OS X Keychain Forensic Artifacts

Breaking the OS X & iCloud

Keychain

n0fate

n0fate@n0fate.com

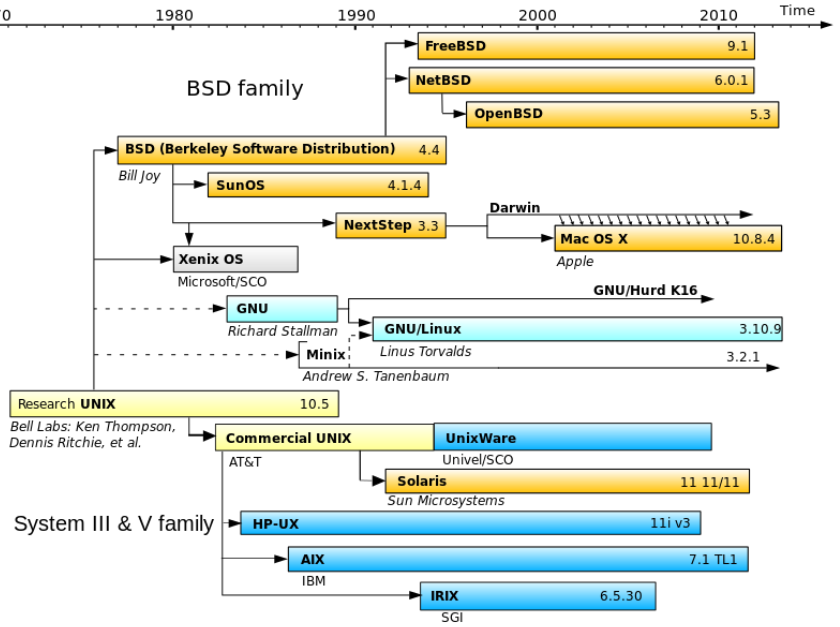
forensic.n0fate.com

목차

서론

- Mac OS X 소개
- OS X Keychain 소개

- 애플에서 개발한 유닉스 기반의 운영체제
  - 2001년 Mac OS X 10.0 Cheetah로 시작
- XNU(XNU is Not Unix) Kernel
  - 커널 : Darwin Kernel
  - 컴포넌트 : BSD + Mach



https://en.wikipedia.org/wiki/OS_X#/media/File:Unix_timeline.en.svg

- 애플의 포터블 디바이스도 OS X의 구조를 가지는 iOS 를 사용
  - OS X : iMac, Mac Pro, Mac Mini, Macbook Pro (Retina) / Air
  - iOS : iPhone, iPad, Apple Watch, Apple TV(1세대 이후)

- 윈도와 맥 아티팩트 연구 현황

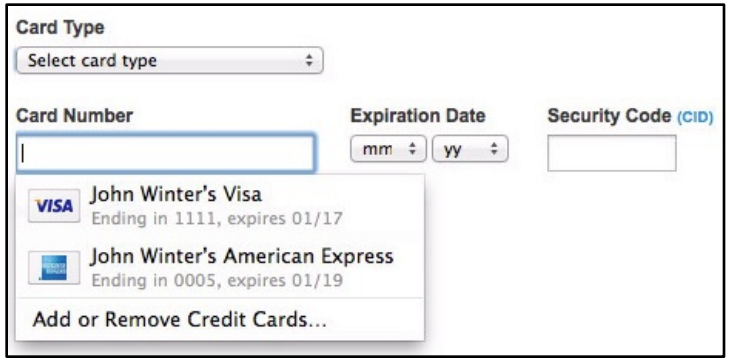
종류	Windows	Mac OS X
시스템 로그	O(이벤트 로그)	O(시스템 로그)
웹 브라우저	O	O
연락처	O	O
이메일	O	O
디스크 암호화	O	O
…	…	…
패스워드 등 기밀 정보	O(or △)	**오늘 주제**

- 패스워드 관리 방식 비교

운영체제	패스워드 보관 방식
Windows	각 애플리케이션에서 별도의 알고리즘 이용 (일부 윈도의 DPAPI 이용)
Mac OS X	키체인 시스템 이용 (일부 별도의 알고리즘 이용)

OS X Keychain : Password Management System

- Mac OS 8.6에서 공개된 패스워드 관리 시스템
  - 사용자 생성, 애플리케이션 생성 기밀 정보를 통합 관리하기 위한 인터페이스
    - ✓ 개발자가 별도의 기밀 암호화를 위한 알고리즘을 개발할 필요가 없음.
  - 애플리케이션 개발자는 Keychain API를 통해 손쉽게 정보를 저장/요청할 수 있음
  - 키체인 시스템은 사용자 기밀 정보를 암호화하여 데이터베이스에 저장함
- 사용자/애플리케이션의 기밀 정보를 통합 관리하기 위한 시스템
  - 계정 / 패스워드 : 메일, 연락처, 일정, 애플리케이션, 원격접근, 암호화 디스크, WiFi, 인터넷 계정
  - 인증 토큰 : Facebook, Google, Twtter, Linked-in, 애플리케이션
  - 개인키/공개 키 쌍, 인증서
  - 카드 정보
  - 보안 노트

