SP2023 Week 02 • 2023-02-05

Bypassing macOS Privacy Controls for Fun and Profit

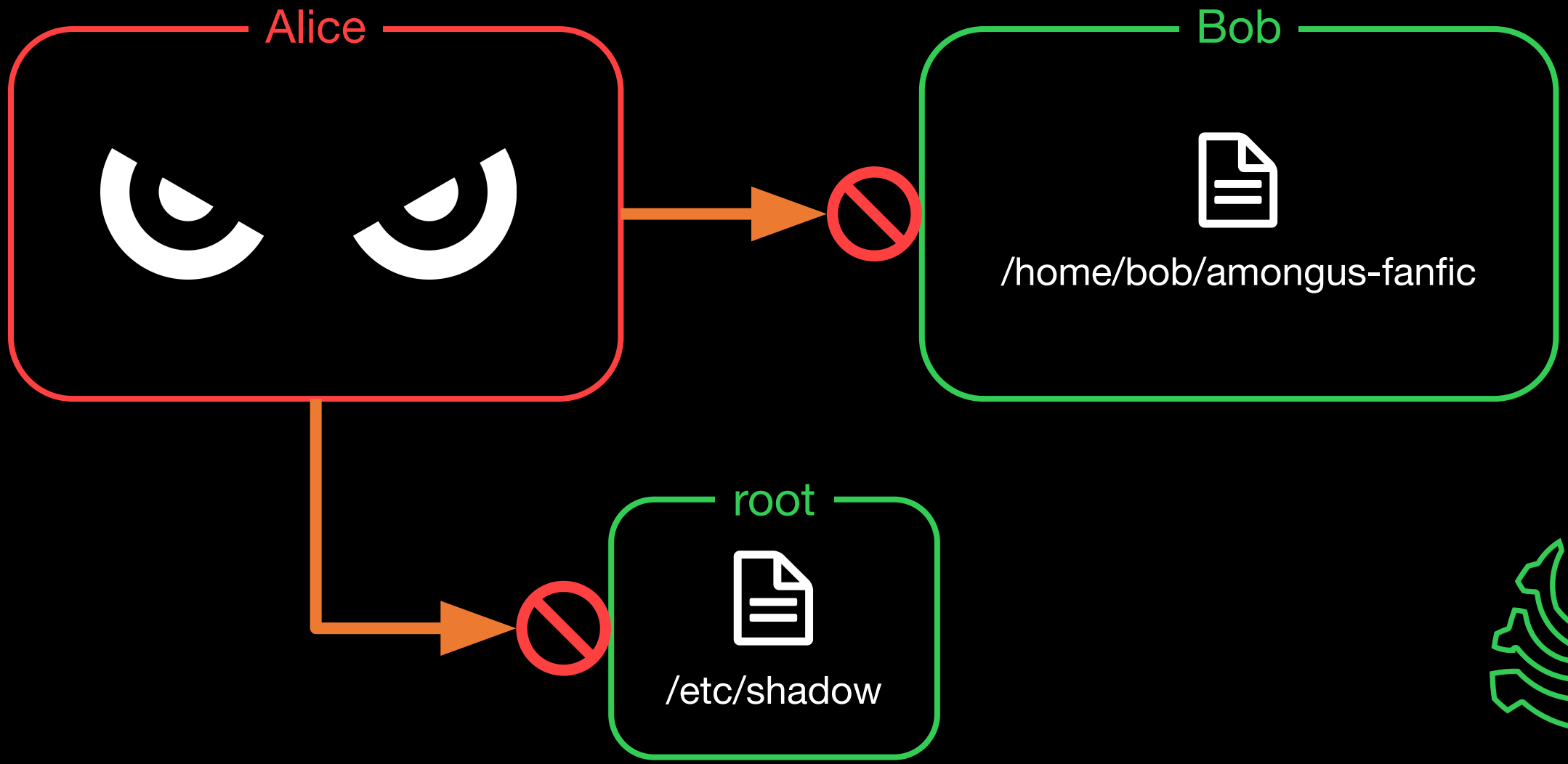
Rohit

How I Got Started

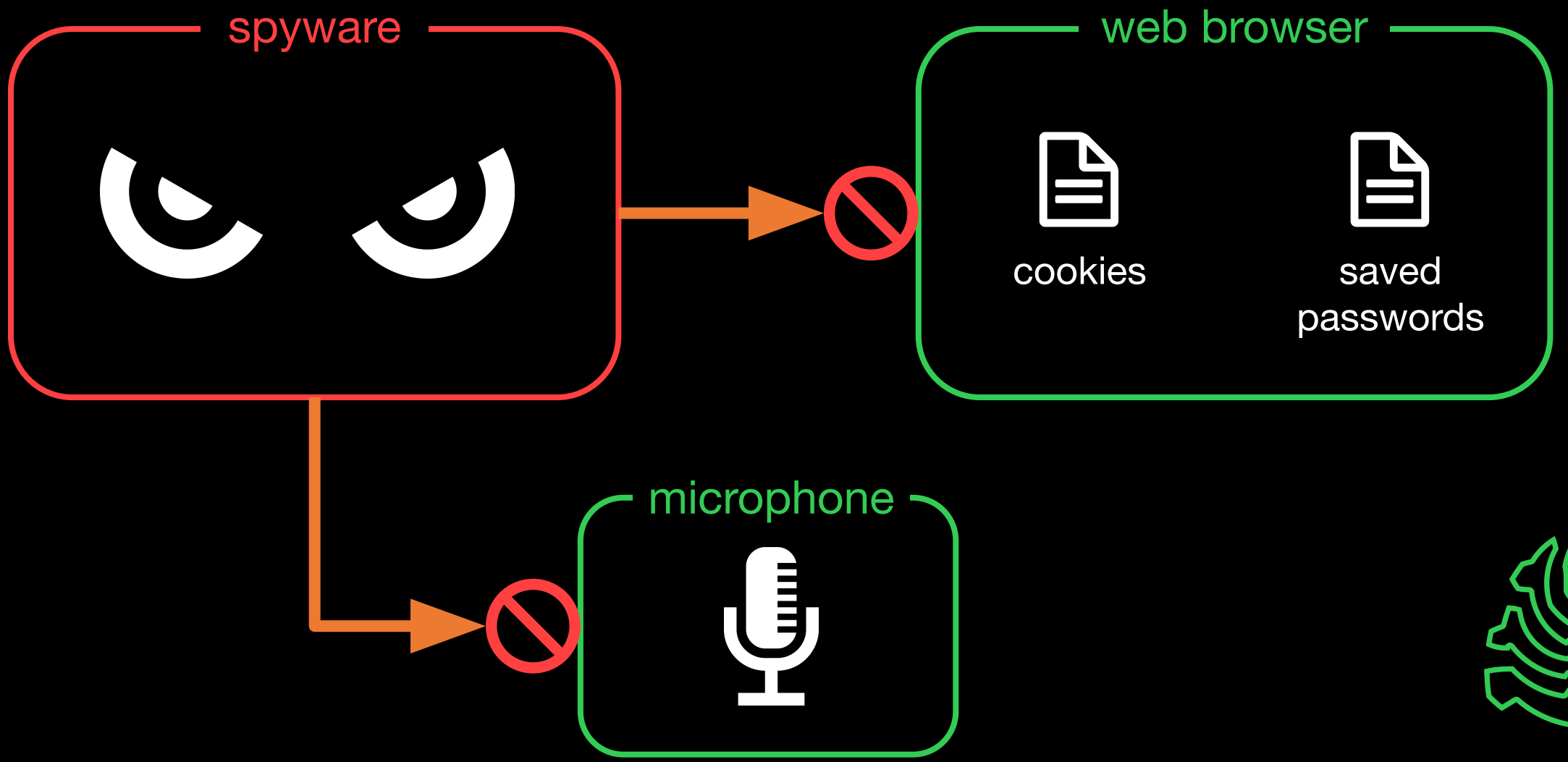
OS Security Crash Course

- If a program gets pwned, the OS can limit what damage can be done
  - A running process cannot access the memory of other processes **(memory isolation)**
  - All communication between a program and the "outside world" must be done through **system calls,** which are processed by the OS***
- Bottom line: an OS can arbitrarily limit what any program can do on the system***
  - ~~In practice, many OSes are bad at this~~

