## The Schedule

<table>
<thead>
<tr>
<th>Outline Concept</th>
<th>Segment</th>
<th>Duration</th>
<th>Speaker</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Welcome</strong></td>
<td>Welcome and Introduction</td>
<td>2 mins</td>
<td>Simon</td>
</tr>
<tr>
<td></td>
<td>Caveman – DNSSEC 5000BC</td>
<td>3 mins</td>
<td>Simon</td>
</tr>
<tr>
<td><strong>Basic Concepts</strong></td>
<td>DNS Basics</td>
<td>5 mins</td>
<td>Matt</td>
</tr>
<tr>
<td><strong>Core Concepts</strong></td>
<td>DNSSEC – How it works</td>
<td>15 mins</td>
<td>Matt</td>
</tr>
<tr>
<td></td>
<td>DNSSEC – Chain of Trust</td>
<td>15 mins</td>
<td>Norm</td>
</tr>
<tr>
<td><strong>Real World Examples</strong></td>
<td>A sample DNSSEC implementation (what it looks like, s/w etc). A simple guide to deployment.</td>
<td>10 mins</td>
<td>Russ</td>
</tr>
<tr>
<td></td>
<td>Audience interaction with examples</td>
<td>10 mins</td>
<td>Russ</td>
</tr>
<tr>
<td><strong>Summary</strong></td>
<td>Session Round up, hand out of materials, Thank you’s</td>
<td>2 mins</td>
<td>Simon</td>
</tr>
</tbody>
</table>
THE ORIGINS OF DNSSEC
5000 B.C.
This is Ugwina. She lives in a cave on the edge of the Grand Canyon...
This is Og. He lives in a cave on the other side of the Grand Canyon...
It's a long way down and a long way round. Ugwina and Og don't get to talk much...
On one of their rare visits, they notice the smoke coming from Og's fire.
...and soon they are chatting regularly using smoke signals
until one day, mischievous caveman Kaminsky moves in next door to Ug and starts sending smoke signals too...
Now Ugwina is really confused. She doesn't know which smoke to believe...
So Ugwina sets off down the canyon to try and sort out the mess...
Ugwina and Og consult the wise village elders. Caveman Diffie thinks that he might have a cunning idea...
And in a flash, jumps up and runs into Ug's cave...!
Right at the back, he finds a pile of strangely coloured sand that has only ever been found in Ug’s cave...
And with a skip, he rushes out and throws some of the sand onto the fire. The smoke turns a magnificent blue...
Now Ugwina and Og can chat happily again, safe in the knowledge that nobody can interfere with their conversation...
DNSSEC Basics and How it Works

Matt Larson, VeriSign
The Name Space
Domains: hp.com
Zones

Diagram showing a hierarchical structure of zones such as cc, tv, com, net, org, name, info, verisign, cnn, hp, holmes, winnie, hpl, and www.
Name Servers

Root Name Servers
root-servers.net

.com Name Servers
gtld-servers.net

cnn.com Name Servers
cnn.com

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
<th>f</th>
<th>g</th>
<th>h</th>
<th>i</th>
<th>j</th>
<th>k</th>
<th>l</th>
<th>m</th>
</tr>
</thead>
<tbody>
<tr>
<td>n</td>
<td>s</td>
<td>1</td>
<td>n</td>
<td>s</td>
<td>2</td>
<td>n</td>
<td>s</td>
<td>3</td>
<td>n</td>
<td>s</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>
Name Resolution

- **Root Name Servers**
  - root-servers.net
  - a, b, c, d, e, f, g, h, i, j, k, l, m

- **.com/.net Name Servers**
  - gtlid-servers.net
  - a, b, c, d, e, f, g, h, i, j, k, l, m

- **cnn.com Name Servers**
  - cnn.com
  - ns1, ns2, ns3, ns4

Diagram:

- Recursive Name Server
- HTTP request
- HTTP response
- Internet User
- www.cnn.com IP
  - www.cnn.com IP
  - www.cnn.com IP
  - www.cnn.com IP
  - www.cnn.com IP

Diagram shows the process of resolving a domain name to an IP address and making an HTTP request to access the CNN website.
DNS Security

• DNS has no security
• One packet for query, one packet for response
• Must rely on source IP-based authentication
• Easily spoofed
• Clever resolvers help a lot
• But we need something better
What DNSSEC Does

• DNSSEC uses public key cryptography and digital signatures to provide:
  – Data origin authentication
    • “Did this DNS response really come from the .com zone?”
  – Data integrity
    • “Did an attacker (e.g., a man-in-the-middle) modify the data in this response since it was signed?”
• Bottom line: DNSSEC offers protection against spoofing of DNS data
What DNSSEC Doesn’t Do

• DNSSEC does not:
  – Provide any confidentiality for DNS data
    • I.e., no encryption
    • The data in the DNS is public, after all
  – Address attacks against the name server itself
    • Denial of service,
    • Packets of death,
    • etc.
Key Pairs

• In DNSSEC, each zone has a public/private key pair
• The zone’s public key is stored in the new DNSKEY record
• The zone’s private key is kept safe
  – Stored offline (ideally)
  – Perhaps held in an HSM (Hardware Security Module)
Digital Signatures

- A zone’s private key signs each piece of DNS data in a zone
- Each digital signature is stored in an RRSIG record
Chain of Trust

