DNSSEC
and the Hassle of Negative Responses

Matthäus Wander
<matthaeus.wander@uni-due.de>

Erlangen, April 20, 2015
Security Goal of DNSSEC

Query: www?
Security Goal of DNSSEC

Query: www?

www A 192.0.2.1

ftp
mail
ns1
www
Security Goal of DNSSEC

Query: www?

www A 192.0.2.1

www A 6.6.6.6
Security Goal of DNSSEC

- Data integrity and authenticity
- Signatures over resource records (data sets)
End-to-End Security

Stub Resolver -> Recursive Resolver -> Recursive Resolver -> Authoritative Name server -> DNS zone
End–to–End Security

- End–to–end security principle
  - Between **validator** and **signer**

- Offline signing
  - Pre–generate all signatures
Public Key Distribution

- Public keys distributed in-band
- Authenticated by parent domain

Resolver has copy of root public key
RESEARCH WORK

NEGATIVE RESPONSES

ATTACKING NSEC3
Research Work

- Measurement analysis
  - DNS injection
  - DNSSEC adoption
    - Server-side: signed domains
    - Client-side: validators
- Attack methods on NSEC3 privacy goal
Research Work

- Measurement analysis
  - DNS injection
  - DNSSEC adoption
    - Server-side: signed domains
    - Client-side: validators

- Attack methods on NSEC3 privacy goal
Research Work

- Measurement analysis
  - DNS injection
  - DNSSEC adoption

- Server-side: signed domains

<table>
<thead>
<tr>
<th>TLD</th>
<th>NSEC(3)</th>
<th>Secure Del.</th>
</tr>
</thead>
<tbody>
<tr>
<td>nl</td>
<td>NSEC3, opt-out, i = 5</td>
<td>2,279,702</td>
</tr>
<tr>
<td>br</td>
<td>mixed²</td>
<td>566,694</td>
</tr>
<tr>
<td>cz</td>
<td>NSEC3, i = 10</td>
<td>448,984</td>
</tr>
<tr>
<td>com</td>
<td>NSEC3, opt-out, i = 0</td>
<td>426,182</td>
</tr>
<tr>
<td>se</td>
<td>NSEC</td>
<td>349,514</td>
</tr>
<tr>
<td>eu</td>
<td>NSEC3, opt-out, i = 1</td>
<td>320,311</td>
</tr>
<tr>
<td>fr</td>
<td>NSEC3, opt-out, i = 1</td>
<td>205,662</td>
</tr>
<tr>
<td>no</td>
<td>NSEC3, opt-out, i = 5</td>
<td>119,759</td>
</tr>
<tr>
<td>be</td>
<td>NSEC3, opt-out, i = 5</td>
<td>92,385</td>
</tr>
<tr>
<td>net</td>
<td>NSEC3, opt-out, i = 0</td>
<td>81,391</td>
</tr>
<tr>
<td>org</td>
<td>NSEC3, opt-out, i = 1</td>
<td>46,382</td>
</tr>
<tr>
<td>ovh</td>
<td>NSEC3, opt-out, i = 1</td>
<td>29,372</td>
</tr>
<tr>
<td>nu</td>
<td>NSEC3, i = 5</td>
<td>21,126</td>
</tr>
<tr>
<td>de</td>
<td>NSEC3, opt-out, i = 15</td>
<td>20,004</td>
</tr>
<tr>
<td>pl</td>
<td>NSEC3, opt-out, i = 12</td>
<td>18,110</td>
</tr>
</tbody>
</table>

Result | Count
---|---
No DNSKEY (dangling DS) | 17,751
No trusted DNSKEY (dangling DS) | 1,066
No RRSIG for trusted DNSKEY | 238
Signature expired | 2,138
Signature verify failure | 5
Validation failure | 21,198
Validation success | 3,416,700

Total: 5,146,705
Client Validation Ratio per Country
Research Work

- Measurement analysis
  - DNS injection
  - DNSSEC adoption
    - Server-side: signed domains
    - Client-side: validators

- Attack methods on NSEC3 privacy goal
RESEARCH WORK

NEGATIVE RESPONSES

ATTACKING NSEC3
Secure Denial of Existence: NSEC

- Query name: $x$

Query: test?

Not found
Secure Denial of Existence: NSEC

- Query name: $x$

Query: test?