User Isolation



Application Isolation

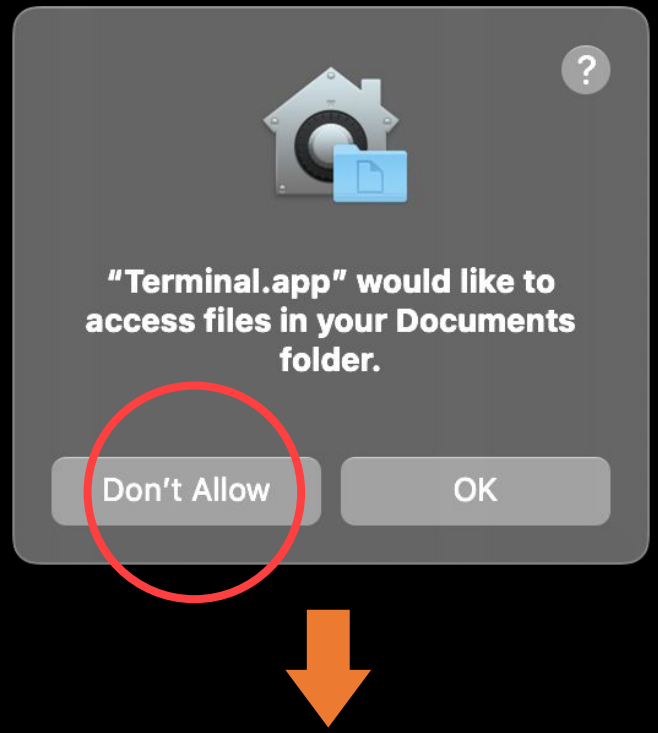


Transparency, Consent, and Control (TCC) Framework

- macOS implementation of application isolation
- Introduced in OS X 10.8 (2012)
- Applications cannot access certain files, services, and hardware without permission from the user

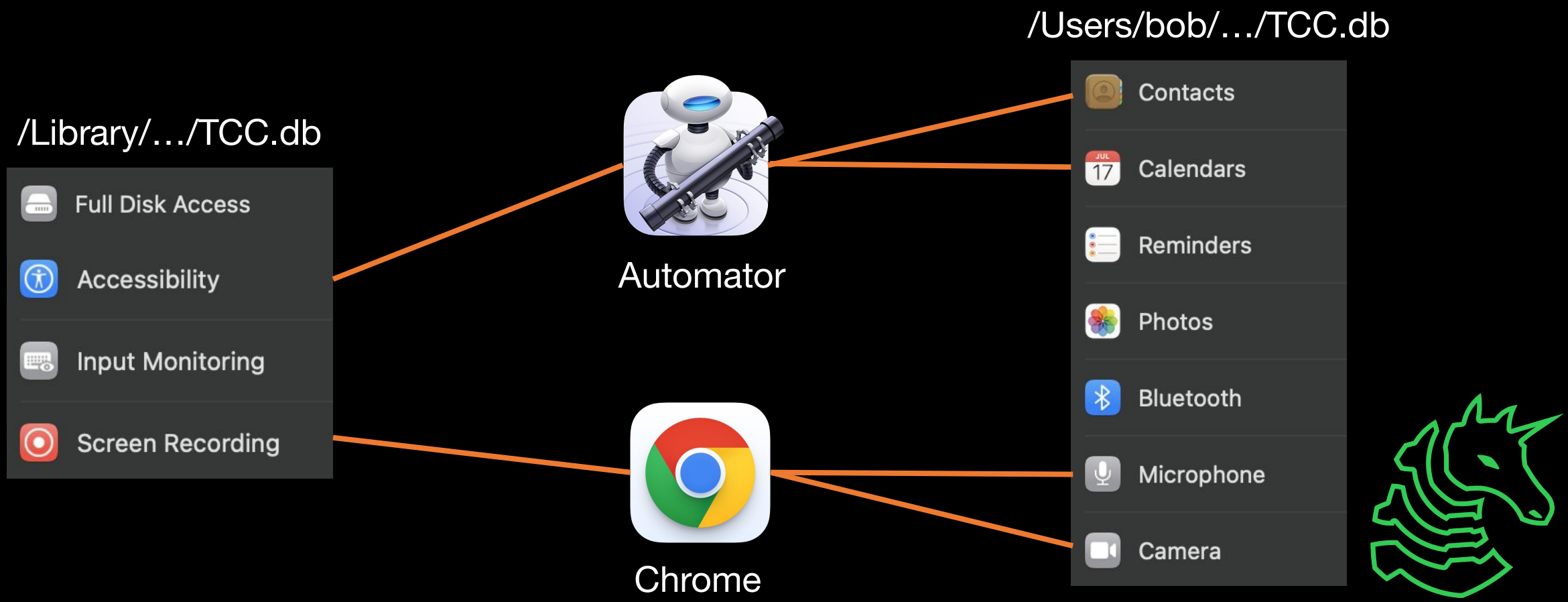
Transparency, Consent, and Control (TCC) Framework

```
ls ~/Documents
```




```
ls: Documents: Operation not permitted
```

