ECDSA P-256 support in DNSSEC-validating Resolvers

Geoff Huston, George Michaelson
APNIC Labs, May 2015

ECDSA

- Elliptic Curve Cryptography allows for the construction of “strong” public/private key pairs with key lengths that are far shorter than equivalent strength keys using RSA

  “256-bit ECC public key should provide comparable security to a 3072-bit RSA public key” *

- And the DNS protocol has some sensitivities over size when using UDP
  - UDP fragmentation has its issues in both V4 and V6

* http://en.wikipedia.org/wiki/Elliptic_curve_cryptography

ECDSA vs RSS

```
$ dig +dnssec u5221730329.s1425859199.i5075.vcf100.5a593.y.do

; <<>> DiG 9.9.6-P1 <<>> +dnssec u5221730329.s1425859199.i507
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61126
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADD

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;u5221730329.s1425859199.i5075.vcf100.5a593.y.dotnxdomain.net

;; ANSWER SECTION:
u5221730329.s1425859199.i5075.vcf100.5a593.y.dotnxdomain.net.
u5221730329.s1425859199.i5075.vcf100.5a593.y.dotnxdomain.net.

;; AUTHORITY SECTION:
ns1.5a593.y.dotnxdomain.net. 1       IN      NSEC    x.5a593.y
ns1.5a593.y.dotnxdomain.net. 1       IN      RRSIG   NSEC 13 5
5a593.y.dotnxdomain.net. 3598 IN     NS      ns1.5a593.y.dotn
5a593.y.dotnxdomain.net. 3600 IN     RRSIG   NS 13 4 3600 202

;; Query time: 1880 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Mar 12 03:59:42 UTC 2015
;; MSG SIZE  rcvd: 527
```

ECDSA signed response – 527 octets

```
$ dig +dnssec u5221730329.s1425859199.i5075.vcf100.5a593.z.dotnxdomain.net

; <<>> DiG 9.9.6-P1 <<>> +dnssec u5221730329.s1425859199.i5075.vcf100.5a59
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25461
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;u5221730329.s1425859199.i5075.vcf100.5a593.z.dotnxdomain.net. IN A

;; ANSWER SECTION:
u5221730329.s1425859199.i5075.vcf100.5a593.z.dotnxdomain.net. 1    IN A 19
u5221730329.s1425859199.i5075.vcf100.5a593.z.dotnxdomain.net. 1    IN RRSI

;; AUTHORITY SECTION:
33d23a33.3b7acf35.9bd5b553.3ad4aa35.09207c36.a095a7ae.1dc33700.103ad556.3a
33d23a33.3b7acf35.9bd5b553.3ad4aa35.09207c36.a095a7ae.1dc33700.103ad556.3a
5a593.z.dotnxdomain.net. 3599 IN     NS      nsz1.z.dotnxdomain.net.
5a593.z.dotnxdomain.net. 3600 IN     RRSIG   NS 5 4 3600 20200724235900 20

;; Query time: 1052 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Mar 12 03:59:57 UTC 2015
;; MSG SIZE  rcvd: 937
```

RSA signed response – 937 octets

So lets use ECDSA for DNSSEC

Yes?

- Is ECDSA a “well supported” crypto protocol?
- If you signed using ECDSA would resolvers validate the signature?

The Test Environment

We used the Google Ad network in March 2015 to deliver a set of DNS tests to clients to determine whether (or not) they use DNSSEC validating resolvers

We used 5 tests:

1. no DNSSEC-signature at all
2. DNSSEC signature using RSA-based algorithm
3. DNSSEC signature using broken RSA-based algorithm
4. DNSSEC signature using ECDSA P-256 algorithm
5. DNSSEC signature using broken ECDSA P-256 algorithm

The Test Environment

d.t10000.u2045476887.s1412035201.i5053.vne0001.4f167.z.dashnxdomain.net Unsigned

e.t10000.u2045476887.s1412035201.i5053.vne0001.4f167.z.dotnxdomain.net RSA Signed

f.t10000.u2045476887.s1412035201.i5053.vne0001.4f168.z.dotnxdomain.net RSA signed (Badly)

m.t10000.u2045476887.s1412035201.i5053.vne0001.4f167.y.dotnxdomain.net ECDSA-Signed

