How to be reasonably secure using mobile off-the-shelf computing

by Fred Cohen

Abstract:
In early May of 2007, Kevin Manson asked me to write up some of the details underlying the comments I made to him about how to be reasonably secure with off-the-shelf mobile computing technology. This is that write-up.

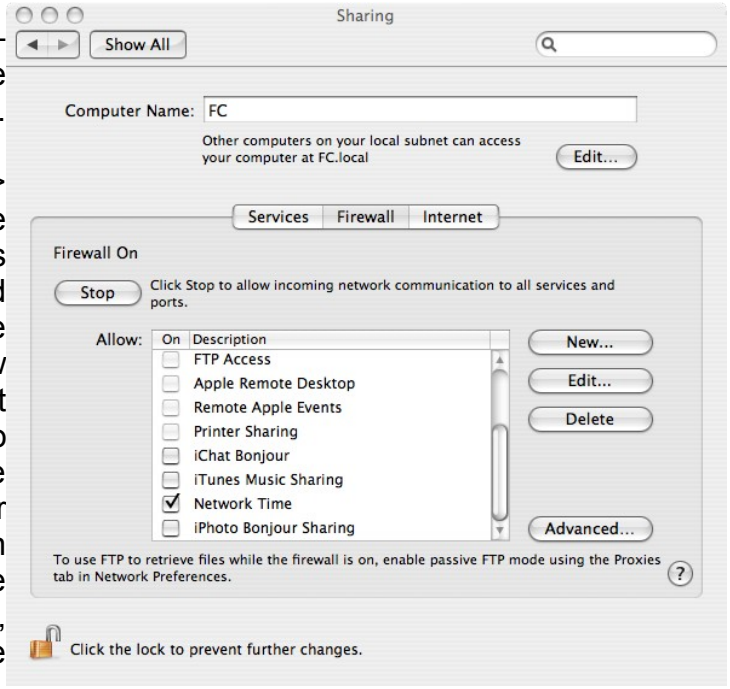
A sound working assumption:
A sound working assumption for any mobile access now and for the foreseeable future is that the wireless or other infrastructure provides no security benefits whatsoever. With this assumption, you will not be disappointed and without it you will be. Therefore, the working assumption should be that all of the security comes from the computer you use to access the network and the pairing of that computer with other computers you work with through that connection. Hence the protection comes exclusively from cryptography and sound security practices on the end points.

The best bang for the buck today:
The best bang for the buck in the market today is the use of OSX (the operating environment of an Apple MacBook) for the traveling end point. This provides (1) all of the functionality normally desired for most users, (2) ease of use even in relatively secure configurations, and (3) lots of good support at a reasonable annual cost. The total cost of a pretty high performance system with 100Gig of disk and more than a Gig of RAM plus and hardware and software support for 3 years is between $1200 and $2500 dollars depending on how big a display you want, and so forth. This includes most of the most important security features you will ever need and, with a few simple and free downloads and installs, you can upgrade it for almost any normal security need. You may also want to purchase a USB drive (2 Gig for $30 or so for a very small one that fits in your pants or vest pocket, change purse, or key ring).

And some extra advice on things we commonly use and do
At the end of the document I have added some of the details of how we configure most of our internal systems (not the high security ones) to allow maximum functionality with minimum risk and cost. We use this document internally as a started for all of our consultants and workers. And of course we are always anxious to get feedback on any risks we aren't aware of – so don't hesitate to let us know.

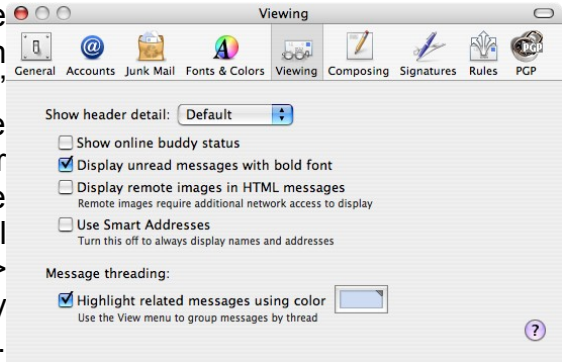
Configuration:

While Apple does reasonably well in out-of-the-box secure configuration, a few things should be done to augment normal security in mobile use. Specifically, you should:

