

# Bios Password Hacking

Mark E. Donaldson

Regardless of how long you've been working with computers, you've likely had the need to reset a BIOS password. You know, those configuration and power-on passwords that often keep us from managing -- sometimes even using -- our computers to get our work done. I used to love working with this kind of stuff in college and when I first started my career. Although I'm still intrigued, I just don't have the time to spend days on end experimenting to find the perfect solution to lost passwords. I'm sure you don't either. That's why I've created a sort of all-in-one reference guide to hacking BIOS passwords.

I won't bore you with tips on soldering chips and programming in assembly language, but I will provide you with some steps and good resources to turn to so you don't have to pull half your hair out or give up altogether. If you really need to get into or reconfigure a desktop or laptop system and one of those pesky passwords is getting in your way, here's how you can get around it.

There are several reasons why you may need to reset a BIOS password:

- You set a configuration password several years ago and now you have to make some hardware configuration tweaks or change the boot order of your drives. Conveniently, you can't remember the password you used.
- Your boss brought you her computer from home that her eight-year-old stepson mischievously locked her out of by setting a power-on password.
- You inherited a new set of computers and the previous administrator set BIOS configuration passwords so you can't enable/disable your built-in wireless or wired network cards.

A malicious person set a password on a physically insecure server or laptop, and now it won't boot. Regardless of why your BIOS password was set, there's likely a workaround. Some fixes are free while others you'll have to pay for. Some fixes are simple while others require you to be mechanically inclined. It'll very well cost you time and/or money, but it's hard to put a price on a non-functioning computer -- especially if it means your efforts could be better spent elsewhere.

I'll forewarn you: There are a lot of good BIOS password hacking and cracking resources on the Web -- several of which I link to in this guide. As with most things, the resources offer some good advice and some bad. Performing some actions can really lock you out of your computer -- to the extent of damaging your hardware and being forced into a service call, so proceed with caution. Also, be careful handling any computer hardware; you can destroy the sensitive circuitry inside the computer with static electricity coming from your hands. It could end up bleeding from the sharp metal that's inside the computer case! Keep in mind that attempting any of these steps can potentially void your computer's warranty as well.

So, if you're up for the challenge, try the following steps to hack, crack or otherwise reset your unwanted BIOS password.

## Step 1: Guess BIOS Passwords

Unlike many password-cracking programs that allow you to simply boot from CD or floppy to crack Windows-based passwords, if there's a power-on password setup in the BIOS, your options can be limited. The best way to get rolling is to simply try and guess the password yourself. For starters, on desktop and server systems, there are a lot of default backdoor passwords you can try. A previously published article, [How to Bypass BIOS Passwords](#), and [Computer Hopes'](#) all-in-one reference guide to hacking BIOS passwords contain comprehensive lists.

# Bios Password Hacking

Mark E. Donaldson

If you know who is/was the user or previous owner of the computer, you should try some common passwords such as their user's name, company name and so on to see if you can get it. Unless you're really into computer hardware hacking and can create a keyboard simulator to send your passwords brute-force style at wire speed, you'll have to enter each password manually. It's slow, but it can work, especially given the fact that most passwords are trivial.

There are a couple of other published tricks for getting around BIOS passwords on Toshiba and IBM Aptiva computers. If you have a Toshiba system, hold down the left shift key during boot. If you have an IBM Aptiva, the trick is to press both mouse buttons in quick succession during boot. You can also hold down one or more keys on your keyboard during boot to try and overload your keyboard buffer. Odds are you'll just end up getting a lot of angry beeps back from your computer, but it's worth a try. You can also take a crack at repeatedly hitting the F1, F2, F10, F11, F12 or ESC key as well.

## Step 2: Hardware

For starters, the tried and true method of resetting BIOS passwords on desktops and servers (i.e., not laptops) is to unplug the battery from the real-time clock. Refer to your owner's manual or vendor Web site for specific information on how to do this. A previous tip, [How to Bypass BIOS Passwords](#), and an article about contacting third-party companies, have links to various manufacturers that may help. Otherwise, contact your computer vendor directly.

Some computers have a password reset jumper or dip switch that you can use to reset BIOS passwords. You must locate this reset point on the motherboard and then, usually, you'll have to power up the computer once or twice with the jumper or dip switch set in the proper position for the reset to occur.

Another trick you can try in order to get into your BIOS without a password is to make a hardware change, such as removing a memory chip or disconnecting a hard drive. Also, you may want to try disconnecting the keyboard before powering on to see how the computer responds. If it boots into the BIOS setup, you can then plug the keyboard back in and you should be able to start typing (and resetting the password).

With laptops, BIOS passwords are stored in a non-volatile security chip, which means you won't be able to simply unplug the battery to reset it. And, if none of the previous methods works, your best bet with laptops is to call on a company such as Password Crackers Inc., which offers replacement chips that allow you to bypass your BIOS password altogether on boot. This requires soldering and other technical work that may be best left up to your local computer repair shop.

