Agenda

- Purpose
- Method
- Media Recovery
- Conclusions
The purpose of the ATA Security Feature Set is to allow the device to authenticate the user:

- If the user supplies the correct password, the device will grant access to the media.
- This level of security is intended to keep an honest person honest...

ATA Security does NOT:

- Protect the data through encryption
- Protect data at rest
- Allow the device to authenticate the host system
- Allow the host system to authenticate the device
Method

- Two password system
  - Master Password – Administers the User Password
  - User Password – Grants access to the media
    - Security is only enabled after a User Password has been enabled

- Two tiered system (Only enabled when the User Password has been set)
  - High Security – Master Password and User Password are used interchangeably
  - Maximum Security – Only the User Password grants access to the media.
    - Media may be erased and user password deleted using the Master Password.
  - If both passwords are lost, the device is rendered unusable
Commands

- Password manipulation commands
  - SECURITY SET PASSWORD, SECURITY DISABLE PASSWORD

- Access control commands
  - SECURITY UNLOCK, SECURITY FREEZE LOCK

- Media recovery commands
  - SECURITY ERASE PREPARE, SECURITY ERASE UNIT
Weakness

- If the media is separated from the device, the data is available
Conclusions

- The ATA Security feature set provides a simple password system for granting access to a device.
- The ATA Security feature set has no effect on the data.