Scribe: Cryptography and Network Security (Week.4.Class.2.A)

Prashant Shishodia

4-Oct-2020

Introduction

Many differnet attacks can be carried out depending on the resources of the attacker. We'll go through the **Kaminsky attack** which makes use of glue records to hijack a whole domain, **BGP Hijacking** that blocks requests to a particular domain by redirecting them to a different address, and the **Dos attack** that is carried out by crashing the target either by exploiting bugs or by exhausting its resources.

Kaminsky Attack

Name Server is a specialized server that handles queries from your local computer, about the location of a domain name's various services.
Glue Record is the IP address of a name server at a domain name registry. It helps resolving the IP address of servers for different services provided by the domain. These glue records gets "glued" in local DNS, so that for further querying IP address for some service of a domain, the nameservers from these glue records are queried. Kaminsky attack works by exploiting this.

Attack

Attacker sets up a malicious website, where he runs the malicious javascript in the background. The user obiously, is unaware of it. The javascript code makes a network request to a service of domain that does not exist, say, *doesnotexist.example.com*. Since, the DNS doesn't know this host, it queries the DNS server for the IP address of *doesnotexist.example.com*. The attaker, ready for this moment, also sets up his own DNS server and floods the user's machine with his own records and different QID's in hope that his his record will reach the victim before actual DNS server's record, and will also match the QID with the QID of request made by the victim. The attacker's record tho, contains glue records that has nameservers for *example.com* mapped to IP addresses under his control. These glue-records, in response gets "glued" in local DNS, and whenever user tries to reach $someValidService.example.com$, users queries the attacker's controlled server, under the impression that it's querying the name server for *example.com*, making the attacker "owner" of the domain *example.com* in a sense.

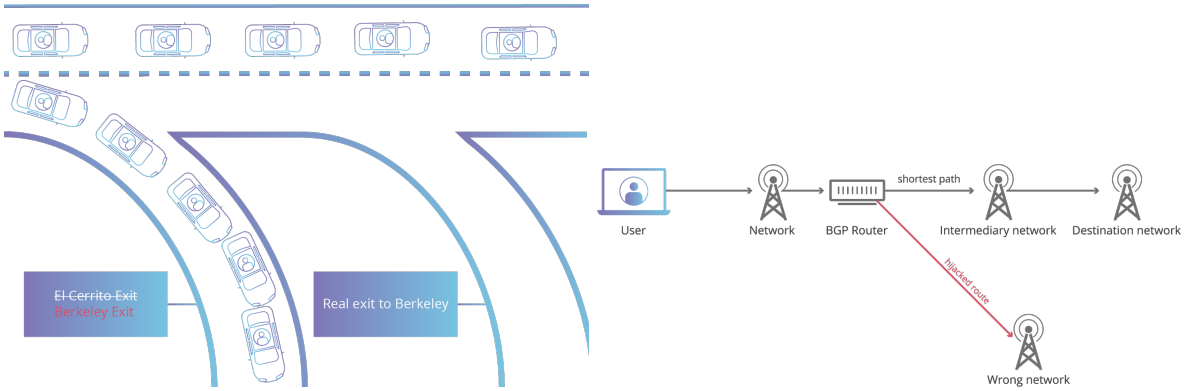
Assuming attacker's records always reach the victim before DNS server's, if the length of QID is 16 bits, the probability of sucessful attack for single record is $\frac{1}{2^{16}}$. To make the attack efficient, attacker can modify the javascript code to send, say, 1000 queries. Now the probability that atleast one QID will match boils down to $\frac{1}{65}$ for a single response from attacker's DNS server.

Solution

- Increase QID size to 32: Probability of attack reduces by a factor of 2^{16}
- Randomize Port: Reduces attack's probabilty by a factor of number of distinct port numbers.
- DNSSEC: slow adoption and high overhead. DNS responses are signed and higher level vouch for the lower levels.

1 BGP Hijacking

Border Gateway Protocol is used to route between two authorative nameservers, and can be hijacked if some nameserver provides "WRONG" information about other servers. It can be used by countries, say, to block some website inside their country. It can be understood with an analogy to the traffic. Some traffic polic, for some of his motives, misleads you by saying that the shortest path to your destination is different from the one you're currently going to, and mislead path leads to a place where the traffic police wants the victim to be.



Solution

- S-BGP: Routes and IP prefix announcements are signed and higher levels vouch for lower levels. But it's costly and the adoption is slow.
- TLS/SSL certification:
  - Certificate Authority issues public key certificates
  - CAs are shipped with browsers
  - Certificates lets you know if you're really talking to the domain you intended to

2 Denial of Service: Dos Attacks

DOS attacks are the easiest to pull, but really difficult to handle. DOS attack can be done either by crashing the service by exploiting some bug, or through the more often technique, by exhausting the resources of the target. The goal is to overload the target thus decreasing its availability, and to minimize the risk of getting tracked down. When a DOS attack is performed through multiple users, it is called **DDos** or **Distributed Dos**.

TCP SYN Flood

The TCP stacks keeps track of the incoming TCP requests, to allow persisting after TIME OUT. The attacker exploits this and floods the target with SYN packets, but drop the packets that the target sends back. The target's memory eventually overflows without affecting the victim, thus indicating a kind of *asymmetry* between the attacker's and target's resources consumed.

Conclusion

System can be attacked in multiple ways by exploiting the methodologies used to communicate between a client and a server. Some methods provides better security but are costly and slow, others on the other hand, provide reasonable security with reasonable cost and fast adoption. While most of the attacks requires more resources on the attacker's side, Dos/DDos attack does not.