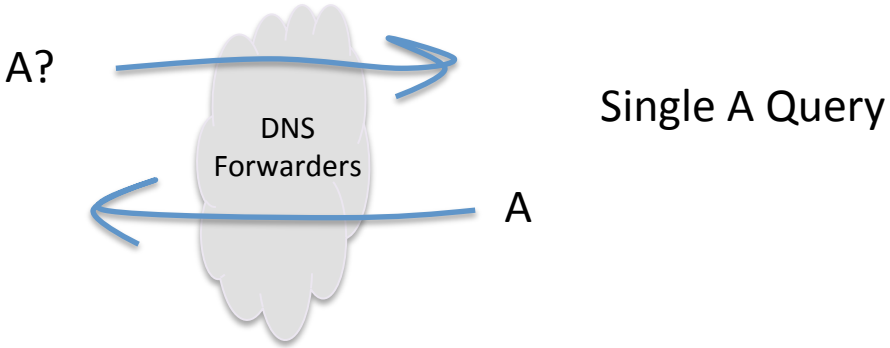
n.t10000.u2045476887.s1412035201.i5053.vne0001.4f168.y.dotnxdomain.net ECDSA-Signed (bad!)

Mapped to a wildcard in the zone file

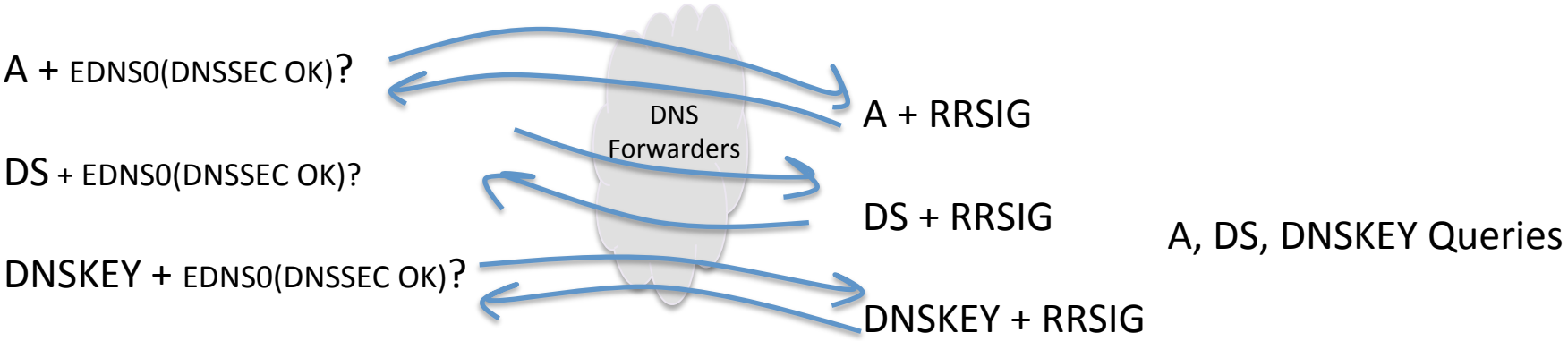
Unique Signed Zone

A Naïve View

A non-DNSSEC-validating resolver query:



A DNSSEC-Validating resolver query:



Theory: DNSSEC Validation Queries

`e.t10000.u2045476887.s1412035201.i5053.vne0001.4f167.z.dotnxdomain.net`

1. Query for the A resource record with EDNS0, DNSSEC-OK

   query: e.t10000.u204546887.s1412035201.i5053.vne0001.4f167.z.dotnxdomain.net IN A +ED

