ASDWL: Mitigating DNS Random Subdomain Attacks for Second Level Domain

Lanlan Pan (潘蓝兰)

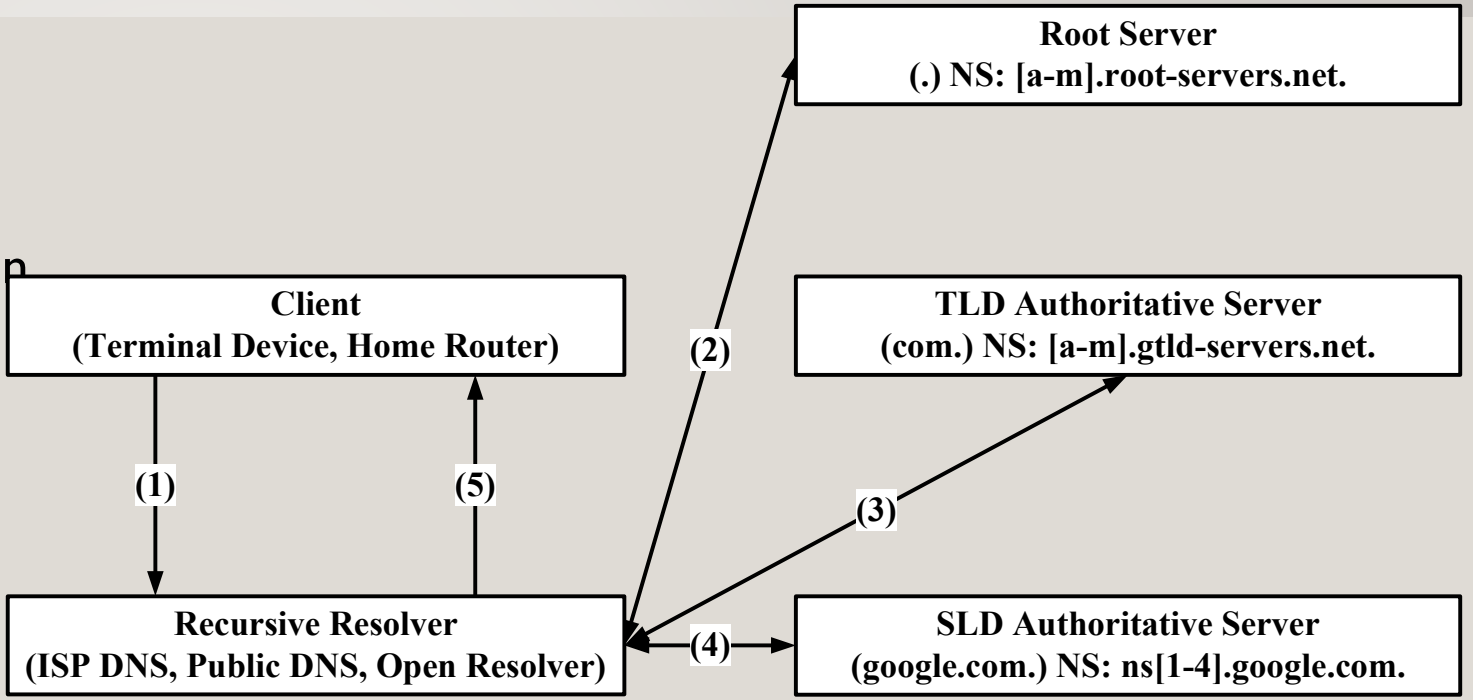
abbypan@gmail.com

Outline

- Introduction
- DNS Random Subdomain Attack
- Related Work
- Our Contribution
- Conclusion

