Report on 'The Hitchhiker's Guide to DNS Cache Poisoning' by Cheng Han

Summary: DNS cache poisoning highly infect the performance of nowadays' Internet. The paper mainly discusses a model of the semantics of DNS caches, which include the bailiwick rule and trust-level logic. By applying it to Internet, it can systematically investigate different types of cache poisoning and generate templates for attack payloads. The paper then explains the impact of the attacks on DNS resolvers and their implications for several defenses against DNS cache poisoning.

Background& Motivation: While DNS is an essential part of the Internet. However, security was not one of the design considerations for DNS. Therefore, many attacks on DNS were found during the years. Cache poisoning is the most prominent and dangerous attack on DNS, it results in a DNS solver storing invalid or malicious mapping between symbolic names and IP addresses. It may poison the cache by compromising an authoritative DNS server or by forging a response to a recursive DNS query sent by a resolver to an authoritative server while DNS protocol is intrinsically vulnerable to it. There are many non-cryptographic approaches tried to solve the problem, but they mainly concentrate on blind response forgery while it is just one of the possible attack vectors and they are vulnerable to trivial eavesdropping attacks. The paper then tries to develop a model to enumerate the consequences of different types of DNS forgery exploits and evaluate the effectiveness of some non-cryptographic defenses against DNS response forgery.

Main idea/solution: The paper then tries to develop a model to enumerate the consequences of different types of DNS forgery exploits and evaluate the effectiveness of some non-cryptographic defenses against DNS response forgery. First, the paper talks about the DNS background. From this part we know that DNS response forgery can take the advantage of the DNS caching strategy: the ability to overwrite existing records makes DNS response forgery a huge problem. Then some of the DNS response forgeries are discussed including cache poisoning without response forgery, blind response forgery using birthday attack, Kaminsky's exploit and response forgery using eavesdropping. Then the paper talks about the bailiwick rule, which is used to prevent malicious authoritative servers from providing DNS mappings for domains outside their authority as part of a referral response. The paper discusses three open source implements which are BIND, Unbound and MaraDNS. Then the paper discusses the caching overwriting strategy. Then researchers then set a formal model of DNS resolver, which is a formal model of the default bailiwick-checking and cache-overwriting rules of BIND and Unbound. And MaraDNS is not considered since it does not cache the authority and additional sections of responses containing an answer RRset and does not use trust levels for overwriting existing records. Then paper then categized cache poisoning attacks, including adding a new name and overwriting the mapping for an existing name. Finally, the article briefly introduce the defenses process.

Results: 1. DNS is a distributed storage system for Resource Records (RR) 2. Each record has a time -to-live (TTL) parameter and it would be purged from the cache once its TTL expires. 3. When a DNS resolver or authoritative server receives a query, it starts searching its cache for a matching label. If no matching label could be found, the server may instead retrieve from the cache and return a referral response or configure to initiate the same query to an authoritative DNS server responsible for the domain name which is the subject of the query. 4. The response would be accepted if the RRset of each section passes bailiwick rule, which is an implementation of the resolver. 5. Poisoning the DNS caching

by adding false records has the ability to overwrite existing records which makes it a huge problem. 6. Cache poisoning without response forgery: When responding to a query from the resolver, without bailiwick rule, a malicious authoritative server can send, an arbitrary mapping from any domain name (including those outside its authority) to an IP address in the additional section of its response. 7. Blind response forgery using birthday attack: Many DNS resolvers used a fixed port to send queries. With the exception of a random TXID, all values used by the resolver to determine the validity of a packet received in response to its query are now predictable. How to successfully apply this birthday attack is that forgery must arrive to the target resolver before the response from the legitimate authoritative server. Else not until its time-to-live (TTL) expires, the resolver can ask the authoritative server to resolve the same domain name, preventing the attacker from poisoning the mapping for that domain. 8. Kaminsky's exploit: It is a new extension of the birthday attack. 9. Response forgery using eavesdropping: Recently proposed defenses against DNS caching poisoning can prevent only blind forgery. DNS remains vulnerable to trivial attacks by compromised servers and/or network eavesdroppers. 10. For BIND resolver, if the attacker wants to compromise the mapping of an existing, there is a complication. The mappings for the name servers of popular domains tend to have long TTLs; they are likely to be already present in the victim's cache and must be overwritten. Unbound caches RRsets from the additional section but does not send them to clients by default. MaraDNS will accept the malicious authority section, but the mapping from the fake name server to an attacker-controlled IP address will not be cached. 11. There exists trust levels in BIND and Unbound, a cached RRset is overwritten if the trust level of the received RRset is higher or equal to the cached one and its TTL is longer. 12. MaraDNS does not use trust levels. There is no query that would give the attacker an opportunity to overwrite an existing A or CNAME record. 13. The primary purpose of the bailiwick rule is to prevent an authoritative server from claiming the mappings from domain names belonging to other authorities. 14. Adding a new CNAME record has the disadvantage via attack since if the attacker fails in a single race, the resolver will cache the failed label and the attacker must change the target name. 15. Adding a subdomain under an existing authority is dangerous to clients using BIND resolvers since many Web security policies are vulnerable to attacks from subdomains. 16. This attack is dangerous to clients of both BIND and Unbound. It results in changing the IP addresses of authoritative servers and enables the attacker to compromise any domain in the server's zone. 17. Overwriting an existing NS record is more serious than Kaminsky's exploit because it effectively hijacks every domain name under the compromised authorities. 18. Cache poisoning enables the attacker to insert a mapping for any domain name into the victim resolver's cache even if the domain does not exist in reality. 19. Hijacking a popular domain via a sub-authority is effective against both BIND and Unbound because it targets the authority section of a zone or the IP address of the zone's authoritative server, not the records in the additional section. 20. The most popular non-cryptographic defense against blind response forgery is UDP source port randomization. Other proposed solutions include increasing TTLs of legitimate records and limiting the number of simultaneous recursive queries.

Conclusion: The paper first introduces some basic concepts and then gave a formal model of DNS cache semantics. The result presents a comprehensive taxonomy of cache poisoning attacks, showing clearly which parts of the cache can be poisoned, conditions necessary for each attack and the if attack occurs. The formal model is an important tool for understanding the subtle caching rules used by modern DNS resolvers and developing defenses against DNS cache poisoning.