THE ORIGINS OF DNSSEC 5000 BC
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...
High level concept of DNS
High level concept of DNS

- A resolver knows where the root-zone is
- Traverses the DNS hierarchy
- Each level refers the resolver to the next level
- Until the question has been answered
- The resolver caches all that information for future use.
High level concept of DNS

• There is no security in the protocol
• Names are easily spoofed
• Caches are easily poisoned
A Skit/Play
Act I
DNS Before DNSSEC
...Ugwina, the resolver, chatting with Og, the server...
A Skit/Play
Act II
Evil Is Afoot
...Ugwina, the resolver is confused. She doesn’t know who the real Og is...
High level concept of DNS

- root
  - uk
  - com
  - ma
  - bigbank.com (www)
  - bigbank.com (www)
DNSSEC adds security to the DNS

• DNSSEC uses **digital signatures** to assure
  – Information has not been tampered with.
  – Originated from the right place.
• The keys and signatures are stored in the DNS
• Since DNS is a lookup system, keys can simply be looked up, just like any data.
High level concept of DNSSEC

- A resolver knows what the root-key is
- It builds a Chain of Trust:
  - Each level signs the key of the next level
  - Until the chain is complete
High level concept of DNSSEC

- root
  - uk
  - com
  - ma
  - bigbank.com (www)
  - bigbank.com (www)
A Skit/Play
Act III
DNSSEC To The Rescue!
Ugwina, the resolver, can verify that the real Og sends the message...
Example of Why You Need DNSSEC and a Simple Guide to Deployment

Russ Mundy, Parsons | ICANN66 | November 2019
Why Worry About DNS?

• Users think in terms of names
  – Applications primarily use DNS names
  – Internet uses network addresses to connect locations

• DNS provides the translation from names to network addresses

• Proper DNS functions required by essentially all Network Applications
  – If DNS doesn’t work right,
    ➔ the applications won’t get to the intended locations
DNS Hijack Threat

• DNS attacks provide a way to divert users’ applications, e.g.,
  – Redirecting user applications to false locations to steal passwords or other sensitive information
  – Redirect to a man-in-the-middle location
    • See and copy an entire session: Web, email, IM, etc.

• Multiple DNS hijack tools available on the Internet
  – Some University courses have required students to write DNS hijack software as a class assignment!

russ.mundy@parsons.com
How Can DNSSEC Help?

• DNSSEC can assure users they are reaching the right location
  – DNSSEC provides cryptographic information that can be used to verify that DNS information:
    • came from the proper source and
    • it was not changed enroute

• Hijack example will show DNSSEC preventing redirection of a web application
  – Web site tailored for effective use of DNSSEC and a web browser that uses DNSSEC
Normal DNS & Web Exchange

1. Query: www.ab.org?
2. www.ab.org=192.168.2.80
3. www.ab.org=192.168.2.80
4. Query: www.ab.org?
5. www.ab.org=192.168.2.80

Auth NS
ns1.ab.org
192.168.2.252

Web Server
www.ab.org
192.168.2.80

Recursive NS
10.2.2.2
10.1.1.253
10.1.1.1
10.2.2.1

“INTERNET”

“Joe User”
192.168.1.3
Attempted DNS Hijacked Web Exchange Stopped by DNSSEC

Auth NS
ns1.ab.org
192.168.2.252

Web Server
www.ab.org
192.168.2.80

Recursive NS
10.2.2.2
10.1.1.2

Redirected Website

Query: www.ab.org?
www.ab.org=10.2.2.1

Query: www.ab.org?
www.ab.org=192.168.2.80

“INTERNET”

DNSSEC Validation stops ‘False’ answer

Dr Evil Hijacker
192.168.1.99

“Joe User”
192.168.1.3

www.ab.org=10.2.2.1

30 June 2010

russ.mundy@parsons.com
1 Webpage = Multiple DNS Name Resolutions
DNS Basic Functions

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

➢ IT’S DNS ZONE DATA THAT MATTERS!
I need to have a WWW record

Simple Illustration of DNS Components

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

russ.mundy@parsons.com
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

russ.mundy@parsons.com
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)

russ.mundy@parsons.com
How Does DNSSEC Fit?

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

- Protect DNS ZONE DATA as much as (or more than) any DNSSEC information
- Including DNSSEC private keys!!

russ.mundy@parsons.com
I need to have a signed WWW record.

Simple Addition of DNSSEC
(there are both much more and less complex setups than this)

Add Zone Data
Sign Signed Data
Publish Authoritative Server

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

Client

russ.mundy@parsons.com
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 do little or nothing directly with their DNSSEC elements but Require DNSSEC from their suppliers.

russ.mundy@parsons.com
Support

DNSSEC for Everybody is an organized activity of the:

- ICANN Security and Stability Advisory Committee (SSAC)
- Internet Society Deploy360 Programme
Thank You and Questions