REPUTE BoF

Murray S. Kucherawy
<msk@cloudmark.com>

Problem Space

- Several security technologies today need to be able to determine the *value* of an identifier
  - *Value* is intentionally undefined here because it will mean different things in different contexts
- Most common examples of these include IP addresses and domain names used when evaluating email
  - Is mail from example.com desirable?
  - Does 1.2.3.4 appear to be hacked?

Problem Space

- We have some very rudimentary reputation services already
  - DNSBLs (RFC5782) can indicate presence of an IP address on a block list
  - Vouch-By-Reference (RFC5518) can indicate that one domain vouches for another in certain specific contexts
- But these replies are binary only

Problem Space

- What's missing is something more general and extensible
  - Extend easily into new application spaces and sub-spaces
  - Allow something other than a Boolean expression of membership in a set
  - A means of indicating the service's confidence in its own answer

Problem Statement

- “Security applications need a general framework for querying one or more authorities about the reputation of an identifier. This framework must be extensible into new applications, and must support a plurality of possible assertions within each application, and an expression of confidence in the answer.”

What's In Scope

- The framework, including media types and other definitions
- A lightweight protocol for simple queries and replies, and a heavyweight protocol for more structured or detailed queries and replies
  - We'll try re-use existing wire protocols to move the data around; only talking about payload here
- Initial application definitions, such as for email

What's Not In Scope

- How a reputation service provider computes reputation or collects data to do so
  - Method of collection (feedback)
  - Specific data to be collected
- How a reputation consumer makes use of the reply from a reputation service
  - Fully a local policy/configuration decision