Mini Crypto chip is a self-contained encryption engine

October 4 2017

Mini Crypto is a self-contained encryption engine that generates its own session based “key.” Designed to be small and lightweight, it is about the size of a cracker. Its power requirement is roughly the same as a hearing aid, at 400 milliwatts, meaning it can be installed on equipment carried by one-person parties operating as scouts and forward air controllers. Credit: U.S. Air Force

The Air Force's new Mini Crypto chip will secure communications and

data between systems like unmanned aerial vehicles and explosive ordnance disposal robots, while being "losable."

Airmen in the field rely on secured communications to accomplish their missions without enemy knowledge of their plans. Historically, the means by which the military encrypts its communications has been cumbersome and subject to interception, like when allies successfully stole a Nazi encryption device, called an enigma machine, during World War II.

"We think it [Mini Crypto chip] will really help forward-deployed warfighters secure sensors, or communications devices, in areas where risk of interception is high, and still protect sensitive data, without burdening folks on the front lines with extra equipment or steps to safeguard the encryption device," said Heidi Beason, Mini Crypto program manager at the AF Life Cycle Management Center, Cryptologic and Cyber System Division, Joint Base-San Antonio, Texas.

Mini Crypto is a self-contained encryption engine that generates its own session based "key." Designed to be small and lightweight, it is about the size of a cracker. Its power requirement is roughly the same as a hearing aid, at 400 milliwatts, meaning it can be installed on equipment carried by one-person parties operating as scouts and forward air controllers.

Beason talked about the work that went into getting to this point.

"Mini Crypto is the result of two years of program development for us," she said. "We took a requirement for a very small, low power encryption device and in less than 20 months successfully designed and tested this unique component. Now we're ready for production."

Beason leads a team of nine at JBSA, who fall under AFLCMC's Command, Control, Communications, Intelligence and Networks

Directorate, headquartered at Hanscom Air Force Base, Mass. Hanscom's proximity to the Massachusetts Institute of Technology Lincoln Laboratory, a federally funded research and development center, enabled testing early in the development process.

"Communications devices all have a processor, where a message is formatted for transmission," said Christopher Edsall, deputy program manager for Mini Crypto. "In the case of a computer, it's the CPU. Mini Crypto is located after the processing center, but before the transmission center, which is usually a radio. Another Mini Crypto chip is installed at the receiver end, after the receiving antennae, but before the CPU. The second Mini Crypto chip decrypts the received message as it comes through the radio where the unencrypted message is processed, and then it is displayed or heard."

Mini Crypto works by establishing a key between sender and receiver. The exact key is required to read a message after encryption. Mini Crypto's unique key management system protects up to secret data and meets NSA standards, the highest standards for encryption. According to Edsall, Mini Crypto's encryption makes the effort of decrypting a message by an adversary difficult and resource-intensive. By the time a message is readable by an adversary after it is encrypted, it is no longer useful information.

It can be used in joint and coalition environments, providing tailored access to data. Data can be segregated based on a need-to-know using Mini Crypto.

"Mini Crypto's portability and losability make it ideal for things like precision air drops of supplies," said Beason. "We think this will allow commanders to send combat material to really austere locations for pickup, and protect their exact location, without putting the troops who need the material at risk."

Provided by Air Force Office of Scientific Research