

Re: BIOS and Hard Drive Passwords – Are they effective security approaches?

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2003-06/0118.html>

From: Gabriel Levi (gabi_at_dao2com.com)

Date: 06/09/03

Date: Mon, 09 Jun 2003 21:18:33 +0300

Doug Fox wrote:

- > *Are the benefits out-weighed the costs of deploying BIOS and/or Hard Drive*
- > *passwords on laptops?*
- >
- > *People supports this idea claim that:*
- > *It has one more layer of defense.*
- >
- > *People who do not support this idea claim that:*
- > *If users forgot the BIOS passwords, the system could not boot up.*
- > *It may increase the support costs.*
- > *The BIOS passwords can be reset by a hardware technician in no time. If the*
- > *"thief" is interested in data, he can remove the hard drive to another*
- > *laptop.*
- > *??*
- >
- > *If the users forgot their hddrive passwords. The system could not boot*
- > *up.*
- > *It could increase the support costs.*
- > *It could "fire" the motherboard. (?)*
- > *??*
- >
- > *A better approach is to use PGP to encrypt the disk, or folders containing*
- > *sensitive information.*
- >
- > *Any comments/input are appreciated.*
- >
- >

Background

BIOS, is a ROM chip, in accordance to every ROM memory chip in the market today the BIOS also uses electricity to retain its definitions

(this is why the CMOS cloack "always" up-to-date)

Where does it take power from...cord?...generator? no....from a small (usually 3V) battery....

So What.....

So...if definitions (IDE, PCI, Cloack and yes also password) are retained

alt.computer.security: Re: BIOS and Hard Drive Passwords – Are they effective security approaches?

using battery powersupply cutting this elec. will delete the definitios.

Realy ???? how???

1. Get access to the MotherBoard (it is mother board day)
2. Locate the battery. (will not be diff. marked with (+) and (-) and have a XXV and look like battery.
3. Take a simple conductor (a copper wire will do the trick) short-circuit th