Searching for Vulnerable DNSSEC RSA Keys

Duane Wessels

June 2012

VERISIGN

“Ron was wrong, Whit is right”

- Feb 2012 paper by Lenstra et al found thousands of factorable RSA keys from a set of millions of SSL certificates and PGP keys.
  - except the vulnerable keys were almost exclusively on low-value embedded hardware devices, not your bank’s web site.
- If two RSA keys happen to have a common (but private) factor, then we can factor both keys.
  - So entropy is important
- Searching for factors can be done in O(*n* log *n*) time.

VERISIGN

RSA Keys in DNSSEC

- Found 36,883 Unique RSA keys
  - Most from zone files
  - Some from DNSSEC Debugger logs
- Found 0 zones with vulnerable keys
- Found 12 zones with questionable keys

geek.nz

```
Protocol:           DNSSEC (3)
Algorithm:          RSASHA256 (8)
Flags:              KSK
Keytag:             31139
Size:               2048 bits

geek.nz.  3600      IN        DNSKEY    257  3  8 (
                              AwEAAbN9I++++THIS/IS/A/DELIBERATELY/
                              INVALID/KEY/AND/SHOULD/NOT/BE/USED//
                              FOR/INFO/CONTACT/SUPPORT/AT/NZRS/NET
                              /NZ++++++++++++++++++++++++++++++++
                              ++++++++++++++++++++++++++++++++++
                              ++++++++++++++++++++++++++++++++++
                              ++++++++++++++++++++++++++++++++++
                              ++++++++++++++++++++++++++++++++++
                              ++++++++++++++++++++++++++++++++++
                              ++++++++++++++++AxNxoP8=
                              ) ; Key ID = 31139
```

VERISIGN

dnskey.test1234.si (now gone)

```
Protocol:             DNSSEC (3)
Algorithm:            RSASHA256 (8)
Flags:                ZSK
Keytag:               52873
Size:                 1024 bits

dnskey.test1234.si. 0         IN        DNSKEY    256  3  8 (
                              AwEAAeDP4DaxDgPtfCGkI6ootB1V0NAEAQCo
                              1wJDgvqYttvu8lBu74Ax6TQXEztVx5/rZbYu
                              oqmeSMWRGnKbs3wA8YJpThdblHtk7VcJO7aH
                              3ClWCTgtMyQbV6BYh2i8+MNa18WxhXS5dZeU
                              fM3tAgpegQn1f70HC52b03t1pb0ExsKM
                              ) ; Key ID = 52873
```

Has 4 as a factor

freestone.net & 9 others

```
Protocol:           DNSSEC (3)
Algorithm:          RSASHA256 (8)
Flags:              KSK
Keytag:             50918
Size:               1456 bits

freestone.net.      3600      IN        DNSKEY    257  3  8 (
                              AwEAAcsXCczIXBzYMfv3eMcgonWfql6lfJjD
                              uB+Mm22qX3WbvipwO9XTnpFmo7wOJP6XYbzP
                              K2Cj+mxPjshFrdgcgSFxbaO6WOYWQLoJSU7T
                              fidANd/rVzDNEbQi1k5G8gWc8WXksqBDh5Q0
                              1gPmXOiMgo6yVI03hEj+BJ5rWiFvugB93kaM
                              rAJSEpxhZw3G+GpjKwMEllpCx7zqmghUtW0Y
                              NxDchGBAD5YBdH49GnX+9WPBjy0HhjIA
                              ) ; Key ID = 50918
```

Has 512 as a factor

VERISIGN

1456-bit Keys

- Affected domains: compricer.org, freestone.ch, freestone.net, ip4.ch, ip6.ch, murleen.org, seventhson.ch, stud.io, ytpteleport.net.mm, 7thson.ch

- What do they have in common…?