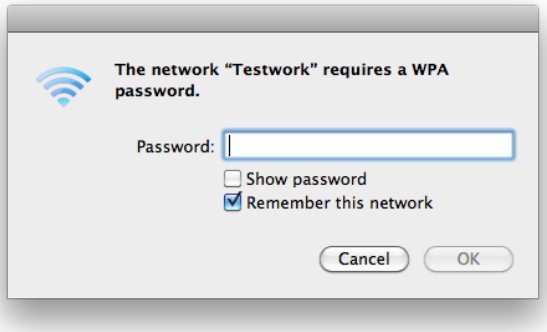


OS X Keychain : How to operate

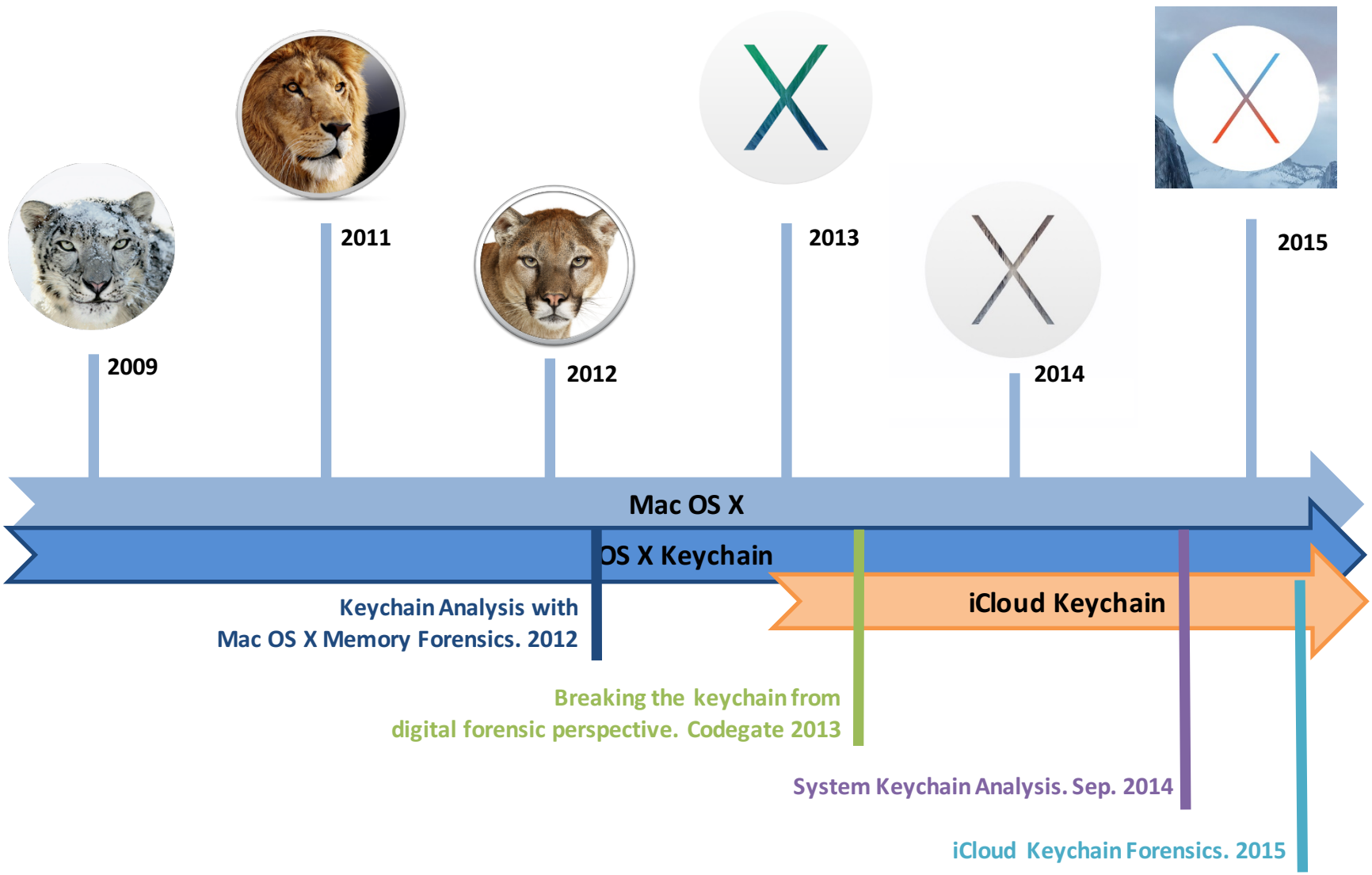
정보 저장
(암호화)

키체인 서비스 인터페이스

정보 입력
(평문)



OS X Keychain : Timeline



키체인 종류 (매버릭스 이전)

- **키체인**

이름	설명	경로
사용자 키체인	사용자 단위의 사용자가 생성한 기밀 정보를 저장 **저장 정보** : 사용하는 애플리케이션의 패스워드, 이메일 계정, 사파리/크롬에서 저장한 계정 정보, 신용카드 정보, SSH/VPN 등 보안 프로토콜의 인증 정보, 보안 노트 등	~/Library/Keychains/login.keychain
시스템 키체인	시스템 운영에 필요한 기밀 정보를 저장 **저장 정보** : 공개키 암호화에 필요한 개인키/공개키 셋, WiFi SSID/패스워드 정보 등	/Library/Keychains/System.keychain
인증서 키체인	디지털 서명에 필요한 인증서를 저장 **저장 정보** : HTTPS 프로토콜의 검증을 위한 인증서 등 루트, CA 인증서	/System/Library/Keychains/System**Certificate.keychain

- **OS X Keychain**
  - 사용자가 필요 시 새로운 키체인을 생성/삭제도 가능
  - 레코드의 임의 추가/삭제도 가능
  - 사용자들이 키체인을 기밀 정보 보관소 용도로 사용하기도 함.