Transparency, Consent, and Control (TCC) Framework



System Integrity Protection (SIP)

- aka "rootless"
- Introduced in OS X 10.11 (2015)
- Prevents root processes from:
  - Modifying system files, preinstalled apps, and certain administrative settings (including TCC)
  - Debugging most processes
  - Changing the startup disk
  - Loading kernel extensions
- Effectively extends TCC to applications running as root
- **Can be bypassed by Apple-signed binaries with specific entitlements**

Previous Exploits

CVE-2020-27937: Wojciech Reguła

- Hijacks user-level TCC privileges
- Changes user's home directory through malicious plugin injected into privileged process
- TCC daemon uses fake TCC.db placed in new home directory
- **Requires root privileges**
- Security bounty awarded (unspecified amount)

Previous Exploits

CVE-2021-30970: Microsoft

- Defeats SIP filesystem protections
  - Makes all TCC databases writable
- Writes payload to /etc/zshenv
  - Executed whenever root user runs zsh
- Installs Apple-signed package with post-install zsh script
  - system_installd → zsh → /etc/zshenv
- system_installd has **com.apple.rootless.install.heritable** entitlement
- Requires root privileges

First Steps

- Binaries with **com.apple.rootless.install.heritable** entitlement
  - diskmanagementd
  - storagekitd
  - system_installd
  - systemmigrationd

systemmigrationd

- aka System Migration Daemon
  - Migrates files and settings from a backup or another computer
- Reads migration request file placed in **/Library/SystemMigration/Queue**
  - Directory is writable by any process with root privileges
- Contents of a migration request
  - Source system (root directory or network location)
  - "type" (integer field, affects what data is migrated)

What Didn't Work

- Planting malicious TCC.db in source system
- Looking for vulnerabilities in systemmigrationd
- Perl script injection
- Environment variable hijacking
- Process injection
- chroot

TCCMigration.bundle

- Loaded by systemmigrationd
- Runs only if migration request "type" is 1 or 4
- **Gives Full Disk Access to SSH daemon**

```
iVar2 = __auth_stubs::_TCCAccessSetForPath
                  (*(undefined8 *)__got::_kTCCServiceSystemPolicyAllFiles,
                   &cf_/usr/libexec/sshd-keygen-wrapper,uVar6);
```

