📓

SandBox(샌드박스)

API Collection

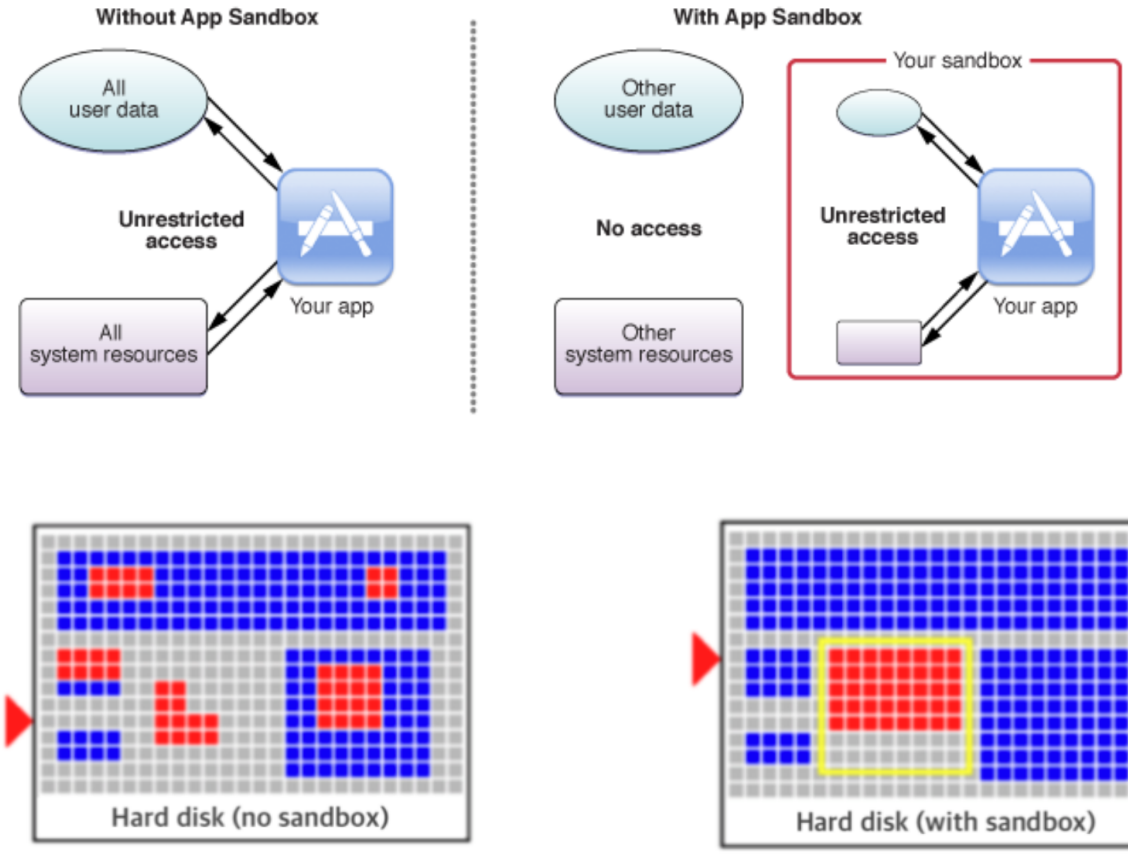
앱이 손상된 경우 손상을 방지하기 위해 macOS 앱의 시스템 리소스 및 사용자 데이터에 대한 액세스를 제한합니다.

Overview(개요)

App Sandbox는 자격을 통해 요청된 리소스에 대한 앱의 액세스를 제한하여 시스템 리소스 및 사용자 데이터를 보호합니다.

> ✅ **Important**
>
> Mac App Store를 통해 macOS 앱을 배포하려면 App Sandbox 기능을 활성화해야 합니다.

App SandBox가 적용되고 안되고의 차이.



복잡한 시스템은 항상 취약점을 갖고, 소프트웨어의 복잡도는 계속 증가합니다.

개발자가 아무리 방어 코딩을 하며, 버그를 경계 하더라도 해커들은 개발자의 방어를 한 번만 뚫어내면 됩니다.

