Using DNS resolvers as certificate validators

Taekyoung (Ted) Kwon, Seoul National University
End hosts validate certificates

• Receive one or more certificates
  • End user certificate
  • Root CA certificate is already installed
  • Intermediate CA certificates may have to be downloaded
• Check whether certificates are not revoked
  • CRL or OCSP
  • Mostly soft-fail approaches
• Validate the certificate chain
• After the validation, its result is not reused
Certificate validation will burden CAs

- CRL servers
- OCSP servers
  - OCSP stapling will mitigate the burden substantially...
Just as local DNS resolvers relieve authoritative DNS servers

- If local DNS resolvers perform certificate validation on behalf of clients
- And if the certificate validation results can be cached

- CA can reduce the cost of running CRL/OCSP servers
  - Cost-effective
Pre-conditions

• DoT/DoH connections between clients and local DNS resolvers

• Local DNS resolvers are trustworthy
  • Remote attestation is needed?
Issues

• How long can validation results be cached?
• Who will decide/recommend the caching period?
  • Local DNS resolver operator?
  • CAB forum?
  • Client?
Fundamental question is...

• End hosts vs intermediaries....
Thank you!