• There are no certificates in DNSSEC
• The trust model is rigid
• The **chain of trust** flows from parent zone to child zone
• Only a zone’s parent can vouch for its keys’ identity
Types of Keys

• Signed zone has DNSKEY records at its apex
  – Usually multiple keys
  – One or more key-signing keys (KSKs)
  – One or more zone-signing keys (ZSKs)

• KSK
  – Signs only the DNSKEY records

• ZSK
  – Signs the rest of the zone
Delegation Signer (DS) Records

• The Delegation Signer (DS) record specifies a child zone’s key
• A zone’s DS records only appear in its parent zone
• DS records are signed by the parent zone
Trust Anchors

- You have to trust somebody
- DNSSEC validators need a list of trust anchors
- A trust anchor is a key that is implicitly trusted
- Analogous to list of certificate authorities (CAs) in web browsers
root KSK → root ZSK → com DS

com KSK → com ZSK → cnn.com DS

cnn.com KSK → cnn.com ZSK → www.cnn.com A record
DNSSEC Chain of Trust

Norm Richie, ISC
A Sample DNSSEC Implementation & Audience Interaction

Russ Mundy, Cobham Solutions
DNSSEC Implementation Samples

• DNSSEC implementation depends upon & is mostly driven by an activity’s DNS functions
  – DNS is made up of many parts, e.g., name server operators, applications users, name holders (“owners”), DNS provisioning
  – Activities with large, complex DNS functions are more likely to have more complex DNSSEC implementation activities
    • Also more likely to have ‘DNS knowledgeable’ staff
DNSSEC Implementation
Samples, Continued

- DNS size and complexity examples:
  - Registry responsible for a large TLD operation, e.g., .com
  - Substantial enterprise with many components with many geographic locations, e.g., hp.com
  - Internet-based businesses with a number of business critical zones, e.g., www.verisign.com
  - Activities with non-critical DNS zones, e.g., net-snmp.org
  - Proverbial Internet end users (all of us here)
Zones
General Principle:

• If an activity does a lot with their DNS functions and operations then they probably will want to do a lot with the associated DNSSEC pieces;

• If an activity does little or nothing with their DNS functions and operations then they probably will want to do little or nothing with the associated DNSSEC pieces.
DNS Zone Content Flow
(for example, www.icann.org or www.cnn.com)
I need to have a WWW record

---

Simple Illustration of DNS Components

- Zone Administrator
- Authoritative Server Administrator
- Authoritative Server
- Recursive Server
- Client
- End User

1. Request www
2. Request www
3. www is 1.2.3.4
4. www is 1.2.3.4

Add Zone Data publish

russ.mundy@cobham.com
Name Resolution

Root Name Servers
root-servers.net

.com/.net Name Servers
gtld-servers.net

cnn.com Name Servers
cnn.com

cnn.com Web Site
www.cnn.com

Recursive Name Server

Internet User

HTTP request
HTTP response

www.cnn.com IP

.com name servers

www.cnn.com IP?

cnn.com name servers

www.cnn.com IP?

www.cnn.com IP?

www.cnn.com IP?
1 Webpage = Multiple DNS Name Resolutions

russ.mundy@cobham.com
DNS Basic Functions

• DNS provides the translation from names to network addresses
• Get the right DNS content to Internet users

➤ IT’S DNS CONTENT THAT MATTERS!
How Does DNSSEC Fit?

• DNSSEC required to thwart attacks on DNS CONTENT
  – DNS attacks used to attack Internet users applications

  ➢ Protect **DNS CONTENT** as much as (or more than) any DNSSEC information
  ➢ Including DNSSEC private keys!!
DNS Zone Content Flow
(for example, www.icann.org or www.cnn.com)

Provisioning Area

Content Input

Registries

Zone Name Servers

Publication Area

DNS Resolvers

Content Output

Content Used Here

User Applications

DNSSEC specs HERE

DNS 'Content Picture'

Content Starts Here

Registrars

Registrants

Content
Input

Content
Starts
Here

russ.mundy@cobham.com
Simple Addition of DNSSEC
(there are both much more and less complex setups than this)

I need to have a signed WWW record

Add Zone Data sign Signed Data publish Authoritative Server Administrator

3. www is 1.2.3.4

2. Request www

1. Request www

4. www is 1.2.3.4

new

End User

russ.mundy@cobham.com
Implementation Samples

- In general, try to do DNSSEC in the same way that you are doing DNS
Implementation Samples

• If you’re running much or all of your DNS functions and operations, DNSSEC implementation could be based on:
  – Extend DNS operation to incorporate DNSSEC;
  – Use open source DNSSEC tools (e.g., from www.dnssec-tools.org or opendnssec.org);
  – Use commercial DNSSEC products;
  – Mix elements from ‘all of the above’
Implementation Samples

• If DNS functions and operations are being done with one (or several) software & hardware products, find out if the product providers have (or will) incorporate DNSSEC to support your DNS functions and operations.
  – If not, push them for adding DNSSEC to their products; or
  – Examine additional or different products or services that will provide DNSSEC, e.g., emerging DNSSEC signing services.
Implementation Samples

- If you are the holder (‘owner’) of names but “out-source” DNS functions and operations, e.g., to your registrar, then determine if the “out-source” offers DNSSEC capability.
  - If not, push on them to develop and offer DNSSEC capability
  - Consider using a different “out-source” DNS service
  - Consider developing “in-house” DNS (and DNSSEC) capabilities
Audience Interaction and Participation
Thank You and Questions