Searching for Vulnerable DNSSEC RSA Keys

Duane Wessels
June 2012
“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.
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
Protocol: DNSSEC (3)
Algorithm: RSASHA256 (8)
Flags: KSK
Keytag: 31139
Size: 2048 bits

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
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 (AwEAAeDP4DaxDqPtfCGkI6ootB1V0NAEAQCo1wJDgqYttvu8lBu74Ax6TQXEztVx5/rZbYuogmeSMWRGnKbs3wA8YJpThdb1Htk7VcJ07aH3ClWCTgtMyQbV6BYh2i8+MNa18WxhXS5dZeUfM3tAgpegQn1f70HC52b03t1pb0ExsKM);

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 (AwEAAcsXczIXBzYMfV3eMg0nWfq161fJjD
uB+Mm22qX3WbvipwO9XTnpFmo7wOJP6XYbzPK2Cj+mxPjshFrdgcgSFXbaO6WOYWQLoJSU7T
fidANd/rVzDNEbQ11k5G8gWc8WXksqBDh5Q01gPmXOiMgo6yVI03hEj+Bj5rWiFvugB93kaM
rAJSEpxhZw3G+GpjKwMEllpCx7zqmgUUtW0Y
NxDchGBAD5YBdH49GnX+9WPByj0HhjIA)
; Key ID = 50918

Has 512 as a factor
1456-bit Keys

• Affected domains: compricer.org, freestone.ch, freestone.net, ip4.ch, ip6.ch, murleen.org, seventhson.ch, stud.io, ytp teleport.net.mm, 7thson.ch

• What do they have in common…?
## Name Server Software (version.bind)

<table>
<thead>
<tr>
<th>Zone</th>
<th>Primary</th>
<th>Secondary 1</th>
<th>Secondary 2</th>
<th>Secondary 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>7thson.ch</td>
<td>icarus.7thson.ch</td>
<td>ns2.interway.ch</td>
<td>ns3.interway.ch</td>
<td>PowerDNS</td>
</tr>
<tr>
<td></td>
<td>PowerDNS</td>
<td>PowerDNS</td>
<td>PowerDNS</td>
<td>PowerDNS</td>
</tr>
<tr>
<td>seventhson.ch</td>
<td>icarus.7thson.ch</td>
<td>ns2.interway.ch</td>
<td>ns3.interway.ch</td>
<td>PowerDNS</td>
</tr>
<tr>
<td></td>
<td>PowerDNS</td>
<td>PowerDNS</td>
<td>PowerDNS</td>
<td>PowerDNS</td>
</tr>
<tr>
<td>compricer.org</td>
<td>ns01.compricer.se</td>
<td>ns0.phonera.net</td>
<td>ns02.compricer.se</td>
<td>ns1.phonera.net</td>
</tr>
<tr>
<td></td>
<td>Compricer AB</td>
<td>PowerDNS</td>
<td>BIND 9.8.2</td>
<td>PowerDNS</td>
</tr>
<tr>
<td>freestone.ch</td>
<td>caladan.freestone.net</td>
<td>ns2.interway.ch</td>
<td>ns3.interway.ch</td>
<td>PowerDNS</td>
</tr>
<tr>
<td></td>
<td>PowerDNS</td>
<td>PowerDNS</td>
<td>PowerDNS</td>
<td>PowerDNS</td>
</tr>
<tr>
<td>freestone.net</td>
<td>caladan.freestone.net</td>
<td>ns2.interway.ch</td>
<td>ns3.interway.ch</td>
<td>PowerDNS</td>
</tr>
<tr>
<td></td>
<td>PowerDNS</td>
<td>PowerDNS</td>
<td>PowerDNS</td>
<td>PowerDNS</td>
</tr>
<tr>
<td>ip4.ch</td>
<td>caladan.freestone.net</td>
<td>ns2.interway.ch</td>
<td>ns3.interway.ch</td>
<td>PowerDNS</td>
</tr>
<tr>
<td></td>
<td>PowerDNS</td>
<td>PowerDNS</td>
<td>PowerDNS</td>
<td>PowerDNS</td>
</tr>
<tr>
<td>ip6.ch</td>
<td>caladan.freestone.net</td>
<td>ns2.interway.ch</td>
<td>ns3.interway.ch</td>
<td>PowerDNS</td>
</tr>
<tr>
<td></td>
<td>PowerDNS</td>
<td>PowerDNS</td>
<td>PowerDNS</td>
<td>PowerDNS</td>
</tr>
<tr>
<td>stud.io</td>
<td>plasma.nj.us.qurex.com</td>
<td>argo.pyxos.net</td>
<td>plasma.bc.ca.qurex.com</td>
<td>PowerDNS</td>
</tr>
<tr>
<td></td>
<td>PowerDNS</td>
<td>PowerDNS</td>
<td>PowerDNS</td>
<td>PowerDNS</td>
</tr>
<tr>
<td>murleen.org</td>
<td>server.murleen.org</td>
<td>a.authns.bitfolk.com</td>
<td>b.authns.bitfolk.com</td>
<td>c.authns.bitfolk.com</td>
</tr>
<tr>
<td></td>
<td>REFUSED</td>
<td>BIND 9.7.3</td>
<td>PowerDNS</td>
<td>PowerDNS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ytpteleport.net.mm</td>
<td>ns2.teleport.net.mm</td>
<td>ns4.teleport.net.mm</td>
<td>tlp-ytpn-ns1.ytpteleport.net.mm</td>
<td>SERVFAIL</td>
</tr>
<tr>
<td></td>
<td>SERVFAIL</td>
<td>SERVFAIL</td>
<td>SERVFAIL</td>
<td></td>
</tr>
</tbody>
</table>
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.

```plaintext
;; ANSWER SECTION:
cenkonzult.cz. 86400 IN DNSKEY 256 3 5 AwEAAAdnWrYQ5f2Y6NCfhQ2UFiKH62p9xhyuq1SeHQFbb19RgY74yVAYV aEcw+42bT7Bp3kPK3K629E/RhqrRDurehkgkf0QdIdze2v7DNZCVkh1F zwe51RzXIjpyM1kbkO3QFITsZUNvbxDGJ0rTXxj/Hyw+KWZZ0Mlx89fX pi806s3t

;; ANSWER SECTION:
8.15.31.in-addr.arpa. 29388 IN DNSKEY 256 3 5 AwEAAAdnWrYQ5f2Y6NCfhQ2UFiKH62p9xhyuq1SeHQFbb19RgY74yVAYV aEcw+42bT7Bp3kPK3K629E/RhqrRDurehkgkf0QdIdze2v7DNZCVkh1F zwe51RzXIjpyM1kbkO3QFITsZUNvbxDGJ0rTXxj/Hyw+KWZZ0Mlx89fX pi806s3t
```
Detecting Truncated Keys

Can you see any problems with this key?

```
ac.lk. 43200 IN DNSKEY 257 3 5 (AwEAAbHaM2Swt8I37htORZn9kuj8C1ZsGBkO6PLLwapWosnBb/sp8oRYAMGUssKzGETSmqRfE5/riurUh19YNuQX3hywQFxLeeLqNgW0ziN1/DSv91q5hHThvP17ectmV0jXUw3RhVHQjAdCGHhmInyp Ko3wKkraIuJi+Sj/kJL5BY0nZzhxgGbhvHrc8Qw+2NTnm5lII5FMV58xaXaTA5Fi8RpSOVUqeFwmsBNZuBCw6M=) ; Key ID = 40156
```

Sure would be nice if DNSKEYs had a “checksum” of some sort, due to their
- Opaque presentation
- Length
- Importance
Thank You