Introduction

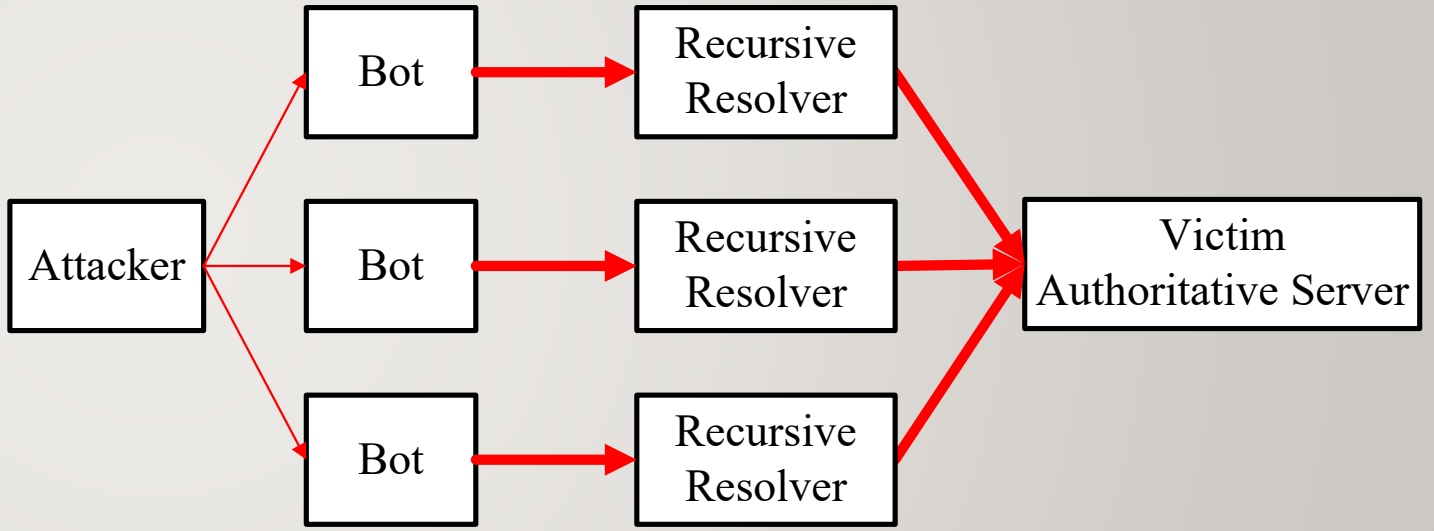
- **Client** sends the recursive domain query for "www.google.com" to recursive resolver.
- **Recursive resolver** sends the iterative domain query for "www.google.com" to "google.com" SLD authoritative server, get the A/AAAA record of "www.google.com".



The default acceptance of domain queries from all over the internet makes DNS vulnerable to distributed denial-of-service (DDoS) attacks.

DNS Random Subdomain Attack

1. The attacker orchestrates huge amounts of bots under their control.
2. These bots are then instructed to send queries to recursive resolvers.
3. These queries are random subdomains under the victim domains, which are not currently cached in recursive resolvers. Consequently, the recursive resolvers must forward these queries to the authoritative servers responsible for the victim domains.
4. This process places a significant burden on both the recursive resolvers and the authoritative servers, potentially leading to service degradation or outright failure.



DNS Random Subdomain Attack

- The attack is hard to mitigate because:
  - The recursive resolvers are legitimate to authoritative servers.
    - Authoritative servers could not block all the queries from recursive resolver on critical second level domain (SLD), but just make rate limiting response.
    - If they fully drop the queries from legitimate clients, the recursive resolvers may make more retry queries, result in DDoS like DYN2016.
  - The bots are legitimate to recursive resolvers.
    - Recursive resolvers, especially the ISP recursive resolvers, could not block all queries from the bots on critical SLD, but just make rate limiting response.
    - If they fully drop the queries from legitimate clients, the bots may make more retry queries, result in DDoS like Baofeng2009.

Related Work

- **DNSSEC**
  - By caching of DNSSEC's NSEC/NSEC3 responses, recursive resolvers can mitigate the random subdomain attacks.
  - Meanwhile, DNSSEC-signed domains could be abused directly on authoritative servers for amplification attacks.
- **Whitelist**
  - Keita H., et al [9] build FQDN-based whitelist filter that registers actually existing FQDN from DNS traffic datasets, and drops the non-existent subdomains created by the attackers.
  - Its effect depends on the accurancy and freshness of DNS traffic datasets.
- **Subdomain Detection**
  - Shir F., et al [10], Takeuchi, et al [11], Keita H, et al [12] provide some random subdomain detection methods.
  - Their effects depend on peace time traffic analysis and ongoing attack time traffic analysis on the proposed algorithm.

Our Contribution

- We propose an authenticated subdomain whitelist (ASDWL) scheme to address the issue of DNS random subdomain attacks specifically targeting second level domains (SLDs).
- We make the cooperation between domain-based authentication of named entities (DANE) and JSON web signature (JWS) for verification.
- We introduce a well-known subdomain to publish the ASDWL.
- We present a mitigation proposal aimed at reducing the query burden between recursive resolvers and authoritative servers, and cutting down on the cache of random subdomains stored by recursive resolvers.

Administrator of SLD: Generate ASDWL

- Private key d_{wl} used to sign the ASDWL
- End-entity X.509 certificate C_{wl} for the corresponding public key pubwl used to verify the ASDWL signature.

- ASDWL follows the flattened JWS JSON serialization syntax.
  - payload: Contains the whitelist subdomains information configured by the domain administrator of SLD.
  - x5c: Contains the X.509 certificate Cwl corresponding to the key d_{wl} used to sign the ASDWL payload.
  - signature: Contains the signature of the payload, which is signed by d_{wl}, and verified by the corresponding certificate C_{wl}.

