FOR IMMEDIATE RELEASE

Allegro Software Expands the Allegro Cryptography Engine™ (ACE) With Support For An Advanced Data-At-Rest Solution Specifically Engineered for the Internet of Things

FIPS 140-2 Validated Cryptography tightly integrated with a secure data-at-rest solution for Internet of Things devices

BOXBOROUGH, MA and SAN FRANCISCO, CA. April 20, 2015 - At the RSA® Conference 2015 in San Francisco, CA, Allegro Software, a leading supplier of Internet component software for the Internet of Things (IoT), today announced the addition of an advanced solution for securing data-at-rest using the FIPS 140-2 validated Allegro Cryptography Engine (ACE) in IoT applications. IoT devices populate the outer edge of the Internet and are often the starting point for information and trends derived from Big Data applications. When IoT devices store persistent data either locally or in the cloud, there is a risk of unintended exposure of sensitive material. Data encryption of stored data in these situations limits the risk of exposure. Allegro's latest addition to ACE provides IoT developers with the advanced ability to easily store and retrieve data-at-rest securely from local or cloud locations. Allegro's ACE along with the full Allegro AE™ product suite are ideally suited for creating secure IoT devices for transportation, military, energy, healthcare, and communications environments.

SECURING DATA AT REST IN THE INTERNET OF THINGS

Securing the Internet of Things represents many new challenges in terms of type, scale and complexity of technologies that are required. IoT devices at the edge of a network have the ability to generate large volumes of information and are often charged with securely acquiring, storing and eventually communicating data to enterprise applications. Before offloading data to cloud based applications, any sensitive information stored by IoT devices faces numerous threats and risks of unintentional exposure. Adding data encryption to the transmission process has been the traditional method for reducing this risk. However, simply encrypting data transmissions doesn't fully address many of the threats aimed at recovering small segments of data or potentially the entire collection.

Allegro's latest addition to Allegro AE and the Allegro Cryptography Engine (ACE) product suite provides IoT design engineers the ability to proactively address the threat surface created when storing sensitive data on persistent media. Rather than encrypting data at a volume or drive level where exposing a single set of keys potentially compromises a significant amount of sensitive data, Allegro's secure data-at-rest solution encrypts information at the file level.

Specifically engineered for resource sensitive embedded IoT environments, Allegro's secure data-at-rest solution uses both data encryption and authentication to detect file system validity (unauthorized modification or addition of files), limit data loss if the contents and keys of a single file are exposed, obfuscate file names and render the contents of any file useless without the application's knowledge to prevent malicious agents from copying useful data to an external storage device. The additional capabilities of the ACE library provide integrated secure file storage and retrieval using HTTP over TLS. The library also includes application programming interfaces for independent secure file storage and retrieval. The new data-at-rest feature (like the rest of the ACE library) includes configuration parameters for tuning performance.

"IoT devices generate and often store data at a scale never seen before. With hundreds of millions of IoT devices deployed today and projections of billions of devices in the near future, the total potential threat for exposing sensitive data is staggering," says Bob Van Andel, President of Allegro. "Finding ways to reduce and control this risk is vital to the continued success of IoT environments. The latest addition to the Allegro AE product suite and ACE for securely protecting data-at-rest gives development teams a greater ability to proactively control risk for their end users with FIPS 140-2 validated cryptography."

The Allegro Cryptography Engine (ACE) is specifically engineered to meet the critical needs of embedded IoT computing environments and is one of the smallest, fastest, and most comprehensive FIPS 140-2 validated modules on the market. ACE enables IoT device developers to perform bulk encryption and decryption, message digests, digital signature creation and validation, and key generation and exchange. ACE includes a platform-independent implementation of the NSA-defined Suite B suite of cryptographic algorithms, as well as other FIPS-approved algorithms.

The full Allegro AE family of toolkits is provided as ANSI-C source code. For more information, stop by **Booth #2238 South Hall** at the RSA Conference or visit our website: https://www.allegrosoft.com/allegro-ae.

About Allegro

Allegro Software Development Corporation is a premier provider of embedded Internet components with an emphasis on industry-leading device management, embedded device security, and UPnP-DLNA networking technologies. Since 1996, Allegro has been on the forefront of leading the evolution of secure device management solutions with its RomPager embedded web server and security toolkits. Also an active contributor to UPnP and DLNA initiatives, Allegro supplies a range of UPnP and DLNA toolkits that offer portability, easy integration, and full compliance with UPnP and DLNA specifications. Allegro is headquartered in Boxborough, MA and can be found on the web at https://www.allegrosoft.com.

Contacts:

Loren Shade
VP Marketing
Allegro Software Development Corporation
978-264-6600
loren@allegrosoft.com

Larry LaCasse
VP Business Development
Allegro Software Development Corporation
978-264-6600
larrylc@allegrosoft.com