키체인 종류 (매버릭스 이후)

▪ 키체인

이름	설명	경로
사용자 키체인	사용자 단위의 사용자가 생성한 기밀 정보를 저장 **저장 정보** : 사용하는 애플리케이션의 패스워드, ~~이메일 계정, 사파리/크롬에서 저장한 계정 정보, 신용카드 정보~~, SSH/VPN 등 보안 프로토콜의 인증 정보, 보안 노트 등	~/Library/Keychains/login.keychain
시스템 키체인	시스템 운영에 필요한 기밀 정보를 저장 **저장 정보** : 공개키 암호화에 필요한 개인키/공개키 셋, 로컬에서 생성한 WiFi SSID/패스워드 정보 저장	/Library/Keychains/System.keychain
인증서 키체인	디지털 서명에 필요한 인증서를 저장 **저장 정보** : HTTPS 프로토콜의 검증을 위한 인증서 등 루트, CA 인증서	/System/Library/Keychains/System**Certificate.keychain
아이클라우드 키체인	아이클라우드를 통해 특정 정보를 공유할 수 있도록 새로운 데이터베이스를 구성 저장 정보 : 이메일 계정, 웹 브라우저에서 저장한 기밀 정보, 신용카드 정보, 아이클라우드로 동기화 되는 모든 WiFi SSID/패스워드 정보가 저장	~/Library/Keychains/[UUID]/keychain-2.db

▪ 아이클라우드 키체인

- iOS 장비의 키체인 분석이 불가능 상황에서 유용한 아티팩트로 활용 가능
- 기존 키체인과 **다른 암/복호화 구조**로 추가 분석이 필요

OS X 키체인 분석

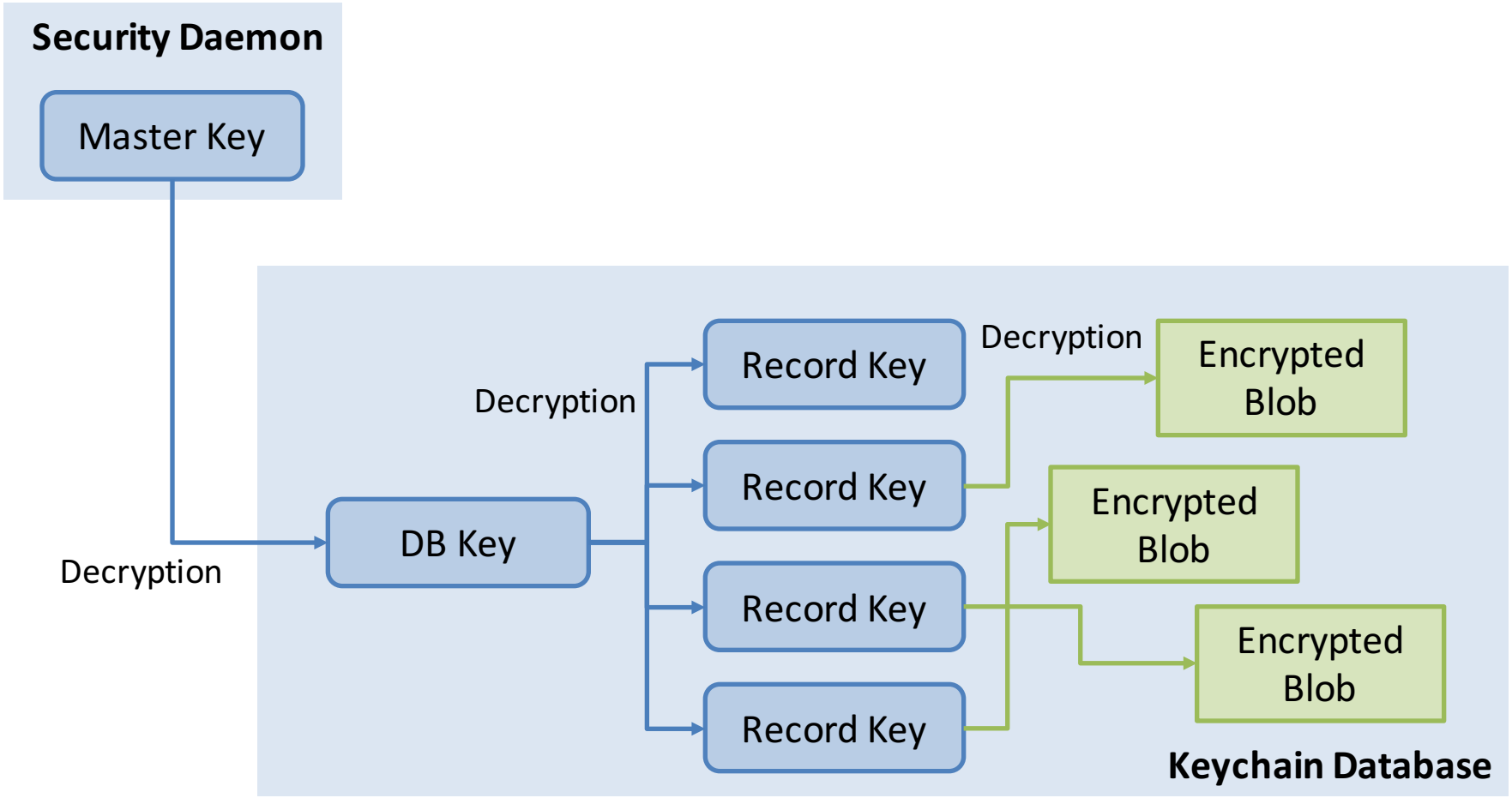
- 키체인의 구조 설명
- 키체인 분석 방법

OS X 키체인 분석

- **2012년 키체인 분석 화이트 페이퍼 공개 및 발표**
  - Kyeongsik Lee, Hyungjoon Koo. *Keychain Analysis with Mac OS X Memory Forensics*. 2012.
  - Kyeongsik Lee. *Breaking the Keychain from digital forensic perspective*. Codegate 2013.

