

10 steps to better secure your Mac laptop from physical data theft

Executive summary:

This paper describes changes Mac users can make to improve the physical security of their laptops, discussing the context and benefits of each change.

Author: Graham Lee
Senior Macintosh Software Engineer, Sophos
graham.lee@sophos.com

Table of contents

Introduction	2
1 Does it need to come with you?.....	2
2 Change your Keychain password and settings	3
3 Lock the screen when away from the computer	4
4 Filevault.....	4
5 Encrypted disk images.....	5
6 Keychain secure notes	6
7 Secure Empty Trash	7
8 Encrypted swap files.....	7
9 Firmware Password	8
10 Automatic logout.....	10

Introduction

Sophos's recent threat report¹ showed that while the Macintosh platform is now becoming the target of the same sort of organized crime that affects Windows users, these attacks are still very limited in scope and in impact. Nonetheless, we Mac users cannot afford to be complacent. The success of many data theft attacks depends more on the target system's user and the way in which they work with their computer, than on which operating system they have chosen to install.

Laptops are more prone to physical attack than desktop systems by their nature – being portable they are often taken out of the office to work from home, on the train or even in the local Starbucks. When you take your machine out on the road, you also take the data it contains away from the safety of the corporate environment with its security controls and into new environments with new risks and threats. Home users too must realize that when taking their MacBook out of the front door, more of their identity is on display than simply their preferred laptop brand.

In this paper I describe 10 steps that can improve the security of a Mac system, paying particular attention to laptop considerations. I concentrate on improving *physical* security – that is, protecting the system from attackers who can get their hands onto the computer.

1 Does it need to come with you?

The first step in securing your remote computing lifestyle is considering whether you need to take everything out. All of the attacks discussed here involve getting data from the computer – the easiest way to stop that from happening is to ensure that the data isn't there in the first place. In some environments, the attacker doesn't even need a computer; I have been sat in numerous cafés and on trains where I could see the online banking pages of other customers, and could (were I so inclined) read their account numbers, balances and the payments they were making. Simply put, I could see all of the information that an identity thief works to collate. While governmental departments such as the UK's HMRC may lose information about millions of people, most of the data on your laptop concerns one important person: you. Deciding whether all of this information really needs to come with you is the first, and most important, step to take on the road to safer computing.

In some cases this might not be so easy. John Gruber, author of Mac blog Daring Fireball², says: "My primary computer is a PowerBook that I use both at home and on the road. The only difference in how I use it on the road is that at home, I'm always connected to the internet, but on the road, network access depends on the availability of Wi-Fi. Otherwise, no difference." In such a situation, leaving everything at home (perhaps on an external drive) loses the convenience of carrying on your work when you're out. But I would say this is a compromise well worth making.

2 Change your Keychain password and settings

I asked John Gruber what changes he had made to his Mac OS X configuration with respect to security. His answer: “The only significant change I’ve made is that I use a different password for my Keychain than for my user account.” That’s a change I also make on all of my systems. The Keychain allows you to keep internet passwords, notes and SSL certificates in an encrypted store, and synchronize them between different machines with .Mac. So far, so good – of course there is only a single password to unlock all of this information, but it means that you can choose one really good password that you can remember, then use different passwords for all of the websites, mail accounts and so on that you use, which you don’t need to keep in your head (or on a Post-It note) because you can always get them out of the Keychain. The problem with the default Keychain configuration is that this password is synchronized with your login password; whenever you are logged in, the items in your Keychain are unlocked and available to any application that asks for them.

It is simple to fix this: firstly, open the Keychain Access application in /Applications/Utilities. In the Edit menu, choose “Change password for Keychain ‘login’...” and set a new password. Now when an application needs a password out of the Keychain, it has to prompt you for that password; a slight reduction in convenience but with a huge payoff in being able to control when your stored passwords are used. You can also control when the Keychain is automatically locked (so that you get re-prompted for the password) through the Keychain’s settings, accessed from the “Change Settings for Keychain ‘login’...” menu item.