Name Server Software (version.bind)

Zone	Primary	Secondary	Secondary	Secondary
7thson.ch	icarus.7thson.ch PowerDNS	ns2.interway.ch PowerDNS	ns3.interway.ch PowerDNS	
seventhson.ch	icarus.7thson.ch PowerDNS	ns2.interway.ch PowerDNS	ns3.interway.ch PowerDNS	
compricer.org	ns01.compricer.se Compricer AB	ns0.phonera.net PowerDNS	ns02.compricer.se BIND 9.8.2	ns1.phonera.net PowerDNS
freestone.ch	caladan.freestone.net PowerDNS	ns2.interway.ch PowerDNS	ns3.interway.ch PowerDNS	
freestone.net	caladan.freestone.net PowerDNS	ns2.interway.ch PowerDNS	ns3.interway.ch PowerDNS	
ip4.ch	caladan.freestone.net PowerDNS	ns2.interway.ch PowerDNS	ns3.interway.ch PowerDNS	
ip6.ch	caladan.freestone.net PowerDNS	ns2.interway.ch PowerDNS	ns3.interway.ch PowerDNS	
stud.io	plasma.nj.us.querx.com PowerDNS	argo.pyxos.net PowerDNS	plasma.bc.ca.querx.com PowerDNS	
murleen.org	server.murleen.org REFUSED	a.authns.bitfolk.com BIND 9.7.3	b.authns.bitfolk.com PowerDNS	c.authns.bitfolk.com PowerDNS
ytpteleport.net.mm	ns2.teleport.net.mm SERVFAIL	ns4.teleport.net.mm SERVFAIL	tlp-ytpn-ns1.ytpteleport.net.mm SERVFAIL	tlp-ytpn-ns2.ytpteleport.net.mm SERVFAIL

PowerDNS

- “This is in all likelihood due to the database schema not having enough room to store the DNSKEY.”

Observations

Detecting Duplicate Keys

- DNSSEC keys do not have any identifiers or ownership information.
- Makes it difficult to differentiate key sharing from collisions.

```
;; ANSWER SECTION:
cenkonzult.cz.            86400    IN       DNSKEY   256 3 5
AwEAAdnWrYQ5f2Y6NCfhQ2UFiKH62p9xhyuqlSeHQFbb19RgY74yVAYV
aECw+42bT7Bp3kPK3K629E/RhqrRDurehgkbf0QdIdze2v7DNZCVkh1F
zwe51RzXIjpyM1kbkO3QFITsZUNvbxDGJ0rTXXj/Hyw+KWZZ0Mlx89fX
pi806s3t

;; ANSWER SECTION:
8.15.31.in-addr.arpa.     29388    IN       DNSKEY   256 3 5
AwEAAdnWrYQ5f2Y6NCfhQ2UFiKH62p9xhyuqlSeHQFbb19RgY74yVAYV
aECw+42bT7Bp3kPK3K629E/RhqrRDurehgkbf0QdIdze2v7DNZCVkh1F
zwe51RzXIjpyM1kbkO3QFITsZUNvbxDGJ0rTXXj/Hyw+KWZZ0Mlx89fX
pi806s3t
```

VERISIGN

Detecting Truncated Keys

- Can you see any problems with this key?

```
ac.lk.   43200    IN       DNSKEY   257  3  5 (
                            AwEAAbHaM2SWt8I37htORZn9kuj8ClZsGBkO
                            6PLLwapWosnBb/sp8oRYAMGUsKzGEtSmqRfE
                            5/riurUh19YNuQX3hywQFxLeeLqNgW0ziNl/
                            DSv9lq5hHThqvPl7ectmV0jXUw3RhVHQjAdC
                            GHhmInypKo3wKkraIuJi+Sj/kJL5BY0nZzhx
                            gGbhvHrc8Qw+2NTnm5lII5FMVV58xaXaTA5F
                            i8RpSOVUqeFwmsBNZuBCw6M=
                            ) ; Key ID = 40156
```

Sure would be nice if DNSKEYs had a “checksum” of some sort, due to their

- Opaque presentation
- Length
- Importance

VERISIGN

Thank You

VERISIGN