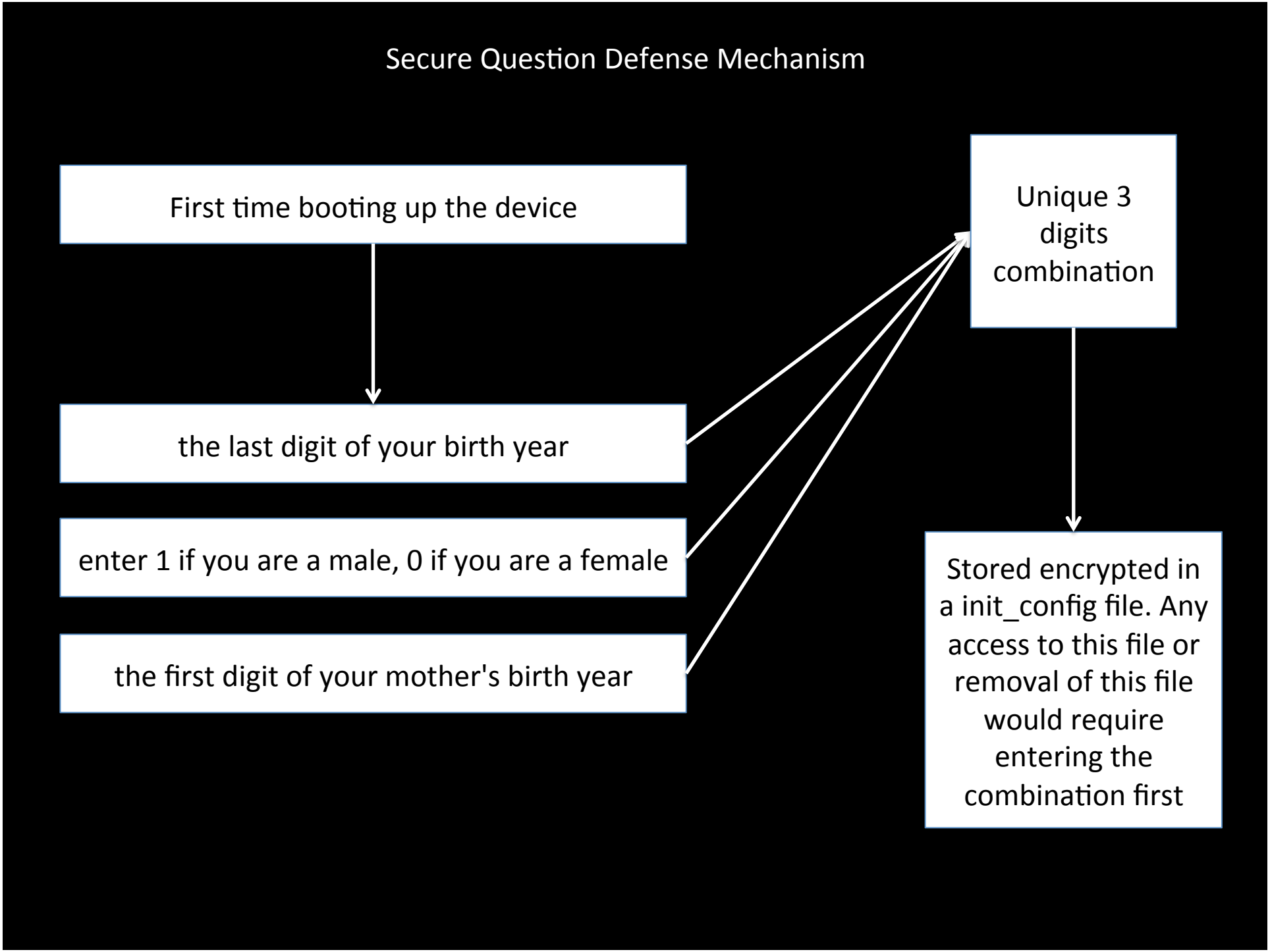
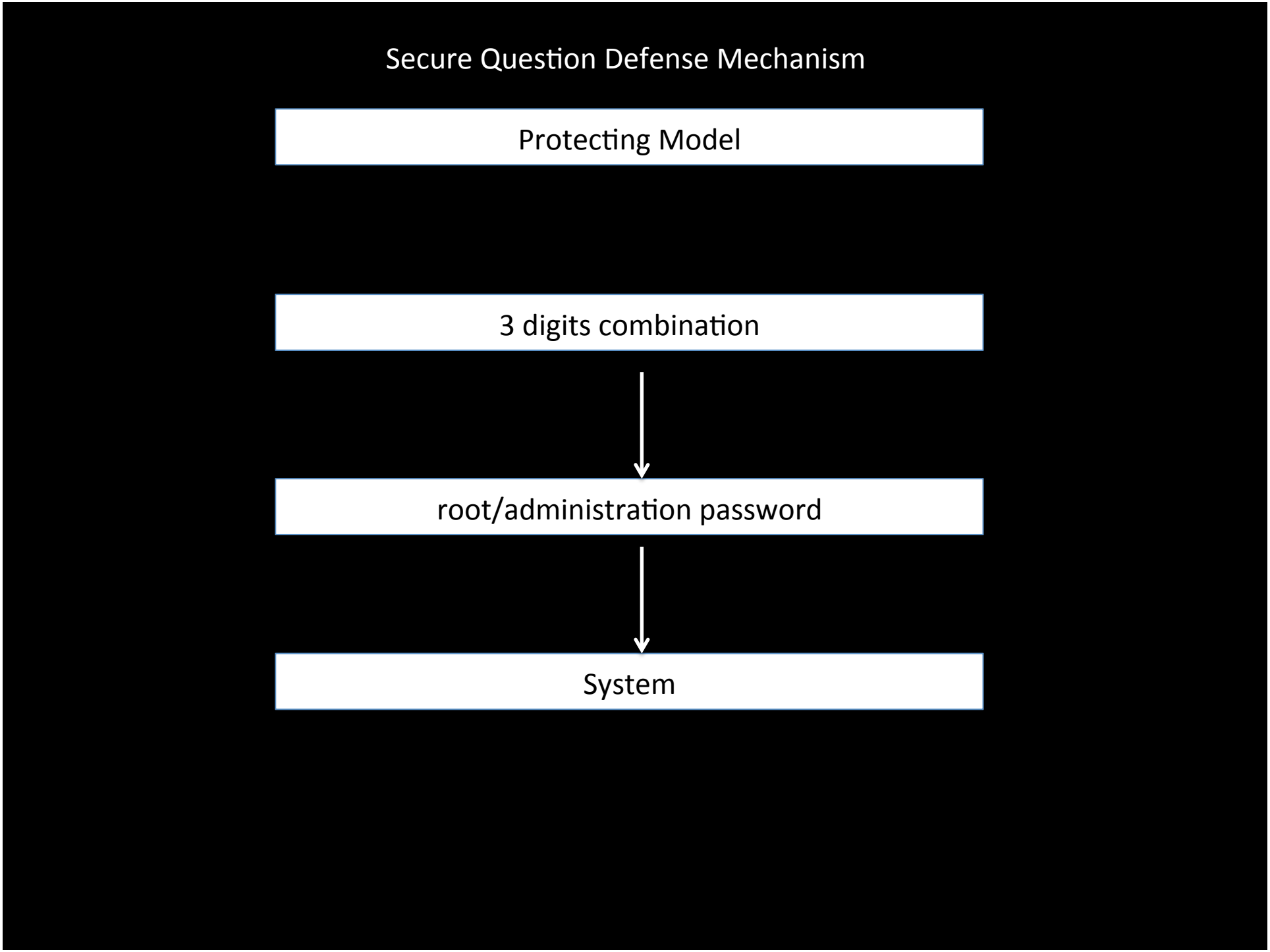