- **구조**
  - Apple Database File Format
    - ✓ SQLite보다 조금 더 단순한 구조를 가지고 있음.
  - 사용자 패스워드를 마스터 키 생성 인자로 활용
- **키 추출 방법**
  - 메모리에서 추출(System Keychain, User Keychain)
  - 마스터 키 저장 파일에서 추출(System Keychain)

OS X 키체인 분석 (복호화 과정)



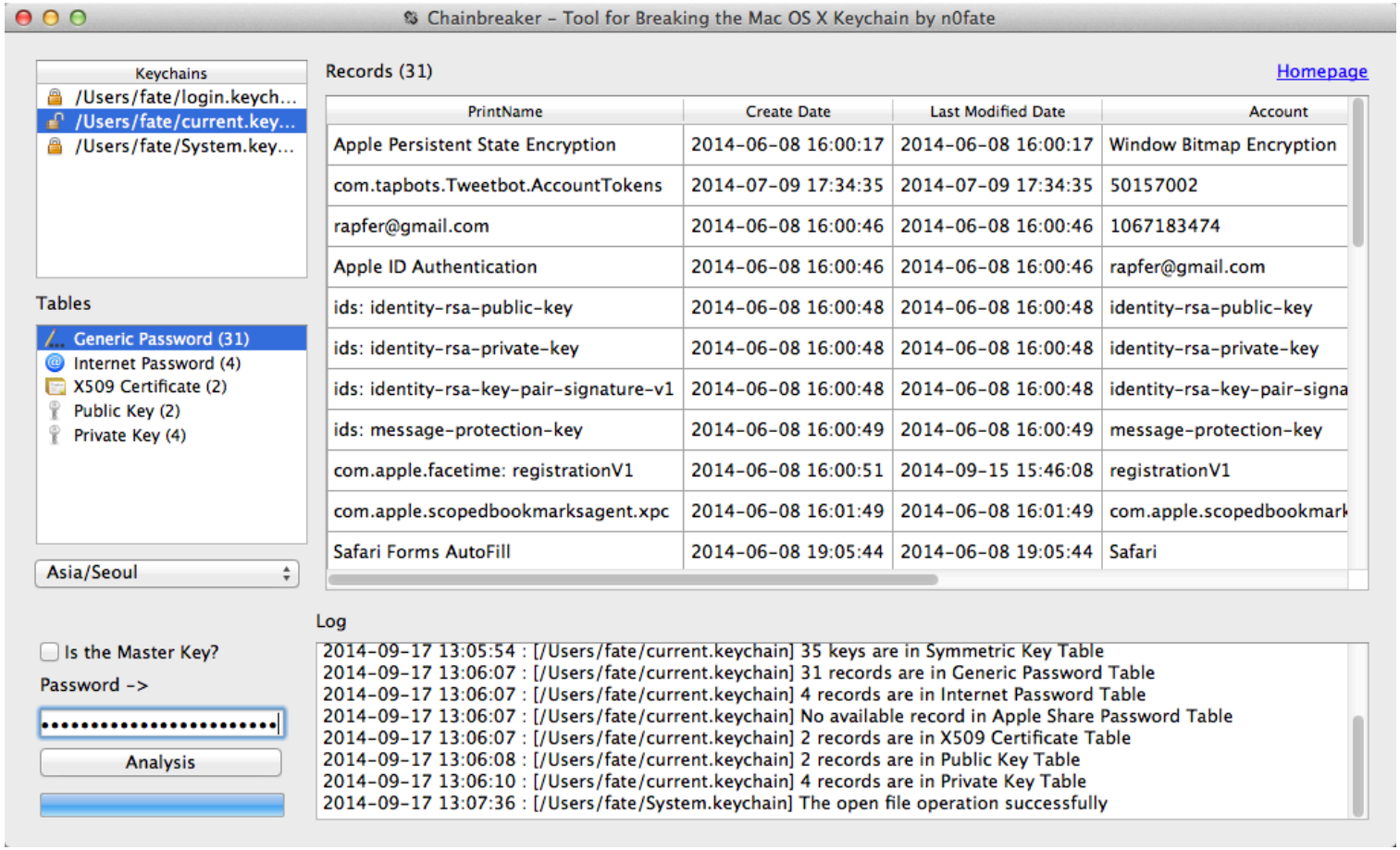
마스터키 추출 방법

- 파일 추출 (시스템 키체인 키만 추출 가능)
  - System Keychain Analysis. *http://forensic.n0fate.com/2014/09/system-keychain-analysis/*
  - Command : sudo xxd –ps /private/var/db/System.key | tr '₩n', '₩0'

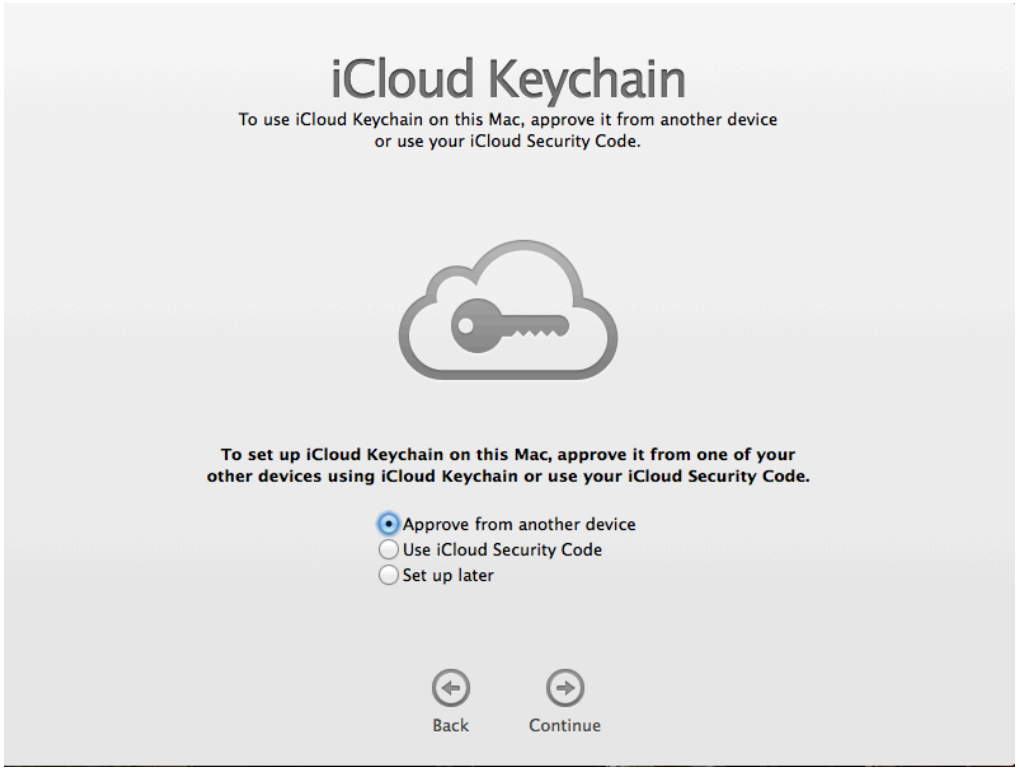
- 메모리 추출 (시스템/사용자 키체인 키 추출 가능)
  - volafox: decrypting the keychain file using volafox.
    - ✓ http://forensic.n0fate.com/2012/09/volafox-decrypting-the-keychain-file-using-volafox/
  - Command : volafox –i [MEMIMG] –o keychaindump

