The Clock is TCCing

OBTS
V6.0

CALUM HALL
LUKE ROBERTS

PHORION

> whoami

Luke Roberts

Phorion

rookuu_

Calum Hall

Phorion

_calumhall

Today's Agenda

1. TCC speedrun
2. An attackers view on TCC
3. Gaining visibility
4. Tool drop

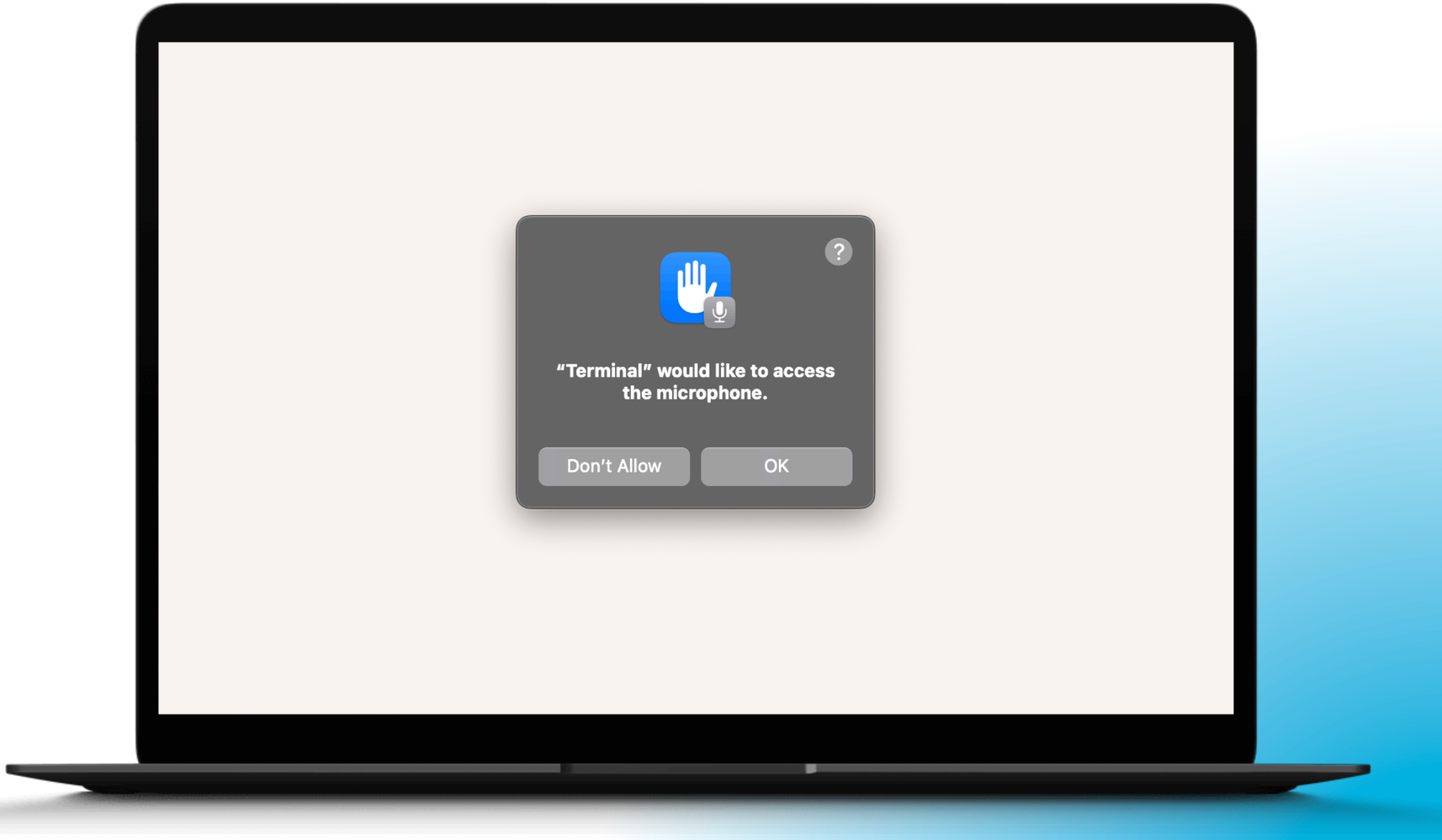
PART 01

What is TCC?