2. Query the parent domain for the DS resource record

   query: 4f167.z.dotnxdomain.net IN DS +ED

3. Query for the DNSKEY resource record

   query: 4f167.z.dotnxdomain.net IN DNSKEY +ED

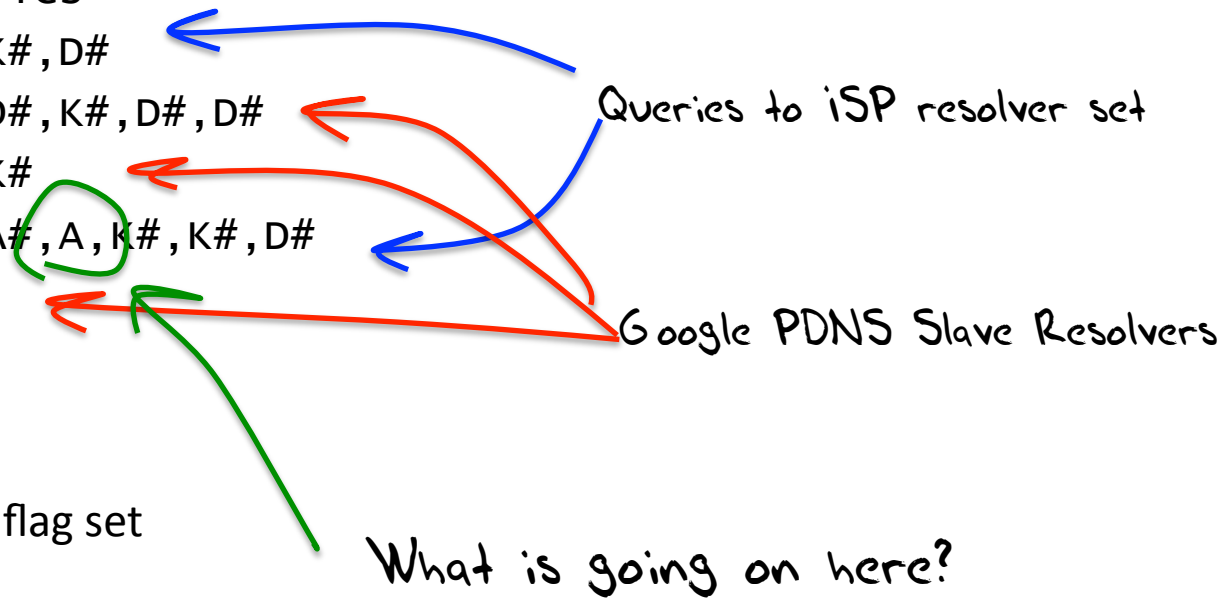
Practice: The DNS is "messy"

- Clients typically use multiple resolvers, and use local timeouts to repeat the query across these resolvers
- Resolvers may use slave farms, so that queries from a common logical resolution process may be presented to the authoritative name server from multiple resolvers, and each slave resolver that directs queries to servers may present only a partial set of validation queries
- Resolvers may use forwarding resolvers, and may explicitly request checking disabled to disable the forwarding resolver from performing validation itself
- Clients and resolvers have their own independent retry and abandon timers

DNS Mess!

Queries for a single badly signed (RSA) name:

```
Resolver        Queries
200.55.224.68:  A#,K#,D#
74.125.19.147:  A#,D#,K#,D#,D#
74.125.19.145:  K#,K#
200.55.224.67:  A#,A#,A,K#,K#,D#
74.125.19.148:  D#
```



#: EDNS(0), DNSSEC OK flag set

DNS Mess!

Queries for a single badly signed (RSA) name:

Resolver	Queries
200.55.224.68:	A#,K#,D#
74.125.19.147:	A#,D#,K#,D#,D#
74.125.19.145:	K#,K#
200.55.224.67:	A#,A#,A,K#,K#,D#
74.125.19.148:	D#

Failed validation (SERVFAIL) from the initial query to ISP resolver causes client to ask Google PDNS resolver

Failed validation appears to cause client to repeat the query to Google PDNS 2 further times

Failed validation appears to cause client to repeat the query to ISP's resolver 2 (or 3?) further times

No clue why this is an orphan DS query!

#: EDNS(0), DNSSEC OK flag set

First Approach to answering the ECDSA question - Statistical Inference

- A DNSSEC-aware resolver encountering a RR with an attached RRSIG that uses a known algorithm will query for DS and DNSKEY RRs

- A DNSSEC-aware resolver encountering a RR with an attached RRSIG that uses an unknown/unsupported crypto algorithm appears ***not*** to query for the DNSKEY RRs

Results

Over 18 days in March 2015 we saw:

11,988,195 completed experiments

2,970,902 experiments queried for the DNSKEY RR of a validly signed (RSA) domain **(24.8%**)

2,391,298 experiments queried for the DNSKEY RR of a validly signed (ECC) domain (**19.9%**)

Results

Over 18 days in March 2015 we saw:

11,988,195 completed experiments

2,970,902 experiments queried for the DNSKEY RR of a validly signed (RSA) domain (**24.8%**)

2,391,298 experiments queried for the DNSKEY RR of a validly signed (ECC) domain (**19.9%**)

If we assume that the DNSKEY query indicates that the resolver "recognises" the signing protocol, then it appears that there is a fall by 20% in DNSSEC validation when using ECDSA

1 in 5 RSA experiments that fetched the DNSKEY did not fetch the ECC DNSKEY

That's better than it was…

Over 22 days in September 2014 we saw:

- 3,773,420 experiments
  - 937,166 experiments queried for the DNSKEY RR of a validly signed (RSA) domain (**24.8%**)
  - 629,726 experiments queried for the DNSKEY RR of a validly signed (ECC) domain (**16.6%**)

1 in 3 experiments that fetched the DNSKEY in RSA did not fetch the ECDSA-signed DNSKEY

Protocol Recognition

- When does the resolver “recognise” the signing protocol?
  - RRSIG field?
  - DS RR?
  - DNSKEY RR?