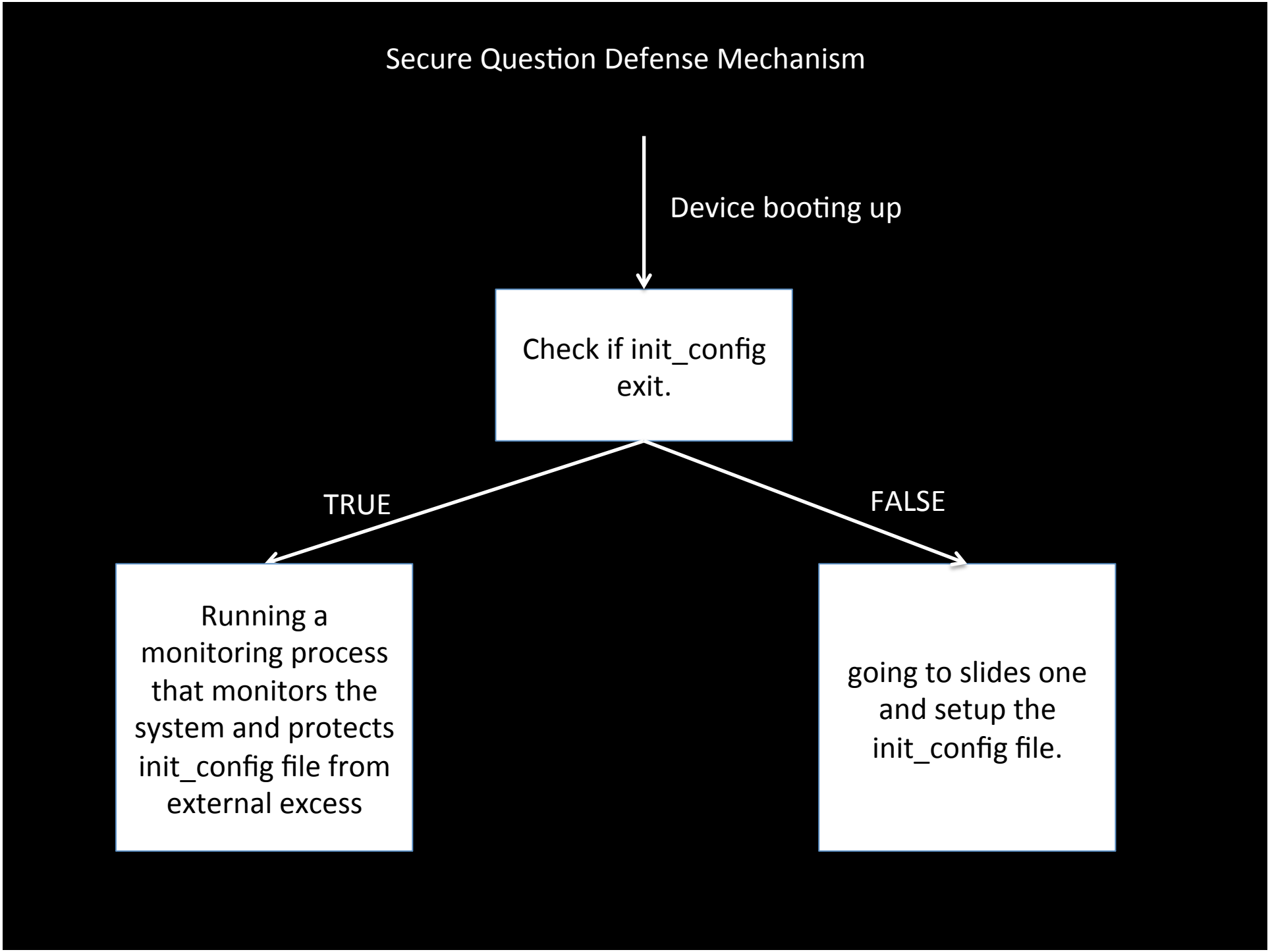