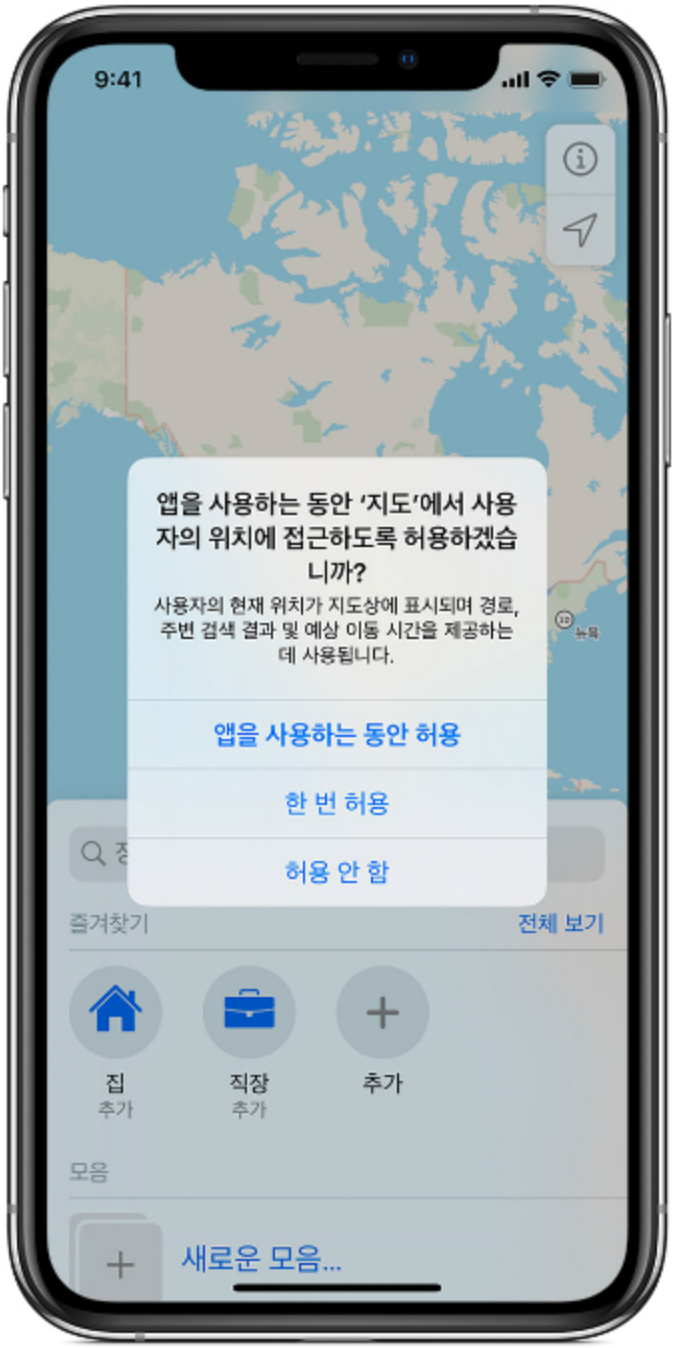
App SandBox가 App을 공격하는 모든걸 막을 순 없지만, 피해를 최소화 할 수는 있습니다.

App SandBox가 적용되지 않은 App은 앱을 실행하는 사용자의 모든 권한을 가지며 사용자가 액세스 할 수 있는 모든 리소스에 접근할 수 있습니다.

만약 그 App이나 그 App과 연결된 어떤 프레임워크에 보안 구멍이 있다면, 해커는 잠재적으로 그 구멍을 이용하여 App을 제어할 수 있습니다.

그리고, 해커는 사용자가 할 수 있는 어떤 것이든 할 수 있게 됩니다.

그렇다는건 App을 통해 접근할 수 있는 사용자의 모든 데이터나 시스템 리소스에 접근해서 무작위로 바이러스 등을 퍼뜨릴 수도 있다는 뜻이 되겠네요.



App SandBox의 전략

그럼 App SandBox는 어떤식으로 피해를 최소한으로 할 수 있다는 걸까요?

