Hash Truncation

Tim Polk

August 1, 2005

Why Hash Truncation?

- Assume we have confidence in a hash algorithm H that produces a digest of length N
- If an application or protocol needs a message digest of length Np, and Np < N
- Truncating the result of H is arguably preferable to developing/deploying a new algorithm that produces a message digest of length Np

Properties Required

- H(Np,M) needs to be distinct from a simple truncation of H(M)
  - Ensures that recipient and receiver are using the same mode of operations
  - Simple truncation does not achieve this goal

General Idea

- Define a new mode of operations for hash algorithms
  - Generate an IV from the combination of base Hash algorithm and truncated length
- Hash the concatenation of (IV, M)
- Truncate the result

Open Issues, I

- Lots of different ways to generate the IV
  - Preferably, method will not require a new IANA registry!
  - Once editors have finalized their IV generation technique, ID will be submitted

Open Issues, II

- No Security Proof
  - Heuristically, if H has security strength commensurate with its output length then the truncated result should have security strength commensurate with its output length

Status

- Editors
  - John Kelsey (NIST)
  - Niels Ferguson (Microsoft)
- -00 draft will be submitted prior to Vancouver
- Strategy
  - Submit general solution in IETF
  - Pursue coordinated, specific solution in X9 to support ECDSA