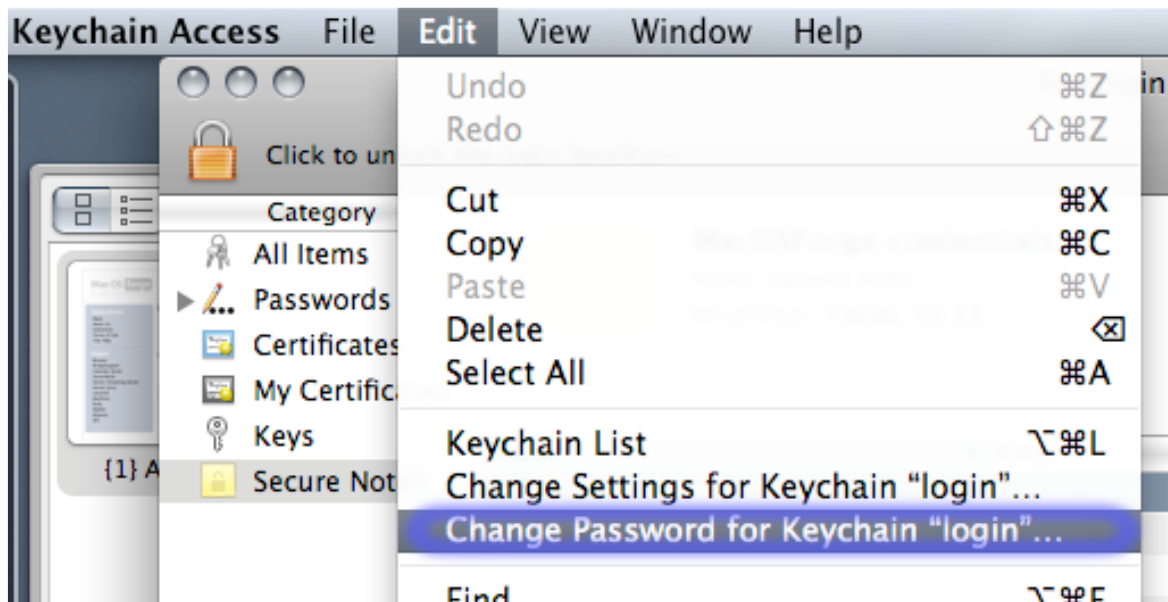


Figure 1: Changing the login Keychain's password

3 Lock the screen when away from the computer

Imagine the scene: you are logged into a website (perhaps checking your credit card balance, or seeing how many people have poked you today) in the coffee shop, when the barista tells you your drink is ready. You won't be far away and you can still see the laptop, so it is not going to get stolen... but while you're up, the nice girl on the next table makes a few notes on a napkin, and by the time you get home your credit card is a few hundred pounds lighter.

This situation can be easily avoided by using the password-protected screen saver built into Mac OS X. In the Security system preferences pane, make sure that "Require password to wake this computer from sleep or screensaver" is enabled. Now it is also useful to have a quick way to activate the screensaver, and two options are available. The first is to set up a *hot corner* in the screensaver preferences, so that when you move the mouse pointer into that corner of the screen, the screensaver will activate. The second can be found in the preferences of the Keychain Access program: choose "Show status in menu bar." The padlock icon which appears shows whether the Keychain is currently locked; clicking on it provides a menu from which one option is to lock the screen.



Figure 2: The Keychain status menu item lets you quickly lock the screen

4 Filevault

It is hard to imagine that you would ever forget your laptop and leave it at the train station, but it does happen. You have probably got insurance to cover the cost of the computer, and while it will be a hassle to recover all those files from a backup (less so with Time Machine, of course) you can soon get back to working again. Anyway, that MacBook Air looks so lonely on the shelf all by itself... but what has happened to the data on the iBook you left behind? If it was picked up by a cracker, then they probably didn't even turn the computer on, but just removed the hard drive and dropped it into a different computer. Then, without even needing to crack your password, all of the files – browser history, downloaded mail, Pages documents and so on – on that drive are ripe for the picking.