1. App SandBox는 개발자가 App과 시스템이 어떤식으로 상호작용하게 할건지 설정할 수 있게 합니다.

   그럼 시스템은 App이 하고자하는 일을 끝내는데 필요한 권한만을 부여하고, 그 이상은 부여하지 않습니다

2. App SandBox는 사용자가 드래그 앤 드롭, 대화 상자 등의 친숙한 인터렉션을 통해 투명하게 앱에게 추가 액세스 권한을 부여할 수 있도록 합니다.

   사용자는 App을 사용하면서 많이 보는 위의 그림과 같은 Alert 창을 통해 App에 추가 접근 권한을 부여할 수 있습니다.

   App SandBox는 무적이 아니며, App은 언제나 손상될 위험에 놓여있습니다.

   하지만 App이 업무를 수행하는데 필요한 최소한의 권한으로 권한을 제한할 경우 잠재적 피해의 범위는 급격하게 줄어들 수 있습니다.

App SandBox의 원칙

각 앱 마다 취약한 리소스에 대한 접근을 제한함으로써, App SandBox는 해커가 앱의 보안 구멍을 뚫었을 경우 사용자 데이터의 도난, 손상, 삭제, 시스템 하드웨어의 해킹에 대한 마지막 방어선을 구축합니다.

예를들어, SandBox App은 다음 리소스 중 하나를 사용하려면 그 위도를 명시적으로 명시해야 합니다.

- Hardware(Camera, Microphone, USB, Printer)
- Network Connections(Inbound or Outbound)
- App Data(Calendar, Location, Contacts)
- User Files(Downloads, Pictures, Music, Movies, User Selected Files)

프로젝트 정의에서 명시적으로 요청되지 않은 리소스에 대한 접근은 런타임 시 시스템에 의해 거절됩니다.

만일 Sketch App을 만든다면, 개발자는 자신이 만든 App이 절대 Microphone에 대한 접근을 하지 않을거란걸 알고 있고, 그냥 단순히 접근에 대해 요청하지 않으면 됩니다.

그리고 시스템 또한 App이 그런 요청을 한다면 거절해야 한다는 것도 알고 있는 것입니다.

반면 SandBox App은 사용자가 요청하는 특정 리소스에 접근할 수 있습니다.

이를 위해서 사용자는 간단한 유저 인터렉션(끌어다 놓기) 등을 사용해서 SandBox를 확장할 수 있고, 다음과 같은 작업들을 자동으로 수행할 수 있습니다.

- Invoking Services from the Services menu
- Reading most world readable system files
- Opening files chosen by the user

