

Press/Analyst Contacts:

Pat Rugg
VP Sales & Marketing
The Athena Group, Inc.
352/371-2567 x307
prugg@athena-group.com

Jon Mellott
CTO
The Athena Group, Inc.
352/371-2567 x302
jon@athena-group.com

February 28, 2005

Athena Expands Security Offering with Two New Products

GAINESVILLE, FL - February 28, 2005 - The Athena Group, a provider of high-performance, low-power signal processing and security products, announced the immediate availability of two new cores to its robust family of security products. The new Secure Hash Algorithm accelerator cores, SHA2-A100 and SHA3-A100, provide a comprehensive new capability to address the evolving demands for secure hash processing.

"The migration to new secure hash algorithms is going to get underway quickly," says Dr. Jon Mellott, CTO of the Athena Group. "New research has demonstrated that SHA-1 is inadequate, and new products must incorporate stronger secure hashing. Athena's SHA2-A100 and SHA3-A100 cores not only deliver higher throughput, but execute the strongest SHA algorithms of the FIPS 180-2 standard, including SHA-224, -256, -384, and -512, while maintaining backwards compatibility with SHA-1 for legacy applications."

A new paper by three researchers at Shangdong University in China has cast considerable doubt on the effectiveness of the SHA-1 hashing algorithm, a standard used around the world for over a decade. The researchers claim to have developed a new method for attacking the SHA-1 algorithm, which is the basis of digital signatures in numerous protocols including SSL (Secure Socket Layer), which is used to encrypt traffic to and from millions of websites.

When the SHA-1 algorithm was introduced in the 1990s as the Secure Hash Algorithm Standard, the National Institute of Standards and Technology stated "The SHA-1 is called secure because it is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which produce the same message digest." The new attack, however, demonstrates that it may be much easier than previously thought to cause the collisions that produce identical signatures.

Noted cryptographer Bruce Schneier, Chief Technology officer of Counterpane Security, Inc., wrote this week on his website that "This attack builds on previous attacks on SHA-0 and SHA-1, and is a major, major cryptanalytic result. It pretty much puts a bullet into SHA-1 as a hash function for digital signatures."

About The Athena Group, Inc.

The Athena Group, Inc. of Gainesville, Florida licenses signal processing and security technology that delivers breakthrough performance, reduced area, and reduced power consumption in a broad range of SoC products. Athena technology is ideal for leading edge applications such as secure e-commerce, wireless communications, and video compression.

Athena was founded in 1986 and is privately held.



The Athena Group, Inc. / 408 W University Avenue, Suite 306 / Gainesville, FL 32601
Phone: (352) 371-2567 / Toll-free: (800) 741-7440 / Fax: (352) 373-5182
www.athena-group.com

Copyright The Athena Group, Inc., 2005. All rights reserved. Reproduction in whole or in part is prohibited without the prior written consent of the copyright owner. The information presented in this document does not form part of any quotation or contract, is believed to be accurate and reliable, and may be changed without notice. No liability will be accepted by the publisher for any consequence of its use. Publication thereof does not convey nor imply any license under patent or other industrial or intellectual property rights.