Experiments	ECDSA DS	ECDSA DNSKEY	RSA DS	RSA DNSKEY
11,988,195	2,957,855	2,391,298	2,963,888	2,970,902

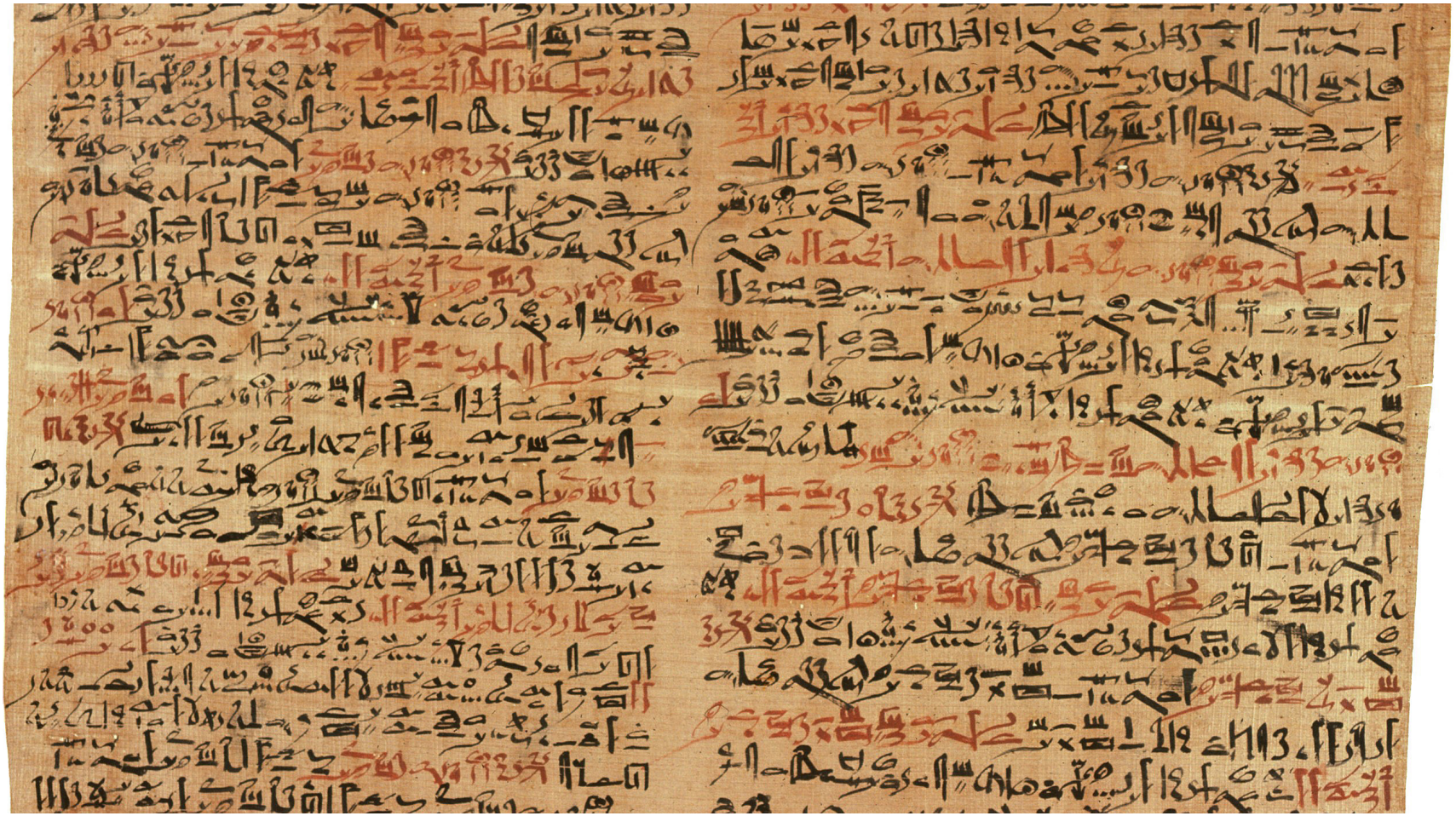
Protocol Recognition

- When does the resolver "recognise" the signing protocol?
  - RRSIG field? ✗
  - DS RR? ✓
  - DNSKEY RR? ✗

