FT-23-7433
Ray Wagner, Gregg Kreizman,
John Pescatore

Gartner FirstTake
23 August 2004

Encryption Flaws Present No Immediate Security Risk

A series of reported flaws in basic encryption "hash" algorithms shouldn't cause immediate concern. But they do show that vendors, cryptographers and certifying agencies should make alternatives available.

Event: On 17 August 2004, speakers at the Crypto 2004 conference in Santa Barbara, California, stated that they have found potential indications of vulnerabilities in Secure Hash Algorithm (SHA-1), a hash algorithm widely used in encryption programs such as PGP (Pretty Good Privacy) and Secure Sockets Layer (SSL). Hash algorithms help to create a message digest — a unique digital representation of an original message that is often used jointly with other encryption algorithms to protect against tampering. The Crypto 2004 announcement follows reports of flaws in two other security algorithms: SHA-0 (the precursor to SHA-1); and Message Digest Algorithm #5 (MD5), which is sometimes used in digital signatures.

First Take: These reports will undoubtedly cause concern among security specialists, because they involve the two basic hash algorithms used in encryption programs. However, the flaws likely pose no serious problem in the short term. They might be of more immediate concern in the few PKI (public-key infrastructure) or other digital signature products that still use MD5. Most other uses of hashes — such as for authentication purposes where the hash of a password is exchanged — are protected by other security mechanisms. Because MD5 and SHA-0 have long been known to have flaws, Gartner has recommended the use of SHA-1 since 1997.

It is unrealistic to expect an encryption algorithm to last forever. DES (Data Encryption Standard) had a life cycle of 25 years (extended by 3DES [Triple Data Encryption Standard]). Although Advanced Encryption Standard (AES) has undergone extensive peer review, it is still comparatively new, and a flaw in it could surface at any time. Because any algorithm can theoretically be compromised, vendors and developers should architect software so that it can use multiple algorithms and is backward-compatible with the broken ones.

Exploiting any theoretical vulnerabilities in SHA-1 would probably take several years, which gives the security industry time to strengthen or replace it. An open process, such as that used to select AES, should be followed in selecting any replacement. Legacy products would need to be re-engineered. As always, re-engineering efforts will depend on how well products were engineered in the first place. If architected correctly, the products will only need to turn off new uses of the flawed algorithms.

Recommendations:

- **Users of encryption products:** Look for updates in the next version of the security products you use (or the next major patch releases).

- **Encryption vendors and the standards community:** Begin work on designing and certifying the next generation of SHA-x.

Analytical Sources: Ray Wagner, Gregg Kreizman and John Pescatore, Gartner Research

Recommended Reading and Related Research

- "Assess Authentication Methods for Strong System Security" — Use two or more authentication methods to control user access to your systems. **By Clare Hirst, Ray Wagner and Vic Wagner**

- "When and How to Use Enterprise Data Encryption" — Network appliances now make data encryption feasible and cost-effective for many businesses — but you must understand this technology and its limitations. **By Rich Mogull**

(You may need to sign in or be a Gartner client to access the documents referenced in this FirstTake.)