DEFENSE SYSTEMS

Independent insight, analysis and perspective for decision makers who develop, acquire and manage defense technologies that facilitate situational awareness & enterprise agility

Cyber Defense

INDUSTRY FIRM PATENTS NEW CYBER ENCRYPTION TECHNOLOGY

WASHINGTON, DC -- A private sector firm is offering a new kind of reinforced encryption technology for the U.S. military services to safeguard mobile phone, radio and computer transactions from brute force cyberattacks.

Torrance, CA-based Internet Promise Group (IPG) has used internal funding to patent a new technical method of securing encrypted military communications by implementing, integrating and changing random bits with an existing encryption key algorithm.

The idea is to strengthen existing encryption keys to make them less vulnerable to brute force attacks where adversaries or cyber intruders use computer algorithms to try multiple combinations of keys until the details are discovered and the key is broken, said Tara Chand, founder and CEO of IPG.

Brute force attacks, which require both substantial coordination and sophistication, are typically thought to be associated with major cyberattacks from near-peer adversaries, such as Russia or China.

“We want to figure out a way to make the key so strong that you cannot break it,” he said. Chand explained that his firm has patented Random Dance Keys, a new class of military encryption technology engineered to be impenetrable to brute force cyberattacks.

“Random Dance Key innovation is based upon its focus on the key space itself rather than encryption algorithms, to provide ultimate defense and protection of critical data and communications. This patented, advanced key management system employs heuristic random wave envelopes derived from the three different types of waves to yield a perpetual sequence of random vectors,” Chand added.

Random Dance Keys, Chand explained, are able to change encryption keys with every data packet by using a new random sequence of bits. Random keys are used and then discarded.

“Every time you have a data packet, you come up with a random key and integrate that with an algorithm and encryption key you already have. You leave them as they are,” he added.

Internet Promise Group is now in the process of introducing this technology to the U.S. military services. Early conversations are underway, Chand explained. Current U.S. military concerns about cyber intrusions are heightened by recent revelations of Russian hacking and China’s previous record of hacking U.S. military databases.

For more information, please visit www.internetpromisegroup.com.

By Kris Osborn Editor-in-Chief of Defense Systems, July 11, 2017