Extended Attributes and TCC on macOS

Justin Bui

Introduction

This blogpost will describe how Transparency, Consent, and Control (TCC) affects extended attributes on macOS.

TCC is a control that limits an application's ability to interact with various services on the operating system. It controls access to services such as camera, microphone, contacts, photos, folders on disc, location services, and more. If you want to know more about TCC, I highly recommend you read this blogpost by Keith Johnson. This blogpost will assume the reader has a basic understanding of TCC.

While doing Hermes development, I ran into an issue where my `ls` implementation caused a TCC popup when attempting to list out the user's home directory (`/Users/slyd0g`). This blogpost details the issue in my original implementation, journey investigating the root cause, and how I fixed the issue within Hermes.

Hermes Generating TCC Popups

In Hermes' original `ls` implementation, I pull as much data as possible from files/folders. This data includes:

- Name
- Size
- Posix permissions
- Owner
- Group

- Hidden
- Create time
- Modify time
- Extended attributes

Whenever `ls ~/` was issued in Hermes, a TCC popup was generated to access the user's TCC-protected folders: `~/Downloads`, `~/Documents`, and `~/Desktop`.

Hermes Generating a TCC Popup

This was especially concerning because in previous testing this did not occur and this could potentially ruin a red team operation if a user reports the suspicious activity. My `ls` implementation was almost identical to Cody Thomas' within his Apfell agent so I also tried it `ls ~/` from Apfell. This also caused a TCC popup.

What data are we pulling that causes this? The `ls` call does not access anything within the TCC-protected folder which would definitely cause a popup.

Root Cause Analysis

I re-wrote my `ls` implementation in a basic Swift program to see if I could pin down what exactly was generating this popup.

LsTest Generating a TCC Popup

The culprit?

```
let attributes = try fileManager.attributesOfItem(atPath: full
```

This returns a `FileAttributeKey` struct which holds various information about a file/folder. Why would accessing this data cause a TCC popup for the TCC-protected folders?

FileAttributeKey Structure

Comparing Attributes

I decided to print the `FileAttributeKey` struct for a single TCC-protected folder under two scenarios:

- TCC-prompt denied

Denying LsTest Access to TCC-Protected Folders

```
/Users/slyd0g/Downloads[__C.NSFileAttributeKey(_rawValue: NSFi
```

- TCC-prompt accepted

Allowing LsTest Access to TCC-Protected Folders

```
/Users/slyd0g/Downloads[__C.NSFileAttributeKey(_rawValue: NSFi
```

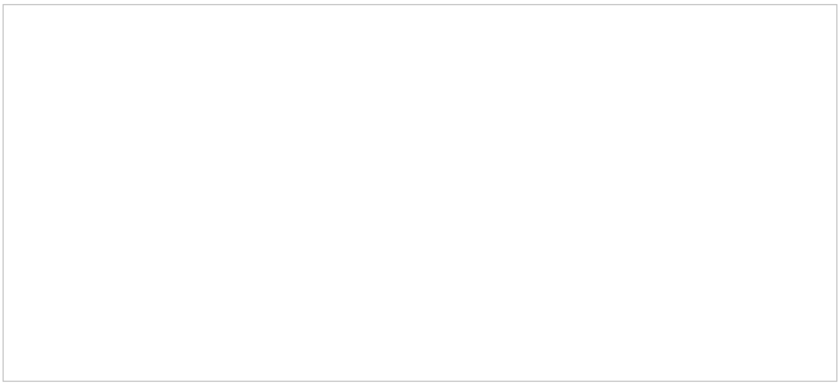
Ah ha! The difference in data generated when TCC permissions were granted was `NSFileExtendedAttributes`. This is weird though, I know that I've printed extended attributes before with `xattr` without generating any TCC prompts.

Investigating Extended Attributes with xattr

Before investigating anything related to TCC, it's always a good idea to reset your TCC database.

```
sudo tccutil reset All
```

After resetting the TCC database, I looked at the extended attributes for all of the TCC-protected folders.



Extended Attributes for Downloads, Documents, and Desktop

This did not cause any TCC popups. Does `xattr` have some sort of entitlement that might allow it to access this information without generating a TCC popup?

