COMP 434 - Short Paper 2 - 40616 - Ahmet Can Turgut

DKIM Modification for DNS Based Attacks.

Introduction

DNS (domain name system) is a naming system for devices which connected to the internet. DNS has a hierarchical structure. For clarifying definition of DNS fallowing scenario can be considered.

Computer “A” request to visit http://www.webpage.com. This request goes to nearest DNS server, if it is not available, then it asks another DNS server to find IP address of the given link. If last server has IP address. Requested web pages ip address reversely fallow the path and goes to computer which request web pages ip address. DNS basically can be defined as text to IP and IP to text translator.

DNS has actually has gaps which should be considered network security gap. Such as DNS spoofing (DNS cache poisoning attack). DNS spoofing is important point for the recent network security issues [1].

A type of coexistence that allows a root DNS server to advertise itself as a competent DNS server by sending a modified tcp / ip packet to its headers and redirect domain name information to the desired location [1]. DNS spoofing explained detailed later.

Against to DNS attacks for mail sides some defend mechanisms implemented such as S/MIME (Secure Multipurpose Internet Messaging Extensions) .

1. DNS Cache Poisoning

With this method, spoof packets are sent to the DNS servers of the opposite site, cached and poisoned the cache of the DNS server by changing the data of the queries that are sent, which is possible with complicated software and tactical DNS queries [1]. When successful, the victims are attacked by attackers and the DNS that the attacker identifies from the poisoned DNS server are starting to resolve the threads, in fact this bind has affected the DNS servers, and these exploits have been shut down in great detail, but there is no rule that it will not go back to the open relay again, similar to other DNS servers can live.

Normally, to apply DNS poisoning a little bit, you need to know the DNS server that the person uses and attack based on it. To know this, you also need to know the ISP used by that person. This is not only for DNS poisoning but also for cache poisoning [1].

2. DKIM and S/MIME

a. DKIM (Domain Keys Identified Mail)

DKIM is a method which implemented between trusted domains for identification of the mail which belongs who. This method shortly implemented for mail spoofing. DKIM allows for two main operations, signing and verifying [2]. It holds the public keys into DNS server. Although it is useful for the email spoofing, it fails DNS spoofing. DKIM scenario shown below.

Email send out with DKIM which is signed with private key. Email request goes to Email service provider. Email service provider receive public key of the sender from DNS server. Than receiver verify email using public key which is obtained from DNS server [3].

b. S/MIM (Secure Multipurpose Internet Messaging Extensions)

A structure that provides secure (signed - encrypted - signed and encrypted) messaging between two end users over internet or similar media [4]. This structure allows to identify and verify received mails comes from supposed to be user. In S/MIME both sender and receiver have own their private keys. S/MIME scenario given fallow.

Sender sign email with private key and encrypt it. Sender also create secret key and encrypted packet. Sender sends secret key within encrypted packet. Then sender sends encrypted email. Receiver first receive encrypted packet contains secret key. Then decrypt packet. Next, receiver decrypt email with using secret key of receiver. Then receiver verify email with public key which is certificated by sender [4].

3. Why DNS Spoofing Successful for DKIM's and Fails for S/MIME

Basic reason is S/MIME did not use any DNS server for public key holding. As above mentioned that DKIM use DNS server for saving public keys. Attacker can use DNS spoofing for attacking DKIM user and replace public key as attacker wanted.

4. DKIM Improvement Against DNS Based Attacks

DKIM public key storage may changed with trusted server or more secure server which secured against DNS spoofing. But this not gives a full trust since receiver or sender never trust security capabilities of the server which stores public keys. Attacker may find this server and use DNS lookup and fallow find trusted server. This creates a problem for server security against DNS spoofing.

How to preventing against DNS based attacks explained fallowing article "DNS security: Poisoning, attacks and mitigation" [5].

According to given article extra solutions below for trusted server [5].

"SOURCE PORT RANDOMISATION
TRANSPORT SECURITY FOR DNS TRAFFIC
MULTIPLE QUERIES
SOURCE CASE RANDOMISATION" [5]

With these solutions trusted server may secured against DNS based attacks.

Moreover receiver and sender should be aware and secure their systems against DNS based attacks.

Other kind of modifications makes DKIM much like S/MIME and it makes non-sense to use DKIM.

Another solution is depends on the user behaviours. Mail providers may hold user behaviours which is DNS addresses and try to compare and detect any DNS based attacks happen or not.

Conclusion

DKIM is much more easy to use mail service when looked from user and developer side. Some times users should choose usability against security. In that case DKIM modification against DNS attacks has important role. Since users cant be pushed to use S/MIME. May be easy to use mail services implemented which use S/MIME type data transfer.

References

[1] Son, S., & Shmatikov, V. (n.d.). The Hitchhiker's Guide to DNS Cache Poisoning. Retrieved from https://www.cs.cornell.edu/~shmat/shmat_securecomm10.pdf

[2] DomainKeys Identified Mail (DKIM). (n.d.). Retrieved April 18, 2017, from http://dkim.org/

[3] Hansen, T., & Hallam-Baker, P. (n.d.). DomainKeys Identified Mail (DKIM) Service Overview. Retrieved from https://tools.ietf.org/html/rfc5585

[4] NIA - NATO Information Assurance. (n.d.). Retrieved April 19, 2017, from http://www.ia.nato.int/s-mime

[5] Agar, R. & Paterson, K. (n.d.). Royal Holloway Series 2010 DNS security: poisoning, attacks and mitigation. Retrieved from http://cdn.ttgtmedia.com/searchSecurityUK/downloads/RHUL_Agar_2010.pdf

——

"Note: Figure, draw. Ahmet Can Turgut using adobe cc." Icons taken from web.
Minimalist Server Icon - https://www.vecteezy.com/free-vector/server Retrieved April 18, 2017