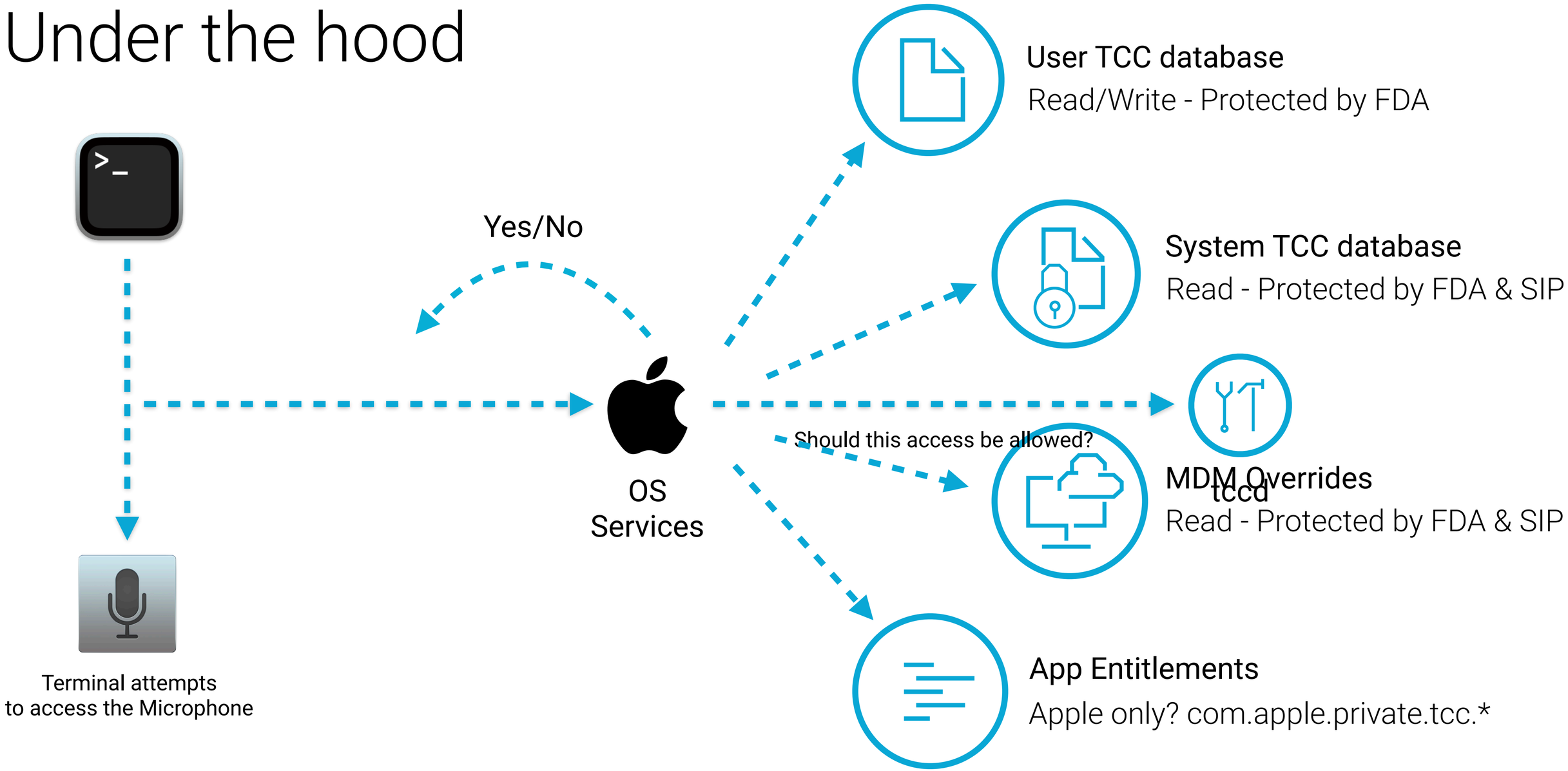
Transparency, Consent and Control?

An Apple privacy feature that prompts Users to permit applications access to various system resources.

- Camera/Microphone
- Various User Folders
  - Downloads
  - Documents
- System Folders
- Other App Bundles (new)