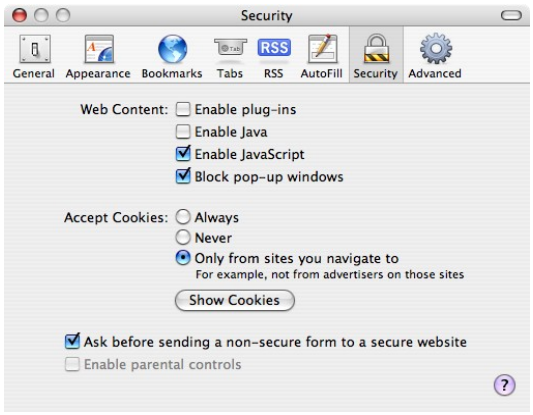


- Turn on the firewall (System Preferences -> Sharing -> Firewall -> On) The picture below shows a configuration that is normally used. Only network time is turned on to allow the time to be kept accurate over the network. See Illustration 1 below for what it should look like. There is almost never a reason to turn the firewall off, so once it is set you should leave it set all the time. Note the “Firewall On” in the upper left hand corner of the firewall configuration area and the check mark only next to the network time service. In almost all cases, nothing else needs to be or should be turned on. If you are an expert, you might, of course, enable other items.

- Turn off things you don't need and that are potentially unsafe. This includes the two most common configuration settings that are most likely to be the brunt of attacks. They are (1) the Web browser (Safari in the example) and (2) the mail client (Mail from Apple). If you use other browsers or mail clients, you are on your own for securing them.
  - For the Mail client, you will want to turn off the default loading of graphics from the Internet on received email. This eliminates most Web “bugs” used by spam sources to track that you got the spam and authenticate your address for further spam, and disables many of the exploits that use graphic display formats to try to gain remote control of your computer. This is done using “Mail -> Preferences -> Viewing” and setting “Display remote images in HTML messages” to unchecked. Whenever a message appears, if there are remote images it will indicate this in the upper right hand corner of the message window. If you think the email is important to you and you want to see the remote images, you can always click on the button provided to see them for this email. This will not prevent you from seeing pictures sent to you in emails, only those that are stored on the Internet and only referenced in emails. Mostly, it eliminates advertisements and other similar things.

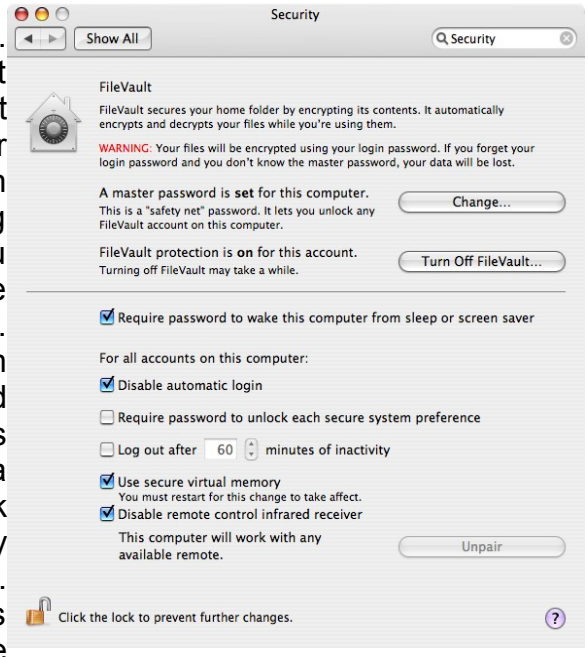


  - For the Web browser, the most dangerous potential problems come from running programs that are embedded in Web pages. Many Web sites now require that you run Java in order to get use of features, but this is potentially dangerous. So I disable Java in normal use and only turn it on when there is a Web site that I think is important enough to enable Java to use. Then I have to disable it after the use. Apple is not the best at facilitating this, but other providers aren't really much better. This is controlled from the Web browser by



selecting “Safari -> Preferences -> Security” and blocking pop-up windows, limiting cookies, asking before accessing insecure sites, and not enabling plug-ins or Java. This is shown in the illustration below. For many users, this is too restrictive, so an alternative approach is provided below that allows maximum flexibility in use by separation of information into different accounts. Finally, make sure that you tell Safari not to automatically 'Open “safe” files after downloading' in “Safari -> Preferences -> General”. Even though they are called “safe” they are not in fact safe.

