Deploying New Hash Functions

Steve Bellovin
smb@cs.columbia.edu

Eric Rescorla
ekr@networkresonance.com

The Problem

- We have to deploy new hash functions — if not today, at some point soon
- We try for algorithm-agility in our protocols — but certificates are a special case
- Certificates rely on hashes
- Goal: maintain security while new code is deployed
- Did we get it right?
- No…

Protocols Analyzed

- We looked at S/MIME, TLS, and IPsec/IKE/IKEv2
- *None* of them got it right: what certificates will the other side understand?
- 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
- 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. Other protocols — DNSsec, SECSH, OpenPGP, and more — should be examined by the appropriate WGs.

  ☞ Most protocols need either an updated version or a BCP describing how to manage the transition.
- Implementors need to think about it, too
- Most of our analysis applies to new signature algorithms
- Full details at `http://www.cs.columbia.edu/~smb/papers/new-hash.ps` (or .pdf)