Filevault solves that problem in a simple way: it replaces your home directory, the area on the hard drive where all your personal files are stored, with an encrypted container. This container can only be unlocked by supplying one of two passwords – either your login password or the "master password", a catch-all password in case the login password is forgotten. The encryption used by Filevault is of a standard deemed safe to use by US government agencies.³

To enable Filevault, go to the Security pane in System Preferences, and choose the Filevault tab. Click on the "Turn On Filevault..." option, and you will be asked both to enter a master password and your own account's password. The Mac will convert your home directory into an encrypted container, and you cannot log in until this is complete. It is important that this step isn't interrupted, so if you are using a laptop plug it into the

mains before enabling Filevault. The master password can be used to remove the Filevault encryption from your home folder, so it's best to use a very complex password here, although if you are going to write it down then of course you have to keep it somewhere it won't be found.

Using Filevault or any other encryption (see below for two more options built-in to Mac OS X) raises a question about backups: do you keep your backups encrypted, or back up the files inside the encrypted container in the clear? There is no right answer, but I choose to keep unencrypted backups because my backup disk stays at home where I can be confident about who accesses it. Time Machine, the built-in backup system on Mac OS X, will only back up the Filevault volume *when you log out*, not on the regular schedule.⁴

5 Encrypted disk images

Covering your whole home directory with encryption may seem like overkill, especially if you only have a few sensitive files. You can use the same encryption mechanism that Filevault employs to create your own *encrypted disk images*, which can be used from the Finder in exactly the same way as regular images except that you cannot see the contents without entering your password.

Launch the Disk Utility application from /Applications/Utilities, and click on "New Image". From the drop-down which appears, choose the 128-bit option from Encryption, and configure the image as you like. (By the way, this is a great way to make an encrypted USB key drive – format the drive, then create an encrypted disk image on it using some – or all – of the free space.)

