Panel: Is Flash Memory Secure Today?

Michael Abraham (mabraham@micron.com)
NAND Solutions Group Architect
Micron Technology, Inc.

How to Make Flash Secure?

- Tamper resistant enclosure/sealing
- Use BGA or LGA packages with underfill/epoxy to prevent bus sniffing
- Use encryption on the drive unit
  - Keep keys out of host system DRAM
  - Keep keys out of on-board DRAM buffer
  - Keep out of other on-board nonvolatile memories (for example, serial NOR)
- Isolate system data from user data
  - Firmware
  - Bad block table
  - SMART or other status

How to Make Flash Secure?

- Add secure erase
  - Erase all user data, including grown bad blocks
  - Make secure erase resume automatically even after power cycle
- Record the unique IDs of each NAND die and verify at power-on that no components have been swapped or are missing
- Strong review of external password-to-decryption handoff
- No backdoors

Questions?

Revisit the Micron FMS presentations at www.micron.com/fms

About Michael Abraham

- Architect in the NAND Solutions Group at Micron
- Covers advanced NAND and PCM interfaces and system solutions
- BS degree in Computer Engineering from Brigham Young University