DNSSEC @ SURFnet
What we’re doing and what we’ve found so far

Paul Dekkers
paul.dekkers [at] surfnet.nl

October 20th 2009
Overview

- First half:
  - Why we think DNSSEC matters

- Second half:
  - What we are doing with DNSSEC

- Questions: please ask!
DNS: Roadsigns for the net
DNS: insecurity by design?

- DNS was designed in the early Internet era
- Everybody more or less knew everybody else
- And everybody trusted everybody else
- Bottom line: Security was not a design criterion
Threats to DNS

- **Availability**
  - If DNS is not available, the internet is broken (users think)
  - A typical DNS resolver services 100000+ end users
  - Some authoritative servers host over 8 million zones

- **Exploitation**
  - On an exploited server availability and integrity are broken
  - Plus the attacker can gain access to all other software on the same server/client

- **Integrity**
  - DNS gives the wrong answer and sends you the wrong way

Slide content courtesy of Bert Hubert (PowerDNS)
Why attack DNS?

- DNS is **everywhere**:  
  - In your phone, in your laptop, in your PC...  
  - But also in your car, in an ATM, in your elevator, ...

- It is very hard to protect DNS against attacks (currently)

- It is very easy to attack a lot of users
Attack vectors
Cache poisoning

- Cache poisoning has been a known attack for years

- It used to have a threat level of ‘meh’ (because of TTL, bailiwick checking, ... and randomization more recently)
Cache poisoning

Question: how can I target a specific name?
Answer: introduce a rogue client
Cache poisoning++

But...

- Dan Kaminsky published an attack at last year’s Black Hat conference

- No need to wait for a resolver to take initiative, no need to wait for TTL expiry...
Attack in action

QID=1234
12345.piggybank.dom A???
go to piggybank auth.

12345.piggybank.dom A???
A: 123.45.67.89

QID=1235

Additional:
NS piggybank.dom

QID=1234
QID=1233
QID=1235
Success!

Rogue responder

Root & TLD servers

Authoritative server

Rogue authoritative

DNS resolver
;; QUESTION SECTION:
;abcde.piggybank.dom.                      IN  A

;; ANSWER SECTION:
abcde.piggybank.dom.               582 IN  A  123.45.67.89

;; AUTHORITY SECTION:
piggybank.dom.                        3161 IN  NS  ns1.piggybank.dom.
piggybank.dom.                        3161 IN  NS  ns2.piggybank.dom.

;; ADDITIONAL SECTION:
ns1.piggybank.dom.                   604800 IN  A  123.45.67.1
ns2.piggybank.dom.                   604800 IN  A  123.45.67.2
Attack in action

Vulnerable end user

DNS resolver

Root & TLD servers

Authoritative server

Rogue authoritative

www.piggybank.dom
A: 123.45.67.89

www.piggybank.dom
A: 123.45.67.89
Roadsigns to where?
Impact on threat level (1)

- Kaminsky is happening (we think, but is damn hard to detect):

- Wide-scale patching has been rolled out
  - But research shows:
    - Poisoning unpatched BIND: ±3 seconds
    - Poisoning patched BIND: 1-11 hours (source: NIC.cz)
Impact on threat level (2)

- Kaminsky may be happening on our network!
Impact on threat level (3)

- Kaminsky may be happening on our network!

![Graph showing DNS query trends over time](image)

<table>
<thead>
<tr>
<th>Type</th>
<th>Cur</th>
<th>Min</th>
<th>Avg</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOERROR</td>
<td>295.71</td>
<td>48.59</td>
<td>233.50</td>
<td>612.15</td>
</tr>
<tr>
<td>SERVFAIL</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>NXDOMAIN</td>
<td>74.33</td>
<td>15.19</td>
<td>66.44</td>
<td>1.80 k</td>
</tr>
<tr>
<td>nodata</td>
<td>59.56</td>
<td>4.98</td>
<td>32.08</td>
<td>72.70</td>
</tr>
<tr>
<td>Answer server</td>
<td>1.07</td>
<td>187.59 m</td>
<td>916.68 m</td>
<td>3.72</td>
</tr>
<tr>
<td>Answer bogus</td>
<td>137.79 m</td>
<td>0.00</td>
<td>104.63 m</td>
<td>708.53 m</td>
</tr>
<tr>
<td>Num rrsets marked bogus</td>
<td>3.34 m</td>
<td>0.00</td>
<td>5.55 m</td>
<td>75.44 m</td>
</tr>
</tbody>
</table>
Impact on threat level (4)

- Kaminsky may be happening on our network!
The slow attack

- Brute force attacks are easy to detect

- But the slow attack is very insidious...

research by Bert Hubert (PowerDNS) shows:

Graph courtesy of Bert Hubert
DNSSEC: the solution? (1)

- DNSSEC is the only effective solution against DNS integrity threats like Kaminsky cache poisoning

- It’s no silver bullet though:
  - Harder to manage
  - Increases likelihood of DDoS attacks
  - Availability of tools is an issue
DNSSEC: the solution? (2)

- We think DNSSEC should be deployed but:
  - The root isn’t signed (yet, expected 07/2010)
  - Our own ccTLD (.nl) isn’t signed (yet)

- Detailed info on the how and why of DNSSEC can be found in our white paper: http://www.dnssec.nu

- Let us know what you are doing, perhaps we can co-operate!
What are we doing? (1)

- Supporting an open source tooling project
  - OpenDNSSEC (www.opendnssec.org)
    Open source secure DNSSEC signer

- Testing other software/appliances
  - Secure64 DNS Signer
  - Xelerance DNSX Signer
  - ZKT (Zone Key Tool, www.hznet.de/dns/zkt)
  - PowerDNS + DNSSEC = PowerDNSSEC
  - Unbound (by NLnetLabs)
  - BIND 9.x and up
  - Windows Server 2008 R2, Windows 7
What are we doing?

(2)

- SURFnet’s resolvers perform DNSSEC validation:
- Extend our managed DNS service with DNSSEC support

- Testing DNSSEC appliances as they appear on the market

- Keep supporting OpenDNSSEC

- Participate in a platform to get the issues for signing .nl out of the way
What can you do?

- Gain knowledge on DNSSEC
  - *SURFnet DNSSEC white paper* ([www.dnssec.nu](http://www.dnssec.nu))

- Update/reconfigure your resolvers to support DNSSEC validation and experiment with it

- Join the TERENA BoF DNSSEC list
  Send subscribe bof-dnssec youremail@domain.com to listmanager@terena.org

- **Work on an open source tool project!**
  - Please try OpenDNSSEC and share your experiences
Questions?

Thank you for your attention!

Paul Dekkers
paul.dekkers [at] surfnet.nl

Roland van Rijswijk
roland.vanrijsjwijk [at] surfnet.nl

Presentation released under Creative Commons
(http://creativecommons.org/licenses/by-nc-sa/3.0/nl/deed.en)