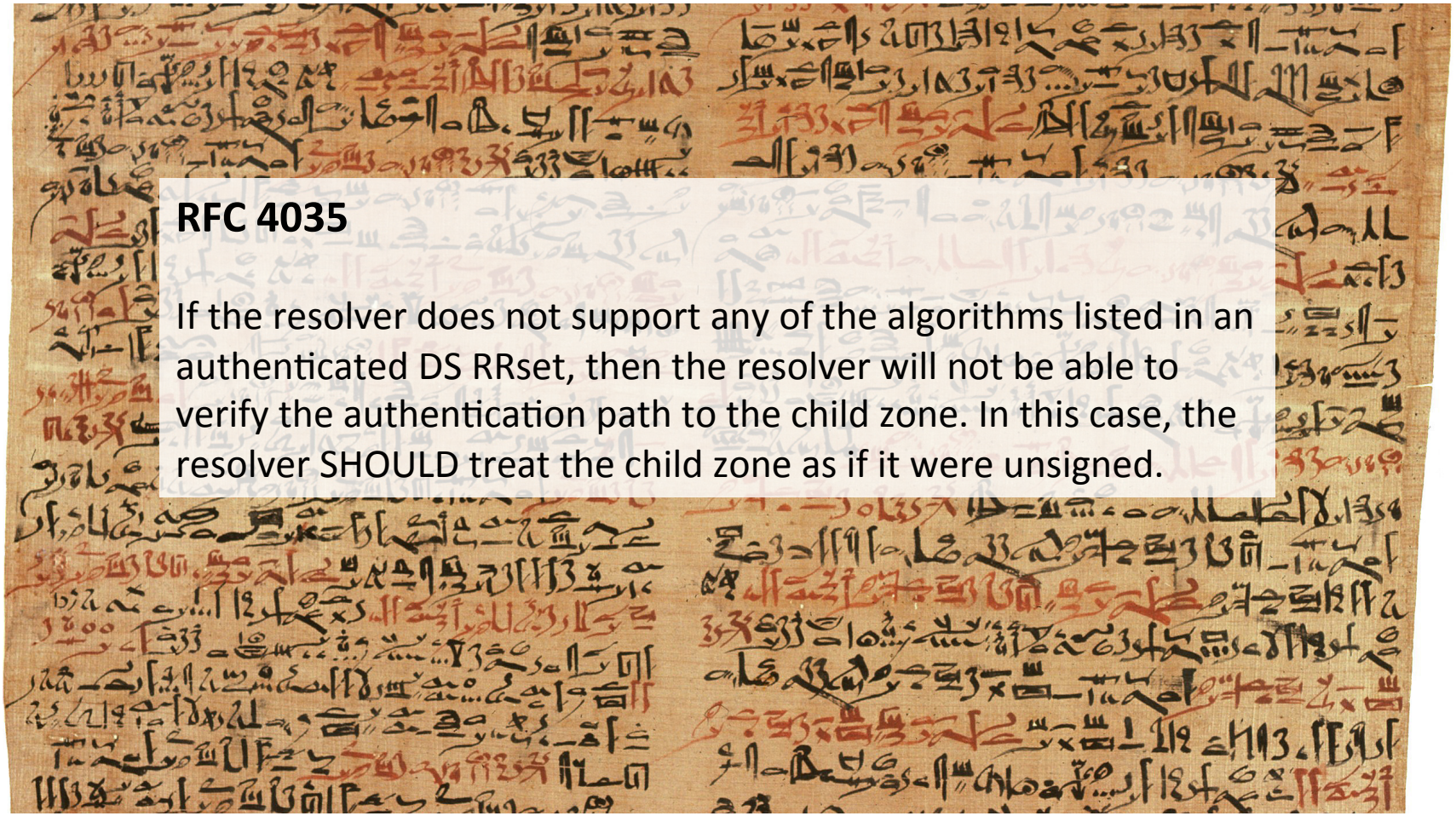
Experiments	ECDSA DS	ECDSA DNSKEY	RSA DS	RSA DNSKEY
11,988,195	2,957,855	2,391,298	2,963,888	2,970,902

This indicates that a validating resolver appears to fetch the DS RR irrespective of the signing protocol, and only fetches the DNSKEY RR if it recognizes the zone signing protocol.

