SAC049 DNS Zone Risk Assessment and Management

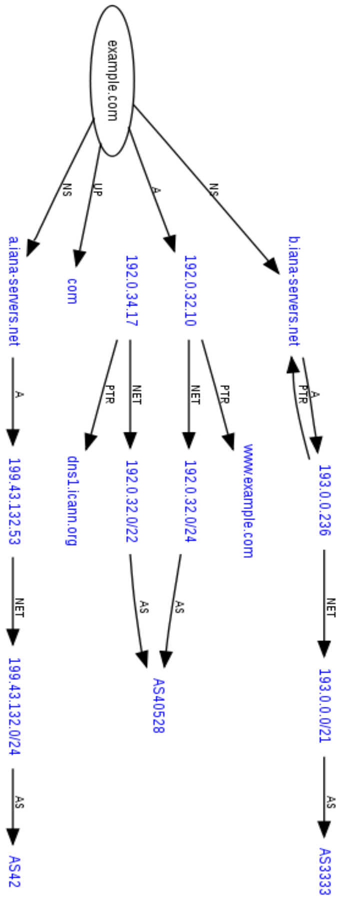
Dave Piscitello, ICANN

ICANN Singapore 41 19-24 June 2011

Background

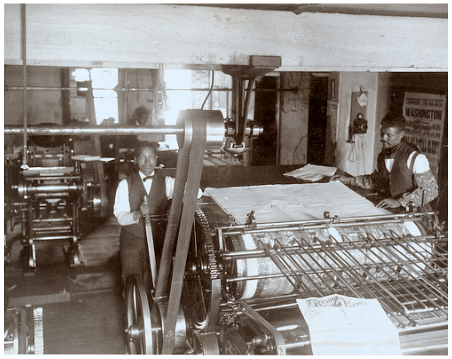
- Domain name resolution relies on zone data:
  - Resource records in a zone file define bindings between names, addresses, services
- Master name servers publish
- Authoritative name servers “host” zone files from “master”
- Recursive name servers ask authoritative name servers for resource records

Who Provides Authoritative NS?



- A DNS hosting provider
- Who is a DNS hosting provider?
  - Registrants
  - Registrant authorized 3rd parties
- An authorized 3rd party may specialize in DNS services
- Authorized 3rd parties often bundle DNS services with some other primary service, for example:
  - A registrar with registration services
  - An ISP with network services
  - A web hosting provider with a web site

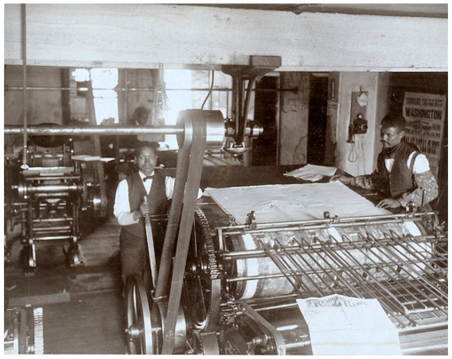
How Does a Registrant Publish a Zone File?



- Compose zone file and publish on own master server
- Compose zone file and send to DNS hosting provider

In these scenarios the registrant knows all resources and bindings.

How Does a Registrant Publish a Zone File?



- Registrant provides some zone data to DNS hosting provider:
  - Out of band, or through a DNS hosting provider's submission form.
- DNS hosting provider provides remainder of zone data and publishes zone file

In these scenarios the registrant may not know all resources and bindings.

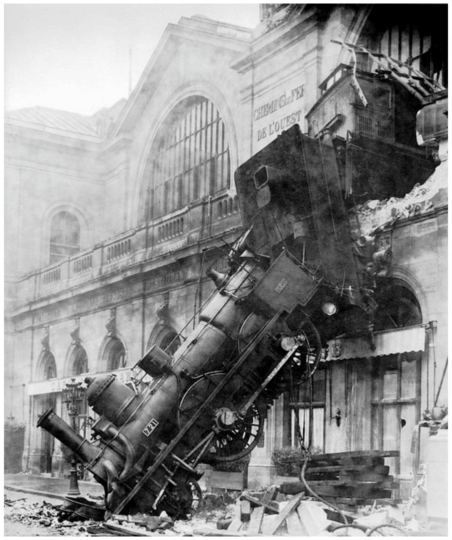
Problem Definition

A registrant who does not have complete knowledge of the information used to create the zone file for a domain is at risk of having name resolution interrupted without the ability to restore name service.

Why Is This Important?

- Name resolution is an essential and critical service.
- Your Internet presence relies on users being able determine the IP addresses of the names of your {web, email…} servers.
- Any circumstance where name resolution is interrupted is a threat.

Threat Landscape



- Technical or business failure of any DNS hosting provider:
  - Temporary or permanent, resulting in loss of original data.
- Account compromise (intentional misconfiguration resulting in loss of original data).
- Unintentional misconfiguration resulting in loss of original data.

Recommendations for Managing Risk

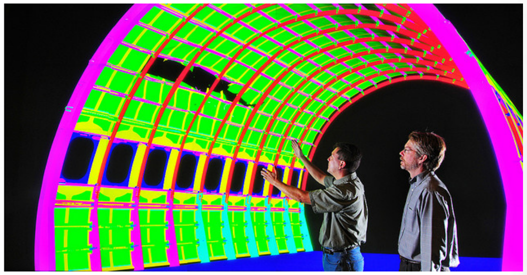
- Document your DNS architecture and operations.
- Design for resiliency.
- Actively manage DNS information.
- Protect domain registration and hosting accounts against attack.
- Proactively monitor name service.
- Track operational statistics and trends.
- Develop a continuity plan.
- Plan carefully, provision accordingly.

Make informed choices

Questions to ask DNS Hosting Providers

- How are zone data managed?
- Hosting footprint (sites, geography)?
- Capacity?
- Security measures?
- Monitoring? Can I integrate with my own?
- Communication: reports, alerts, alarms?
- Service level agreements?

Next Steps for the SSAC



- Share report with ICANN community, registrars, and DNS hosting providers.
- Presentations to community at large (e.g., ESNET/Internet2, APWG, MAAWG).
- Study and report on DNSSEC specific issues for DNS hosting.