Under the hood



An attacker's perspective

FULL DISK ACCESS

Ability to edit user's TCC.db

No user interaction required

System TCC.db is SIP protected

EXPLOITATION

We find a TCC bug

A few in this room have experience 👀

We piggyback a legitimate app

Inherit TCC permissions

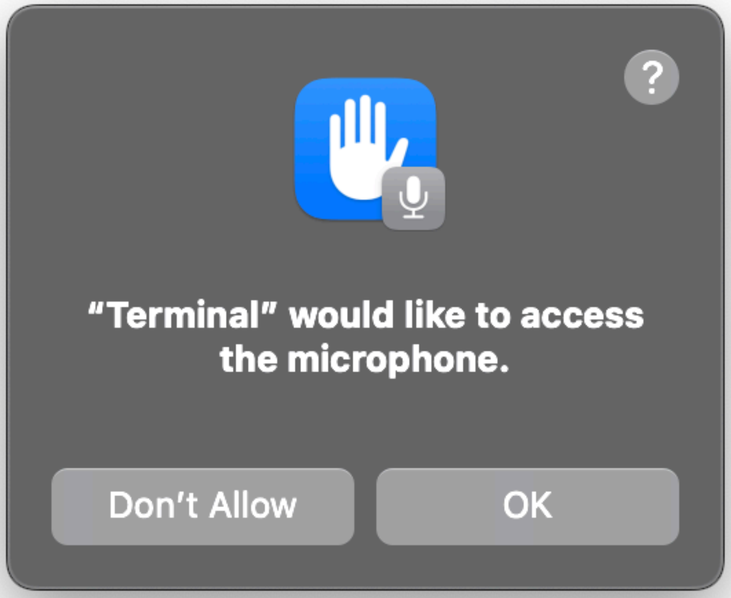
ANNOYING APPROACH

Let's just ask… repeatedly!

macOS is a world of unexpected prompts

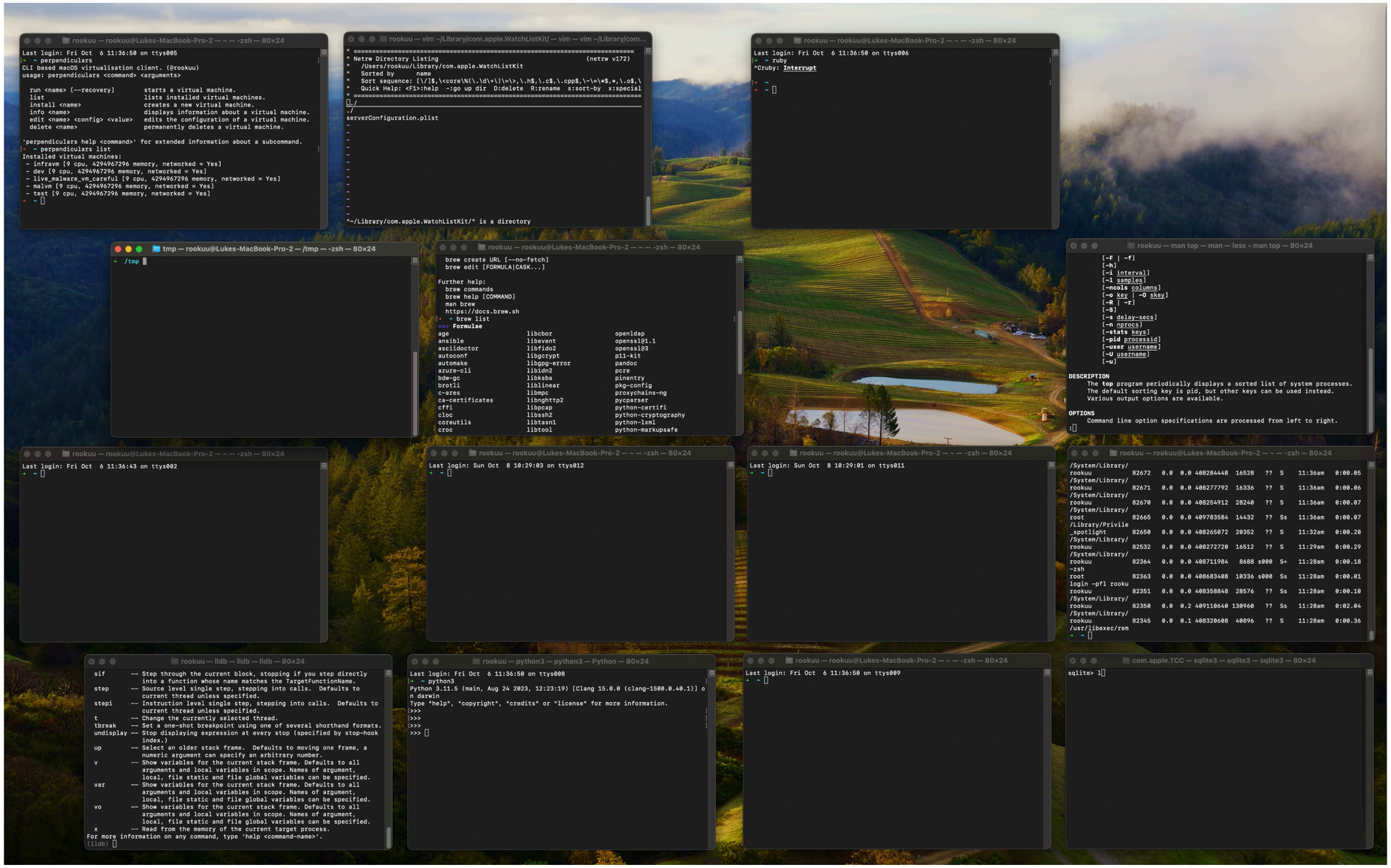
TCC prompts aren't verbose, it's not overly suspicious to prompt the user

Problem #1



Digging deeper

Take a look at the prompt on the left. What does this *actually* tell you?