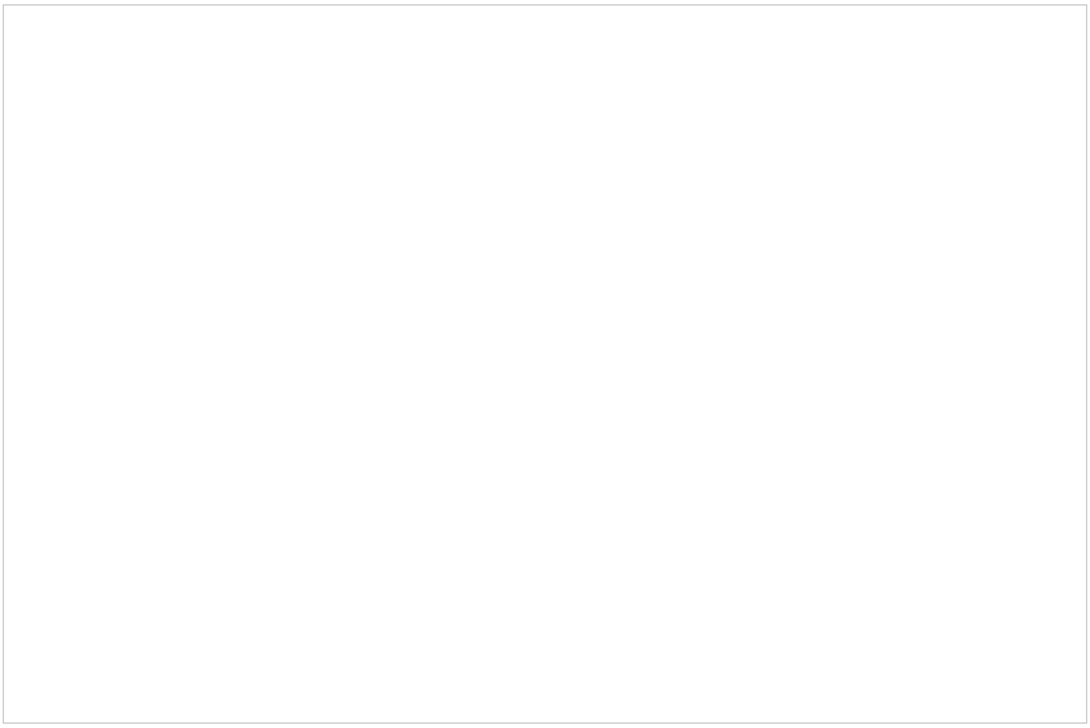
Enumerating Entitlements of xattr

`xattr` isn’t signed and doesn’t have any special entitlements. On macOS Big Sur, `xattr` is simple a wrapper for the Python `xattr` package.

While enumerating the `FileAttributeKey` struct, there appeared to be some binary blob associated with the extended attribute.

```
__C.NSFileAttributeKey(_rawValue: NSFileExtendedAttributes): {
```

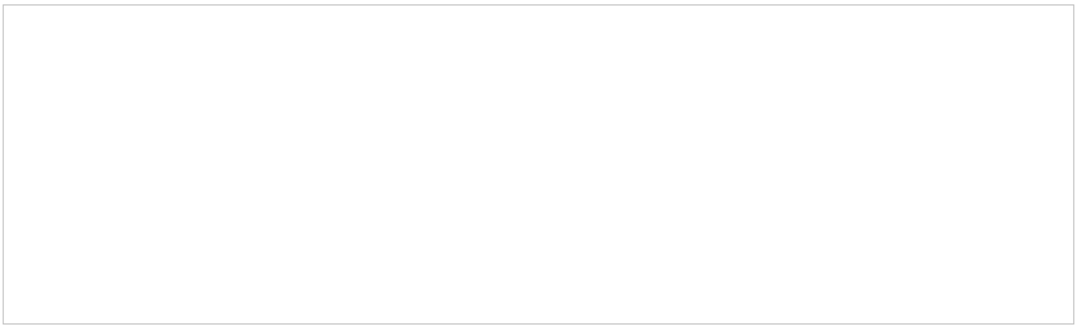
Let’s try to enumerate this binary blob with `xattr`



Enumerating Extended Attribute Values with xattr

Interesting! It appears that the extended attribute is a key-value pair where the **key** is not protected by TCC, but the **value** is protected by TCC.

After accepting the TCC popup, we see the binary blob that matches our Swift program.



xattr Enumerating Extended Attribute Binary Value

Fixing Hermes Is Implementation

In Hermes, I have two situational awareness commands to help enumerate your current TCC permissions:

- fda_check

- tcc_folder_check

The former attempts to grab a file handle to `~/Library/Application Support/com.apple.TCC/TCC.db`, if a file handle is obtained, our current process has `Full Disk Access` permissions. The latter uses `MDQuery*` APIs to determine if you have access to TCC-protected folders. Both techniques were inspired by @cedowens here.

If `fda_check` or `tcc_folder_check` is successful, I set various global variables that allow future `ls` calls to enumerate the attributes for TCC-protected folders.

Tracking TCC Permissions with Global Variables

Checking Enumerated TCC Permissions within `ls` command

I went with this approach to minimize the amount of API calls within the `ls` command and to hopefully minimize behavior that could be signatured. This way the TCC enumeration does not have to happen for every single `ls` command and only needs to be done once per agent.

Conclusion

In this post, I walked through the initial bug, root cause, things learned along the way, and how I handle the bug in Hermes. To recap, attempting to get folder attributes for TCC-protected folders using Swift/ObjC APIs will result in a TCC popup.

The TCC popup occurs because the extended attribute **value** is protected by TCC, while the extended attribute **key** is not.

Enumerating Extended Attribute Value Causes TCC Popup

Thanks for taking the time to read this post, I hope you learned a little about macOS, TCC, and extended attributes!

References

GitHub - MythicAgents/hermes: Swift 5 macOS agent

Hermes is a macOS agent written in Swift 5 designed for red team operations. Hermes currently supports Mythic 2.3...

A deep dive into macOS TCC.db | Rainforest QA

A deep dive into what the TCC database contains and the meaning of the various fields present in it. TCC (Transparency...

GitHub - cedowens/Spotlight-Enum-Kit: JXA and swift code that can perform some macOS situational...

NOTE: THIS REPO DOES NOT CONTAIN ANY TCC BYPASSES. INSTEAD THIS REPO CONTAINS EXAMPLE SCRIPTS OF SEARCHING THE...