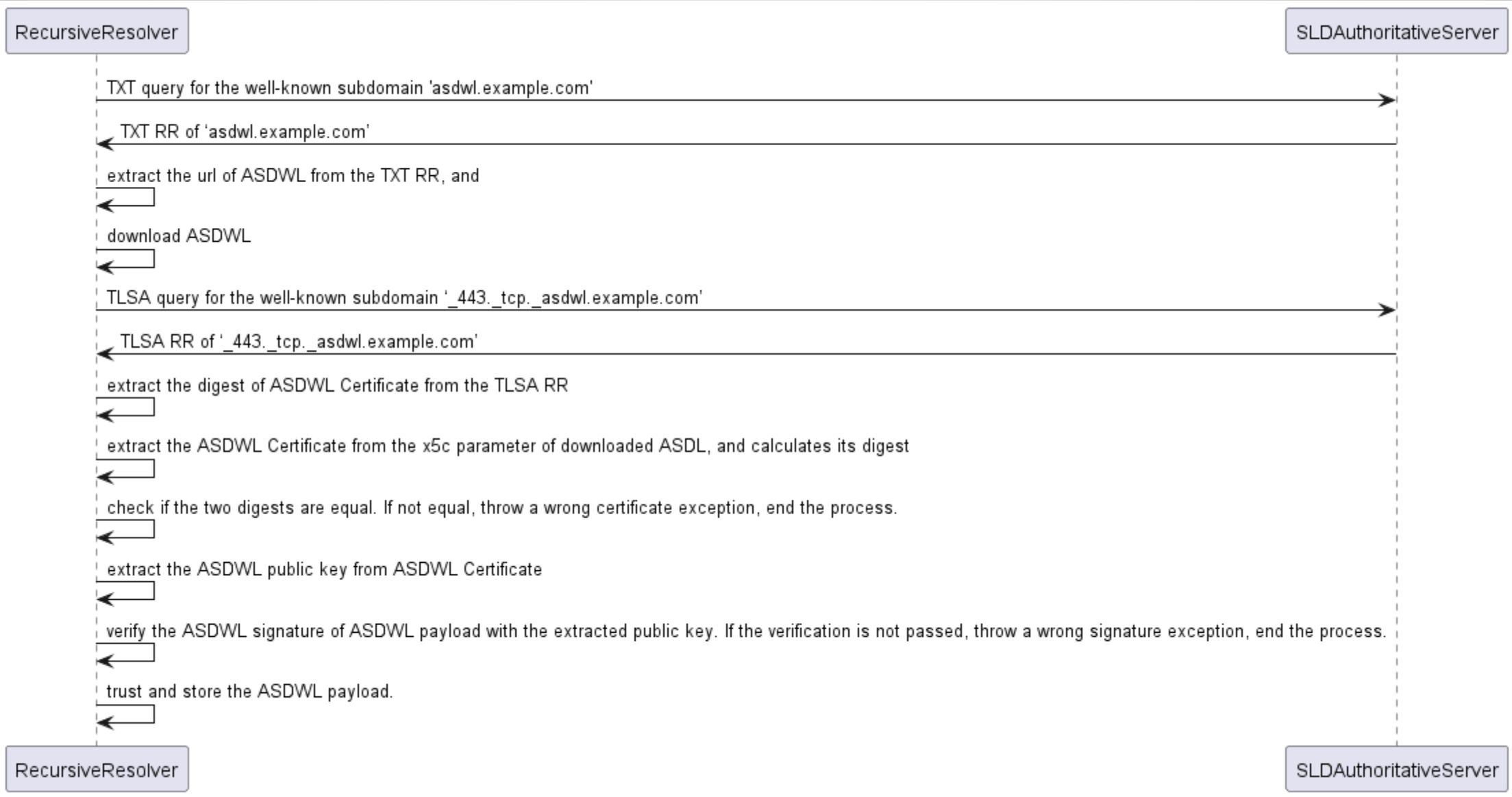
```
{
  'payload': {
    'dom': 'example.com',
    'date': '2023-12-25',
    'subdoms': [
      'abc'
    ],
    'wildcard_subdoms': [
      'xxx'
    ]
  },
  'header': {
    'alg' : 'ES256',
    'x5c' : ....,
  },
  'signature': ...
}
```

Administrator of SLD: Publish ASDWL

- Administrator of SLD defines a well-known subdomain ‘ asdwl.example.com’ for the SLD to publish its ASDWL, and configure a DANE TLSA RR [2] and a TXT RR [14] for it.

