DNSSEC at Akamai Technologies

David C Lawrence
Principal Software Engineer

ICANN Silicon Valley
DNSSEC Workshop
16 March 2011

About Akamai Technologies

Akamai is a distributed computing company

- Originally begun as a content distribution network
  - Provides increased website performance by delivering content from servers near the end user
- Grown to more than a dozen different services, such as:
  - Simple DNS hosting
  - Complex traffic management
  - Wide area application acceleration
- Powered by more than 84,000 servers in 72 countries

Swans, The Swiss Army Nameserver

One program handles authoritative DNS for all services

- Runs on tens of thousands of servers
- Several different modes for determining DNS answers
  - Each server tailored to demands of service it supports
  - Simplest mode serves traditional zones
  - More complex modes potentially have millions of updates per minute
- Most efficient method for signing answers varies by mode

Enhanced DNS Service

Hosting of DNS zones that are managed by the customer

- First, and currently only, swans mode to support DNSSEC
- Full service signing of zones, complete with key management
- Will also just serve zones signed by customer as-is
- Implemented due to mandate from US Federal Government
- Very low adoption rate by government customers
  - Perception that there is no negative consequence for ignoring mandate
  - Provides little incentive to cover other modes
  - Want to see DNSSEC advanced? Sell the customers on it

Enhanced DNS Service, Continued

Full service still requires regular customer involvement

- Secure delegations need records updated in parent zone
- Registry / Registrar / Registrant model has no explicit Operator role
- Non-DNSSEC, having Akamai host a zone is largely fire-and-forget
  - Customer updates nameserver records to point to Akamai
  - Doesn't need to interact with registrar afterward
- With DNSSEC, customer needs more involvement
  - Has to interact with registrar for some key rotations
  - Akamai has no formalized relationship with registrar on customer's behalf
  - Recognizing an independent operator role would help

Content Distribution Services

Highly dynamic, thus difficult to sign

- Answers are generated from many different variables
- On-the-fly signing is computationally expensive
- Pre-signing all possible answers is storage prohibitive
- Hybrid of on-the-fly and pre-signed is algorithmically complex
- All solutions mean additional hardware investment to maintain resiliency

Other Services

Varying degrees of complexity for signing other modes

- None as simple as Enhanced DNS Service
- ***Probably*** not quite as complex as the Content Distribution Services
- Still require significant engineering effort

Summary

Significant Challenges to Advancing DNSSEC

- Lack of universally recognized DNS Operator role hampers deployment
- Efficient signing of highly dynamic zones is a financial barrier
- Customers still don't see much value in DNS spoof protection
  - Some have indicated that even if they were signed, so many resolvers don't validate that the value of signing is diminished
- Hard to justify engineering effort and capital costs for services that customers are not requesting, even if the overall goal is good