DNSSEC in Windows

33rd ICANN Meeting
Cairo, Egypt

Shyam Seshadri
(sseshad(at)microsoft.com)
Program Manager
Microsoft Corporation
Instances of DNS exploits increasing

In many cases, patches are just a stop-gap

DNSSEC for the long run...

Microsoft recognizes the important role that DNSSEC will play in securing the DNS in the coming years
Announcing DNSSEC in Windows

- DNSSEC support as per RFCs 4033, 4034 & 4035 in
  - Windows Server 2008 R2 DNS Server
  - Windows 7 / Windows Server 2008 R2 DNS Client

- Solution can integrate with
  - IPsec
  - Group Policy

- Allows for compliance with security controls proposed by the US Govt. in NIST SP 800-53
Implementation Overview

DNSSEC on Windows DNS Server
- Sign zones using offline sign-tool
- Configure and manage trust anchors; build chain of trust
- DNSSEC validation as per RFC

DNSSEC on Windows DNS Client
- Non-validating security-aware stub resolver
- Policy based; relies on DNS server for validation

Last-hop security
- Use of IPsec to secure last-hop communication is strongly recommended
## Implementation Examples

<table>
<thead>
<tr>
<th>Case 1</th>
<th><a href="http://www.example.com">www.example.com</a></th>
<th>Client policy</th>
<th>Server TA</th>
<th>Wire behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Set DO/check AD</td>
<td>TA for *.example.com</td>
<td>-- Client sets DO bit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use IPsec</td>
<td></td>
<td>-- Server performs validation; returns RRSIGs and sets AD bit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-- Client checks AD bit in response</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Case 2</th>
<th><a href="http://www.microsoft.com">www.microsoft.com</a></th>
<th>Client policy</th>
<th>Server TA</th>
<th>Wire behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Don’t set DO</td>
<td></td>
<td>No TA for *.microsoft.com</td>
<td>-- Client does not set DO bit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-- Server does not perform validation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Case 3</th>
<th><a href="http://www.contoso.com">www.contoso.com</a></th>
<th>Client policy</th>
<th>Server TA</th>
<th>Wire behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Don’t set DO</td>
<td></td>
<td>TA for *.contoso.com</td>
<td>-- Client does not set DO bit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-- Server performs validation; does not return RRSIGs or set AD bit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-- Client does not check for AD bit in response</td>
</tr>
</tbody>
</table>
Implementation Example: DNS Client

Name Resolution Policy Table

*.example.com IPsec DNSSEC OK

Trust Anchors

example.com contoso.com

DNSSEC aware IPsec compatible server

Case 1

Q: www.example.com DO

Q: www.example.com A: 192.168.1.2 AD RRSIG

Case 2

Q: www.microsoft.com

Q: www.microsoft.com A: 10.132.12.2

Case 3

Q: www.contoso.com

Q: www.contoso.com A: 172.16.34.4
Implementation Example: DNS Server

Windows Server 2008 R2

Trust Anchors
example.com
contoso.com

Forward/recurse queries

Case 1
- Q: www.example.com
  - A: 192.168.1.2
  - RRSIG: a23adcd60...

Case 2
- Q: www.microsoft.com
  - A: 10.132.12.2

Case 3
- Q: www.contoso.com
  - A: 172.16.34.4
  - RRSIG: f930a87b...
Interoperability

Interop with non-Microsoft DNS servers and clients is key

Focus of our pre-Beta and Beta testing

More interop testing...
Roadmap

Pre-release availability
- Pre-Beta builds made available to participants of
  - Microsoft WinHEC 2008 [Nov 5-7]

General availability
- Windows Server 2008 R2 and Windows 7 to be available approx. three years after Vista
Contacting us...

The DNS team @ Microsoft
- dnscore(at)microsoft.com
- www.microsoft.com/dns

Shyam Seshadri
- sshedad(at)microsoft.com
- blogs.technet.com/ssshedad
Q&A