# Something Interesting

Jay Daley
ccNSO Technical Day
Sydney 2009

p: (+64) (4) 931 6977 e: registry@nzrs.net.nz
f: (+64) (4) 931 6979 w: www.nzrs.net.nz
P.O. Box 24361, Wellington, New Zealand
New Zealand Domain Name Registry Limited

# Agenda

- Rethinking EPP
- NSCP/DCOMA- standards for nameservers
- Phishing URLs and how we might manage them
- What now for DNS with DNSSEC on the horizon

# The world before EPP – part 1

- Cryptographic signatures
  - Non-repudiation and tamper-proofing
  - No concerns on source IP address
  - Registrar responsible for key security
  - EPP – passwords and SSL – backward step
- Local data models
  - Fit with local need or requirements
    - e.g. Registrant type, identification numbers
  - Allows innovation and experimentation
  - Does make it harder for registrars though
  - EPP – single (thin registry) data model

# The world before EPP – part 2

- Control and manageability
  - Each controlled our own interface
  - Could add/change/remove as we liked
  - Even harder for registrars of course
  - EPP – horrible extension mechanism
  - EPP – opaque process for change (IETF group that does not officially exist)
- Not really cross-registry provisioning
  - Federations may be our future

# Rethinking EPP – part 1

- Adding cryptographic signatures
  - Easy, lots of XML apps do this
    - PGP in special tags <pgp></pgp>
    - S/MIME as used in XMPP (Jabber)
    - SAMLv2.0 HTTP POST 'SimpleSign' Binding
    - Detached PGP signatures (as per .nz DNRS)
    - BUT NOT XML-Dsig – complete disaster
    - http://www.cs.auckland.ac.nz/~pgut001/pubs/xmlsec.txt

# XMPP S/MIME Method

- <presence to="receiver">
  - <e2 xmlns="…">
    - <![CDATA[
      - S/MIME message
        - S/MIME header for two sections
        - Section 1 - Full XML document of presence info
        - Section 2 - S/MIME signature
      - End of S/MIME
    - ]]>
  - </e2e>
- </presence>

# .nz DNRS Method

- <!DOCTYPE NZSRSRequest SYSTEM "protocol.dtd”>
- <NZSRSRequest RegistrarId="90”>
  - <DomainCreate>
  - … details here
  - </DomainCreate>
- </NZSRSRequest>
- -----BEGIN PGP SIGNATURE-----
  - … signature data …
- -----END PGP SIGNATURE-----

# Rethinking EPP – part 2

- Supporting a local data model
  - More complicated but still achievable
  - Make EPP describe the data, not define it
  - Create default description of currently defined data -> backwards compatibility

# Rethinking EPP – part 3

- Easy extensions
  - XML-Schema has an excellent mechanism for extensions so use that
  - Object-oriented so extensions look like built-in parts of the syntax

# Rethinking EPP – part 4

- Real cross-registry support
  - Again, describing not defining data
  - A registry can say “we support X federation”
  - Registrar can then use X federation identifiers and operations
  - Of course these federations don’t exist yet

# Rethinking EPP - summary

- Add cryptographic signatures
  - Bring back some real security
- Support a local data model
  - Bring back control of data
- Support a proper extension mechanism
  - Bring back control of features
- Add cross-registry support
  - Look to the future

# NSCP/ DCOMA

- Currently
  - BIND – rndc command and config files
  - NSD – nsdc command and config files
  - ANS – proprietary XML interface
  - UltraDNS – proprietary XML interface
  - PowerDNS – PowerAdmin GUI
- Different tools, protocols and options

# NSCP / DCOMA – why?

- Standard way of controlling nameservers
  - Manufacturers would have to support
- One tool to control many nameservers
  - Supports TLD policies of genetic diversity
- Greater variety of tools/better quality
- Better backwards compatibility
- No vendor lock-in
  - We can change nameservers at lower cost

# DCOMA

- Attempt to define functionality for NS management
  - Dns COnfiguration Management
  - Languishing in IETF DNSOP working group
    - Not enough active supporters
  - Follows recent IETF pattern of defining requirements then protocol
  - Draft at http://tools.ietf.org/html/draft-ietf-dnsop-name-server-management-reqs-03

# NSCP – part 1

- Proposed protocol to implement DCOMA
  - (though actually predates it)
- Full command set
  - Commands - start, stop, halt etc.
  - Zone manipulation - add zone, remove zone, ACL creation, etc.
  - Parameters - control nameserver behaviour
  - Statistics - obtain information from nameserver
  - Zone data - manipulation of small amounts of zone data

# NSCP – part 2

- Full object model:
  - Server, Views, ACLs, RRsets, RRs and so on
- Ruled out of scope by dnsop (protocol)
- Needs a home and supporters
- Contact the lead author:
  - Stephen.morris@nominet.org.uk