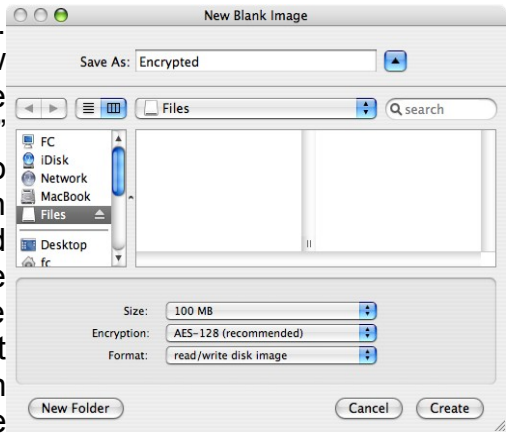
To be even safer:

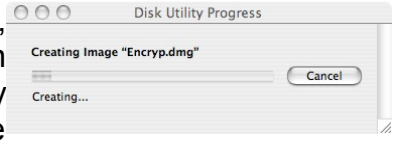


If you want to be safer, turn on home directory encryption. This encrypts all of the content in your user directory so that if someone takes your computer or breaks into a different account on your computer, they will not gain access to your files and their content unless they can break the encryption system. Note that if your computer is set to automatically log you in after reboot or to not ask for a password after you close and re-open the display, then this won't stop someone who takes your computer from accessing your information. These features are controlled by the Apple “System Preferences -> Security”. The encryption capability is called “File Vault” and when you turn it on. the computer takes some time to encrypt all of your content. Requiring a password in both reboot and screen saver eliminates risk from theft of the computer. Using secure virtual memory eliminates a path for attack that sophisticated attackers use. Disabling remote infrared communications eliminates attacks from local devices and should be checked unless you are using the infrared interface. This is completely transparent and automatic and has almost no effect on system performance. It has always been reliable for me, however, you should always have a backup of important content so that if there is a disk problem, you will be able to get it back.

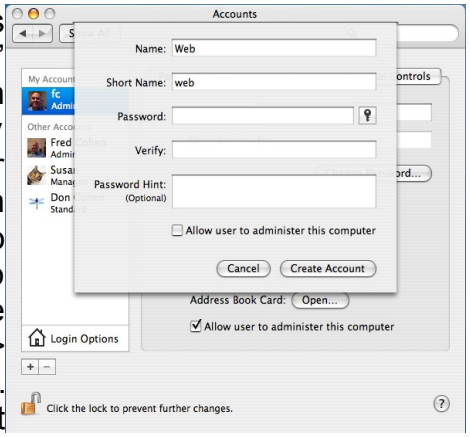
The same encryption capabilities can be used for removable devices. For extra security when I am traveling with higher valued content, I use an encrypted removable disk drive or USB drive. iOmega sells an enclosure for a 110Gig SATA drive that connects to the Firewire or USB port and is powered by the computer. It fits in my short pocket, but it is a bit large to be covert. So I more often use my pocket USB drive for quantities up to a few Gig. It stays in my pants pocket all the time and I pull it out and use it when I want to back up something I just did while on the road for a client. The contents are encrypted by using the file vault capability, so I have to type a password to access the drive when I put it into the USB port. Other than that, it works like any other USB drive. This is controlled by the Disk Utility application. To create an encrypted disk or portion of a disk, use the finder to “Go -> Utilities -> Disk Utility”. By double clicking on the program, the disk utility program will start up. From there, put the USB or other mountable drive into the computer. It will show up in the disk utility and you should select it. Next you have to create a new image to store the encrypted files on the drive. You can make the whole disk encrypted, but I usually prefer to keep the USB drive available for other