키체인 데이터베이스 분석

- chainbreaker (http://forensic.n0fate.com/tools/chainbreaker)



아이클라우드 키체인

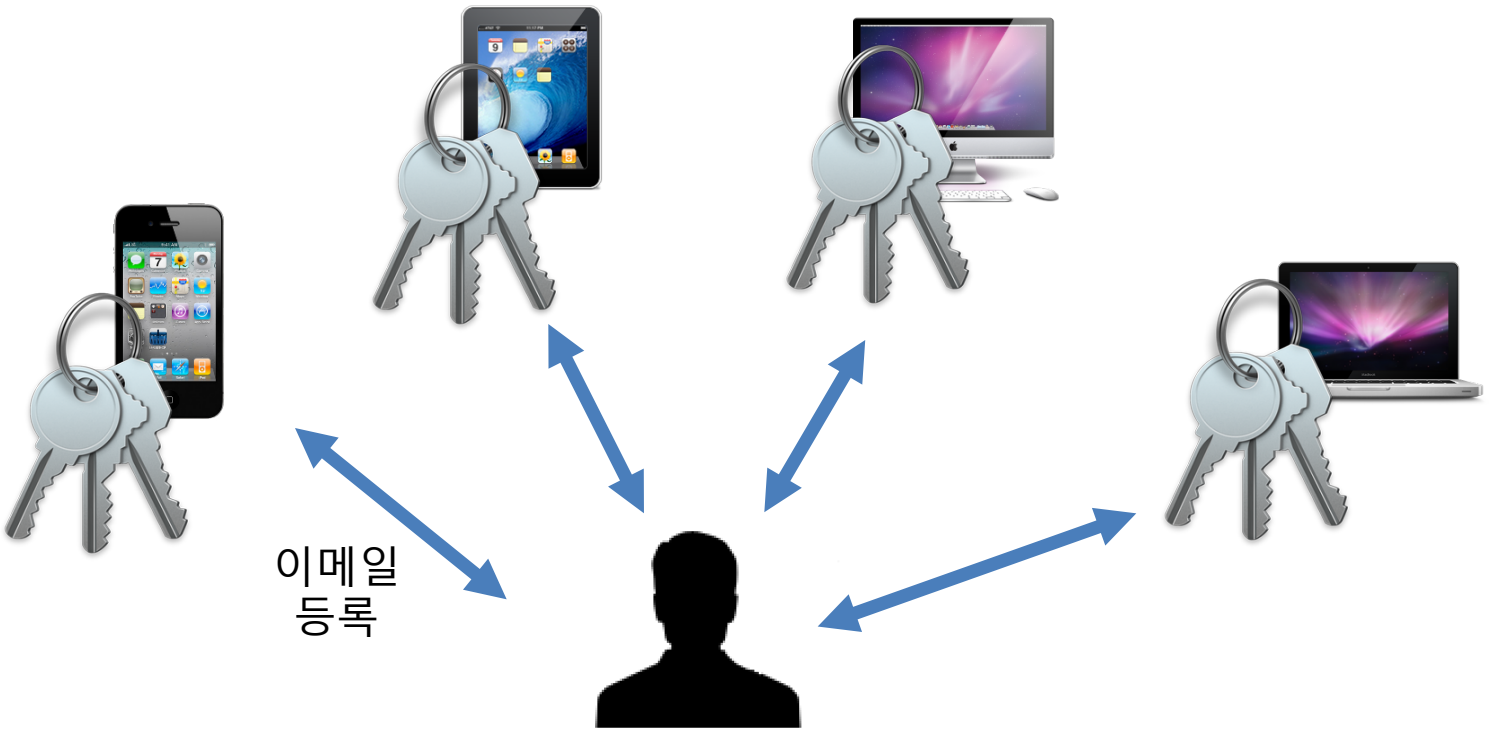

iCloud Keychain
To use iCloud Keychain on this Mac, approve it from another device or use your iCloud Security Code.
To set up iCloud Keychain on this Mac, approve it from one of your other devices using iCloud Keychain or use your iCloud Security Code.
Approve from another device
Use iCloud Security Code
Set up later
Back
Continue