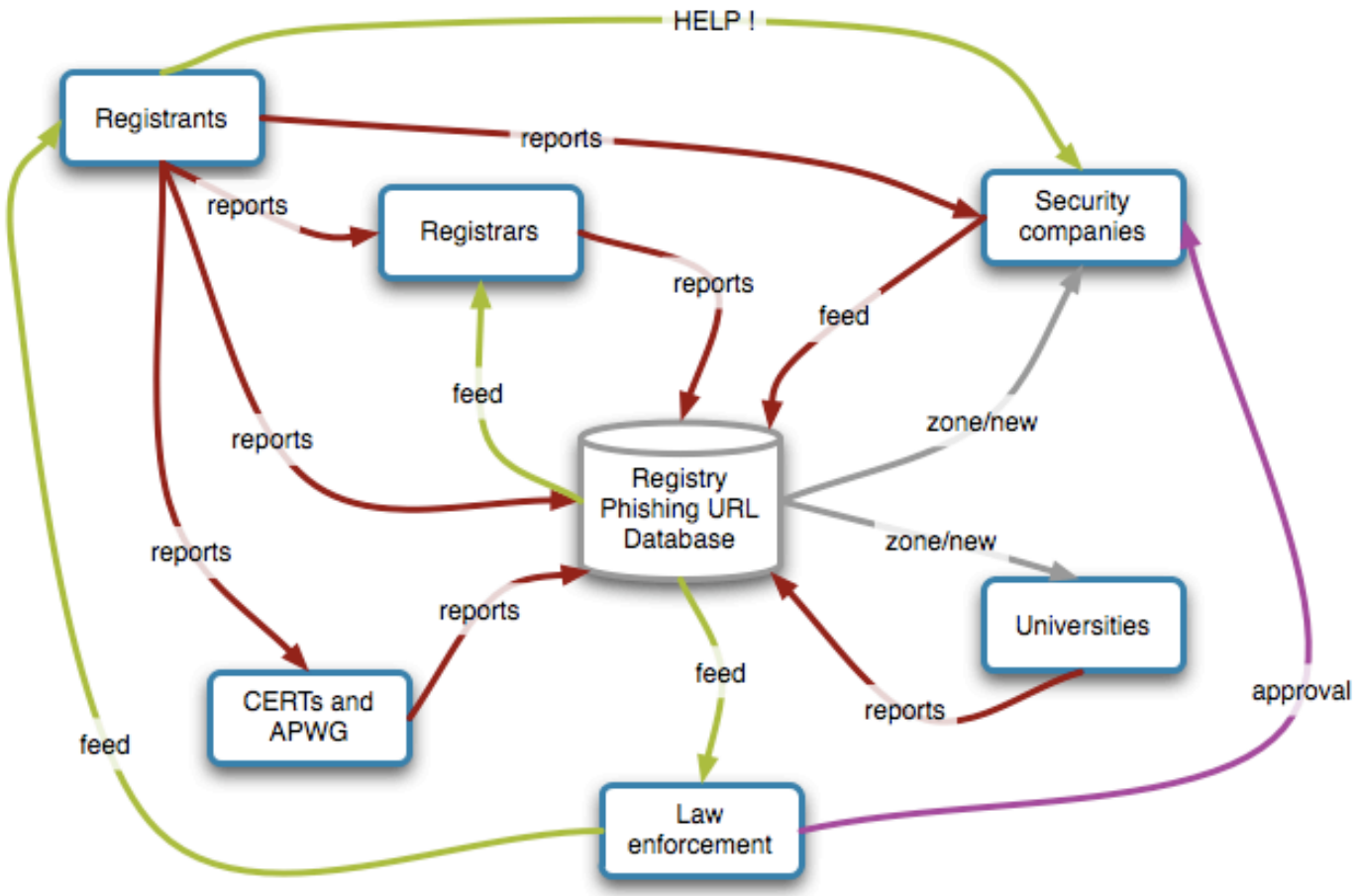
# Phishing URLs

- Increasingly important information
- Phishing has direct impact on ccTLDs
  - Invalid McAfee report impact on .hk reputation
  - WHOIS data mining by US “security” company Intrusion.com
- Significant commercial opportunity
- Yet strong community support and action

# Phishing URLs

- Initial data comes from
  - Consumer reports via toolbars/protection systems
  - Spam traps
  - Newly registered domains
- Then processed by
  - Security companies (commercial feed)
  - Anti-Phishing Working Group (free)
  - Local community (free)
    - Registrars
    - Universities
    - Research groups (e.g. CERTs)

# Registry DB of Phishing URLs



# What now for DNS after DNSSEC

- DNSSEC changes DNS
  - We can trust the answers
  - Greater use/support for TCP
- Certificates and identity?
  - CERT RR - RFC4398 – X.509, OpenPGP, etc
- Geo-location
  - LOC RR – RFC1876 – longitude, latitude, etc

# Any questions?

jay@nzrs.net.nz

p: (+64) (4) 931 6977
e: registry@nzrs.net.nz
f: (+64) (4) 931 6979
w: www.nzrs.net.nz
P.O. Box 24361, Wellington, New Zealand
New Zealand Domain Name Registry Limited