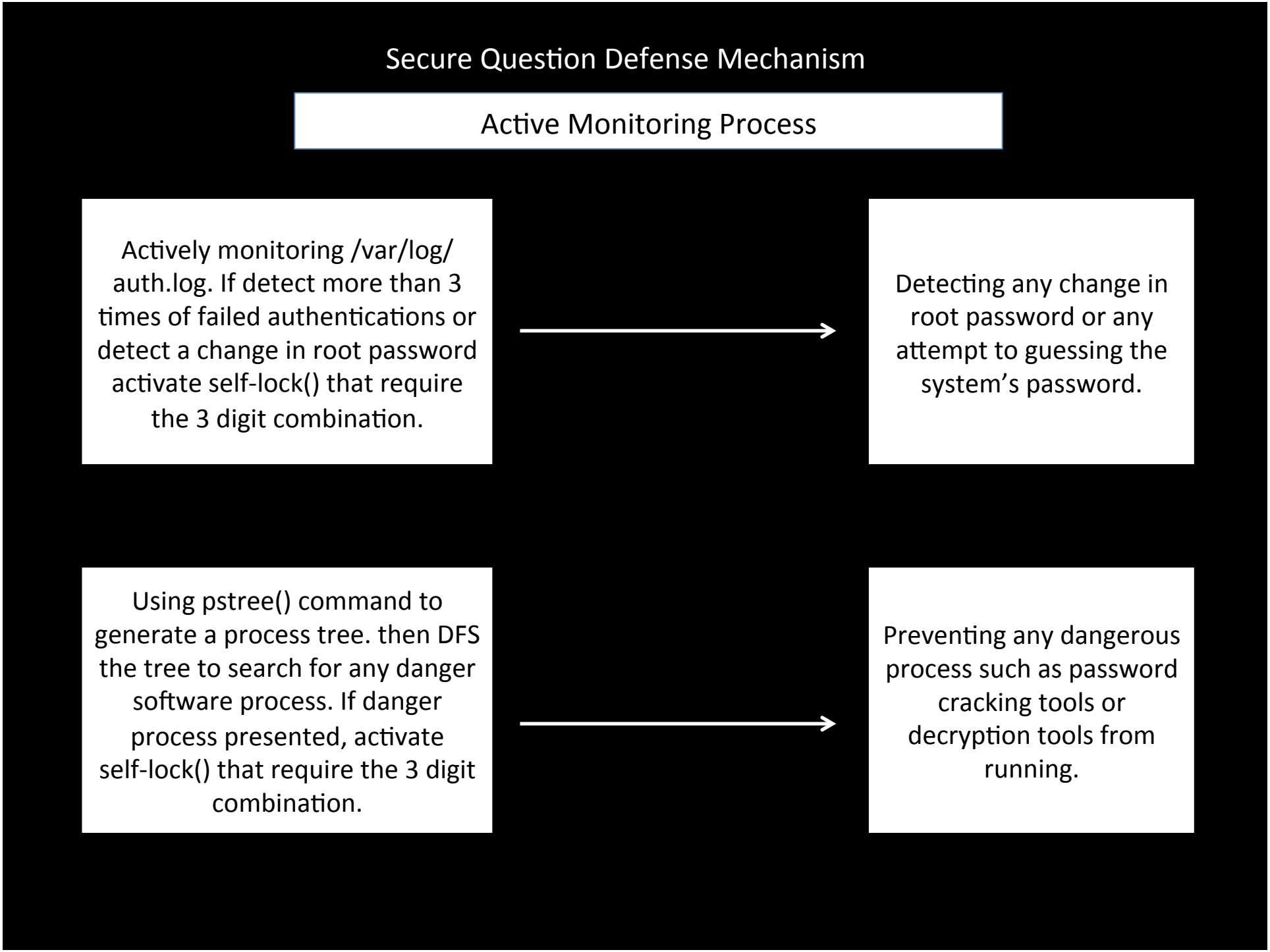
Supporting Material for COMP116 Final Project