RR
_443._tcp._asdwl.example.com. 3600 IN TLSA (3 0 1 d2abde240d7cd3ee6b4b28c54df034b9 7983a1d16e8a410e4561cb106618e971)
_asdwl.example.com. 3600 IN TXT ‘url=https://www.foo.com/asdwl_example_com.json’

Recursive Resolver: Get ASDWL



Mitigate Random Subdomain Attacks with ASDWL

Recursive Resolver (RS):

- RS allows all the legitimate queries of the whitelist subdomains from clients, and sends the queries to AS_{sld}.
- RS allows all the legitimate queries of the whitelist wildcard subdomains from clients, only sends one query to AS_{sld} for each wildcard subdomain zone, and store one response for all queries in the wildcard subdomain zone.
- RS makes rate limiting responses on other subdomains queries when it could afford. RS drops the queries of other subdomains when the traffic is overwhelmed.

SLD Authoritative Server (AS_{sld}):

- AS_{sld} allows all the legitimate queries of the whitelist subdomains from RS.
- AS_{sld} allows all the legitimate queries of the whitelist wildcard subdomains from RS.
- AS_{sld} makes rate limiting responses on other subdomains queries from RS when it could afford. AS_{sld} drops the queries of other subdomains from RS when the traffic is overwhelmed.

Evaluation

Scheme	Random Subdomain Detection	Wildcard Cache Reduction	NXDOMAIN Cache Reduction	Online Queries for Filtering	Offline Traffic Analysis
NSEC/NSEC3 [4] [7]	×	√	√	√	×
Keita H., et al [9]	×	×	√	×	√
Shir F., et al [10]	√	×	√	×	√
Takeuchi, et al [11]	√	×	√	×	√
Keita H, et al [12]	√	×	√	×	√
Our Scheme	×	√	√	×	×

Conclusion

- Our Work
  - We describe an authenticated subdomain whitelist (ASDWL) scheme to mitigate DNS random subdomain attacks.
  - We focus on how to make authoritative server provide its own subdomain whitelist, and make recursive resolver get the whitelist securely.
  - Our scheme is simple to deploy, compatible with DNSSEC and other subdomain detection scheme.
- Limitation
  - We don't discuss about how to identify random subdomain attacks, or how to extracts subdomains from DNS traffic.
- Future Work
  - Do more evaluation on our scheme, and deploy it on DNS system.

THANK YOU

Q&A

Reference

[1] P. Mockapetris, “Domain names-concepts and facilities,” Tech. Rep.,1987.

[2] P. Hoffman and J. Schlyter, “The dns-based authentication of named entities (dane) transport layer security (tls) protocol: Tlsa,” Tech. Rep., 2012.

[3] M. Jones, J. Bradley, and N. Sakimura, “Rfc7515: Json web signature (jws),” Tech. Rep., 2015.

[4] P. Hoffman, “Rfc 9364: Dns security extensions (dnssec),” 2023.

[5] Wiki, “Ddos attacks on dyn,” 2016, https://en.wikipedia.org/wiki/DDoS attacks on Dyn.

[6] ComputerWorld, “Dns attack downs internet in parts of china,” 2009, https://www.computerworld.com/article/2525397/dns-attack-downsinternet-in-parts-of-china.html.

[7] G. Miek, “Rfc 7129: Authenticated denial of existence in the dns,” 2014.

[8] R. van Rijswijk-Deij, A. Sperotto, and A. Pras, “Dnssec and its potential for ddos attacks: a comprehensive measurement study,” in Proceedings of the 2014 Conference on Internet Measurement Conference, 2014, pp. 449–460.

[9] K. Hasegawa, D. Kondo, and H. Tode, “Fqdn-based whitelist filter on a dns cache server against the dns water torture attack,” in 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM). IEEE, 2021, pp. 628–632.

[10] S. L. Feibish, Y. Afek, A. Bremler-Barr, E. Cohen, and M. Shagam,“Mitigating dns random subdomain ddos attacks by distinct heavy hitters sketches,” in Proceedings of the fifth ACM/IEEE workshop on hot topics in web systems and technologies, 2017, pp. 1–6.

[11] Y. Takeuchi, T. Yoshida, R. Kobayashi, M. Kato, and H. Kishimoto, “Detection of the dns water torture attack by analyzing features of the subdomain name,” Journal of Information Processing, vol. 24, no. 5, pp. 793–801, 2016.

[12] K. Hasegawa, D. Kondo, M. Osumi, and H. Tode, “Collaborative defense framework using fqdn-based allowlist filter against dns water torture attack,” IEEE Transactions on Network and Service Management, 2023.

[13] N. SP, “Recommendations for discrete logarithm-based cryptography,”2023.

[14] P. V. Mockapetris, “Rfc1035: Domain names-implementation and specification,” 1987.

[15] NIST, “Estimating ipv6 & dnssec deployment snapshots,” 2023, https://usgv6-deploymon.antd.nist.gov/snap-all.html.

[16] Rbsec, “Wordlist-based dns subdomain scanner,” 2002, https://github.com/rbsec/dnsscan