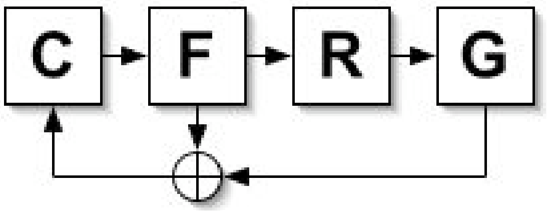
Problems and Progress with Crypto Hash Functions

David McGrew

mcgrew@cisco.com

IRTF CFRG Chair

IRTF Crypto Forum



- Advise Internet community on crypto
- Bridge between theory and practice
- Bringing new cryptographic techniques to the Internet community
- Promoting an understanding of these mechanisms via Informational RFCs

www.irtf.org/rg/cfrg
www1.ietf.org/mail-archive/web/cfrg

Crypto hash functions

- Crypto ‘hammer’
  - Commonly used and misused
- Theoretical uncertainties
  - ‘Random oracle’ model useful but imperfect
- Recent breaks
  - NIST Secure Hash Algorithm (SHA1)
  - Message extension attacks

Standard crypto hashes

	Goal	Status	Standard
MD5	2^{64}	2^{20}	RFC 1321
SHA1	2^{80} (<2011)	2^{63}	FIPS 186
SHA-224	2^{112} (<2031)	?	RFC 3874
SHA-256	2^{128} (>2030)	?	FIPS 180-2
Whirlpool	2^{128}	?	ISO 10118-3:2004

SHA1 Uses

		Status
Digital Signatures	Third Party	Broken!
	Entity Authentication	OK for now
Message Authentication	Raw SHA1	Broken!
	HMAC-SHA1	OK for now
Key Derivation	Raw SHA1	OK for now
	HMAC-SHA1	OK for now
Other	?	?

RFC hash citations

	SHA1	HMAC	SHA2	MD5
Total	151	121	5	360
Standard	101	84	4	190
Informational	40	33	1	33
Obsoleted	19	22	0	22

www.mindspring.com/~dmcgrew/crypto-cite.htm

CFRG and hashing

- Evaluating alternative hash functions
  - SHA-224, SHA1-IME, SHA-256, Whirlpool
- Identifying places where hashes can be replaced by something else
  - AES-based Message Authentication Codes (MACs) and Authenticated Encryption
    - CMAC, CCM, GCM, GMAC, UMAC, POLY1035
  - Randomized hashing
    - Requires protocol and/or API changes

What you should do

- Replace SHA1 (and MD5!)
  - MAC: use AES-based MAC or authenticated encryption mode
  - Other applications: use SHA-256, or carefully analyze security needs
- Build in algorithm agility
  - Need agile signatures, KDFs, …
  - Expect more changes
- Bring issues to CFRG and participate