If you are able to replace your security chip but then reach a point where you cannot continue booting and accessing your hard drive, your drive is likely password protected with (hopefully) the same BIOS password. In this case, you can send in your laptop security chip to Password Crackers and they can recover the password for you. You could also set up your own memory chip reader/programmer and do this yourself. I don't recommend it, but if you're adamant about tinkering with and programming your own memory chips, the program notes file (cmospwd.txt) for the CmosPwd program outlines where these passwords are stored on the memory chips of various late-model laptops.

I've seen situations where people assume they need a BIOS password to boot a computer. In fact, you may see a flashing cursor or hear a few beeps right after you turn the power on that makes you think the computer is prompting you for a power-on password. In fact, quite the opposite may be taking place.

Your computer may be experiencing a hardware failure. It could be bad memory installed, the wrong memory installed, motherboard problems, video card failure -- you name it. Usually, you can find out

# Bios Password Hacking

Mark E. Donaldson

what the beeps mean at your BIOS or motherboard manufacturer's Web site, the owner's manual that came with your computer or at computer hardware sites such as BIOS Central. If you're not comfortable going down this path and opening up your computer to remove/swap/replace hardware, then, again, hire an expert to take a look-see and find the problem.

## Step 3: Crack With Software

If your computer won't boot because of a power-on password, and you've tried the previous recommendations, there's not a whole lot else you can do other than call a local computer shop technician to get his take on it.

However, if you have a BIOS setup password that needs to be reset, you can try using one of the free BIOS hacking programs; it may be able to get you in. It is very risky, though, so go into it with your eyes wide open and know that BIOS corruption and/or damage may very likely occur. You can run a tool such as WipeCMOS, Bios, RemPass, and CmosPwd. Those programs can read and write your BIOS information, including passwords and hardware configuration information, and potentially allow you to get in. The problem with this method is that some tools will reset everything, and you may not be able to configure your BIOS back to the point it needs to be for your motherboard and other chipsets to work. Again, read all the documentation with any tool you use and proceed with caution!

For Toshiba laptops, there's a parallel port or USB-based "key" you can purchase from Password Crackers that allows you to reset the existing BIOS password. You can also create your own makeshift key disk with a simple floppy and hex editor as outlined on Elf Qrin's Web site, How to Bypass BIOS Passwords.

If all else fails, you may be able to use DOS debug program running from a bootable floppy or CD to manipulate your BIOS directly as outlined here. Again, this is dangerous stuff, so go forward knowing that your computer might end up worse off than it was before you started tinkering with it.

If you're into learning more about the computer BIOS, check out BIOSMods.com and the book that helped me through many computer engineering courses in college way back when: Hans-Peter Messmer's The Indispensable PC Hardware Book.

## Step 4: Managing BIOS Password

Once you've guessed, cracked or somehow reset your BIOS password, it's time to think about handling things differently in the future. For starters, consider adding your own BIOS passwords yourself. I've always recommended at least protecting the BIOS configuration with a password. Sure, if it's easy to guess or accessible via a backdoor default, that can defeat the purpose. But, if anything, it can keep your non-technical users from going in and making configuration changes to their systems, locking you out and preventing administrative headaches down the road.

You could also consider adding power-on passwords to critical systems such as servers and laptops. It could be argued that every system is critical if it provides network access or contains sensitive information. (I haven't come across a computer that doesn't meet at least one of these criteria.) This could certainly add some administrative overhead, especially for remote users and servers stored in unmanaged offices or data centers that have to be rebooted occasionally. As I've shown here, adding BIOS passwords is not a foolproof measure, and they may just cause more trouble than they're worth, so proceed with caution. BIOS passwords do offer another layer of security that can buy you time or force an amateur hacker to give up. Bottom line, determine what's really at risk, how BIOS passwords would fit into your organization's culture and politics, and refer back to some alternate recommendations listed at the end of my laptop hacking guide.

## How to Bypass BIOS Passwords Backdoor passwords

# Bios Password Hacking

Mark E. Donaldson

Many BIOS manufacturers have provided backdoor passwords that can be used to access the BIOS setup in the event you have lost your password. These passwords are case sensitive, so you may wish to try a variety of combinations. Keep in mind that the key associated to "\_" in the US keyboard corresponds to "?" in some European keyboards. Laptops typically have better BIOS security than desktop systems, and we are not aware of any backdoor passwords that will work with name brand laptops.

