Where should we go from here?

Bill Burr

NIST

SHA-1 Collisions

- Current best estimate 2^{63}
  - Still a fair amount of work
    - How much farther will it go?
  - Would be nice to verify this result
    - May be dangerous to do so
- How important are collisions? Two extremes:
  - Relatively minor, only matter for rare instances where we have to prove to a 3rd party (e.g. PKI - but PKI is a failure anyhow), or;
  - Canary in the mineshaft, crack in the dyke – a warning of much bigger dangers close at hand

SHA-1 Policy

- Getting rid of MD5 is highest priority
- OK to continue using SHA-1 a few more years in old apps (really have to) but new apps must use something else (SHA2?)
  - But we don't want apps to roll their own crypto
    - SHA2 support doesn't arrive until Vista
      - Long tail to XP
  - Can't issue only SHA2 certs (if you believe PKI still lives) until clients can do SHA2

SHA2

- Very little analysis yet - rather complex
- May well be theoretical break within a decade
- Probably won’t be a practical attack within a decade
- Not very efficient in hardware
- Can fix problems with more rounds
  - Need to be more conservative with number of rounds generally (think block cipher)
- Does NIST have a choice for relatively near term?

General Observations

- MD hash as random oracle => trouble
- Algorithm agility is needed
  - Resilience: several hash standards
- But: algorithm agility “sucks” in hardware
- So: we should overbuild
- But: everybody pays all the time for that

The Future

- Still confused about what all we want
- Beyond MD: block “generic attacks”
- Maybe we need more specialized functions
  - MACs, Digital Signatures, PRFs, KDF?
- Better design
  - Higher hamming weights
  - Better compression functions
- Provable security?
  - Number theoretic or equivalent to breaking something?
- Improve protocols to rely less on hash properties

Future Hash Standard Strategy

- For reasonably long term, not a crash program
  - Still discussing requirements/criteria
  - Not as mature as block cipher design in late 90s
- Flesh out requirements & criteria
  - additional workshop(s) ; competition for competition?
  - Tag the next onto Crypto2006?
- Competition
  - Probably 2 stages as with AES
- Selection
  - How many?