DNS Risks, DNSSEC

Olaf M. Kolkman and Allison Mankin

olaf@nlnetlabs.nl and mankin@psg.com
DNSSEC evangineers of the day

Allison:
- Independent consultant
- Member of the Internet2 Tech. Advisory Comm.
- IETF Transport Area Director
- Member of ICANN’s SSAC

Olaf:
- NLnet Labs (www.nlnetlabs.nl)
  - DNS and DNSSEC research
    - Protocol and software development (NSD)
- Co-Chair of the IETF DNSEXT working group
  (Shinkuro is acknowledged for sponsoring our trip)
Why DNSSEC

- Good security is multi-layered
  - Multiple defense rings in physical secured systems
Why DNSSEC

• Good security is multi-layered
  – Multiple defense rings in physical secured systems
  – Multiple ‘layers’ in the networking world

• DNS infrastructure
  – Providing DNSSEC to raise the barrier for DNS based attacks
  – Provides a security ‘ring’ around many systems and applications
The Problem

- DNS data published by the registry is being replaced on its path between the “server” and the “client”.
- This can happen in multiple places in the DNS architecture
  - Some places are more vulnerable to attacks than others
  - Vulnerabilities in DNS software make attacks easier (and there will always be software vulnerabilities)
Solution

a Metaphor

• Compare DNSSEC to a sealed transparent envelope.
  • The seal is applied by whoever closes the envelope
  • Anybody can read the message
  • The seal is applied to the envelope, not to the message
DNS Architecture

- Registrar/Registrant
- Registry DB
- edu as DNS provider
- Provisioning
- DNS Protocol
- edu as ‘friend’
- edu institution as ISP
- Cache server
- Secondary
- Primary
DNS Architecture

Server compromise

Inter-server communication

Cache Poisoning

DNS Protocol

Provisioning
Example: Unauthorized mail scanning

Subject: tenure

Astrophysics Mail Server

Where?

There!

Central Admin Mail Server

DNS
Example:
Unauthorized mail scanning

Subject: tenure

Astrophysics Mail Server

Central Admin Mail Server

Where?
Elsewhere

DNS

Bad Guy

http://www.nlnetlabs.nl/
Where Does DNSSEC Come In?

• DNSSEC secures the name to address mapping
  – Transport and Application security are just other layers.
DNSSEC secondary benefits

- DNSSEC provides an “independent” trust path
  - The person administering “https” is most probably a different from person from the one that does “DNSSEC”
  - The chains of trust are most probably different
  - See acmqueue.org article: “Is Hierarchical Public-Key Certification the Next Target for Hackers?”
More benefits?

- With reasonable confidence perform opportunistic key exchanges
  - SSHFP and IPSECKEY Resource Records
- With DNSSEC one could use the DNS for a priori negotiation of security requirements.
  - “You can only access this service over a secure channel”
DNSSEC properties

- DNSSEC provides message authentication and integrity verification through cryptographic signatures
  - Authentic DNS source
  - No modifications between signing and validation
- It does not provide authorization
- It does not provide confidentiality
DNSSEC deployment practicalities

• RIPE NCC deployed DNSSEC on the reverse tree
  – 202.in-addr.arpa etc are now signed and you can get secure delegations
  – We followed the architecture to plan the changes to our system

• You may want to follow the same steps when planning for local DNSSEC deployment
DNSSEC
Architecture modifications

Zone signer
Primary DNS
Secondary DNS
DNSSEC aware servers
Provisioning DB
DNS and input checks
Customer interfaces
DNSSEC aware provisioning

Zone Creation

Provisioning DB

DNS and input checks
Server Infrastructure

- Part of keeping up to date
  - Your most recent version of BIND and NSD run DNSSEC
- Memory might be an issue
  - Predictable (see RIPE352)
- Coordination with secondaries
Provisioning

• Realize that interaction with child is not drastically different.
  – DS and NS have the same security properties
  – You may need to respond a bit different to ‘child’ emergency cases

• Thinking “security” will make you notice “security”
Key Mastering and Signing

• Key management and signing needs to be reliable
  – Failure will lead to loss of service

• Cost factors:
  – Automation and Education
How about the ‘client’ side

• Set up your caching nameserver to perform validation and the infrastructure behind it is protected
• DNSSEC has not yet been pushed to the host or application
• Costs are in maintaining trust anchors
  – There is no standard to automate against.
What’s keeping folk

• New technology; chicken and egg
• Zone walking possibility
  – Is this really an issue in your environment?
  – Solutions are being engineered
• Automated key rollover and distribution
Why would you be an (early) player

• Keeping the commons clean
  – EDU and international research nets are important parts of the commons
  – Significant ‘hot spots’ of delegation
  – EDU networks have ‘interesting’ properties for the black hats.
Early players

• Demonstrate the ability to self-regulate
  – Before the guys up the hill force it down your throat
  – Before a bad thing happens and you are woken up at 2 am

• Lead by example
  – Break the egg
What you can do

• Deploy in your own domain
  – [www.dnssec.net](http://www.dnssec.net) contains a myriad of information resources.

• Ask your registry and your registrar?
  – Educause, ARIN, Verisign, CC-TLD registries, .gov etc.

• Ask your OS and network equipment and application vendors
  – Microsoft, Cisco, Firewalls vendors, etc
This Week

- Get involved in an Internet2 pilot
  - Charles Yun, Internet2 Security Program Director, organizing now
  - Talk to him this week
- Get to our workshop
  - http://dnssec-nm.secret-wg.org
- Talk to your colleagues for bilateral pilots
- Talk to us.
Next Week

• Deploying locally provides immediate security benefits
  – Sign your own zone and configure your keys

Buy now... get one free
Mitigate by Deploying SSL?

• Claim: SSL is not the magic bullet
  – (Neither is DNSSEC)

• Problem: Users are offered a choice
  – Far too often
  – Users are annoyed

• Implementation and use make SSL vulnerable
  – Not the technology
Confused?

Web Site Certified by an Unknown Authority

Unable to verify the identity of bert.secret-wg.org at a trusted site.

Possible reasons for this error:
- Your browser does not recognize the certificate of the site.
- The site's certificate is incorrect or has expired.
- You are connected to a site that is not secure or does not have a valid certificate.

Please notify the site's webmaster.

Before accepting this certificate you should ensure that the following are true:
- The certificate was issued by a trusted company that you are willing to accept.
- You want to download or exchange data with the site.
- The certificate is not expired and is still valid.
- The certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

Yes No View Certificate

Warning - Security

Do you want to accept the certificate from web site "www.p3.postbank.nl" for the purpose of exchanging encrypted information?

Publisher authenticity verified by: "VeriSign, Inc."

The security certificate was issued by a company that is not trusted.

The security certificate has not expired and is still valid.

Caution: "www.p3.postbank.nl" will not accept this content if you trust this certificate

Yes No

Certificate signer not found

The server's certificate chain is incomplete, and the signer(s) are not registered. Accept?

Yes No View Certificate

- The certificate for "bert.secret-wg.org" is signed by the unknown Certificate Authority "secret WG Certificate Authority". It is not possible to verify that this is a valid certificate.