TOM PUSATERI
WILLEM TOOROP

IETF 102 JULY 2018

DHCPV6 DNS THREATS

VULNERABILITIES PRIOR TO NEW DHCPV6 OPTIONS

- **Information disclosure** - unencrypted local observation of DNS packets
- **Information disclosure** - logging, analyzing, use of private DATA at the DNS resolver supplied by DHCP
- **Spoofing** - rogue DHCP servers sending decoy DNS resolver information
- **Tampering** - DNS queries could be modified or responses modified or filtered
- **Repudiation** - NXDOMAIN can be returned for records that exist
- **Denial of service** - NXDOMAIN responses or error injection

MITIGATIONS PRIOR TO ADN DHCPV6 OPTION

Threat	DNSSEC	Other
Information disclosure on wire	✗	TLS w/delay
Information disclosure @ resolver	✗	✗
Spoofing of resolver	✗	PTR w/delay CERT val
Tampering	✓	
Repudiation	✓	
Denial of service	✓	

MITIGATIONS WITH ADN DHCPV6 OPTION

Threat	DNSSEC	Other
Information disclosure on wire	✗	TLS no delay
Information disclosure @ resolver	✗	Reputation
Spoofing of resolver / MITM	✗	CERT/DANE/SPKI PIN
Tampering	✓	Reputation / SIG(0)
Repudiation	✓	Reputation
Denial of service	✓	Reputation

DO WE NEED A DNS RESOLVER REPUTATION SERVICE?

How would that work?

REPUTATION SERVICE

- HTTPS uses OCSP to get certificate revocation info
- DNS Resolvers could have a similar but different reputation service
- Operating system / DHCP client vendors could use whitelists/blacklists to filter DHCP resolvers from operators
- dnsprivacy.org has provided a starting point of trustworthy DoT/DoH servers
- Authenticated resolvers with certs / DANE records are the basis for correctly identifying and cataloging the resolvers

SUMMARY

- DNSSEC provides the biggest gain in integrity when using DHCP provided DNS resolvers
- Authenticating the certificate of a TLS DNS resolver (DoT/DoH) provides integrity of the service and prevents MITM
- Knowing the ADN ahead of time, reduces delays, increases confidence
- Reputation services can augment trust relationship with unfamiliar resolvers and allow the community to effectively block bad actors
- Is it time to deprecate DNS over UDP between client and resolver to allow DNSSEC to proliferate?