The Words of the Ancients



The Words of the Ancients



RFC 4035

If the resolver does not support any of the algorithms listed in an authenticated DS RRset, then the resolver will not be able to verify the authentication path to the child zone. In this case, the resolver SHOULD treat the child zone as if it were unsigned.

DNS resolver failure modes for an unknown signing algorithm

If a DNSSEC-Validating resolver receives a response DS with an unknown crypto algorithm does it:

- ❑ Immediately stop resolution and return a status code of SERVFAIL?
- ❑ Fetch the DNSKEY RR and then return a status code of SERVFAIL?
- ☒ Abandon validation and just return the unvalidated query result?

Hmmm

- How does this relate to affected users?
- How do validating resolvers manage an unrecognised algorithm failure?

- Lets try again and look at both DNS query and web log data

Second Approach to answering the ECC question - DNS + WEB

Data collection: 2/3/15 – 19/3/15

1,830,668 clients who appear to be exclusively using RSA DNSSEC-Validating resolvers

ECC Results:

Success:	79.9%	1,461,772	Saw fetches of the ECC DNSSEC RRs and the well-signed named URL, but not the badly signed named URL

Failure (fetched both URLs):

Mixed Resolvers	5.1%	93,746	Used both ECDSA-Validating and non-validating resolvers
NO ECC	13.3%	243,794	Saw A, DS, no DNSKEY, fetched both URLs
Mixed	1.3%	24,420	Saw some DNSSEC queries, fetched both URLs
No Validation	0.4%	6,836	Did not fetch any DNSSEC RRs
Apparent Fail:	**20.1%**	**368,796**	

1 in 5 clients that use resolvers that perform DNSSEC validation with RSA fail to validate with ECDSA

Results

- These results show that 80% of clients who appeared to exclusively use RSA DNSSEC-Validating resolvers were also seen to perform validation using ECDSA
- Two thirds of the the remaining clients fetched both objects (13% of the total), but did not fetch any DNSKEY RRs.
- Of the remainder (5%), most were using a validating resolver (which returned SERVFAIL for the badly signed object), and then the client failed over to a non-validating resolver *

* This is curious, because these clients did not failover to a non-validating resolver on a badly signed RSA structure

Where?

ECDSA failure rates – the % of users in each country who use RSA DNSSEC validating resolvers, but fail to validate when the DNSSEC crypto algorithm is ECDSA. Top 24 countries, ranked by Observed ECC Validation failure rates

Rank	CC	Failure	Samples	Country Name
1	CY	94.1%	5,638	Cyprus
2	MT	92.3%	1,973	Malta
3	BB	92.0%	1,402	Barbados
4	GE	84.4%	5,478	Georgia
5	ZA	81.6%	4,618	South Africa
6	KE	76.4%	2,377	Kenya
7	MN	75.6%	1,412	Mongolia
8	AU	73.4%	5,785	Australia
9	FI	72.7%	5,137	Finland
10	LU	71.3%	1,027	Luxembourg
11	YE	62.9%	2,524	Yemen
12	BA	60.1%	11,910	Bosnia and Herzegovina
13	BY	59.4%	10,574	Belarus
14	SI	55.7%	16,587	Slovenia
15	MK	51.8%	3,722	The former Yugoslav Republic of Macedonia
16	AM	51.4%	3,235	Armenia
17	TN	50.9%	4,241	Tunisia
18	PS	46.6%	11,255	Occupied Palestinian Territory
19	IQ	42.2%	20,469	Iraq
20	LT	41.1%	2,544	Lithuania
21	CA	40.3%	13,633	Canada
22	GT	38.0%	3,007	Guatemala
23	JP	36.9%	12,149	Japan
24	NO	36.6%	3,625	Norway
25	CZ	35.8%	26,813	Czech Republic

Which AS?

