



July 13, 2016

## **Boeing Licenses Rambus DPA Countermeasures to Protect Critical Aerospace and Defense Systems from Security Threats**

*World's largest aerospace company implements advanced security technologies to prevent against the threat of reverse engineering and exploitation*

SUNNYVALE, Calif. & CHICAGO--(BUSINESS WIRE)-- [Rambus Inc.](#) (NASDAQ: RMBS) today announced that its Cryptography Research Division and The Boeing Company (NYSE: BA), the world's largest aerospace company and the leading manufacturer of commercial jetliners and military aircraft combined, have signed a license agreement for the inclusion of advanced differential power analysis (DPA) countermeasures in Boeing products. Rambus Cryptography Research DPA countermeasures enable Boeing to protect against security attacks that are used to reverse engineer or exploit critical technologies built into aircraft and other defense-related products.

"The threat of DPA attacks is on the rise, and companies like Boeing need the utmost security solutions to safeguard its customers' high-value data," said Dr. Martin Scott, general manager of the Rambus Security Division. "By licensing our DPA countermeasures, Boeing showcases its commitment to building products with the highest level of security."

Concerns about DPA security attacks have originated in the smart card market, but these attacks have been spreading into other segments, including aerospace and defense. Government and military systems can be protected from cyber adversaries with a hardware-centric security approach, which helps prevent the threat of reverse engineering and exploitation.

DPA is a type of side-channel attack that involves monitoring variations in the electrical power consumption or EM emissions from a target device. These measurements can then be used to derive cryptographic keys and other sensitive information from chips. Rambus DPA countermeasures are a proven solution for protecting devices against the extraction of cryptographic keys and private data through side-channel attacks. Highly flexible, these solutions can be optimized for performance, size and security level, allowing customers to help fend off unauthorized access to critical information.

Rambus Cryptography Research has developed a comprehensive portfolio of application-specific hardware core and software library solutions that can be used to build DPA resistant products. Strong countermeasures can protect devices and applications used for government and military purposes, finance, mass transit and wireless communications. For additional information, please visit [www.rambus.com/dpa](http://www.rambus.com/dpa).

### **Follow Rambus:**

Company website: [rambus.com](http://rambus.com)

Rambus blog: [rambusblog.com](http://rambusblog.com)

Twitter: [@rambusinc](https://twitter.com/rambusinc)

LinkedIn: [www.linkedin.com/company/rambus](http://www.linkedin.com/company/rambus)

Facebook: [www.facebook.com/RambusInc](http://www.facebook.com/RambusInc)

### **About Rambus Security Division**

The Rambus Security Division is dedicated to providing a secure foundation for a connected world. Our innovative technologies span areas including tamper resistance, content and media protection, network security, secure payment, smart ticketing, and transaction services. Our technologies protect nearly nine billion licensed products annually, providing secure access to data and creating invaluable trust between our customers and their customer base. Additional information is available at [rambus.com/security](http://rambus.com/security).

### **About Rambus Inc.**

Rambus creates cutting-edge semiconductor and IP products, spanning memory and interfaces to security, smart sensors and lighting. Our chips, customizable IP cores, architecture licenses, tools, services, training and innovations improve the competitive advantage of our customers. We collaborate with the industry, partnering with leading ASIC and SoC designers, foundries, IP developers, EDA companies and validation labs. Our products are integrated into tens of billions of devices and systems, powering and securing diverse applications, including Big Data, Internet of Things (IoT), mobile, consumer

and media platforms. At Rambus, we are makers of better. For more information, visit [rambus.com](http://rambus.com).

## **RMBSTN**

View source version on [businesswire.com](http://www.businesswire.com): <http://www.businesswire.com/news/home/20160713006158/en/>

### **Press contacts:**

#### **For Rambus**

Simone Souza, 408-462-8859

[ssouza@rambus.com](mailto:ssouza@rambus.com)

or

#### **From Racepoint Global**

Hilary Costa, 415-694-6705

[hcosta@racepointglobal.com](mailto:hcosta@racepointglobal.com)

Source: Rambus Inc.

News Provided by Acquire Media