Not found

ftp
mail
ns1
www

NSEC
Secure Denial of Existence: NSEC

- Query name: \( x \)
- Response: \( (r_1, r_2) \) with \( r_1 < x < r_2 \)
Zone Enumeration

- Copy DNSSEC zone by crawling NSEC records
- Nominet (.uk) position:

„Zone file enumeration is a show-stopper for us that will prevent us from fully implementing DNSSEC.“

- DENIC (.de) position:

„In conflict with Germany’s Federal Data Protection Act“
Secure Denial of Existence: NSEC3

Query: test?

Not found

ftp
mail
ns1
www

NSEC
Secure Denial of Existence: NSEC3

- Hash query name: $h(x)$
Secure Denial of Existence: NSEC3

- **Hash query name:** $h(x)$
- **Response:** $(h(r_1), h(r_2))$ with $h(r_1) < h(x) < h(r_2)$
NSEC3 Definition

- Repeated SHA1 computation
- Salt is identical for all names in a DNSSEC zone

$h(x, s, 0) = SHA1(x||s)$

$h(x, s, i) = SHA1(h(x,s,i-1)||s)$, for $i > 0$
NSEC vs. NSEC3

- **NSEC:**
  - Discloses domain name database
  - Compatible with offline signing

- **NSEC3:**
  - Privacy: Protects from zone enumeration
  - Compatible with offline signing
  - CPU: overhead on server for hashing query names
  - Network: 40–50% larger response sizes

⇒ How well does NSEC3 prevent zone enumeration?
RESEARCH WORK

NEGATIVE RESPONSES

ATTACKING NSEC3
ATTACKING NSEC3

1. Collect hashes
2. Reverse hashes
GPU Computing
ATTACKING NSEC3

1. Collect hashes
2. Reverse hashes
Hash Crawling

- Retrieve NSEC3 hashes from name server
  - Send queries for random non-existing names

M8eZcl8.com?

78a1 NSEC3 8e5d

Not found

- Check hash before sending query

| NSEC3 | gap | NSEC3 | gap | NSEC3 | gap |
Crawling 345,000 Hashes from .com

Time in hours

Hashing attempts

Gaps in use

00:00 02:00 04:00 06:00 08:00 10:00 12:00

Universität Duisburg-Essen
Verteilte Systeme

May 2014
ATTACKING NSEC3

1. Collect hashes
2. Reverse hashes
Hash Breaking Methods

- Brute-force attack
  - Exhaustive search (aaa, aab, aac, ...)

- Dictionary attack
  - Read candidate names from file

- Markov attack
  - Derive candidate names from language model
Brute-Force Attack

Number of names found

Time in hours

Brute force

1 to 8 characters

9 characters

Universität Duisburg-Essen
Verteilte Systeme

Matthäus Wander

33
Dictionary Attack

- Effectiveness depends on dictionary quality
  - Good public lists (Alexa, Quantcast)
- 7.1 mio candidate names
- Generate more candidates by inserting strings
  - Insert most common 200,000 n-grams (with $1 \leq n \leq 15$)
  - $1.7 \times 10^{13}$ candidate names

```
feoo.com.
foeo.com.
fooe.com.
```
Dictionary Attack

![Graph showing the number of names found over time for Bruteforce and Wordlist.]
Effectiveness of Insertion Wordlist

Index of n-grams, sorted by frequency in dictionary
Markov Attack

- Some strings are more probable than others
  - ’th‘ more common in English than ’tx‘
  - Model language with 1st order Markov chains
- Markov attack requires training
  - Use hits from brute-force and dictionary attacks
  - Markov model derived from names found
- Enumerate most probable names
  - Omit others (with given time frame)
Markov Attack

![Graph showing the comparison between Brute Force, Markov, and Wordlist methods over time in hours. The x-axis represents time in hours, ranging from 0 to 50, and the y-axis represents the number of names found, ranging from 0 to 200,000. The graph shows the effectiveness of each method over time.]
Countermeasure: Adjust Iterations

- Iterations increase workload linearly
  - For attacker and server operator
  - Unlike e.g. cipher key length
Adjusting iterations

- Iterations increase workload linearly
  - For attacker and server operator
  - Unlike e.g. cipher key length
Adjusting iterations

- Iterations increase workload linearly
  - For attacker and server operator
  - Unlike e.g. cipher key length
Efficiency of CPU vs. GPU
Conclusions

- DNSSEC authenticates domain name data
- Negative responses with NSEC/NSEC3
  - NSEC discloses domain database
  - NSEC3 incurs additional server costs
- Break NSEC3 hashes efficiently with GPUs
  - Best method: dictionary with inserted n-grams
- Reversed 65% .com NSEC3 hashes in 5 days
- Increasing iterations is not economical