



FPGA Cluster Demonstrates Massively Parallel, Hardware-Accelerated DES Cracking

Scalable key recovery algorithm to be shown at Black Hat DC conference, uses 176 Xilinx FPGA devices

Arlington, VA – January 29, 2010 – Pico Computing today announced that it has achieved the highest-known benchmark speeds for 56-bit DES decryption, with reported throughput of over 280 billion keys per second achieved using a single, hardware-accelerated server.

The FPGA computing platform assembled by Pico Computing for this demonstration, based on 11 Pico EX-Series cards, reportedly consumes less than 1000 peak watts of power and fits into a single off-the-shelf 4U server.

The 56-bit Data Encryption Standard (DES) is now considered obsolete, having been replaced by newer and more secure Advanced Encryption Standard (AES) encryption methods. Nonetheless DES continues to serve an important role in cryptographic research, and in the development and auditing of current and future block-based encryption algorithms.

“This DES cracking algorithm demonstrates a practical, scalable approach to accelerated cryptography,” said David Hulton, Pico Computing Staff Engineer and an expert in code cracking and cryptography. “Previous methods of acceleration using clustered CPUs show increasingly poor results due to non-linear power consumption and escalating system costs as more CPUs are added. Using FPGAs allows us to devote exactly the amount of silicon resources needed to meet performance and cost goals, without incurring significant parallel processing overhead.”

Hulton’s DES cracking algorithm uses brute force methods to analyze the entire DES 56-bit keyspace. The massively parallel algorithm iteratively decrypts fixed-size blocks of data to find keys that decrypt into ASCII numbers. This technique is often used for recovering the keys of encrypted files containing known types of data. The candidate keys that are found in this way can then be more thoroughly tested to determine which candidate key is correct.

Such brute force attacks are computationally expensive and beyond the reach of software algorithms running on standard servers or PCs, even when equipped with GPU accelerators. According to Hulton, current-generation CPU cores can process approximately 16 million DES key operations per second. A GPU card such as the GTX-295 can be programmed to process approximately 250 million such operations per second.

When using a Pico FPGA cluster, however, each FPGA is able to perform 1.6 billion DES operations per second. A cluster of 176 FPGAs, installed into a single server using standard PCI Express slots, is capable of processing more than 280 billion DES operations per second. This means that a key recovery that would take years to perform on a PC, even with GPU acceleration, could be accomplished in less than three days on the FPGA cluster.

“Our research efforts in cryptography and our real-world customer deployments have given us unique insights into parallel computing methods for other domains, including genomics and simulations,” said Dr. Robert Trout, Pico Computing Founder and President. “The use of an FPGA cluster greatly reduces the number of CPUs in the system, increases computing efficiency and allows the system to be scaled up to keep pace with the data being processed.”

Pico Computing will demonstrate the FPGA-accelerated DES decryption algorithm at the Black Hat DC 2010 digital security conference, January 31 through February 3 in Arlington, Virginia.

About Pico Computing

Pico Computing, based in Seattle, Washington specializes in FPGA computing platforms for cryptography, networking, signal processing, bioinformatics, and scientific computing. For more information about Pico Computing products and services, visit www.picocomputing.com.

###

Editorial Contact: Mark Hur, Pico Computing, (206) 283-2178, mhur@picocomputing.com