

Hard disk ATA Security

Adrian Leuenberger
adrian.leuenberger@csnc.ch

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

- Overview
- ATA specs
- Insecurities
- Problems with protected hard disks
- Password bypass procedures
- Further References

Overview

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

Short overview of the security features

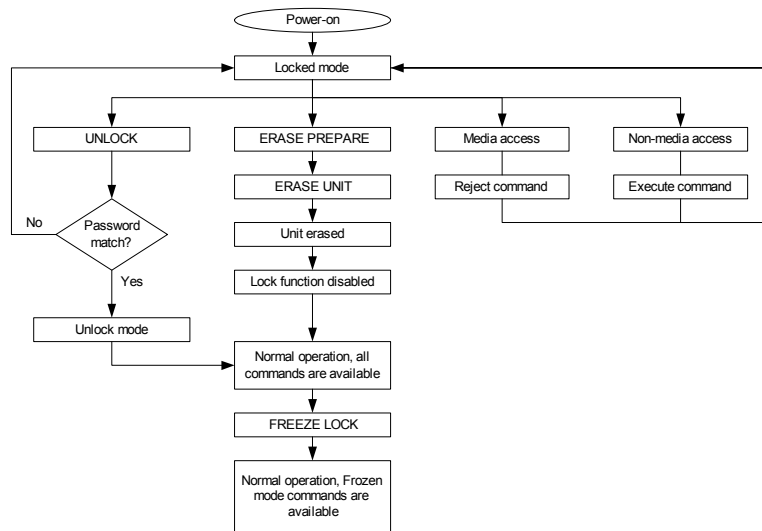
- Modern hard disks allow the setting of hard disk passwords that have to be entered whenever a computer is started.
- The password can usually be set in the computers BIOS or with 3rd party tools.
- The password is stored in the hard disk itself (not to be confused with the BIOS password, which is stored in the computer).
- Was firstly defined in the ATA-3 ANSI Standard (2008D AT Attachment - 3 Interface).
- Two passwords can be specified (each one 32 Bytes long)
 - User Password
 - Master Password
- The passwords are stored in the service area of the hard disk.
- The actual data is not encrypted on the hard disk.

ATA Specs

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

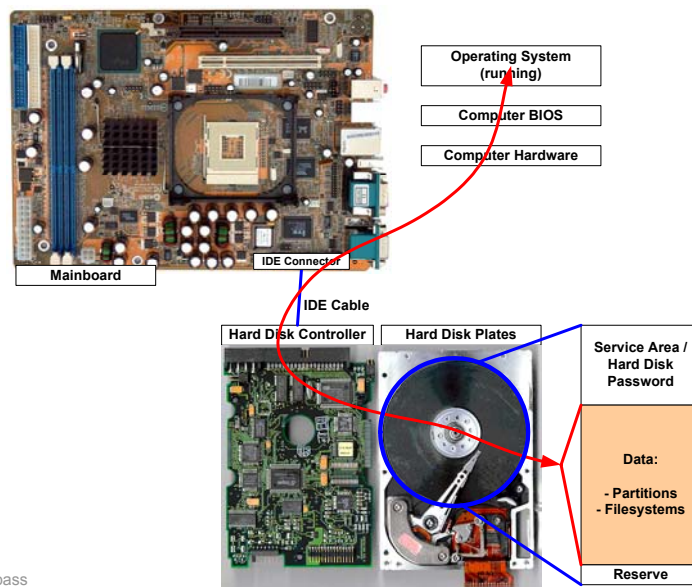
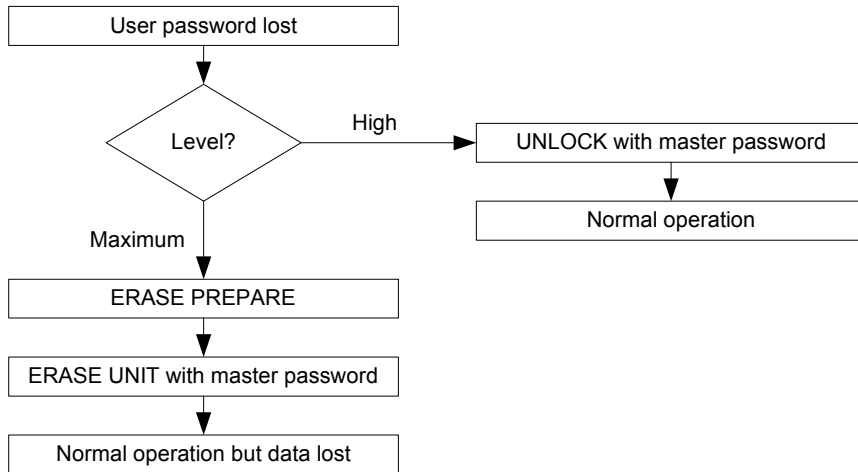
Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

- Two security modes can be set
 - High Security
 - The administrator can reset the user password
 - Data remains „as-is“
 - Maximum Security
 - The administrator can reset the user password
 - Data is overwritten with „0“ (wiped)
- Most often, the security mode cannot be set in the BIOS of the computer. Default is High Security.
 - Usually just the user password can be managed in the BIOS.
- Setting the security mode can be done with 3rd party tools.
 - Every computer type has to be carefully evaluated concerning the ATA security settings.



