DNSSEC: A Vision

Anil Sagar
Additional Director
Indian Computer Emergency Response Team (CERT-In)
Outline

• DNS Today
• DNS Attacks
• DNSSEC: An Approach
• Countering DNS Attacks
• Conclusion
DNS Today

• DNS is a distributed dynamic database application with a hierarchical structure and offering a dependable service

• Originally DNS design was focused on data availability and did not include its security

• DNS major components:
  – The Database
    • Domain name space (DNS Tree)
    • Resource Records
  – The Server
    • Name Server
  – The Client
    • Resolvers
DNS Namespace

DNS uses a hierarchical namespace to locate computers

- Root-level Domains
  - .com
  - .net
  - .org
  - .mil

- Top-level Domains
  - .Country
codes

- Second-level Domains
  - microsoft.com
  - cisco.com

- Sub-domains
  - support.microsoft.com
  - srv1.support.microsoft.com

- Host (FQDN)
  - support.microsoft.com
DNS Attacks

• June 1997, Eugene Kashpureff (Alternic founder) redirected the internic.net domain to alternic.net by caching bogus information on the Internic name server.

• In early February 2006, name servers hosting Top Level Domain zones were the repeated recipients of extraordinary heavy traffic loads.

• On 6 February 2007, starting at 12:00 pm UTC, for approximately two-and-a-half hours, the system that underpins the Internet came under attack. Three-and-a-half hours after the attack stopped, a second attack, this time lasting five hours, began.
DNS Hacking Objectives

• Attacking DNS server data
• Attacking the DNS server
DNS Today: Potential Problems

• Original DNS design focused on data availability and did not include security

• DNS design included no authentication

• The DNS protocol does not allow you to check the validity of DNS data

• DNS data can be spoofed and corrupted between master server and resolver or forwarder
Securing DNS

• Built security into DNS systems

• TSIG Transactions
  – Enhancements to secure Server-Server transactions

• DNS Security Extensions (DNSSEC)
  – Enhancements to secure Server-Client transactions
DNSSEC: An Approach

- DNSSEC (short for Domain Name System Security Extensions) adds security to the Domain Name System’s query / response

- Protects against unauthorised DNS data corruption and DNS spoofing

- It provides:
  - origin authentication of DNS data
  - data integrity but not confidentiality
  - authenticated denial of existence

- It is designed to be interoperable with non-security aware implementations
DNSSEC: Characteristics

- Changes to DNS Protocol
  - DNSSEC adds four new Resource Records (RR)
    - KEYRR(DNSKEY): Key Resource Record specifies:
      - the type of key (zone, host, user)
      - the protocol (DNSSEC, IPSEC, TLS, etc.)
      - the algorithm (RSA/MD5, DSA, etc.)

- SIGRR : Signature resource record specifies:
  - the RR type covered (SOA, A, NS, MX, etc.)
  - the algorithm (RSA/MD5, DSA, etc.)
  - the inception & expiration times
  - the signer key footprint

- DS: Delegation Signer
  - a pointer to the next key in the chain of trust
DNSSEC: Characteristics

• NXTRR(NSEC): Next Secure
  – the next name in the zone
  – all the RR types covered by the current name

• The private key is kept off-line and is used to sign the RR sets of the zone file

• The public key is published in the KEY RR

• The public key of a zone is signed by the parent zone private key

• The parent zone signature on the zone’s public key is added to the zone file
What DNSSEC does NOT do

• Does NOT provide confidentiality of DNS responses
• Does NOT protect against DDOS attacks
• Does NOT protect against IP Spoofing
• Is NOT about privacy
• Is NOT a PKI
DNSSEC Query

Root Name server (".")

Second-level Authoritative Server (cnn.com)

Top-level Domain Authoritative Server (.com)

Request for www.cnn.com

Reply [SIG (IP add & PK of .com server) by its private key]

Request for www.cnn.com

Reply [SIG (IP add & PK of cnn.com server) by its private key]

Request for www.cnn.com

Reply [SIG (x.x.x.x) by its private key]

Request for www.cnn.com

Reply

Client

DNS Server

Requested for www.cnn.com

DNS Query

Request for www.cnn.com
DNSSEC – Response Validation

• Validation of a DNS response:
  – Did the matching private key sign the RRSIG RR?
  – Does the hash match the RR data?
  – Does the public key validate?
    • Does the parent have a DS RR?
    • Has the Parent signed the matching RRSIG RR?
    • Does the parent’s key validate?