- Haoyang Mao


Secure Question Defense Mechanism
First time booting up the device
the last digit of your birth year
enter 1 if you are a male, 0 if you are a female
the first digit of your mother's birth year
Unique 3 digits combination
Stored encrypted in a init_config file. Any access to this file or removal of this file would require entering the combination first


Secure Question Defense Mechanism
Protecting Model
3 digits combination
root/administration password
System

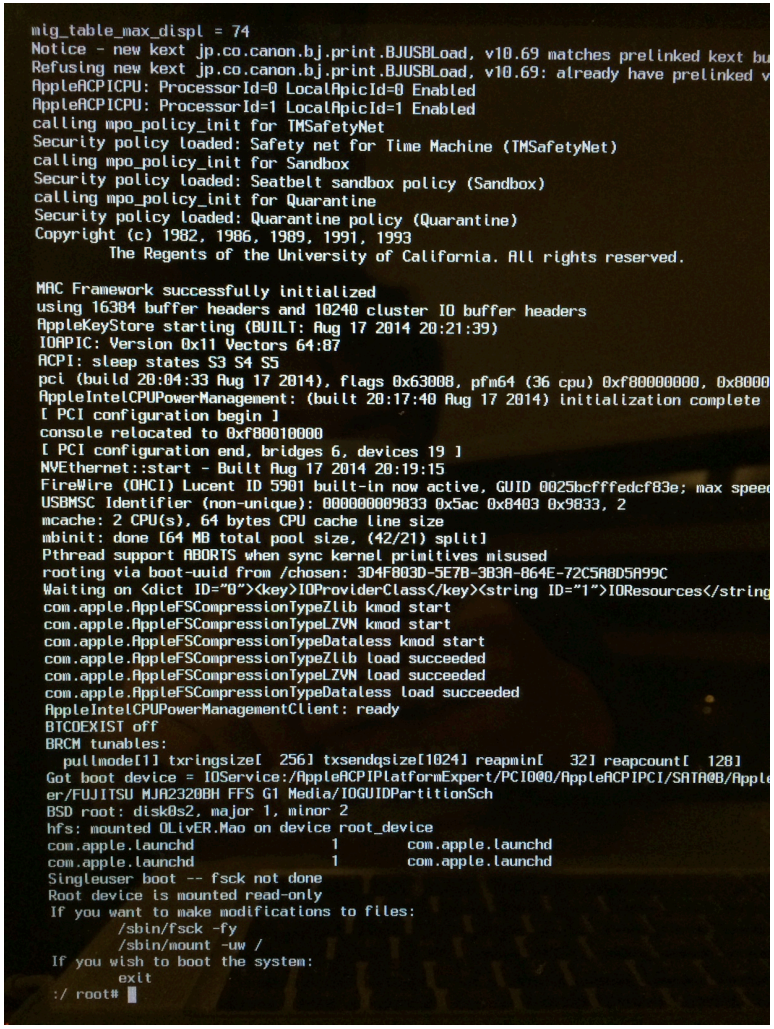

Secure Question Defense Mechanism
Device booting up
Check if init_config exit.
TRUE
FALSE
Running a monitoring process that monitors the system and protects init_config file from external excess
going to slides one and setup the init_config file.