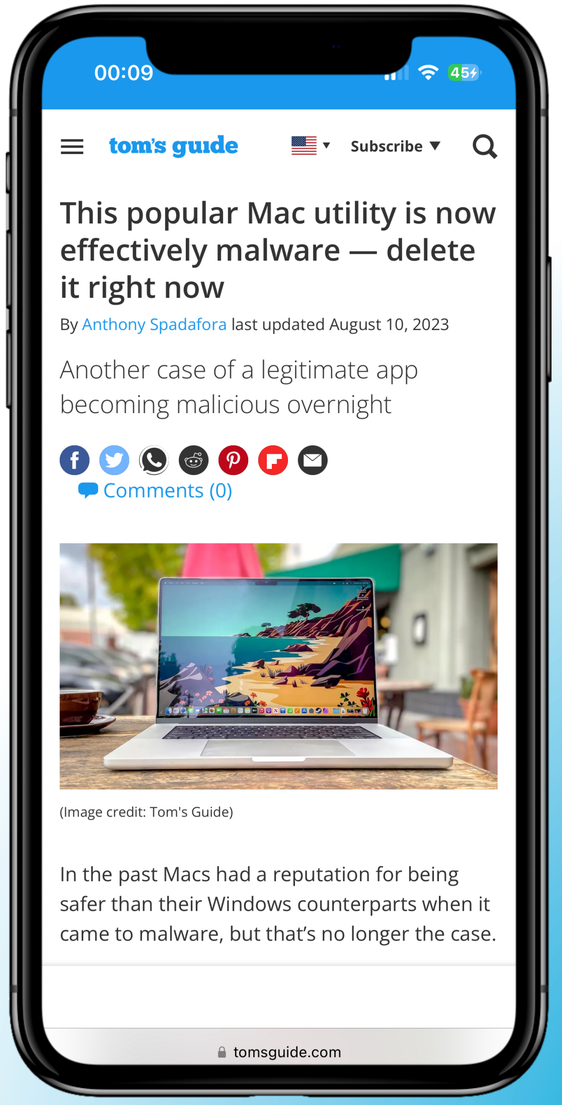
This happened to me

Terminal is requesting access to the Microphone… oh no.

Problem #2

TCC is gated by Bundle ID, not version

- Do you remember why you granted an app access back in 2019?
- Vulnerabilities introduced
- Change of application ownership
  - Nightowl a macOS dark mode app
  - Purchased in 2022
  - Turned into adware



Problem #3

Lack of TCC usage information

- No visibility into resource usage
  - Unable to monitor for unexpected resource access
  - Not able to monitor applications for failed access attempts
- Difficult to determine if an application *actually* needs resource permissions