SSH daemon

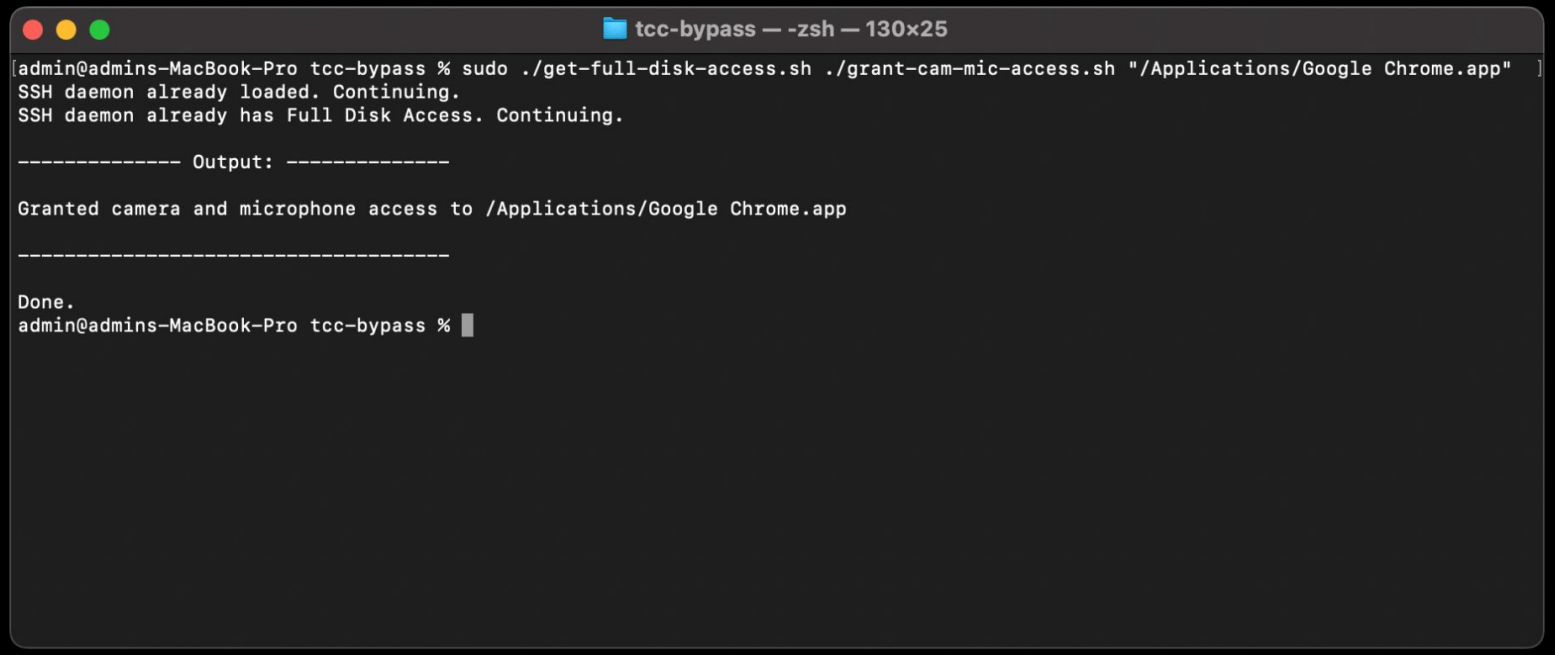
Full Disk Access

The Exploit

1. Enable SSH daemon
2. Create malicious migration request file with "type" set to 1 and invalid source system
3. Place request file in /Library/SystemMigration/Queue (starting systemmigrationd)
4. Generate SSH keys, copy public key to ~/.ssh/authorized_keys
5. When SSH daemon is granted Full Disk Access, execute payload in SSH session

The Exploit

- Requires root privileges
- Silently gains Full Disk Access and all user-level TCC privileges (camera, microphone, etc.)



Communicating with Apple

- 3 Jun 2022: I send report to Apple Product Security; Apple begins investigation
- 14 Jul 2022: Apple confirms that they will fix the issue in a security update in the fall
- 6 Oct 2022: Apple registers vulnerability as **CVE-2022-32862**
- 24 Oct 2022: Apple releases updates and awards security bounty
  - Vulnerability fixed in macOS 13, 12.6.1, and 11.7.1
  - /Library/SystemMigration/Queue no longer writable

Vulnerability Disclosure How-To

- Make sure vendor has a responsible disclosure program
  - Even if they don't award money
- Read terms and conditions before starting research
- What to include in your report
  - Working exploit with source code
  - Detailed explanation of exploit
  - Recommended mitigations
- "reports with more details typically receive higher bounty rewards"

Taxes

Security bounty payments are self-employment income

- Subject to self-employment tax IN ADDITION TO income tax
  - 15.3% for 2023
- Must pay estimated tax at end of quarter (exceptions apply)
  - January through March: April 15
  - April through May: June 15
  - June through August: September 15
  - September through December: January 15 (following year)
- State laws vary

SIGPwny