Domain name system problems

Technology, Information Technology

Domain Name System (DNS)

The Domain Name System (DNS) is a distributed naming system that is defined by hierarchy of systems, computers, or other resources connected to private network or internet. The DNS usually associates domain name information assigned to every entity. DNS is a platform that translates memorized domain names easily to the numerical IP addresses to allow easy location of devices and computer services globally. Hence, it is worth noting that DNS is a vital functionality component of the internet; however, the applicability and functionality of DNS is associated with numerous problems especially in its internet application components. These problems are usually associated with the system's sparse documentation particularly in relation to maintaining and managing DNS data (National Research Council (U. S.), 2005). These problems make its master zone file to be prone to error. Therefore, this essay aims at addressing fundamental problems associated with DNS application and probable solutions to such identified problems. There are numerous but distinct DNS threat categories. Most of the problems are usually general; however, few of them are DNS protocol problems with specific peculiarities. Some of the DNS problems include packet interception, ID query and guessing prediction, name chaining, trusted server betrayal, service denial, domain names authenticated denial, and wildcards.

a. Packet Interception

Packet interception forms are the simplest threats on DNS including eavesdropping that translates to spoofed responses. This usually takes the real back response to the resolver. In this case, the attackers will simply tell

any resolver whatever it intends the party to believe. It should be noted that the attacks from the packet interceptions are not usually unique to the DNS; however, they unencrypted the UDP packets thereby making the attacked data vulnerable to the people who can intercept such data packets; hence, transmitting or sharing them to other networks (Deturbide and Scassa, 2004). Moreover, the attacker intercepts are likely to return the desired results through reply message with other parts of the correct message; thus, generating further complications to the desired data.

The solutions to the interception attacks may include assigning DNS messages through a security mechanism including IPsec or encrypting messages using IPsec. These solutions are not the best since they are expensive especially for the heavy internet or private service data users. TSIG may also be a solution since it provides a platform specific trust relationships among specific clients concerning DNS protocol corners (Funabashi et al., 2005). In addition, it allows dynamic data updates, zone data transfers, and or data resolvers; however, does not guarantee checking of all available DNSSEC signatures since the DNESSEC signatures usually check its systems on its own. Nonetheless, TSIG allow communication integrity among the involved severs; hence, it the best solution to this DNS problem.

b. ID Query Prediction and Guessing

It should be noted that DNS is mostly used over UDP/IP; therefore, it is often easier for the attackers to generate packets that match parameters of the transport protocol. The DNS header ID field has only 16-bit field with UDP port server associated with DNS of a known value. In this case, there are

only 2**32 client UDP port and ID possible combinations for specific server and client. This combination does not provide large range and sufficient protection against brute force search. Hence, it is easier for the attackers to predict ID and client UDP port using the previous traffics. Moreover, the problem usually reduces the search space to as smaller range as 2**16. This problem can be resolved using the DNSSEC signatures that will detect forged responses; however, the resolvers that cannot use DNSSEC signatures to check themselves can use TSIG for integrity communication between servers (National Research Council (U. S.), 2001). Both resolving systems will hinder the attackers from ID Query Prediction and Guessing of the server users' activities thereby prompting their attacks to such internet or other computer services.

References

Deturbide, M. E., & Scassa, T. (2004). Electronic commerce and internet law in Canada. Toronto, Ont: CCH.

Funabashi, M., Grzech, A., & IFIP Conference on E-Commerce, E-Business, E-Government, I3E. (2005). Challenges of expanding Internet: E-commerce, e-business, and e-government : 5th IFIP Conference on e-Commerce, e-Business, and e-Government (I3E'2005), October 28-30, 2005, Poznan, Poland. New York, N. Y: Springer.

National Research Council (U. S.). (2001). The Internet's coming of age. Washington, D. C: National Academy Press.

National Research Council (U. S.). (2005). Signposts in cyberspace: The Domain Name System and internet navigation. Washington, D. C: National Academies Press.