ECDSA failure rates – the % of users in each AS who use RSA DNSSEC validating resolvers, but fail to validate when the DNSSEC crypto algorithm is ECDSA – top 25 Ases ranked by ECC failure rate

	AS	Fail Rate	Samples	AS Description
1	7155	100.0%	887	WB-DEN2 - Viasat Communications Inc.,US
2	44143	99.7%	1,225	VIPMOBILE-AS Vip mobile d.o.o.,RS
3	12644	98.6%	2,418	TELEMACH Telemach Autonomous System,SI
4	7679	98.5%	583	QTNET Kyushu Telecommunication Network Co.,Inc.,JP
5	28926	98.4%	501	DONTELE-AS Telenet LLC,UA
6	4804	98.2%	4,030	MPX-AS Microplex PTY LTD,AU
7	27813	98.2%	3,915	Teledifusora S.A.,AR
8	198589	98.1%	1,334	JT-AS Al-Jazeera Al-Arabiya Internet LTD,IQ
9	16232	97.9%	2,419	ASN-TIM TIM (Telecom Italia Mobile) Autonomous System,IT
10	34797	97.8%	4,585	SYSTEM-NET System Net Ltd,GE
11	23700	97.2%	7,931	FASTNET-AS-ID Linknet-Fastnet ASN,ID
12	15735	97.1%	1,873	DATASTREAM-NET GO p.l.c.,MT
13	6407	96.9%	785	PRIMUS-AS6407 - Primus Telecommunications Canada Inc.,CA
14	37457	96.5%	2,924	Telkom-Internet,ZA
15	5603	96.3%	6,178	SIOL-NET Telekom Slovenije d.d.,SI
16	11815	96.2%	967	Cooperativa Telefonica de V.G.G. Ltda.,AR
17	7992	96.1%	3,651	COGECOWAVE - Cogeco Cable,CA
18	43132	96.1%	589	KBT-AS OJSC Rostelecom,RU
19	21310	95.8%	550	ASN-SATELLITE ISP Satellite,UA
20	6866	95.6%	7,067	CYTA-NETWORK Cyprus Telecommunications Authority,CY
21	41557	95.4%	809	TELEKABEL-AS Trgovsko kablovska televizija ROBI DOOEL Stip,MK
22	34449	95.4%	563	MORDOVIA-AS OJSC Rostelecom,RU
23	8473	94.9%	859	BAHNHOF Bahnhof Internet AB,SE
24	262928	94.5%	635	DIRECTV COLOMBIA,CO
25	29695	94.3%	981	LYSE-AS Altibox AS,NO

Which Resolver?

Most intensively used RSA-validating resolvers that appear to lack support for ECDSA

Rank	Resolver	Use	AS	AS Description
1	83.66.2.163	13,415	12978	DOGAN-ONLINE DOGAN TV DIGITAL PLATFORM ISLETMECILIGI A.S.,TR
2	202.73.99.4	10,905	23700	FASTNET-AS-ID Linknet-Fastnet ASN,ID
3	59.108.128.141	10,229	4847	CNIX-AP China Networks Inter-Exchange,CN
4	211.136.115.194	9,840	24400	CMNET-V4SHANGHAI-AS-AP Shanghai Mobile Communications Co.,Ltd.,CN
5	211.136.115.198	9,208	24400	CMNET-V4SHANGHAI-AS-AP Shanghai Mobile Communications Co.,Ltd.,CN
6	181.48.0.231	8,801	14080	Telmex Colombia S.A.,CO
7	4.31.99.79	8,457	3356	LEVEL3 - Level 3 Communications, Inc.,US
8	165.254.103.209	7,747	2914	NTT-COMMUNICATIONS-2914 - NTT America, Inc.,US
9	4.53.108.207	7,605	3356	LEVEL3 - Level 3 Communications, Inc.,US
10	212.73.224.143	7,413	3356	LEVEL3 - Level 3 Communications, Inc.,US
11	182.48.200.3	7,386	45769	DVOIS-IN D-Vois Broadband Pvt Ltd,IN
12	4.31.99.81	7,053	3356	LEVEL3 - Level 3 Communications, Inc.,US
13	4.53.108.209	7,021	3356	LEVEL3 - Level 3 Communications, Inc.,US
14	181.48.0.232	6,854	14080	Telmex Colombia S.A.,CO
15	186.130.130.21	6,839	22927	Telefonica de Argentina,AR
16	206.183.111.4	6,595	33480	WEBWERKSAS1 - Web Werks,US
17	165.254.103.207	6,555	2914	NTT-COMMUNICATIONS-2914 - NTT America, Inc.,US
18	189.124.128.172	6,399	28220	CABO SERVICOS DE TELECOMUNICACOES LTDA,BR
19	202.73.97.42	6,139	23700	FASTNET-AS-ID Linknet-Fastnet ASN,ID
20	202.73.97.44	5,790	23700	FASTNET-AS-ID Linknet-Fastnet ASN,ID
21	4.31.108.209	5,735	3356	LEVEL3 - Level 3 Communications, Inc.,US
22	124.161.87.93	5,477	4837	CHINA169-BACKBONE CNCGROUP China169 Backbone,CN
23	4.31.108.207	5,372	3356	LEVEL3 - Level 3 Communications, Inc.,US
24	103.15.63.4	5,180	59164	APOLLOONLINE-AS Apollo Online Services Pvt ltd,IN
25	218.29.129.3	5,124	4837	CHINA169-BACKBONE CNCGROUP China169 Backbone,CN