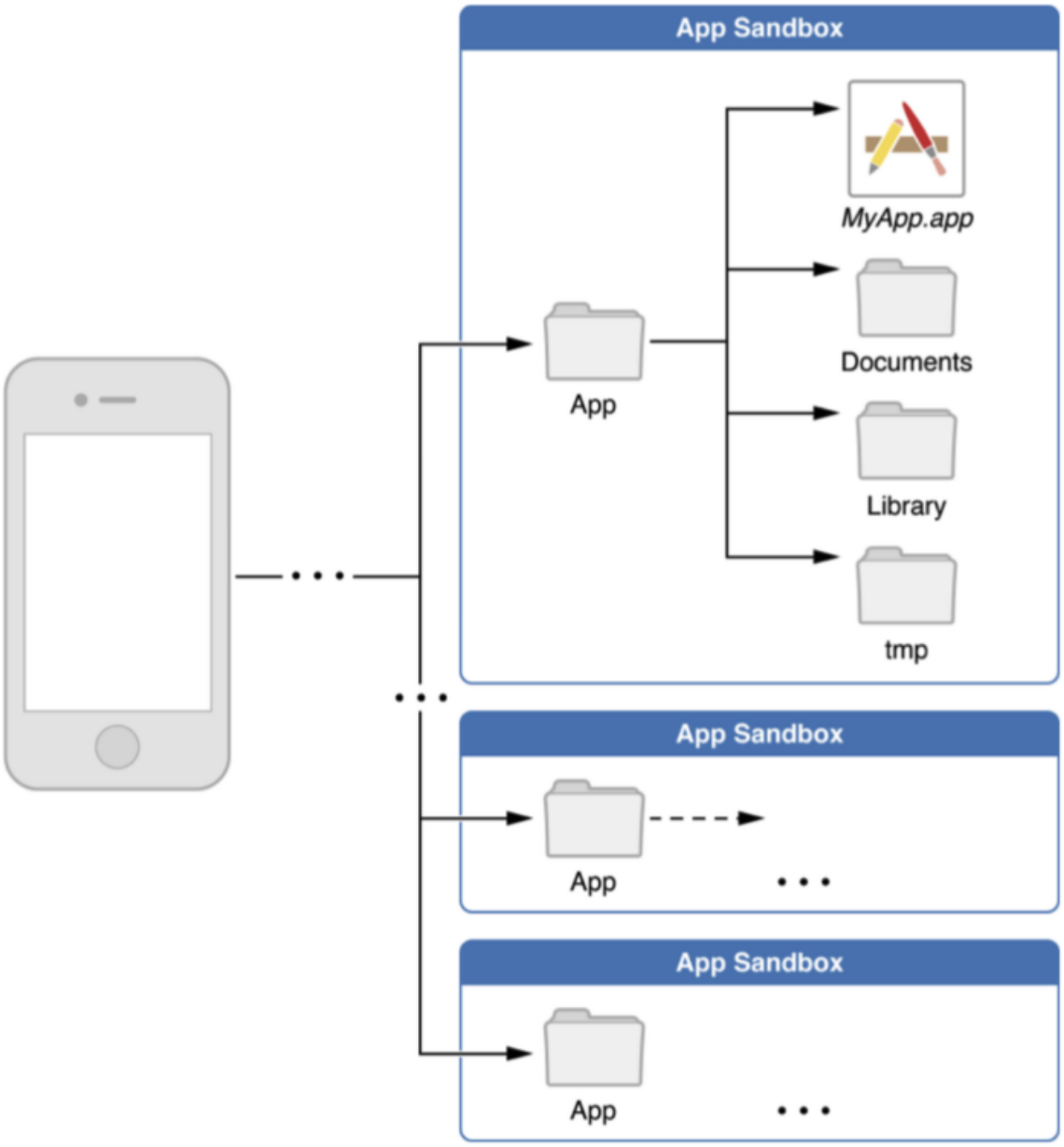
App SandBox의 구성은 다음과 같습니다.

1. 사용 권한(entitlement)
2. 컨테이너 디렉토리
3. 사용자 결정 권한
4. 권한 분리
5. 커널 적용

이를 다 함께 사용하면, App SandBox를 사용해서 App 업무 수행에 필요한 만큼의 권한에만 접근시킬 수 있습니다.

App SandBox가 적용되는 방식

그래서 어떻게 적용된다는 걸까요?



