Hash Function Lifecycles and Future Resiliency

September 30, 2005
Don B. Johnson, Entrust CygnaCom, djohnson@cygnacom.com

A secure hash function is an unkeyed cryptographic primitive that is used in many critical ways. A secure hash function can be expected to go through the following summarized life cycle:

Design	Analysis & Theoretical Attacks	Deployment & Actual Attacks	Retirement from Active Use, Continued Passive Use

The design phase and analysis phase are each measured in years, while the deployment phase is (often) measured in decades. Experience has demonstrated that once a cryptographic primitive is deployed, its can take on a life of its own, as any security is considered better than none, interoperability with existing products may be essential, and continued passive use can be expected.

Future resiliency is the ability for a system to be resilient to the unknowns of the future. There are three things that can be said with confidence about the future:
1. Knowledge is increasing and it is increasing at a faster and faster rate; therefore crypto attacks can only be expected to get better, they never get worse.
2. We do not know what we do not know. In the nightmare scenario, when a hash function fails in a fundamental way due to a new breakthrough insight, the effects could be so large that we simply hope this will never happen. If someone discovers a way to find hash collisions then, for example, the non-repudiation attribute of digital signatures might literally vanish overnight. This ability to operate in the future to attack cryptosystems designed today is an inherent advantage of an adversary.
3. An adversary does not need to act according to our understanding of the rules; he or she may act in an unsportsmanlike manner or even cheat.

With the recent cryptanalysis of SHA-1 presented at Crypto 2005, there are only 2 NIST hash functions that have the full confidence of the cryptographic community, SHA-256 and SHA-512, as the possible SHA-160, and SHA-224 and SHA-384 are derivative. This is simply too few for such a critical primitive. Especially as they were designed by the same organization, the designs may be similar in a way that an attack on one could translate to an attack on the other.

ANSI X9 has a mandated five year review cycle for every standard. There is wisdom in this, after five years it has often been the case that ways are discovered to improve the standard. While we hope that a hash function may survive for decades, we know from experience that this may not be true, so we should plan accordingly.

This paper's first recommendation is that a hash function design competition be held soon and thereafter on a regular basis (for example, every five or ten years) in order to be able to incorporate the lessons learned.

Also, we have a choice, we can depend on one hash function for a specific output size and hope it remains strong or we can choose to have alternatives available, even if they may not be actually be used. While the first scenario is conceptually simpler, the latter scenario has much better future resiliency. As we have seen with SHA-1, when a weakness is discovered, it is not immediately clear how to proceed. When operating in Internet time, this lack of an immediate known response is not acceptable when we can choose to mitigate this risk.

This paper's second recommendation is that the results of a hash function competition be the selection of a primary hash function for each output size (security level) and the selection of at least one alternate as a backup in case the primary should fail.

In the Middle Ages, every count had his stone castle and taller walls meant that it was harder for men with ladders to scale them. But the invention of cannon meant that high walled stone castles were obsolete. What were able to survive in this new environment were forts with lower walls which absorbed cannonballs.

The cryptographic community needs to acknowledge the value of algorithm diversity and actively encourage it. The alternate hash should preferably use different design principles (as much as possible) to achieve their security. NIST already does this for digital signatures, by supporting RSA, DSA and ECDSA. This gives the cryptographic community some options in preparing for the possibility of a newly discovered weakness. By selecting at least one alternate, cryptosystems can be designed that support algorithm agility, for example, supporting algorithm changeover by either including this alternate backup or supporting code updates. Updating a cryptosystem to use an alternate hash function would not need to delay while a new hash was designed and analyzed, perhaps under time pressure.

Let us do our best to not find ourselves like the counts in their high-walled castles being attacked by cannon. Let us recognize that we are fighting an unfair battle with a future adversary and realize that there is strength in diversity.

CYGNACOM
SOLUTIONS

Hash Function Lifecycles and Future Resiliency

Don B. Johnson
Entrust CygnaCom

CYGNACOM SOLUTIONS

A Hash Function Lifecycle

Design	Analysis & Theoretical Attacks	Deployment & Actual Attacks	Retirement from Active Use, Continued Passive Use
(years)	(years)	(decades?)	(decades?)

CYGNACOM SOLUTIONS

A Life of Its Own?

- Once a cryptographic primitive is deployed, its can take on a life of its own:
- Any security is often considered better than no security
- Interoperability with existing products may be essential
- Continued passive use by receiving party can be expected, ex: Signature Verification

CYGNACOM SOLUTIONS

Future Resiliency

Future resiliency: the ability for a system to be resilient to the unknowns of the future.

We know 3 things about the future:

1. The increase of knowledge is accelerating, therefore crypto attacks only get better, they never get worse.
2. We do not know what we do not know. (Q: How do we know that?)
3. An adversary may not play by the rules.

CYGNACOM SOLUTIONS

A New Breakthrough Insight?

- If a new insight into how to attack the collision resistance of a hash function is developed, the non-repudiation property of digital signatures might vanish overnight.
- Witness Crypto 2005 papers
- Today, we have full assurance only for SHA-256 & SHA-512 and their derivatives (SHA-160(?), SHA-224, SHA-384).
- This is too few for a critical primitive.

CYGNACOM SOLUTIONS

Hash Function Design Competition

- ANSI X9 and ISO SC27 mandate a 5 year review of published standards
- **Recommendation 1: We should agree we need to have a hash function design competition now and every 5 or 10 years.**

CYGNACOM SOLUTIONS

Second Place Counts!

- **Recommendation 2: We should agree that the results of the hash competition is the selection of a primary and at least one alternate for each output size, in case the primary should fail.**
- The alternate should preferably be based on different design principles, as much as possible.

CYGNACOM SOLUTIONS

Benefits of Selecting an Alternate

- Cryptosystems might build-in alternate hash, to allow automatic switchover
- Cryptosystems can be designed to allow updates and update the hash immediately, rather than wait for design of a new hash
- The above options reduce the potential payoff to an adversary; may help avoid actual attacks
- In Internet time, the lack of a known way to proceed is not acceptable