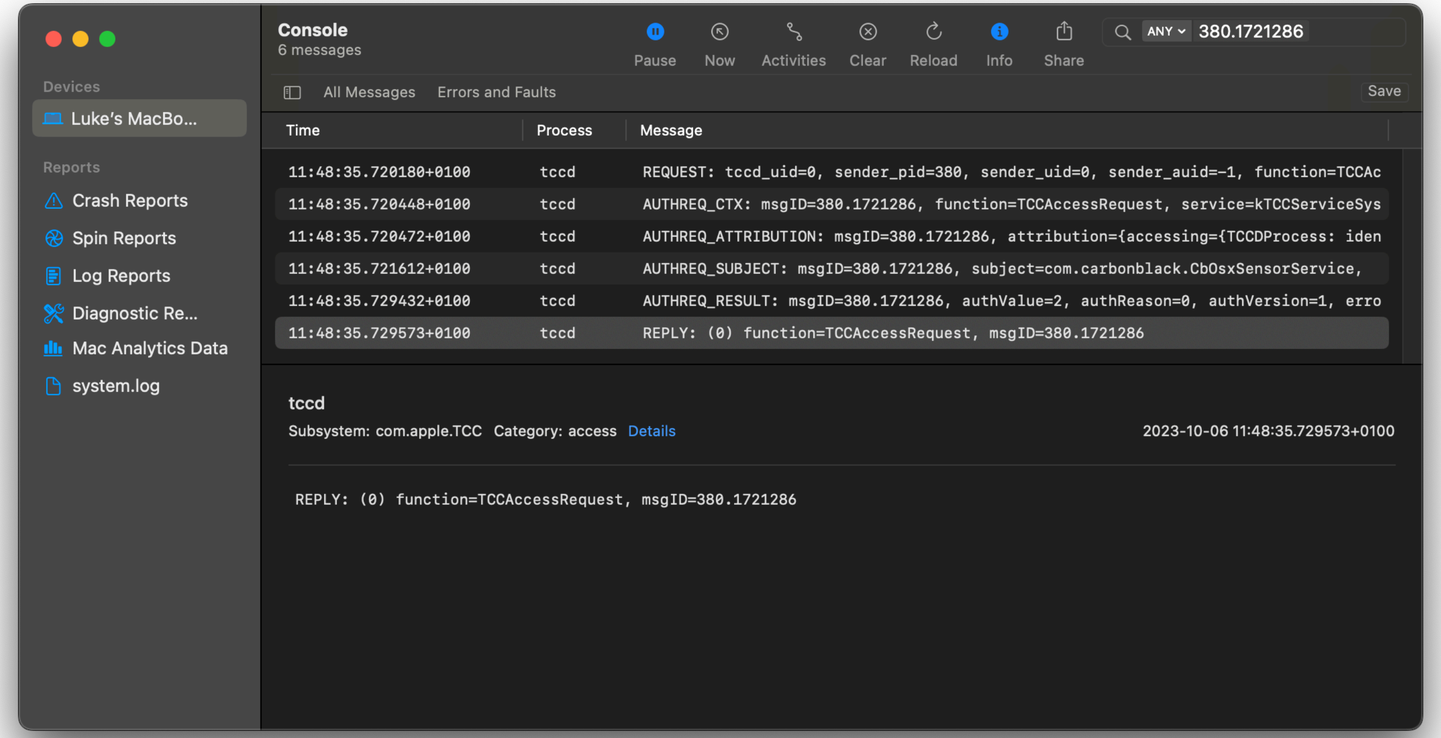
PART 02

Gaining Visibility

Knowledge is power

Helpfully TCCd logs fairly useful messages to the system unified log. Included in here we have;

- What the app was requesting access for?
- The **responsible** process, and **accessing** process.
- The result, whether it was denied or approved and why.



Log diving

1. // REQUEST
2. // AUTHREQ_CTX
3. // AUTHREQ_ATTRIBUTION
4. // AUTHREQ_SUBJECT
5. // AUTHREQ_PROMPTING
6. // AUTHREQ_RESULT

```
// AUTHREQ_ATTRIBUTION:
msgID=150.34,
attribution={
                responsible=
                                {<TCCDProcess:
                                identifier=com.apple.Terminal,
                                pid=436
```

```
// AUTHREQ_PROMPTING:
msgID=150.34,
service=kTCCServiceSystemPolicyDownloadsFolder,
subject=Sub:{com.apple.Terminal}
Resp:{<TCCDProcess:
```

```
// AUTHREQ_RESULT:
msgID=150.34,
authValue=0,
authReason=3,
authVersion=1,
error=(null),
```

```
                binary_path=/System/Applications/Utilities/
Terminal.app/Contents/MacOS/Terminal
},
```

```
                requesting={<TCCDProcess:
                                identifier=com.apple.sandboxd,
                                pid=150,
                                auid=0,
                                euid=0,
                                binary_path=/usr/libexec/sandboxd
                >},
},
```

macOS 11

```
accessing={identifier=com.apple.ls, pid=4581, auid=501,
euid=501, binary_path=/bin/ls},
```

macOS 12

```
accessing={<TCCDProcess: identifier=com.apple.ls, pid=4581,
auid=501, euid=501, binary_path=/bin/ls>}
```

macOS 13

```
accessing={TCCDProcess: identifier=com.apple.ls, pid=4581,
auid=501, euid=501, binary_path=/bin/ls},
```

Balancing on a knife edge.

Interfacing with TCC to augment an existing security system has not been easy. The OS does not want to help us.

We're using debug log messages from a private Apple service. These might change format (sad regex), introduce new or remove information or even just remove them entirely.

- Lets provide provide ourselves with some assurances.We've written a GitHub Actions workflow that matrices CI jobs across macOS versions.
- These Actions check that each log message we rely on exists, and is of the format we expect.

