupted within the cloud but also during the process of exchanging data between users and cloud providers. Mazhar, Samee, and Athanasios talked about the issues in user authentication due to lack of hierarchy of user's roles. They discussed lack of clarification of users' levels can also affect data integrity. While Deyan and Hong

discussed the cluster of data will affect one another within the data center. Both paper draw people's attention to the architecture of data within the cloud so that it can be rearranged for a better performance.

However, the arguments of all the previous researches mentioned before are built on the statement: cloud providers are always online, but it's not the case in real life. The paper Aich, Sen, and Dash wrote mentioned the potential problems of data in long term availability. They focused on data persistence within the cloud in long term, but there's more imminent threat, which is DDoS.

The main purpose of DDoS (Distributed Denial of Service) attack is letting specified target can not provide normal services, or even disappear from the Internet. If there's DDoS attack on the servers of cloud providers, users will not able to access their data, or even worse, lost their data. DDoS attack can be simply divided into three categories.The first category is sending massive data packets from the Internet to plug the IDC entrance. Since the entrance is blocked, it makes a variety of hardware defense system within the cloud useless. The second category is sending packages every few minutes, which makes servers unresponsive due to overloading workload. This type of attack is mainly initiated by the use of protocol or software vulnerabilities. While the third category is the mixture of the two, like HTTP Flood, which is the current mainstream attack nowadays.

HTTP Flood is a kind of attack targeted on Web service in the seventh layer protocol. It does great harm mainly in three aspects: easy to launch, filtering difficulties, far-reaching impact. Instead of going through the port scanner on the Internet looking for anonymous HTTP proxy or SOCKS proxy, the attacker goes through an anonymous proxy to the target HTTP

request(Karnwal, et al. 1). Since anonymous proxy is a relatively rich resources, and it is not difficult to get hold of some anonymous proxies, which makes it easy to implement and can be sustained long-term high-intensity.

On the other hand, HTTP Flood attack in the HTTP layer imitates the normal user's Web page request behavior, so the cloud providers will have a hard time to distinguish between HTTP Flood attacks and the requests from the normal users. It is nearly impossible to provide a sophisticated solution without affecting the normal users. HTTP flood attacks can also cause serious chain reactions. It not only directly leads to the slow response of the attacked Web front end and causing users not able to access their data in time, but also has indirect effects to the back-end Java and other business logic and more back-end database services. The attacks increases the pressure of database services, or even causing them shut down abnormally and lost the data within it.

The key idea for HTTP Flood is to break through the front-end cache by going through the HTTP header field settings and attack directly to the Web Server itself. In HTTP protocols, HTTP Request sends "\r\n\r\n" to notify the server that the client has done, and the server can begin to process. So what happens if "\r\n\r\n" is never sent? The attacker in the HTTP request header will be set to Keep-Alive Connection, Web Server that maintains TCP connections will not disconnect the connection, then the attacker sends a key-value format data to the server, such as "a:b\r\N", resulting in the server that the HTTP header is not complete and waiting to receive. The server's Web container will soon be filled with TCP connections and no longer accept new requests, and users will not be able to access their data until the server is back to normal.

Rather than focusing data security in cloud computing with the perspective of the cloud providers and users, like research papers we mentioned before, this paper addresses the outside threat, HTTP Flood attack, would impact the data in the cloud, and how the attacks are being done. As the cloud services become more and more popular, the probability of getting attacked by HTTP Flood increases. It is crucial to protect data in cloud computing from the attacks. Further studies could be done with a focus in defending HTTP Flood attack by using detecting the frequencies of requests that come from the same IP address.

Works Cited

T. Karnwal, T. Sivakumar and G. Aghila, "A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack," *Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on*, Bhopal, 2012, pp. 1-5.

Zhang, Qi, Lu Cheng, and Raouf Boutaba. "Cloud Computing: State-of-the-art and Research Challenges." Journal of Internet Services and Applications 1.1 (2010): 7-18. Web.

Ali, Mazhar, Samee U. Khan, and Athanasios V. Vasilakos. "Security in Cloud Computing: Opportunities and Challenges." Information Sciences (2015): 1-27. Web. 18 Oct. 2016.

Chen, Deyan, and Hong Zhao. "Data Security and Privacy Protection Issues in Cloud Computing." International Conference on Computer Science and Electronics Engineering (2012): 1-5. Web. 18 Oct. 2016.

Subashini, S., and V. Kavitha. “A Survey on Security Issues in Service Delivery Models of Cloud Computing.” A Survey on Security Issues in Service Delivery Models of Cloud Computing, 2011, pp. 1–11.

Aich, Asish, Alo Sen, and Satya Ranjan Dash. "A Survey on Cloud Environment Security Risk and Remedy." International Conference on Computational Intelligence & Networks (2015): 1-2. Web. 18 Oct. 2016.