<u>ATA Command</u>	<u>Mode where cmd is available</u>
■ SECURITY DISABLE PASSWORD	Unlocked
■ SECURITY ERASE PREPARE	Locked/Unlocked/Frozen
■ SECURITY ERASE UNIT	Locked/Unlocked
■ SECURITY FREEZE LOCK	Unlocked/Frozen
■ SECURITY SET PASSWORD	Unlocked
■ SECURITY UNLOCK	Locked/Unlocked

- The correct password has to be provided of course!
- See table 7 in the ATA-3 specs for more details on which command is available in which context.

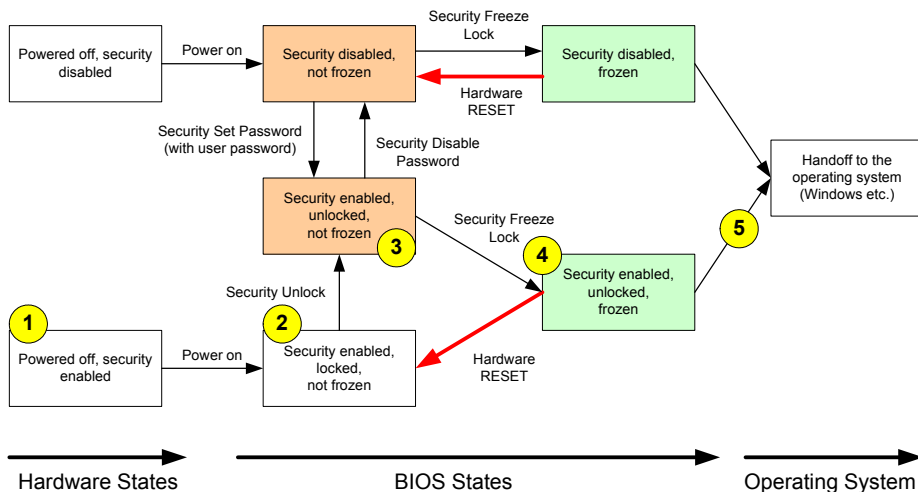


- It should be noted, that every access to the hard disk is made via the hard disk controller. There is no way to bypass the controller.
- The controller limits access to the data area on the disk. Other areas are not accessible in the normal operation mode.
- However, all disks know a maintenance mode where access to all areas of the disk is possible.
 - How to put the disk into maintenance mode is a secret known only to the manufacturers.
 - Recovery service companies (such as Kroll Ontrack or IBAS) might also get the information from the manufacturers or have reverse engineered the required techniques.

Insecurities

- The ATA security mechanism allows insecure states and transitions if the computers BIOS is not implemented correctly.
 - This allows viruses and worms to set arbitrary hard disk passwords.
- If a hard disk gets locked that way, the following solutions exist
 - If only a user password is set and the master password is known and the security level is HIGH, then a new user password can be set without any data loss.
 - If only a user password is set and the master password is known and the security level is MAXIMUM, then a new user password can be set but all data on the hard disk is overwritten with zeroes.
 - If an unknown master password is set, the hard disk can be either sent to a data recovery company or thrown away.
- The conclusion is, that the ATA security has to be implemented correctly or 3rd party solutions have to be evaluated to limit the damage a virus/worm could possibly cause.

Insecure States and Transitions



- Every BIOS has to be checked whether the FREEZE command has been correctly implemented.
- The correct working is as follows
 1. The computer is powered up.
 2. The user enters the hard disk password.
 3. The hard disk controller unlocks the hard disk.
 4. Directly after unlocking the FREEZE command is sent to the hard disk.
 5. Now the operating system can be booted. The operating system cannot change the ATA security settings anymore.
- This can be tested using a tool developed by Heise/ct
 - <http://www.heise.de/ct/ftp/projekte/atasecurity/windows.shtml>
- A 3rd party Windows service allows sending the FREEZE command in an early boot stage (also available from the link above) if the BIOS does not implement it correctly.

Problems with protected disks

- Forensic investigations (disk imaging) are impossible without first removing the hard disk password.
- The data on the disk itself is still unencrypted. It is usually just a matter of time until tools become available to bypass such security mechanisms.