• Loop until you get to a recognised “trust anchor”

This interlocking of parent signing over child is a critical aspect of the robustness of DNSSEC. It’s also DNSSEC’s major weakness in today’s partial DNSSEC deployment world.
DNSSEC: Chain of Trust

Client

Request for KEY for .com

Reply KEY, SIG RR of .com

Top-level Domain Authoritative Server (.com)

Second-level Authoritative Server (cnn.com)
## DNS Defenses

<table>
<thead>
<tr>
<th>Protocol Based Exploits</th>
<th>Defense</th>
</tr>
</thead>
</table>
| DNS reconnaissance                       | Split-level DNS topologies  
Network and Name Server monitoring, intrusion detection  
**DNSSEC** digital signatures to secure DNS data  
Server-side access controls  
Configuration audit and verification tools |
| Protocol-based denial-of-service        | Split-level DNS topologies  
DNS redundancy  
Stateful firewalling  
Server-side access controls  
Network and Name Server monitoring, intrusion detection  
Patches and service packs |
| Dynamic DNS (DDNS) hacking              | Split-level DNS topologies  
Network and Name Server monitoring, intrusion detection  
Server-side access controls for DDNS  
**DNSSEC**: authentication of DDNS requests  
Configuration audit and verification tools  
Patches and service packs |
## DNS Defenses

<table>
<thead>
<tr>
<th>Application Based Exploit</th>
<th>Defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer overflow attacks</td>
<td>System and service hardening</td>
</tr>
<tr>
<td></td>
<td>Network and Name Server monitoring, intrusion detection</td>
</tr>
<tr>
<td></td>
<td>Stateful firewalls</td>
</tr>
<tr>
<td></td>
<td>Split-level DNS topologies</td>
</tr>
<tr>
<td></td>
<td>DNS redundancy</td>
</tr>
<tr>
<td></td>
<td>Patches and service packs</td>
</tr>
<tr>
<td></td>
<td>Third-party application-layer security tools</td>
</tr>
</tbody>
</table>
## DNS Defenses

<table>
<thead>
<tr>
<th>Trust Based Exploits</th>
<th>Defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS registration hacking</td>
<td>Imposition of registration controls</td>
</tr>
<tr>
<td>DNS spoofing</td>
<td>Split-level DNS topologies&lt;br&gt;Stateful firewalls&lt;br&gt;Server-side access controls&lt;br&gt;Network and Name Server monitoring, intrusion detection&lt;br&gt;&lt;b&gt;DNSSEC&lt;/b&gt; digital signatures to secure DNS data&lt;br&gt;Patches and service packs&lt;br&gt;Upgrade to latest version(s) of Name Server software (protections against DNS ID hacking)</td>
</tr>
<tr>
<td>Cache poisoning</td>
<td>Split-level DNS topologies&lt;br&gt;Stateful firewalls&lt;br&gt;Server-side access controls&lt;br&gt;Network and Name Server monitoring, intrusion detection&lt;br&gt;&lt;b&gt;DNSSEC&lt;/b&gt; digital signatures to secure DNS data&lt;br&gt;Patches and service packs</td>
</tr>
<tr>
<td>DNS hijacking</td>
<td>Split-level DNS topologies&lt;br&gt;Stateful firewalls&lt;br&gt;Server-side access controls&lt;br&gt;Network and Name Server monitoring, intrusion detection&lt;br&gt;&lt;b&gt;DNSSEC&lt;/b&gt; digital signatures to secure DNS data&lt;br&gt;Patches and service packs</td>
</tr>
</tbody>
</table>
DNSSEC: Deployments

• DNSSEC test deployment at IANA
  – This data, including the signed zones, are purely for test purposes and are not to be used in any production capacity

• DNSSEC testbed in
  – Sweden (.se)
  – Russia (.ru)
  – United Kingdom (.uk)
  – Mexico (.mx)
  – Puerto Rico (.pr)
  – Netherlands (.nl)
  – Bulgaria (.bg)
  – Brasil (.br)
  – Malaysia (.my)

• VeriSign
Why DNSSEC is important?

Is this ROI or Return on Risk?

- Total dependence on DNS for the functioning of Internet
- Low security awareness
- Rise in threats

How costly is the exploitation that occurs if we don’t have this protection?
References

• http://www.dnssec.net
• http://www.dnssec-deployment.org
• http://www.ripe.net
• http://www.icann.org
• RFCs: 4033, 4034, 4035 and 3833
Thank you

anil@cert-in.org.in

Incident Response HelpDesk

Phone: 1800 11 4949

FAX: 1800 11 6969

e-mail: incident@cert-in.org.in

http://www.cert-in.org.in