Why?

- These resolvers all generate queries for the A record and the DS record, but did not query for the DNSKEY record when the signing algorithm was ECDSA
- It appears that these resolvers who do not perform the DNSKEY query do not have local support for ECDSA
  - Resolvers do not, in general use a custom crypto library
  - As we saw with the Heartbleed bug, there is a preponderance of use of OpenSSL
  - So perhaps the question is: why doesn't OpenSSL support ECDSA?

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikimedia Shop

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Create a book

ECC patents

From Wikipedia, the free encyclopedia

Patent-related uncertainty around elliptic curve cryptography (ECC), or **ECC patents**, is one of the main factors limiting its wide acceptance. For example, the OpenSSL team accepted an ECC patch only in 2005 (in OpenSSL version 0.9.8), despite the fact that it was submitted in 2002.

According to Bruce Schneier as of May 31, 2007, "Certicom certainly can claim ownership of ECC. The algorithm was developed and patented by the company's founders, and the patents are well written and strong. I don't like it, but they can claim ownership."[1] Additionally, NSA has licensed MQV and other ECC patents from Certicom in a US$25 million deal for NSA Suite B algorithms.[2] (ECMQV is no longer part of Suite B.)

However, according to RSA Laboratories, "*in all of these cases, it is the implementation technique that is patented, not the prime or representation, and there are alternative, compatible implementation techniques that are not covered by the patents.*"[3] Additionally, Daniel J. Bernstein has stated that he is "not aware of" patents that cover the Curve25519 elliptic curve Diffie–Hellman algorithm or its implementation.[4] RFC 6090, published in February 2011, documents ECC techniques, some of which were published so long ago that even if they were patented any such patents for these previously published techniques would now be expired.

Contents [hide]

Why?

- OpenSSL added ECDSA support as from 0.9.8
- Other bundles and specific builds added ECDSA support later
- But deployed systems often lag behind the latest bundles, and therefore still do not include ECC support in their running configuration

Is ECDSA a viable crypto algorithm for DNSSEC?

If the aim is to detect efforts to compromise the DNS for the signed zone, then signing a zone with ECDSA limits the number of DNS resolvers who will validate the signature

Which is a shame, because the shorter key lengths could be attractive for DNS over UDP

ECDSA in the (semi-)wild

```
$ dig +dnssec www.cloudflare-dnssec-auth.com

; <<>> DiG 9.9.6-P1 <<>> +dnssec www.cloudflare-dnssec-auth.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7049
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.cloudflare-dnssec-auth.com.   IN    A

;; ANSWER SECTION:
www.cloudflare-dnssec-auth.com.    300 IN      A     104.20.23.140
www.cloudflare-dnssec-auth.com.    300 IN      A     104.20.21.140
www.cloudflare-dnssec-auth.com.    300 IN      A     104.20.19.140
www.cloudflare-dnssec-auth.com.    300 IN      A     104.20.22.140
www.cloudflare-dnssec-auth.com.    300 IN      A     104.20.20.140
www.cloudflare-dnssec-auth.com.    300 IN      RRSIG A 13 3 300 20150317021923 20150315001923 35273
cloudflare-dnssec-auth.com. pgBvfQkU4Il8ted2hGL9o8NspvKksDT8/jvQ+4o4h4tGmAX0fDBEoorb
tLiW7mcdOWYLoOnjovzYh3QOOdu0Xw==

;; Query time: 237 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Mar 16 01:19:24 UTC 2015
;; MSG SIZE  rcvd: 261
```

Thanks!