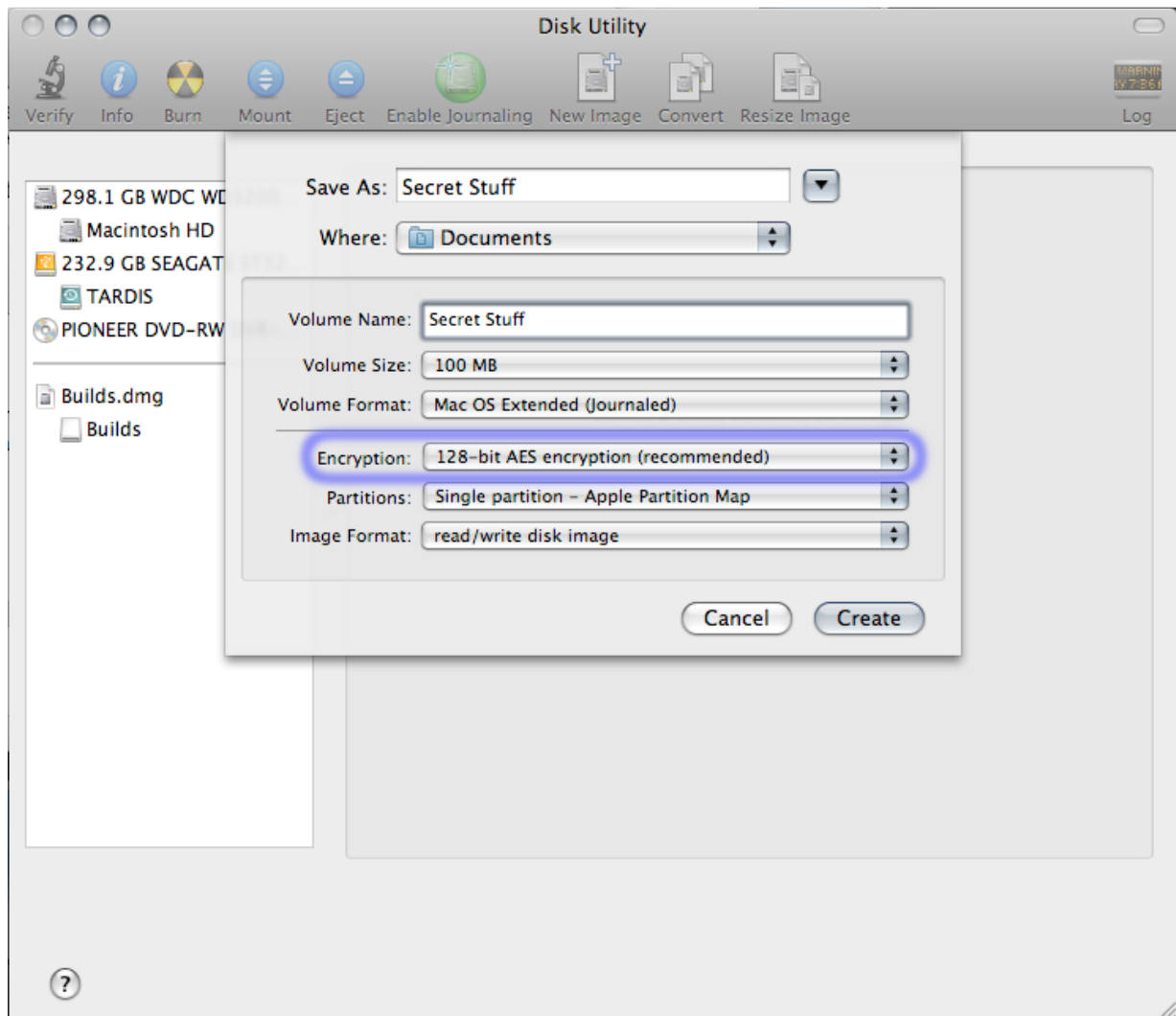


Figure 3: Creating an encrypted disk image

6 Keychain secure notes

For short notes which should be hidden from the view of others, you can create *Secure Notes* in the Keychain Access application which can then only be viewed by entering your Keychain password. This could be useful if you want to write yourself a reminder without letting anyone else see it, for example to remind you about a task in your online banking website.

7 Secure Empty Trash

When you delete a file from the hard drive in your Mac, it is not really deleted – the info telling the computer where to find the file is removed, but the data will remain on the disk until the space is needed to store something else. It is really easy to recover deleted files, you can buy off-the-shelf programs such as FileSalvage⁵ which can do it. Therefore even your deleted files are not safe from the interested cracker.

By selecting “Secure Empty Trash” from the Finder menu to empty the Trash, you can make recovery of the deleted files much harder. It’s still not impossible, although it will require complex (and expensive) forensics equipment to do. Secure Empty Trash writes over the files a number of times before deleting them, which makes it difficult to discover the original contents. Securely deleting files can be a slow process.