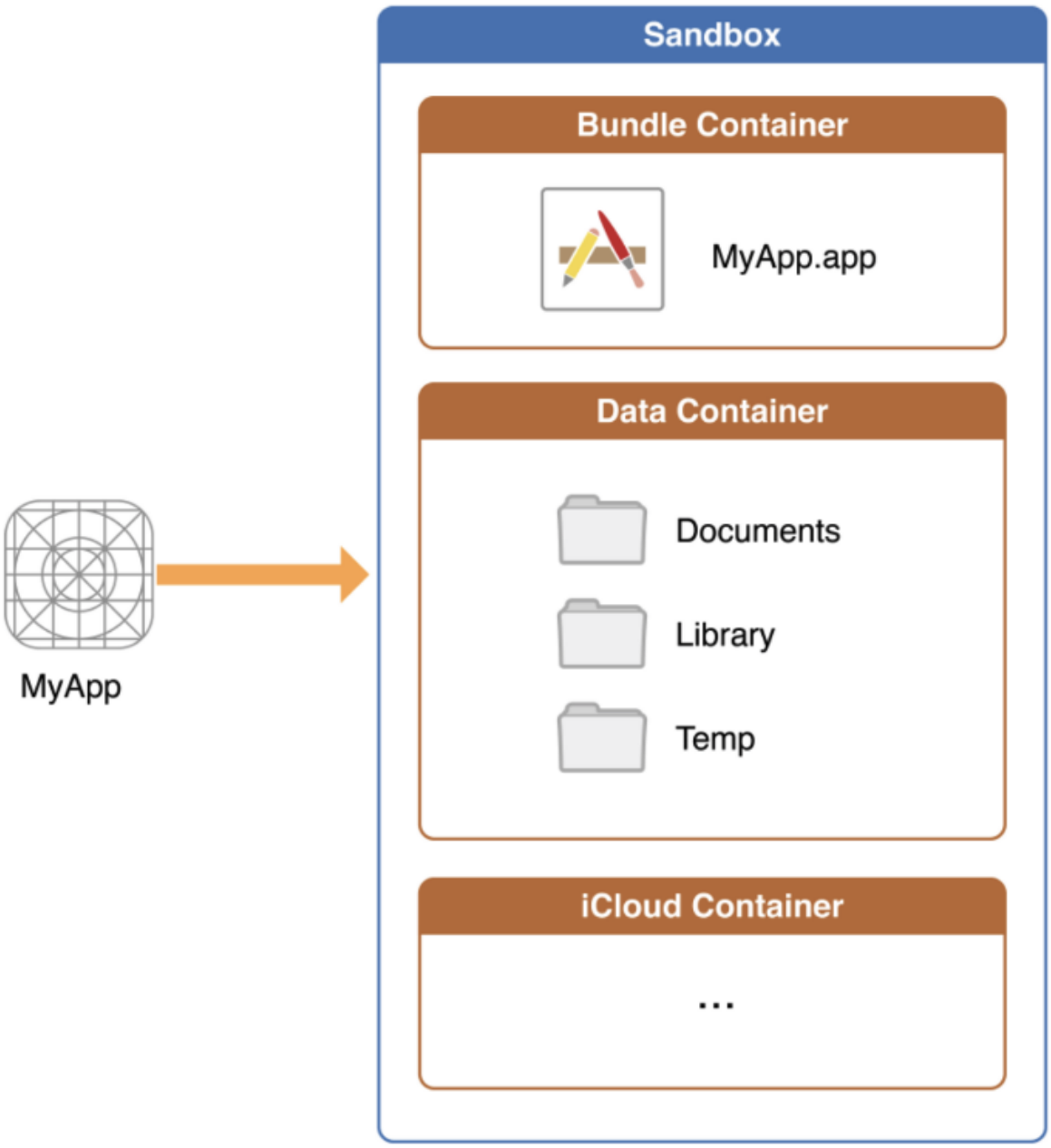
iOS는 각 App 마다 전부 SandBox화 되어 있습니다.

App SandBox는 각 App에 대한 파일, 환경설정, 네트워크 리소스, 하드웨어 등에 대한 앱의 접근을 제한하는 세분화된 제어 집합이라 볼 수 있습니다.

이렇게 App마다 구분되어 있기 때문에 이 App을 사용하는 사용자는 이 App의 데이터에만 접근할 수 있습니다.

외부에 있는 데이터에 접근하려면, SandBox 정책에 따라 접근 권한을 부여받아야 합니다.

반대로 이 App의 데이터도 다른 곳에서 접근할 수 없습니다.



App의 SandBox 디렉토리는 이런식으로 되어 있습니다.

앱의 설치 시점에 각각의 SandBox Directory에 위치시키며, 이 Directory는 각 앱의 Home Directory가 됩니다.

보안을 위해 App과 시스템의 상호 작용은 App의 SandBox Directory에 있는 Directory로 제한됩니다.

Home Directory는 각각 특별한 역할을 가진 Container Directory들을 하위 Directrory로 가집니다.

각 Container에는 역할이 있습니다.

1. Bundle Container
    - App의 Bundle을 보유합니다.

2. Data Container
    - App 및 사용자 데이터를 보유, 앱이 데이터를 정렬화 하고 그룹화 하는데 사용할 수 있는 여러 하위 디렉토리로 나뉩니다.

3. iCloud Container
    - 런타임에 접근을 요청할 수 있는 추가 컨테이너 디렉토리입니다.
