Application Security with DNSSEC and DOSETA

D. Crocker ~ Brandenburg InternetWorking ~ bbiw.net
ICANN DNSSEC Session ~ 16 March 2011
An Amateur's View of Security

- Ambiguous uses of terminology

- Very high barriers to entry
  - Administration, operations, HCI usability
  - For example: certificates...

- Authentication/Validation of...
  - Actor – author vs. recipient vs. handler
  - Content validity means content is truthful vs. accurate vs. ...?

- Compare precision and implications:
  - “XML Signatures provide integrity, message authentication, and/or signer authentication”
  - “DKIM... permit[s] verification of the source and contents of messages”
  - “DKIM permits a person, role, or organization to claim some responsibility for a message”
Domain Security Tagging (DOSETA)

- Domainkeys* $\Rightarrow$ DKIM** $\Rightarrow$ DOSETA
  - DNS-based identifiers $\rightarrow$ Organization, not individual, granularity

- Template for tailored authentication services
  - Header/content model

- Self-certifying key service
  - `<selector>._domainkey.<domain name>`
  - Selector permits multiple keys per domain name, for admin convenience

- Object-oriented crypto wrapper
  - Meta-tag (header field) key information encoding
  - Can be invisible to end-user & non-supporting app

- Transit and handling ~robustness
  - Transform-tolerant canonicalizations
  - Selective header field coverage

* Thank you, Mark Delany (then of Yahoo!)
** RFC 4871
DOSETA Specification*

- Example data coverage
  - JSON structure, XMPP message, XML object, vCard, vCal, Web page signing, Web ad authentication

- DOSETA authentication template

  **D-Signature association:** how is signature data linked to content and attribute data

  **Semantics signaling:** how is consumer application to know that semantics apply

  **Semantics:** the meaning of a signature

  **Header/Content mapping:** Mappings between generic template and a particular service

* Base (library + authentication template)
  draft-crocker-doseta-base
Exemplar: MIME Authentication

* Template

D-Signature association: Content-Authentication: field

Semantics signaling: Content-Authentication: signals use

Semantics: [owner of signature domain takes direct responsibility for content]?

Header/content mapping: DOSETA Content to MIME Body; Header to Content-Type: + cited fields

* MIMEAUTH
draft-crocker-doseta-mimeauth (preliminary)
**DOSETA/DNSSEC**

- **DNS “safety” foundation**
  - Integration $\Rightarrow$ very strong end-to-end assurance

- **Complementary application security and infrastructure protection**
  - Separate net service ops from apps ops

- **Requires compelling market “pull”**
  - *Who wants strong data assurance (yesterday)?*
  - Financial services, legal, ops reporting, ops data sharing...?