Obligatory exercise 01
Has OS X a Trusted Path implementation

Jan Kerkenhoff
141628
IMT3501, Software Security

September 3, 2014

A Trusted Path is a way for the operating system to authenticate itself to the User. The most common known implementation of trusted path is found in Windows, where the shortcut of STRG+ALT+DELETE opens a Trusted Path via the login prompt.

Mac OS X doesn't implement a traditional trusted path, which means there is no way to get a trusted shell on Mac OS X. But it uses some other tools to create a more secure environment for programs running, which will be described in the following.

1 Sandboxing in Mac OS X

Since version Mac OS X 10.7 (Lion)[2] the system uses sandboxing for all apps installed via the app store, although it was available before, but only for internal usage.[4] All apps that use sandboxing are only executed in a closed environment and only have access to a virtual copy of the users home directory and any other files must be explicitly shared with the Application through a dialogue in which the user navigates to the file he wants to open. Every resource the application wants to access outside of the sandbox is specified in Entitlement Keys which need to be set during development to give the application access to them. [1]

2 Gatekeeper

Another security measure in place to prevent the installation/running or malicious code is called Gatekeeper which was added in Mac OS X 10.8 (Mountain Lion).[3] Gatekeeper offers 3 different options to protect against malicious code. It can either let you only install applications from the App store or only applications from the App store and all applications whose code is signed with a certificate of a developer registered with Apple. The Third option basically just lets you install any application from any source on the OS.[5]

3 Execute Disable

New in Mac OS X 10.9 is a feature called Execute Disable which separates memory used for data in RAM from memory used by executables and their instructions. Its implemented at kernel level and protects against malicious software that tries to trick a cpu in reading executable instruction in data blocks. To achieve this it uses Address Space Layout Randomization (ASLR) to separate the data in memory to different locations to make it harder for attackers to guess locations.[4]

4 File Quarantine

Mac OS X also has an feature which is close to a trusted path implementation, it's used by all the standard applications like mail,messages, iCloud and every browser on the system. When you download a file from the internet it's put into Quarantine. If Gatekeeper finds a valid certificate with which the file was signed it can be opnend without warnings, otherwise you get an warning popup that this file can cause harm to your system. Prior to opening Also files are checked by X Protect Mac OS X own malware and virus scanner.[6]

5 TPM in Mac OS X

Some machines from apple used to have a TPM module but no official supplied driver.[8] Models which came after the switch to Intel processors in 2006 until 2009 were equipped with a TPM module.[7]

References

[1] Apple, *Entitlement key reference*, Website, 2013, Available from: `https://developer.apple.com/library/mac/documentation/Miscellaneous/Reference/EntitlementKeyReference/Chapters/EnablingAppSandbox.html`; [1 September 2014].

[2] ———, *Whats new in os x*, Website, 2013, Available from: `https://developer.apple.com/library/mac/releasenotes/macosx/whatsnewinosx/Articles/MacOSX10_7.html`; [1 September 2014].

[3] ———, *Whats new in os x 10.8*, Website, 2013, Available from: `https://developer.apple.com/library/mac/releasenotes/macosx/whatsnewinosx/Articles/MacOSX10_8.html`; [1 September 2014].

[4] ———, Website, 2014, Available from: `https://www.apple.com/osx/what-is/security.html`; [1 September 2014].

[5] ———, *Os x: About gatekeeper*, Website, 2014, Available from: `http://support.apple.com/kb/HT5290`; [1 September 2014].

[6] ———, *Os x: About the "are you sure you want to open it?" alert (file quarantine / known malware detection)*, Website, 2014, Available from: `http://support.apple.com/kb/HT3662`; [1 September 2014].

[7] Mel Beckman, *Your laptop data is not safe. so fix it.*, Website, 2009, Available from: `http://www.osxbook.com/book/bonus/chapter10/tpm/`; [1 September 2014].

[8] Amit Singh, *Trusted computing for mac os x*, Website, 2006, Available from: `http://www.osxbook.com/book/bonus/chapter10/tpm/`; [1 September 2014].