Password Recovery/Bypass Procedures

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

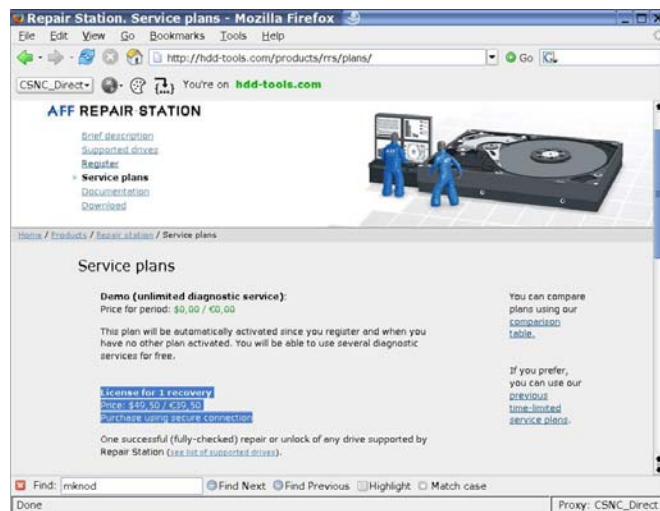
Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

- Unlocking of a Hitachi HTS721060G9AT00 hard disk
- Hard disk in a desktop pc using a 3,5" to 2,5" converter cable.
 - No access to the disk is possible (Knoppix, Windows, various boot disks).
- Hard disk in an old notebook
 - No access to the disk is possible (Knoppix, Windows, various boot disk).
- Hard disk in a forensic workstation (Freddie) with Encase
 - Encase does not recognize the hard disk.

- Unlocking of a Hitachi HTS721060G9AT00 hard disk
 - Security settings of the password
 - Locked / High Security / Not frozen
 - Brute forcing the master password is not possible as the hard disk has to be power cycled every 5 tries. This is annoying slow...
 - Several well-known master passwords have been tried without success (HDAT2 reports that the default password is still in place).
 - "WDCWDCWDCWDCWDCWDCWDCWDCWDCWDCWD"
 - "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
 - "Seagate"
 - "Maxtor"
 - "Maxtor INIT SECURITY TEST STEP "
 - 32 x 0xFF (Hex 255)
 - 32 x 0x20 (Space)

- Unlocking of a Hitachi HTS721060G9AT00 hard disk
 - Test with TAFT (see references)
 - Device cannot be detected.
 - ATAPWD (see references)
 - Hard disk was detected successfully
 - Not possible to get or change the password.
 - HDAT2 (see references)
 - Hard disk was detected successfully
 - Not possible to get or change the password.

- A-FF Repair Station (€39.50 for 1 unlock)



- Statement from A-FF regarding the Hitachi HTS721060G9AT00 (mail from 05.01.2006):

Dear Adrian,

Unfortunately, Repair Station cannot unlock the drive, but we can do that in our lab which is located in the Ukraine. Unlocking of such a drive will cost 229,95 EUR.

You may want to visit our lab website: <http://lab.a-ff.com>

Sincerely,

Daniel Clay

A-FF Support

Support@hdd-tools.com

- Ultratec (UK)
http://www.ultratec.co.uk/services/password_recovery.asp
- Nortec
<http://www.nortek.on.ca/nortek/>
- Kepler Data Recovery
<http://www.kepler.cl/en/pages/unlock.htm>
- And many more...
 - Just google for "password ata security" or similar.

■ Statement from Hitachi concerning the password protected hard disk:

■ First statement

The password function of a drive is a powerful Security Feature. If a password has been set on the drive, and you now no longer know the password, then you will be unable to access the data or the drive.

As this is a Security Feature designed to prevent unauthorized access to the drive, Hitachi will be unable to assist you further with this request.

■ Second statement

We know that the data recovery companies can get around the password protection. This doesn't mean that we are able to help you gain access as well.

"As this is a Security Feature designed to prevent unauthorized access to the drive, Hitachi will be unable to assist you further with this request."

I am sorry but we cannot help you anymore, if you need the data on the drive then I would like to advice you to contact a data recovery company.

■ Password Cracking POD from Vogon

- The laptop hard drive password cracker module enables the user to remove passwords from platter locked hard disk drives. It then allows the drive to be imaged and the original password to be replaced, all in a forensically sound manner. This may be essential when conducting field or covert investigation work. The techniques used are passive, and attachment to the host drive is via the drives' own interface.
- Works only in conjunction with the Vogon imaging hardware.



References

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

- Windows
 - WinAAM and ATA Security Service
<http://www.heise.de/ct/ftp/projekte/atasecurity/windows.shtml>
- Linux
 - Hdparm (Version tested: 6.3)
<http://sourceforge.net/projects/hdparm>
 - # `hdparm --security-help`
- DOS
 - TAFT – The ATA Forensics Tool
<http://vidstrom.net/stools/taft/>
 - ATAPWD
<http://www.rockbox.org/lock.html>
 - HDAT2
<http://www.hdat2.com/>

- ATA-3 Specification
<http://www.t13.org/project/d2008r7b-ATA-3.pdf>
- Drive construction
<http://www.ancelab.ru/products/pc-en/articles/ModernHDD/index.html>
- ATA password recovery service
<http://www.dataclinic.co.uk/password-protected-hard-drive.htm>
- ATA password recovery program
<http://hdd-tools.com/products/rrs>
- Computer Forensics and the ATA Interface
<http://www.foi.se/upload/rapporter/foi-computer-forensics.pdf>
- Password Cracking POD (Vogon)
<http://www.vogon-forensic-hardware.co.uk/forensic-hardware/data-capture/password-cracker-pod.htm>

