



Pico Computing Accelerates Cracking of NTLM Authentication Protocol by 500X

Company to demonstrate FPGA-based security auditing techniques at Black Hat in Las Vegas

Las Vegas, NV – July 26, 2010 – Pico Computing, the leading provider of hardware-accelerated cryptography solutions, announced today that it has successfully accelerated cracking of the NTLM (NT LAN Manager) authentication protocol, resulting in performance of over 144 billion keys per second using a cluster of 36 Xilinx FPGA devices installed in a single 4U system consuming under 1500 watts. This compares with typical performance of less than 20 million keys per second using a modern dual-core CPU, or 250 million keys per second when using a GPU-accelerated system.

“NTLM is widely used to protect user passwords and authentication on nearly all Windows-compatible servers and workstations,” said David Hulton, Pico Computing Director of Security R&D and an expert in accelerated key recovery algorithms. “CPU- and GPU-based approaches to password recovery are limited by power consumption and do not scale well when more processors are added. Clusters of FPGAs allow us to apply the resources needed to exactly match the parallel processing requirements of password recovery.”

According to Hulton, a hardware-optimized MD4 core and key generator running on the FPGA is able to generate NTLM passwords for any given character set and length. This processing module is then replicated and scaled up within a single FPGA device, and across multiple FPGAs on one or more PCI Express cards. Optimizations to increase performance in the FPGA devices include the use of reduced word sizes (only seven bits are needed to represent password characters) and by pre-computing and pipelining the stages of computation to exploit hardware-level parallelism. The resulting NTLM cracking application is linearly scalable, making it possible to recover passwords in minutes or hours, rather than in days or weeks.

Pico Computing will demonstrate cracking of NTLM and other encryption systems at the Black Hat Technical Security event being held on July 24-29, 2010, at Caesars Palace in Las Vegas, Nevada. At this event, Pico Computing will be showing its latest-generation FPGA computing platforms that include small form-factor, laptop-compatible cards as well as rack-mounted systems containing dozens or hundreds of FPGA modules.

About Pico Computing

Pico Computing offers scalable, FPGA-based platforms for high performance computing as well as design services. Customer applications include cryptography, bioinformatics, signal processing, and financial computing. The company is headquartered in Seattle, Washington and has customers and resellers worldwide. For more information about Pico Computing products and services, visit www.picocomputing.com.

About Black Hat Technical Security Events

The Black Hat Briefings have become the biggest and the most important security conference series in the world. Black Hat serves the information security community by delivering timely, actionable security information in a friendly, vendor-neutral environment. For more information about Black Hat Technical Security events, visit www.blackhat.com.