# TTP Detail – T1548.006

## TTP Information

Name: TCC Manipulation

Description: Adversaries can manipulate or abuse the Transparency, Consent, & Control (TCC) service or database to grant malicious executables elevated permissions. TCC is a Privacy & Security macOS control mechanism used to determine if the running process has permission to access the data or services protected by TCC, such as screen sharing, camera, microphone, or Full Disk Access (FDA).

When an application requests to access data or a service protected by TCC, the TCC daemon (`tccd`) checks the TCC database, located at `/Library/Application Support/com.apple.TCC/TCC.db` (and `~/` equivalent), and an overwrites file (if connected to an MDM) for existing permissions. If permissions do not exist, then the user is prompted to grant permission. Once permissions are granted, the database stores the application's permissions and will not prompt the user again unless reset. For example, when a web browser requests permissions to the user's webcam, once granted the web browser may not explicitly prompt the user again.(Citation: welivesecurity TCC)

Adversaries may access restricted data or services protected by TCC through abusing applications previously granted permissions through [Process Injection](https://attack.mitre.org/techniques/T1055) or executing a malicious binary using another application. For example, adversaries can use Finder, a macOS native app with FDA permissions, to execute a malicious [AppleScript](https://attack.mitre.org/techniques/T1059/002). When executing under the Finder App, the malicious [AppleScript](https://attack.mitre.org/techniques/T1059/002) inherits access to all files on the system without requiring a user prompt. When System Integrity Protection (SIP) is disabled, TCC protections are also disabled. For a system without SIP enabled, adversaries can manipulate the TCC database to add permissions to their malicious executable through loading an adversary controlled TCC database using environment variables and [Launchctl](https://attack.mitre.org/techniques/T1569/001).(Citation: TCC macOS bypass)(Citation: TCC Database)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

**•** mitre-attack: privilege-escalation

## Malware

* XCSSET