**WARNING:** Some BIOS configurations will lock you out of the system completely if you type in an incorrect password more than 3 times. Read your manufacturers documentation for the BIOS setting before you begin typing in passwords

## Award BIOS Backdoor Passwords:

ALFAROME	BIOSTAR	KDD	ZAAADA
ALLY	CONCAT	Lkwpeter	ZBAAACA
aLLy	CONDO	LKWPETER	ZJAAADC
aLLY	Condo	PINT	01322222
ALLY	d8on	pint	589589
aPAf	djonet	SER	589721
_award	HLT	SKY_FOX	595595
AWARD_SW	J64	SYXZ	598598
AWARD?SW	J256	syxz	
AWARD SW	J262	shift + syxz	
AWARD PW	j332	TTPTHA	
AWKWARD	j322		
awkward			

## AMI BIOS Backdoor Passwords:

AMI  
AAAMMMIII  
BIOS  
PASSWORD  
HEWITT RAND  
AMI?SW  
AMI\_SW  
LKWPETER  
A.M.I.  
CONDO

## PHOENIX BIOS Backdoor Passwords:

phoenix, PHOENIX, CMOS, BIOS

## Misc. Common Passwords

# Bios Password Hacking

Mark E. Donaldson

ALFAROME	LKWPETER
BIOSTAR	lkwpeter
biostar	setup
biosstar	SETUP
CMOS	Syxz
cmos	Wodj

## Other Bios Passwords By Manufacturer

Manufacturer	Password
VOBIS & IBM	merlin
Dell	Dell
Biostar	Biostar
Compaq	Compaq
Enox	xo11nE
Epox	central
Freetech	Posterie
IWill	iwill
Jetway	spooml
Packard Bell	bell9
QDI	QDI
Siemens	SKY_FOX
TMC	BIGO
Toshiba	Toshiba

## Toshiba Bios

Most Toshiba laptops and some desktop systems will bypass the BIOS password if the left shift key is held down during boot

## Ibm Aptiva Bios

Press both mouse buttons repeatedly during the boot

## Password cracking Software

The following software can be used to either crack or reset the BIOS on many chipsets. If your PC is locked with a BIOS administrator password that will not allow access to the floppy drive, these utilities may not work. Also, since these utilities do not come from the manufacturer, use them cautiously and at your own risk.

- Cmos password recovery tools 3.1
- RemPass
- KILLCMOS
- Using the Motherboard "Clear CMOS" Jumper or Dipswitch settings

# Bios Password Hacking

Mark E. Donaldson

Many motherboards feature a set of jumpers or dipswitches that will clear the CMOS and wipe all of the custom settings including BIOS passwords. The locations of these jumpers / dipswitches will vary depending on the motherboard manufacturer and ideally you should always refer to the motherboard or computer manufacturer's documentation. If the documentation is unavailable, the jumpers/dipswitches can sometimes be found along the edge of the motherboard, next to the CMOS battery, or near the processor. Some manufacturers may label the jumper / dipswitch CLEAR - CLEAR CMOS - CLR - CLRPWD - PASSWD - PASSWORD - PWD. On laptop computers, the dipswitches are usually found under the keyboard or within a compartment at the bottom of the laptop. Please remember to unplug your PC and use a grounding strip before reaching into your PC and touching the motherboard. Once you locate and rest the jumper switches, turn the computer on and check if the password has been cleared. If it has, turn the computer off and return the jumpers or dipswitches to its original position.

## Removing the CMOS Battery

The CMOS settings on most systems are buffered by a small battery that is attached to the motherboard. (It looks like a small watch battery). If you unplug the PC and remove the battery for 10-15 minutes, the CMOS may reset itself and the password should be blank. (Along with any other machine specific settings, so be sure you are familiar with manually reconfiguring the BIOS settings before you do this.) Some manufacturers backup the power to the CMOS chipset by using a capacitor, so if your first attempt fails, leave the battery out (with the system unplugged) for at least 24 hours. Some batteries are actually soldered onto the motherboard making this task more difficult. Unsoldering the battery incorrectly may damage your motherboard and other components, so please don't attempt this if you are inexperienced. Another option may be to remove the CMOS chip from the motherboard for a period of time.

Note: Removing the battery to reset the CMOS will not work for all PC's, and almost all of the newer laptops store their BIOS passwords in a manner which does not require continuous power, so removing the CMOS battery may not work at all. IBM Thinkpad laptops lock the hard drive as well as the BIOS when the supervisor password is set. If you reset the BIOS password, but cannot reset the hard drive password, you may not be able to access the drive and it will remain locked, even if you place it in a new laptop. IBM Thinkpads have special jumper switches on the motherboard, and these should be used to reset the system.

## Overloading the KeyBoard Buffer

On some older computer systems, you can force the CMOS to enter its setup screen on boot by overloading the keyboard buffer. This can be done by booting with the keyboard or mouse unattached to the systems, or on some systems by hitting the ESC key over 100 times in rapid succession.

## Jumping the Solder Beads on the CMOS

It is also possible to reset the CMOS by connecting or "jumping" specific solder beads on the chipset. There are too many chipsets to do a breakdown of which points to jump on individual chipsets, and the location of these solder beads can vary by manufacturer, so please check your computer and motherboard documentation for details. This technique is not recommended for the inexperienced and should be only be used as a "last ditch" effort.