아이클라우드 키체인

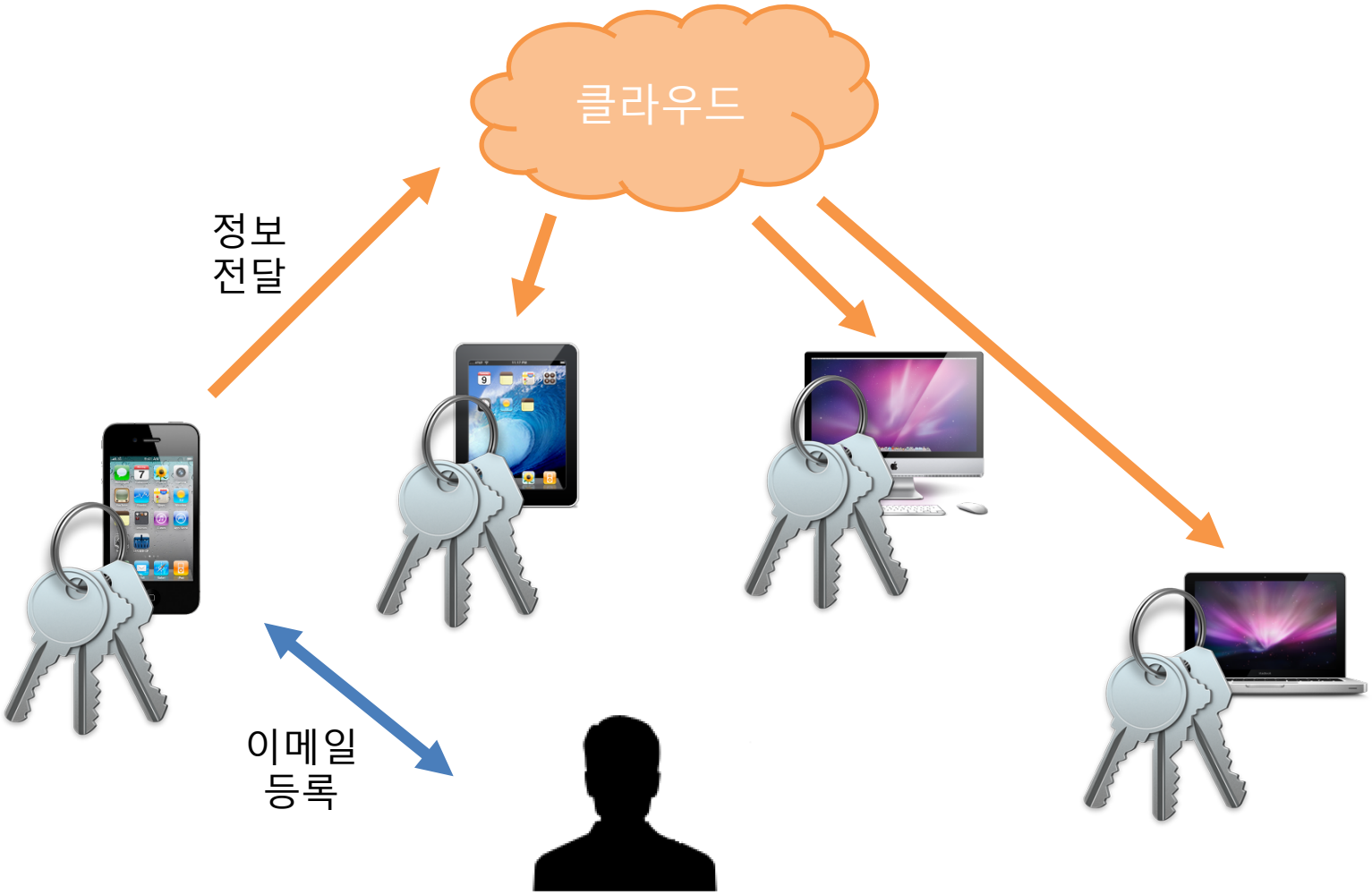
- **2013년 6월 OS X Mavericks(10.9) 공개**
  - 현재는 Yosemite (10.10, 2014년 6월 발표)이 최신 운영체제
  - 올해 6월에 El Capitan(엘 케피탄) 발표 (현재 베타테스트)

- **Mavericks 이 후의 변화 (iOS와의 통합 시작)**
  - App Nap (Mavericks) – 전원 관리 관련 기능으로 분석할 내용은 없음
  - Compressed Virtual Memory (Mavericks) **– 메모리 압축, volafox에서 분석 가능**
  - **iCloud Keychain (Mavericks)**
  - Continuity (Yosemite) – Forensic Insight를 통해 발표
  - iCloud Drive (Yosemite) – Sans Euro DF Summit 2013에서 아이클라우드 정보 수집 관련 발표

