Overview of Data Security Methods:
Passwords, Encryption, and Erase

Chris Budd

SMART High Reliability Solutions

Overview of Data Security Methods

- Introduction
- Data Protection
  - Passwords
  - Encryption
  - Write Protect
- Questions to Ask
- Conclusion

- Data Elimination
  - Erasing
  - Overwrite
  - External Triggers

Introduction

- Data security important in all areas of storage
- Data security has two main components
    - Data Protection
    - Data Elimination
- Opposites?
    - No. Both guard data from unauthorized access

Introduction

- Data protection guards data from access
  - First step of data security
  - Keeps data for use only by authorized users
  - Includes passwords and encryption

Introduction

- Data elimination guards data from access
  - Must be last step before adversary obtains drive
  - Removes data before adversary can access it
  - Includes erasing encryption key, and possibly data

Introduction

- Additional features for military and industrial
  - Write protect
  - Overwrite after an erase
  - External erase triggers

Data Protection – Passwords

- Passwords are similar to combination lock on storage shed
- ATA specifies 32-byte password
  - Binary: 1 in 256^{32} or 1 in 1.16×10^{77}
  - ASCII: 1 in 95^{32} or 1 in 1.94×10^{63}
- Automatically locks after reset or power cycle
- 5 attempts to unlock; then drive must be reset

Data Protection – Encryption

- Self-Encrypting Drives (SED)
- No user or host intervention
- Could erase encryption key in milliseconds
- If user did not erase before adversary acquires the drive, then encryption is worthless without a password

Data Protection – Encryption

- If no password, adversary has access to data
- If password set, adversary must break password or remove flash chips
  - Wear leveling places data “randomly”
  - Similar to jigsaw puzzle with picture distorted

Data Protection – Write Protect

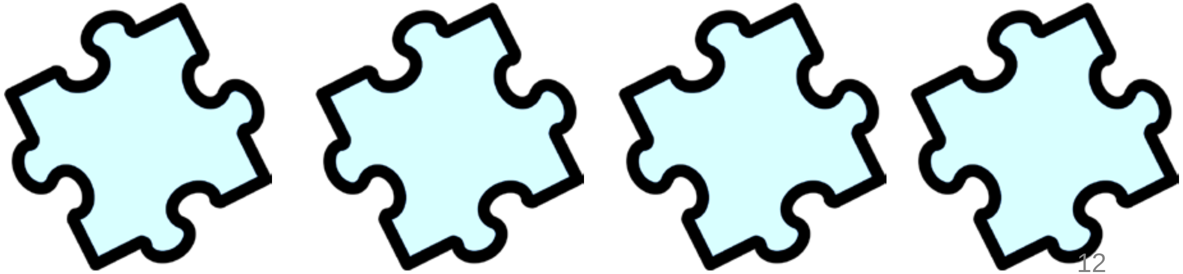
- Reasons
  - Protect collected data after mission
  - Protect map data during flight
- Activation
  - Vendor specific ATA command
  - External pins, but implementation varies

Data Elimination – Erase

- First step for SED is erase encryption key
  - Crypto or cryptographic erase
  - Normal read/write access useless
  - Encrypted data remains in NAND

Data Elimination – Erase

- Some SSDs may erase data blocks
- If user set a password, and if SSD includes crypto and block erase
  - Adversary removing flash chips is similar to jigsaw puzzle with all pieces same shape and same blank picture



Data Elimination – Overwrite

- Crypto and block erase not always sufficient
- Some agencies require overwrite
- IRIG 106-13, Chapter 10
  - Two overwrites: 0x55, then 0xAA
  - All blocks processed; no exclusions

Data Elimination – External Triggers

- If cannot rely on SW erase command
- Erase based on hardware input
  - Push button or electrical switch
- Implementation varies
  - Front or back
  - Shorted or power

Questions to Ask

- Crypto or block erase?
- If block erase, which blocks?
  - Mapping information?
  - User data?
  - Entire contents of NAND flash?
- Overwrite blocks?

Questions to Ask

- How does user know when drive done?
  - LEDs for states: normal, erasing, initializing?
  - Software commands (S.M.A.R.T. attributes)?
- Does the drive resume after power cycle?
- Can end user read entire contents of NAND flash to verify?

Conclusion

- Data protection
  - Passwords and encryption
  - Keeps data only for authorized users
- Data elimination
  - Crypto erase and block erase
  - No more data; not even for authorized users

Conclusion

- Additional requirements
  - For military and industrial applications
  - Write protect, overwrite, & external erase triggers
- Ask your SSD vendor tough questions
  - Complete your overall system security design
  - Pass the scrutiny of IA security officer

Conclusion

- SMART High Reliability Solutions
  - Has over 20 years of experience in solid-state storage
  - Knows well the data security requirements of military and industrial applications
- Ask us your data security questions
  - See us in booth #627