Secure Question Defense Mechanism
Active Monitoring Process
Actively monitoring /var/log/ auth.log. If detect more than 3 times of failed authentications or detect a change in root password activate self-lock() that require the 3 digit combination.
Detecting any change in root password or any attempt to guessing the system's password.
Using pstree() command to generate a process tree. then DFS the tree to search for any danger software process. If danger process presented, activate self-lock() that require the 3 digit combination.
Preventing any dangerous process such as password cracking tools or decryption tools from running.

Bypass a Macbook Pro's Authentication

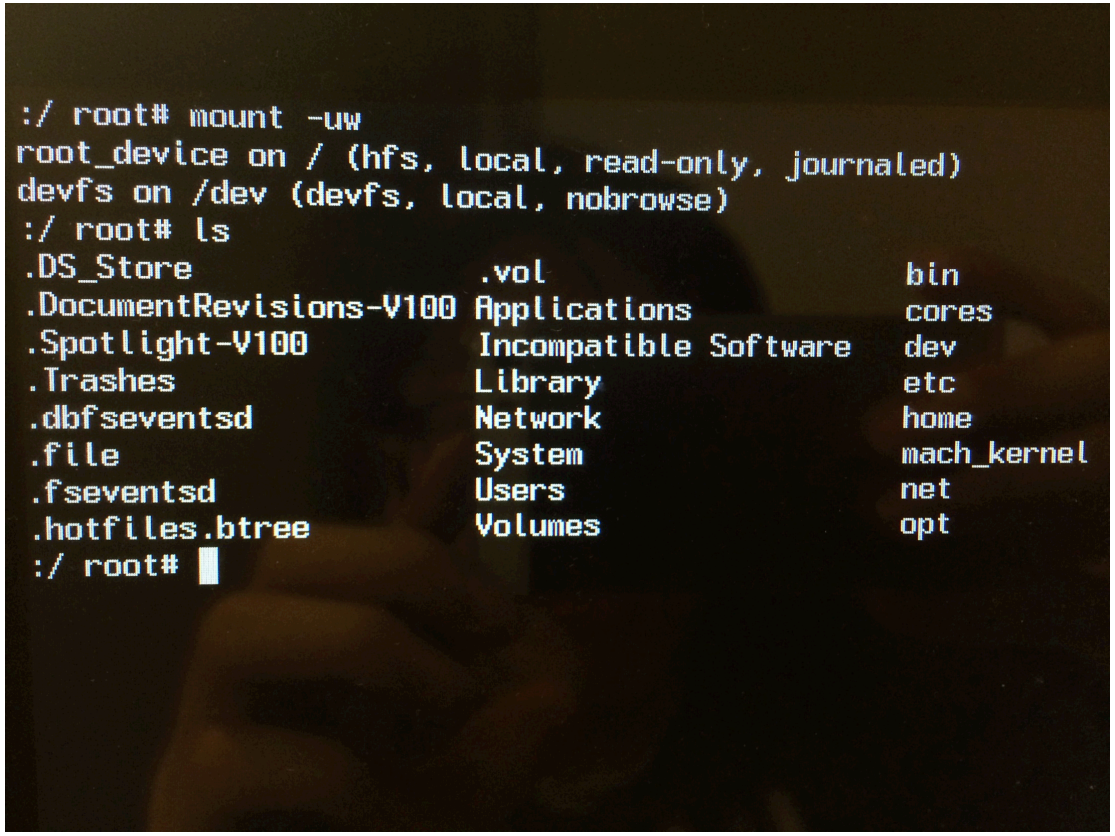
When booting up a password protected Mac, holding the command key along with the x key would interrupt the normal boot up and automatically enter the single user mode .