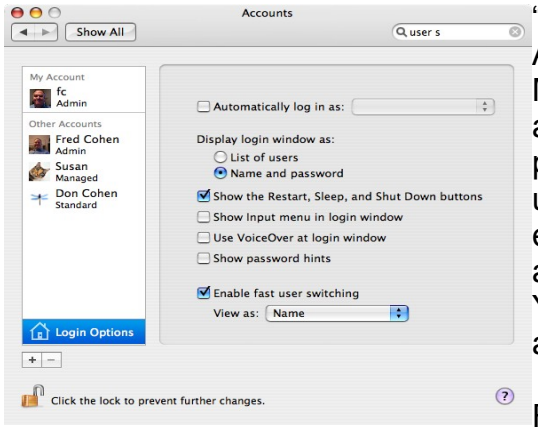
purposes and only use a portion of it for confidential information. Select “File -> New -> Blank Disk Image” to create a new encrypted file system on your USB drive. This is done from the control bar and not from the window itself. Under “Encryption” select AES-128 (as an example), select the amount of space to use for the encrypted file system, name the image, and click on “Create”. It takes some time to create an encrypted compressed file system, so be patient. It will then ask for a password for the encrypted file area. If you want the computer you are using to use its keychain to remember the password and automatically use it to mount the USB drive, you can do so, or if you want to type the password each time, you can do that. Select an appropriate password for the desired level of security, and tell it “OK” and it will start to create the file system. When it is done, the new file system will be mounted on your computer and accessible like any other disk device. You can drag and drop into and out of it, delete, use the trash, and treat it like any other disk. You can “Eject” it when you are done, mount it by clicking on it, and remove the USB drive or other disk when it is not in use. You can use it on other computers, but the encrypted file areas will only be available on Apple computers and only when you mount them. By using this capability, very sensitive data can be kept entirely off-line when you are connected to the network, or it can be used only when needed and removed at all other times. And remember, you only have to set it up once and it will work from then on. So the few minutes you spend once is really very simple compared to alternative solutions.





Another safety precaution that I use is to have separate accounts on my computer for different uses. The “fast user switching” capability of the Apple environment allows me to immediately log in as a different user and use the computer from that account at any time. With encryption enabled, users cannot read content of other user areas, even if they manage to break into the computer on those accounts. When I am mobile, I login as a different user to “cruise the Web”. To do this, all you have to do is add a new user to the computer and switch users for different uses. To add a user, use “System Preferences -> Accounts” and add a new user. Make certain that they are not authorized to administer the computer and, if you like, add parental controls. Once the user is created, you can switch users by clicking on the user name from the menu bar and entering the password of the other user. Use the Web from that account and switch back to your trusted account for other work. You can also move files between accounts if desired using drag and drop from the more trusted account.





Finally, use the auto-updates to update the computer whenever they come out from Apple. They help keep you secure. Safe computing on the road!

Some other things we do to maximize functionality and minimize risk and cost

For the Mac to view Windows videos, we use Flip4Mac. You can find it by going to Google.com and searching for “flip 4 mac” - download it from the Web, install, and off you go. You will have to enable browser plug-ins for this to work (see the security options from Safari above). This allows us to watch videos from all over the place, but it introduces a little risk because the viewers may have weaknesses that allow them to be remotely exploited in content you download, and enabling plug-ins increases the number of potentially risky formats you can end up automatically interpreting from your browser.

We use NeoOffice (Open Office with the native Mac GUI) to deal with documents and presentations of all sorts. For output we export to PDF format, which everybody seems to be happy with getting. NeoOffice is available on the Web for free as well. Got to: http://www.neooffice.org/ and download the newest version. It periodically updates (asks you to do so) and has some reliability problems with large documents kept open for long times, so make sure to save documents often (as you should in any system). You can also donate money for support.

We also use java – from Sun. To download, go to http://java.sun.com/ and download the latest java virtual machine so you can run java programs on your local computer. We only load programs from trusted sources (like http://all.net) and don't run them automatically from browsers.

Sometimes you need to use Windows. While I have managed to do without it for many years, you can use it via remote desktop connection from your Mac if you really need to use an application. If you go to Microsoft and lookup “Remote Desktop Connection for OSX” or some such thing you can find a free download. Of course you do this at your own risk. A less secure alternative is to use a virtual Windows machine within your Mac computer. Several of these are available, but don't believe the folks who tell you this is safe. It is risky and, as I said earlier, I have never encountered a situation where I actually need to use Windows, so why introduce all of that additional risk for no real value?

Finally, I have to say, that while I enjoy the capabilities and ease of use of the Apple OS-X (Unix) operating environment, it also carries significant risks that cannot be ignored. Security is a trade-off. Today, in my view, Apple does the best job of high functionality, capability, compatibility, performance, and ease-of-use for reasonably low cost. But while I am half smiling about the benefits, the dark side is still there, looming just below the surface. Apple is far from secure, and the claims I hear from Apple store employees about the safety from viruses and security afforded by OS-X are, while not exaggerated when compared the the poor safety record of Windows, a bit too optimistic for my taste. Linux is, in most cases slightly safer if properly administered, but support is not as good as it is for Mac, and Apple's security updates come with reboots often up to once a week. While most Windows users think that daily reboots are to be expected, my Linux bootable CDs and other Linux environments I run typically need be rebooted... when the power supply within the computer breaks every few years.