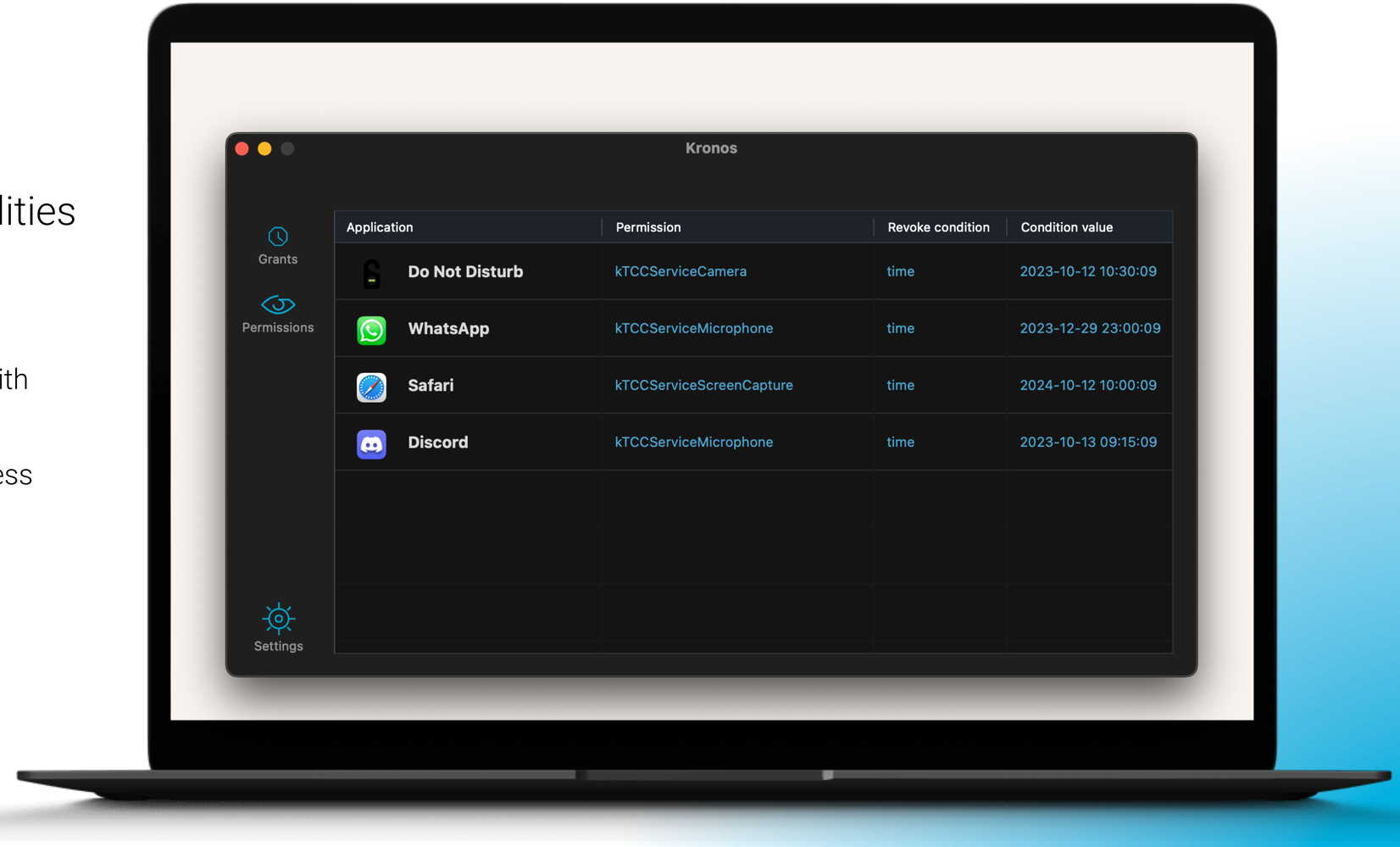
PART 04

Introducing Kronos

Kronos

Designed to enhance the capabilities of TCC

- Improve the verbosity of TCC prompts
- Encourage the principle of least privilege with application access
- Provide historical logging for resource access
- And it's open source!