Bypass a Macbook Pro's Authentication



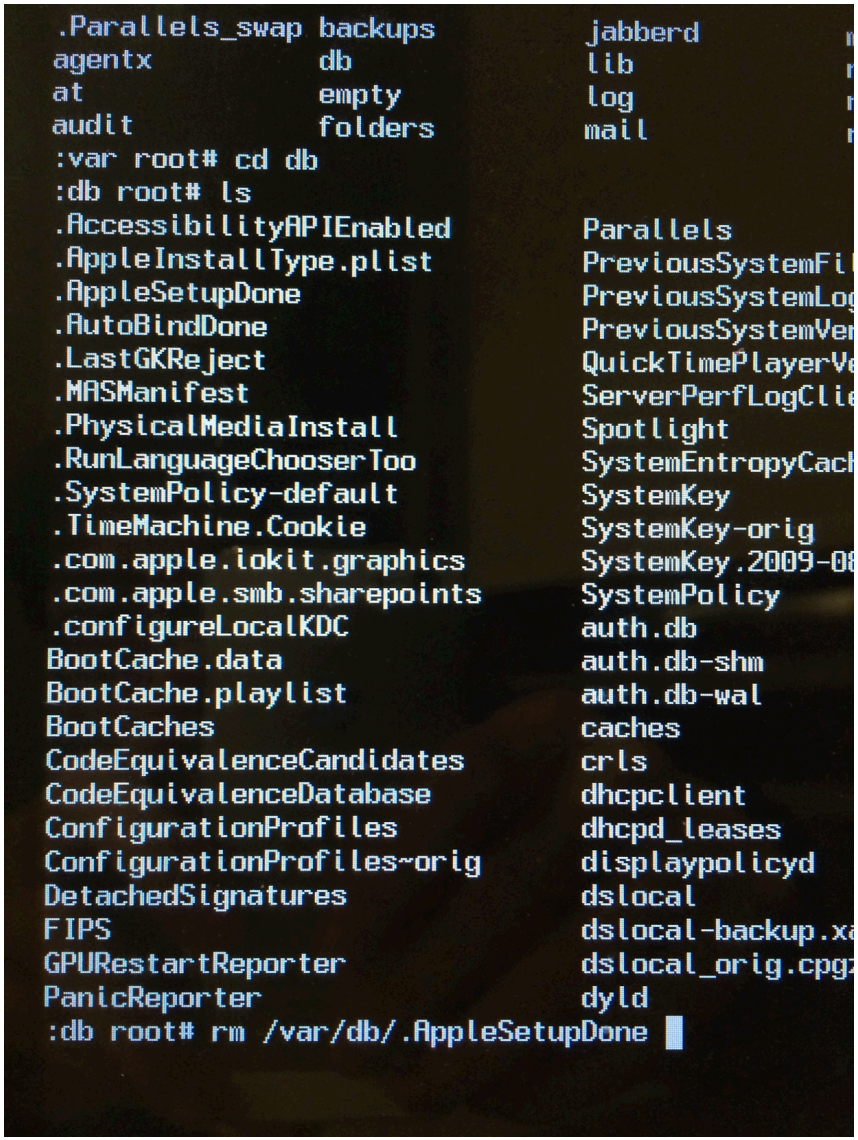
After entering the single user mode, a command line interface would appear. Notice before the cursor, the system automatically believes that I am the root and grants me root privileges.