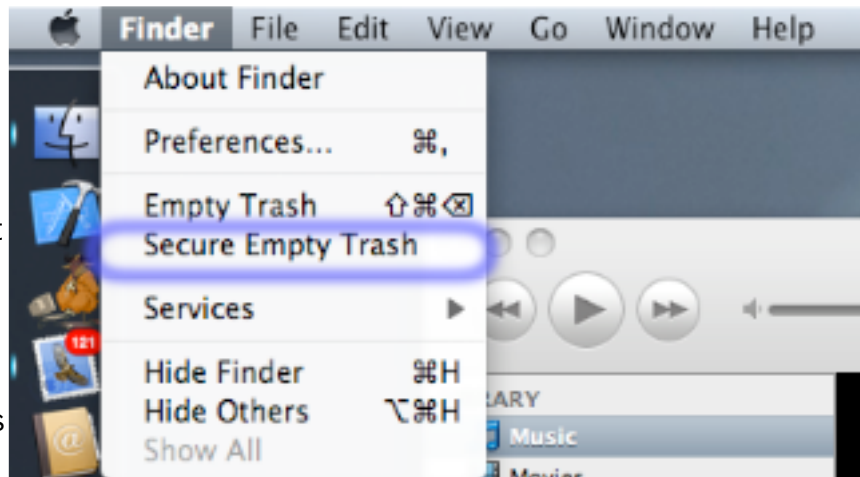


Figure 4: Using Secure Empty Trash to completely delete files

8 Encrypted swap files

Many news websites have reported the story that security researchers have found a way to recover passwords⁶ from the RAM of computers running a variety of operating systems including Mac OS X. The constraints on that particular attack are very limited (the attacker needs physical access, and must be able to reboot the system, then boot from their own removable media within less than a minute), but the applicability is wider on Mac OS X for a simple reason: it is possible for your login password to get into the *swap file*, a file on the hard drive used to simulate more memory. When that happens anyone who can get access to the files on the hard drive – locally or remotely – can read the password.



Figure 5: Enabling secure virtual memory

Luckily, a solution to this problem is incredibly simple. From the security pane in System Preferences tick “Use secure virtual memory”. Once you have done this, reboot and the swap file will be stored in an encrypted format.

9 Firmware Password

Referring back to the attack described above in “Encrypted swap files”, the attacker needed to be able to boot into their own operating system to recover the passwords from RAM. It is possible to stop that from happening by password-protecting the firmware. Doing so is slightly more involved than encrypting the virtual memory, but it may make sense on workstations as well as laptops, depending on the environment – without the password, an attacker can’t reboot from the OS X installation disk to reset administrator passwords or otherwise manipulate the contents of the hard drive. It also stops computers with unrestricted physical access, such as those in internet cafés or university computing labs, from being booted into another operating system to circumvent any local policy.

On the installation disk that came with your Mac, go to the Applications/Utilities folder (Apple has hidden this folder on my copy, which means that to get there I had to choose “Go To Folder...” (Command-Shift-G) in the Finder, and type “/Volumes/Mac OS X Install Disc 1/Applications/Utilities.” The good news is that you don’t have to type all of that, you can type the first few characters of each part then hit Tab to complete it). The application is called “Open Firmware Password.app” on PowerPC computers and “Firmware

Password.app” on Intel Macs. You need to provide an administrator password before you set the firmware password, and it is very important not to forget that password as without it you cannot change what operating system the computer boots into, nor boot in Verbose, Safe or Single-User modes. Apple has a support article⁷ with a detailed description of the consequences of entering a firmware password.



Figure 6: Setting a firmware password

Setting a firmware password also gives protection against attackers using a FireWire connection to snoop the contents of your computer’s memory, which can include your login password. By connecting a FireWire cable to any Mac in its default configuration, a bad guy can see, or even change, what is in the Mac’s memory⁸ without having to install any software on the system and without any record of the intrusion. Setting the firmware password causes the FireWire drivers to operate in a secure mode, removing this direct memory access.

10 Automatic logout

The last item in this discussion of Mac OS X features to improve physical security is also the least, because it offers little additional security at a cost of some convenience. In the Security preference pane you can configure the Mac to log you out automatically if you are not active for a certain amount of time. The problem with that is that the inactivity time gives bad guys a chance to use the computer, while locking the screen (or even shutting the computer down) would stop them from being able to do that.

Sources

- 1 www.sophos.com/security/whitepapers/sophos-security-report-2008
- 2 daringfireball.net/
- 3 images.apple.com/macosx/pdf/MacOSX_Leopard_Security_TB.pdf
- 4 www.macosxhints.com/article.php?story=20071123090741653
- 5 www.subrosasoft.com/OSXSoftware/index.php?products_id=1&main_page=product_info
- 6 citp.princeton.edu/memory/
- 7 docs.info.apple.com/article.html?artnum=106482
- 8 www.quinn.echidna.id.au/Quinn/WWW/Hacks.html#FireStarter