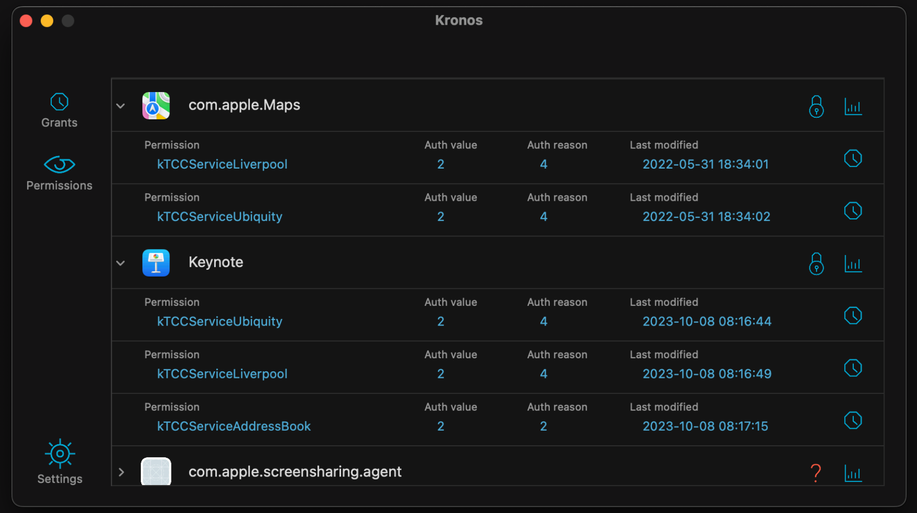
Transparency

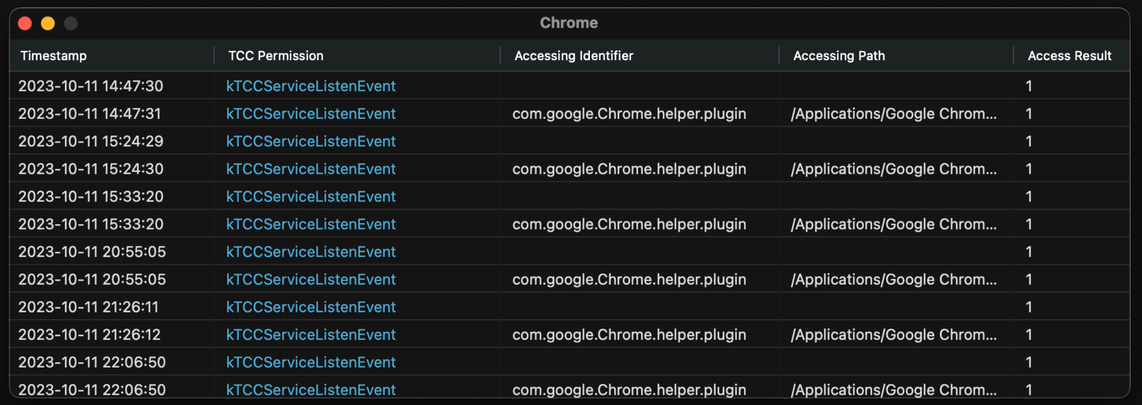
Permissions

- TTC auth values & auth reasons. i.e. user permitted, system set
- Permission last modified
- Signing information

Usage

- What does my app do with it's permissions?
- Historical resource access data
- Responsible and accessing process/path
- Resource access result, i.e. allowed/denied



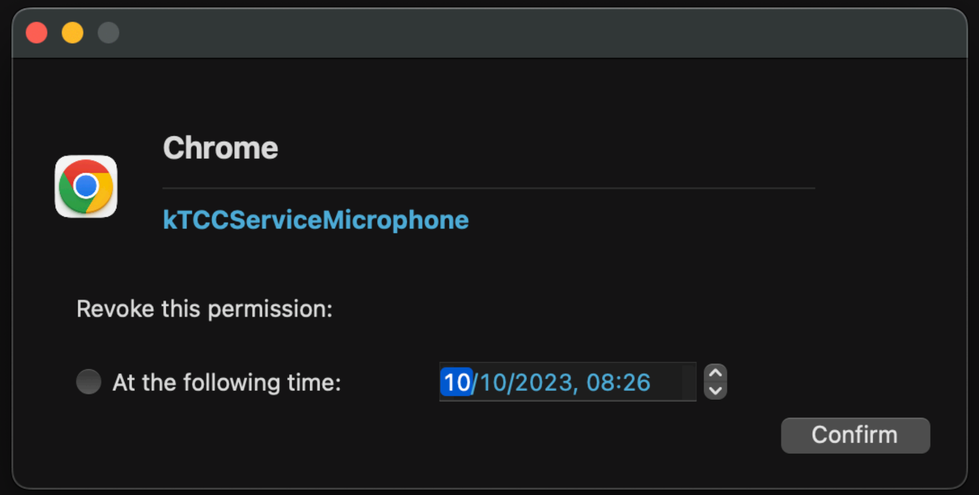


Timestamp	TCC Permission	Accessing Identifier	Accessing Path	Access Result
2023-10-11 14:47:30	kTCCServiceListenEvent			1
2023-10-11 14:47:31	kTCCServiceListenEvent	com.google.Chrome.helper.plugin	/Applications/Google Chrom...	1
2023-10-11 15:24:29	kTCCServiceListenEvent			1
2023-10-11 15:24:30	kTCCServiceListenEvent	com.google.Chrome.helper.plugin	/Applications/Google Chrom...	1
2023-10-11 15:33:20	kTCCServiceListenEvent			1
2023-10-11 15:33:20	kTCCServiceListenEvent	com.google.Chrome.helper.plugin	/Applications/Google Chrom...	1
2023-10-11 20:55:05	kTCCServiceListenEvent			1
2023-10-11 20:55:05	kTCCServiceListenEvent	com.google.Chrome.helper.plugin	/Applications/Google Chrom...	1
2023-10-11 21:26:11	kTCCServiceListenEvent			1
2023-10-11 21:26:12	kTCCServiceListenEvent	com.google.Chrome.helper.plugin	/Applications/Google Chrom...	1
2023-10-11 22:06:50	kTCCServiceListenEvent			1
2023-10-11 22:06:50	kTCCServiceListenEvent	com.google.Chrome.helper.plugin	/Applications/Google Chrom...	1