Bypass a Macbook Pro's Authentication



With the root access, I can browse all the directories and check any file I want

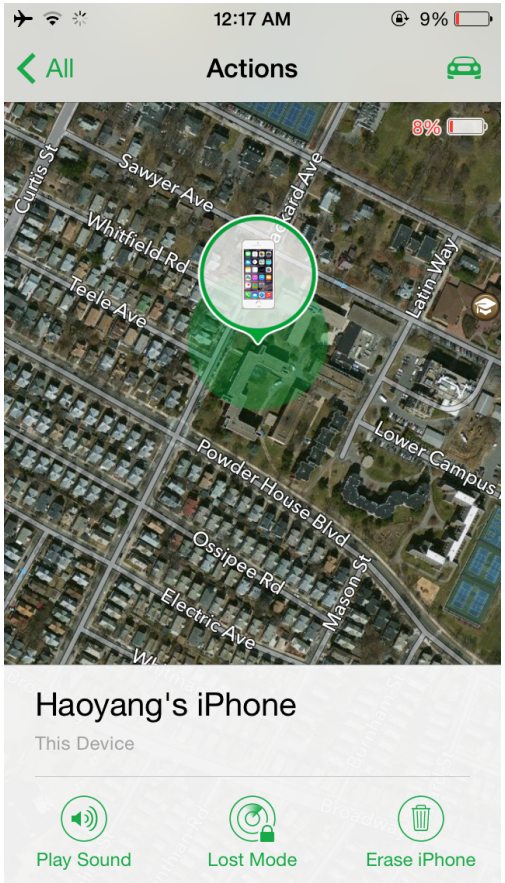
Bypass a Macbook Pro's Authentication



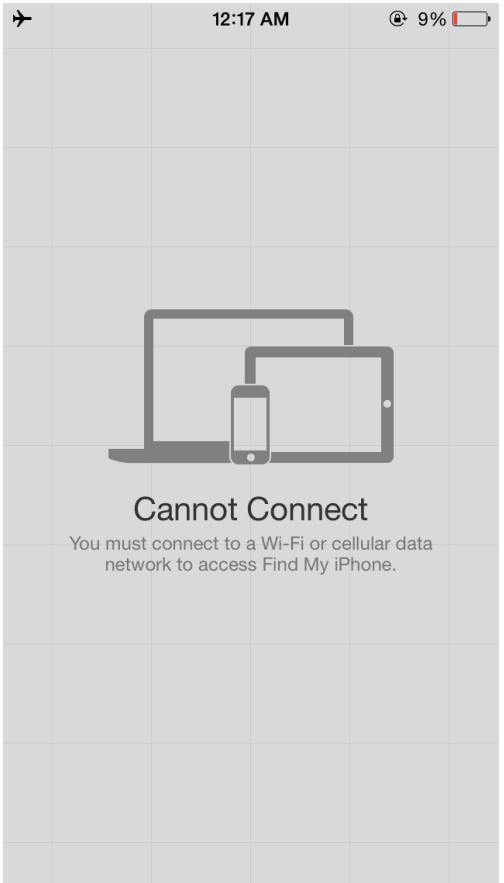
I can also create another root account by removing the .AppleSetupDone file. This removal would make the system believes that the device has never been boot up before. It would then automatically create another root account for me.

