CERIAS
The Center for Education and Research in Information Assurance and Security

FPGA Password Cracking

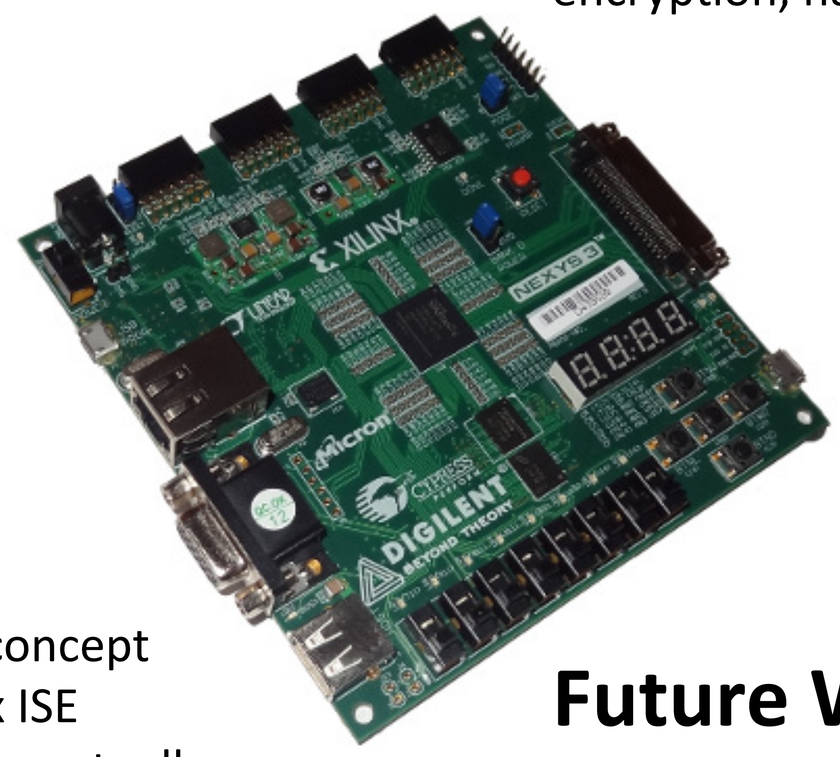
Max DeWees, Michael Kouremetis, Matthew Riedle, Craig West

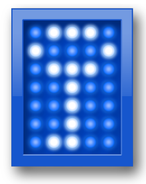
Background & Scope

- **Field Programmable Gate Array** (FPGA) – programmable hardware used in a variety of applications, where all logic runs concurrently
- No operating system or software overhead
- Commonly used in aerospace, communications, sensor networks, radio, data mining, diagnostics
- Recently used in BitCoin mining with Application Specific Integrated Circuits (ASICs)

Problem Description

- Using an FPGA to crack encryption keys and/or hash algorithms, including:
  - DES
  - MD5
  - SHA1
  - RIPEMD-160
- Applications in container encryption, full disk encryption, hashes, signatures, etc.





Method

- Current generation is a proof-of-concept
- Using Verilog language with Xilinx ISE
- Starting with a dictionary attack, eventually moving to a full brute-force approach
- Main questions:
  - Performance
  - Brute-forcing speed
  - Efficiency (hashes per cycle)
  - Scalability

Future Work

- Moving from a single FPGA board to a cluster
- Cracking AES encryption keys
- Cracking TrueCrypt containers and volumes
- Windows BitLocker and Mac OS X FileVault