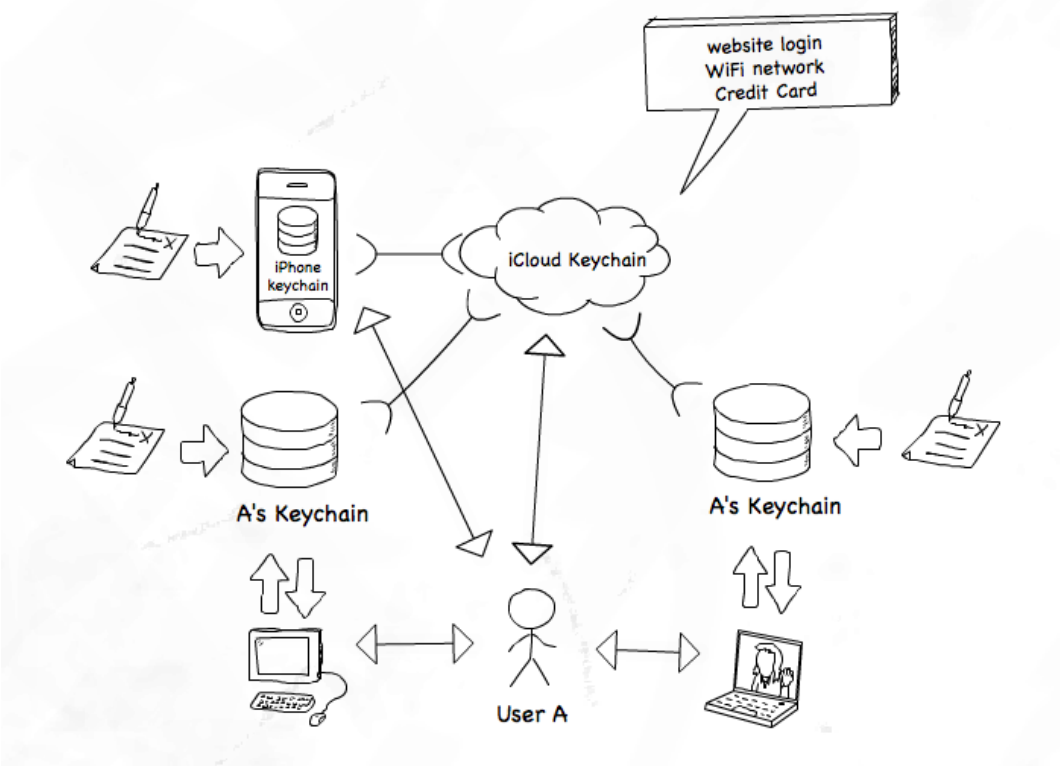
기존 키체인 운영



아이클라우드 키체인



아이클라우드 키체인



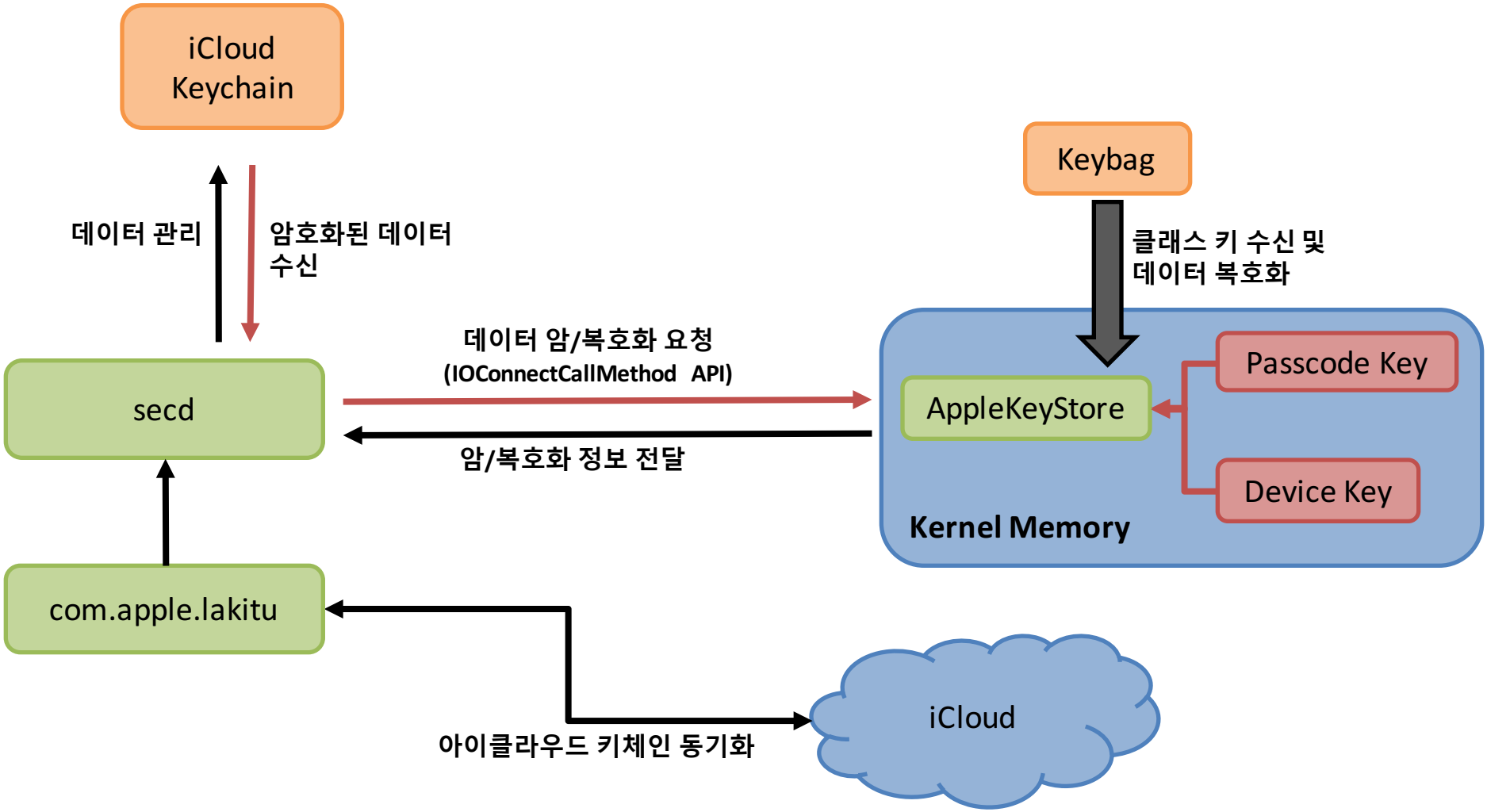
- 애플 장비 간의 연동성을 높이기 위한 기능
- 패스워드 관리 시스템인 키체인(Keychain)의 정보 공유 기능

아이클라우드 키체인 분석

- **아이클라우드 키체인**
  - ~/Library/Keychains/[UUID]/ 에 저장함.
    - ✓ [UUID] : 각 OS X 장비의 고유ID를 말하며, Mac에서는 **IOPlatformUUID**로 불림
    - ✓ # ioreg –lw0 | grep PlatformUUID
  - 분석을 위해 2개의 파일이 필요함
    - ✓ user.kb : Keybag. 아이클라우드 키체인의 데이터 암호화에 사용되는 클래스 키(Class Key) 저장
    - ✓ keychain-2.db : iCloud Keychain DB. SQLite 포맷으로 사용자 데이터를 암호화하여 보관