Revoking permissions

Avoid indefinite permissions

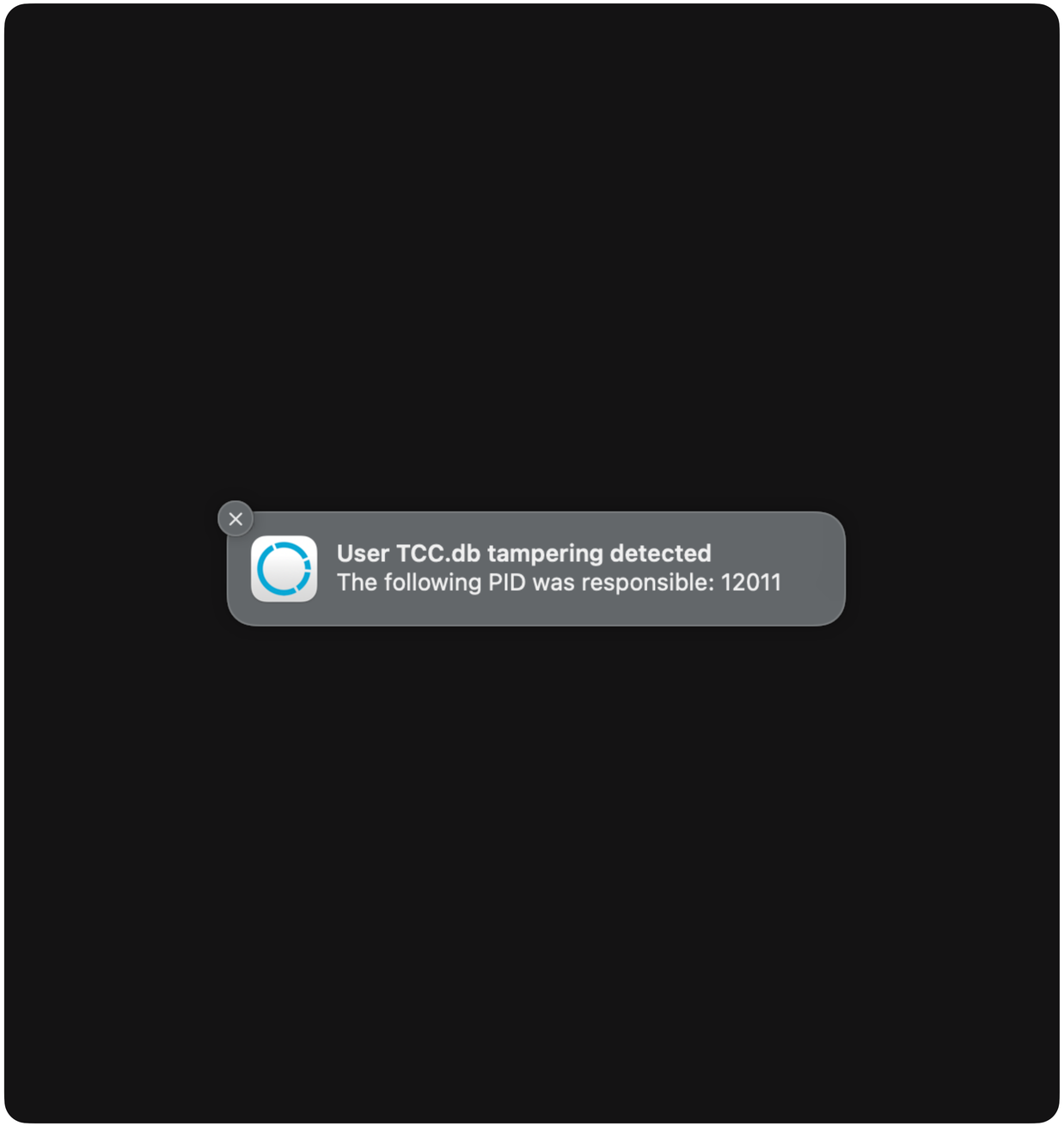
- **JIT access** for TCC permissions
  - Short term permissions for rare actions
  - Long term permission grants to allow for periodic decisions as to the requirement for app access



Protecting the user’s TCC.db

Endpoint Security Framework

- Monitor for direct file writes to the TCC.db
- Notify the user on potentially malicious tampering
- TCC.db integrity for personal use



Next Steps

1. Bug fixes
2. Application version change revocation
3. Application closing revocation
4. Filtering and searching improvements
5. Open source driven features

PHORION

github.com/PhorionTech/Kronos