Less is More
Cipher-Suite Negotiation for DNSSEC

Amir Herzberg
Bar-Ilan University

Haya Shulman
Technische Universität Darmstadt

Bruno Crispo
Trento University

12/12/2014 Herzberg, Shulman and Crispo: Cipher-Suite Negotiation for DNSSEC
Domain Name System (DNS)

- Lookup services
  - Locate resources: via names
  - Authentication: black lists, policies, security mechanisms (SPF, ROVER, ...)

- Problem: no authentication of DNS responses
Domain Name System (DNS)

- Problem: no authentication of DNS responses
- Attacker can provide spoofed records
- Resolver caches
- Clients redirected to incorrect (malicious) hosts

www.foo.com  A 6.6.6.6
Domain Name System (DNS)

- Problem: no authentication of DNS responses
  - Attacker can provide spoofed records
  - Resolver caches
  - Clients redirected to incorrect (malicious) hosts
DNS Security (DNSSEC)

• DNSSEC prevents attacks
  • On-path (MitM) attacks (NSA, China, GCHQ,...?)
  • Off-path attacks [HS12, HS13a-c, SW14]
  • Vulnerable name servers

• DNSSEC provides evidences
  • Enables forensic analysis, detection of attacks see [SW14]

• DNSSEC would facilitate security protocols
  • ROVER, DANE...
DNS Security (DNSSEC)

- Zone file is signed
- Name server sends keys and signatures over DNS records
- Resolver validates signatures
- Enables detection of spoofed responses
DNS Security (DNSSEC)

• Only few support it
• Many resolvers signal `DNSSEC OK´
  • Only <5% validate
• Many (important) zones got signed
  • Forward DNS: Root, >62% TLDS, but only <1% SLDs
  • Reverse DNS (IPv4): arpa, in-addr.arpa
    but only <1% subdomains
Obstacles to DNSSEC Adoption

• Zone file is signed with *all supported ciphers*
• Name server sends *all keys and signatures* over DNS records
• Resolver validates *all signatures*
• Overhead!!
Servers Send Key/SIGs for ALL Supported Algs. \( \rightarrow \) Large Responses!

- Blocked at intermediate devices e.g., firewalls

- Off-path attacks DoS and poisoning [HS12,HS13a-c,SW14]
Servers Send Key/SIGs for ALL Supported Algs. → Large Responses!

- Transition to TCP?
  - Not all support
  - Overhead
- Low motivation to adopt ``shorter´´ algs
  - Mandatory support of RSA 1024
- More algs. increase responses sizes
Supported DNSSEC Algorithms

- Weak ciphers
  Mandatory support of RSA1024
- No motivation to adopt better ciphers
  - Shorter signatures
  - More secure
Cipher-Suite Negotiation for DNSSEC

• Goals:
  • Protect DNS transaction with optimal cipher
    • Reduce responses size and latency
  • Robust to downgrade
  • Interoperability with legacy proxies
• Hop-by-hop or end-to-end?
Hop-by-Hop Cipher-Suite Negotiation

- EDNS allows to introduce new options to DNS
- Resolver signals its ciphers and priorities in EDNS in DNS request
- Server sends records protected with the optimal cipher
  - Prevent downgrade → attach a signed list of supported ciphers in response
Hop-by-Hop Cipher-Suite Negotiation

1. Check CIPHER contains correct negotiated option.
2. Validate signature RRSIG over CIPHERS.
3. Forward to Resolver

DNS request
A?www.foo.bar

Add list of ciphers to EDNS

DNS response
www.foo.bar IN 1.2.3.4

Store ciphers list and forward to name server

www.foo.bar IN 1.2.3.4

Cipher-Suite Negotiation for DNSSEC

Herzberg, Shulman and Crispo:

12/12/2014
Hop-by-Hop Cipher-Suite Negotiation

- But: intermediate proxies
  - Respond with cached signatures → may not be the priority/ciphers supported by requesting resolvers
  - Legacy proxies fall back to traditional DNSSEC
End-to-End Cipher-Suite Negotiation

- Server signals its ciphers in a special DNSKEY record (with new code)

- DNSKEY encodes the public verification key of the zone

```
foo.bar. 3379 IN DNSKEY 257 3 42
(RSA/SHA1(3), RSA/SHA1-NSEC3-SHA1(2), ECDSA Curve P-256 with SHA-256(1)= ) ; key id = 12319
```
End-to-End Cipher-Suite Negotiation

- Server signals its ciphers in a special DNSKEY record
  - Key is cached by the resolvers

- Resolver concatenates cipher to query `cipher.delimiter.domain: 13._csn_.foo.bar`

- Name server returns requested record protected with the optimal cipher

5  - RSA/SHA1
7  - RSA/SHA1-NSEC3-SHA1
13 - ECDSA Curve P-256 with SHA-256
42  - CIPHERS NEGOTIATION
End-to-End Cipher-Suite Negotiation

- Resolver identifies supporting name servers in advance
  - Via the special DNSKEY record
  - DNSKEY is requested once and cached according to TTL
- No redundant queries
- Optimal utilisation of intermediate caches
Conclusions

• DNSSEC-adopters use all supported ciphers
• **Overhead** is obstacle to DNSSEC adoption
• **Mitigation**: cipher suite negotiation
• Challenge: intermediate proxies
  • Hop-by-hop cipher suite negotiation is non-interoperable
  • End-to-end cipher suite negotiation
    • Resolver identifies supporting name servers in advance
    • No redundant queries and optimal utilisation of intermediate caches
Questions?

Thank you!