Credentials from Password Stores: Securityd Memory, Sub-technique T1555.002 - Enterprise

An adversary with root access may gather credentials by reading `securityd`'s memory. `securityd` is a service/daemon responsible for implementing security protocols such as encryption and authorization.[1] A privileged adversary may be able to scan through `securityd`'s memory to find the correct sequence of keys to decrypt the user's logon keychain. This may provide the adversary with various plaintext passwords, such as those for users, WiFi, mail, browsers, certificates, secure notes, etc.[2][3]

In OS X prior to El Capitan, users with root access can read plaintext keychain passwords of logged-in users because Apple's keychain implementation allows these credentials to be cached so that users are not repeatedly prompted for passwords.[2][4] Apple's `securityd` utility takes the user's logon password, encrypts it with PBKDF2, and stores this master key in memory. Apple also uses a set of keys and algorithms to encrypt the user's password, but once the master key is found, an adversary need only iterate over the other values to unlock the final password.[2]
