Deploying a New Hash Function

Steve Bellovin
smb@cs.columbia.edu

Eric Rescorla
ekr@networkresonance.com

The Problem

- All of our cryptographic protocols depend on hash functions
  - All of our major hash functions are under successful attack
  - Oops!
- Clearly we need to transition to new hash functions
  - Including ones we've never seen before
- We try for algorithm-agility in our protocols
  - Goal: maintain security while new code is deployed
  - Did we get it right?
  - By the way, this depends on hash functions

Protocols Analyzed

- We looked at S/MIME, TLS, and IPsec/IKE/IKEv2
- *None* of them got it right
  - Certificates are the big problem
- For S/MIME, implementations need to permit multiple signatures where some are invalid
- For TLS and IKE/IKEv2, need proper client signaling in initial message
  - We're working on this in TLS
- Caution: must avoid downgrade attacks

Conclusions

- Agility is hard to get right unless you actually try deploying a new algorithm
- All of the protocols we looked at need more work.
- We expect others do too
  - SECSH, OpenPGP, OCSP, ...
- Most of our analysis applies to new signature algorithms, too
- Full details at `http://www.cs.columbia.edu/~smb/papers/new-hash.ps` (or .pdf)