Disabling Find My iPhone

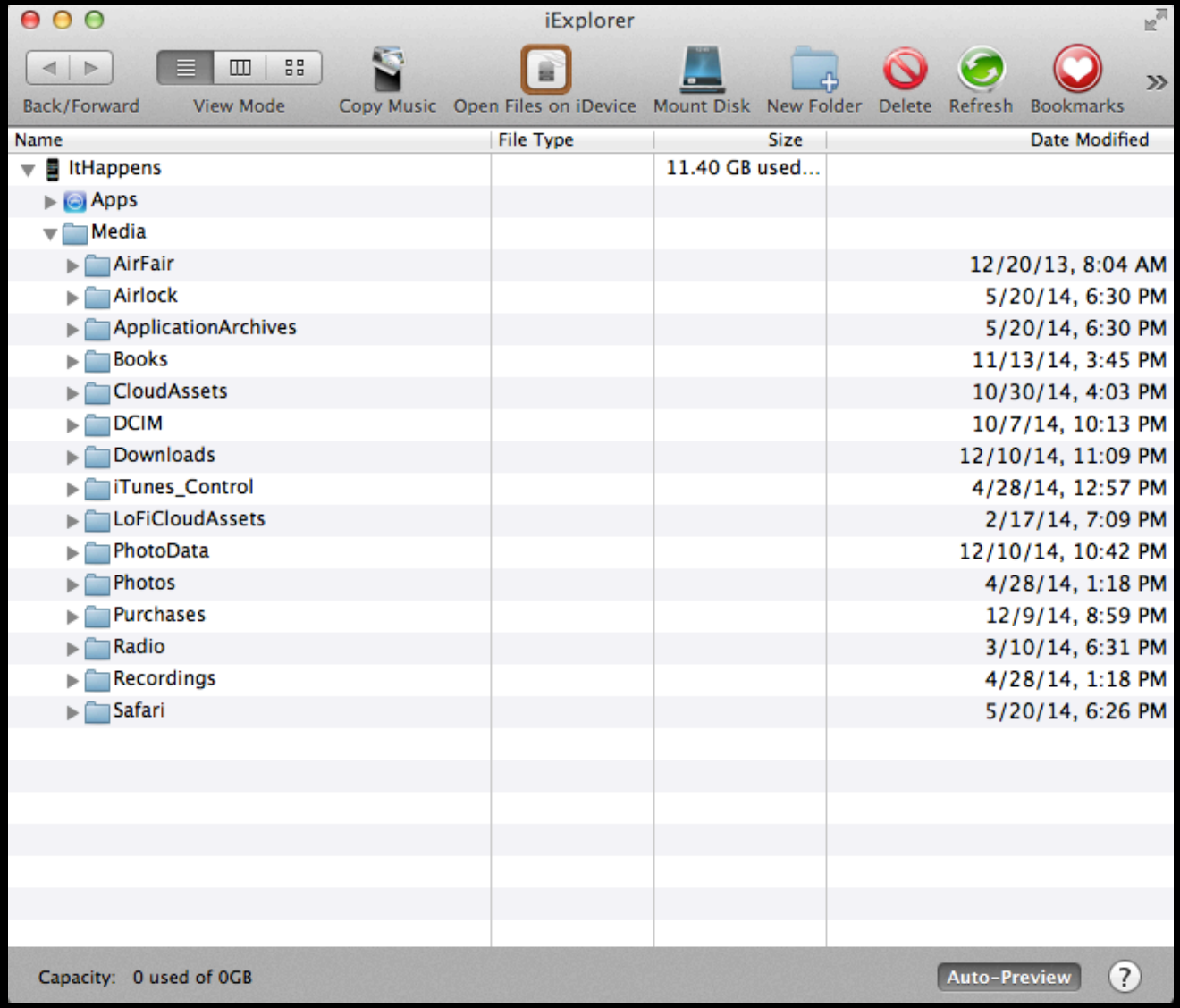
Wi-Fi Connected



Wi-Fi Disconnected

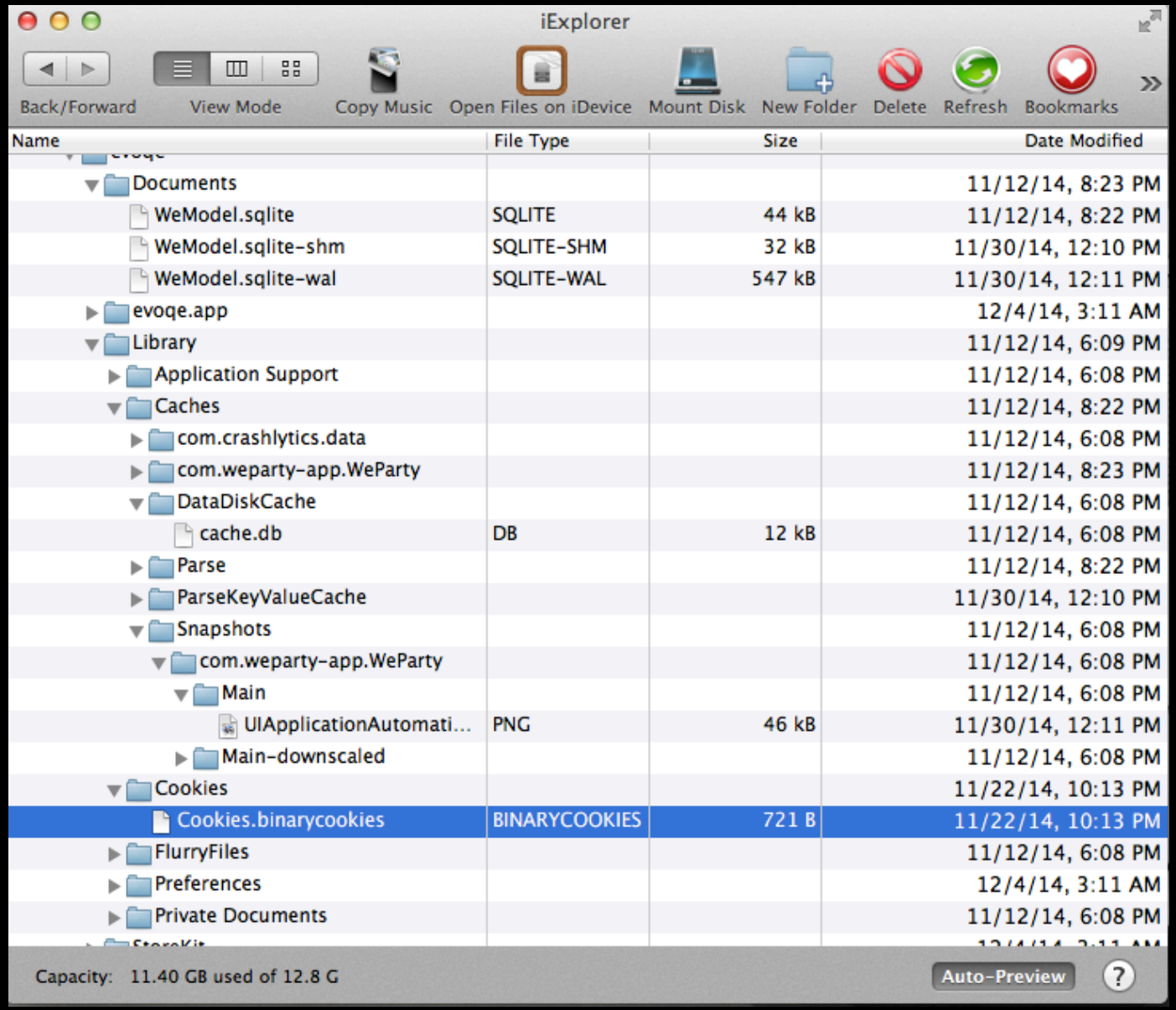


iExplorer Visiting a Password Protected iPhone



After an iOS device being physically plugged in, I can view any directory and check any cookies or photos I want without even deal with the password.

iExplorer Visiting a Password Protected iPhone



I can also view all the files stored by the application. I find some cookies that was stored locally in a binary form as well as some .sqlite that contains interesting information about the user.