- **iCloud Keychain DB를 클래스 키로 암호화하는 방법은 iOS와 유사**

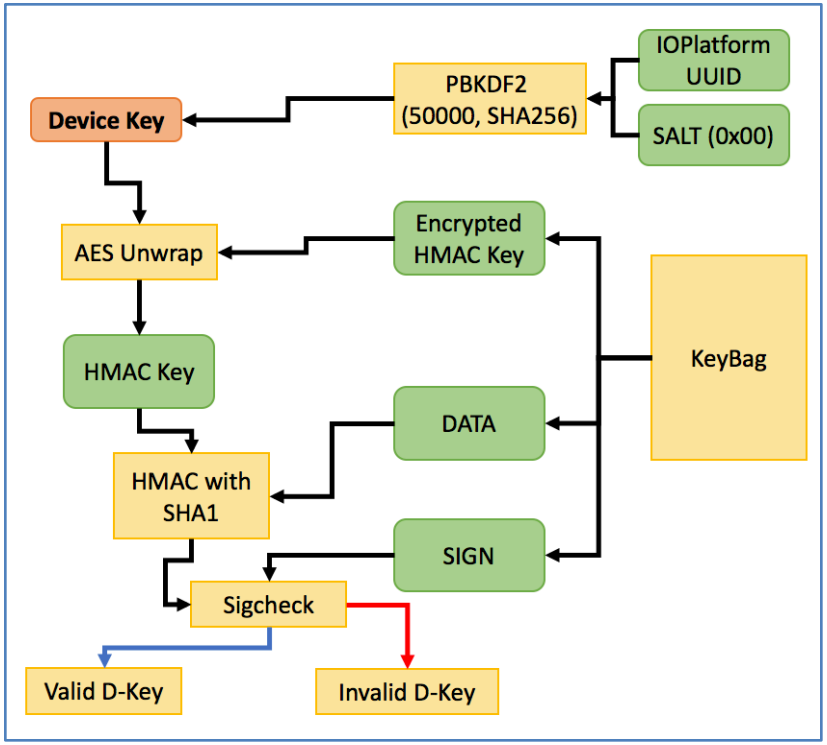
복호화 과정


iCloud
Keychain
데이터 관리
암호화된 데이터
수신
Keybag
클래스 키 수신 및
데이터 복호화
데이터 암/복호화 요청
(IOConnectCallMethod API)
secd
AppleKeyStore
Passcode Key
Device Key
Kernel Memory
암/복호화 정보 전달
com.apple.lakitu
iCloud
아이클라우드 키체인 동기화

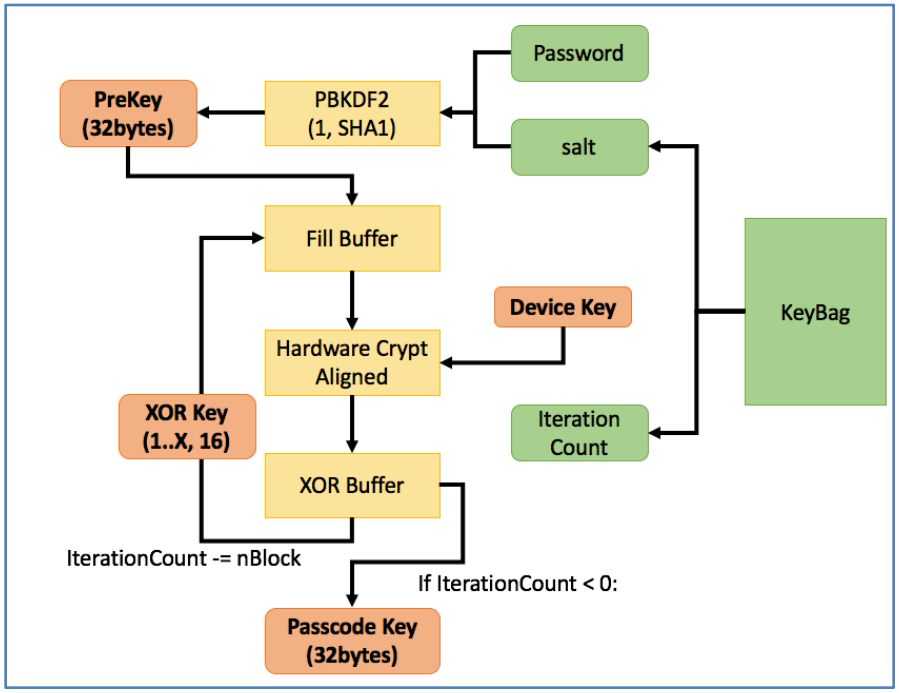
키백(Keybag) 분석

- **키백 관리 프로세스 : secd**
  - 아이클라우드 키체인 관리, 클라우드 동기화 지원 프로세스
  - 키백/아이클라우드 데이터베이스 해석 수행
  - 키백/아이클라우드 컨텐츠의 암/복호화 기능은 키백 데몬을 호출
- **키백 데몬 : AppleKeyStore.kext**
  - 디바이스 키(Device Key), 패스코드 키(Passcode Key)를 생성
    - ✓ 디바이스 키 생성 : **IOPlatformUUID**를 인자로 사용
    - ✓ 패스코드 키 생성 : 디바이스 키, User Password 필요, 특허(System and method for content protection based on a combination of a user pin and a device specific identifier, Apple. Inc, US20110252243)을 약간 변형
  - 전달받은 데이터를 해당 클래스 키로 암/복호화

키백(Keybag) 분석



Device Key Generation

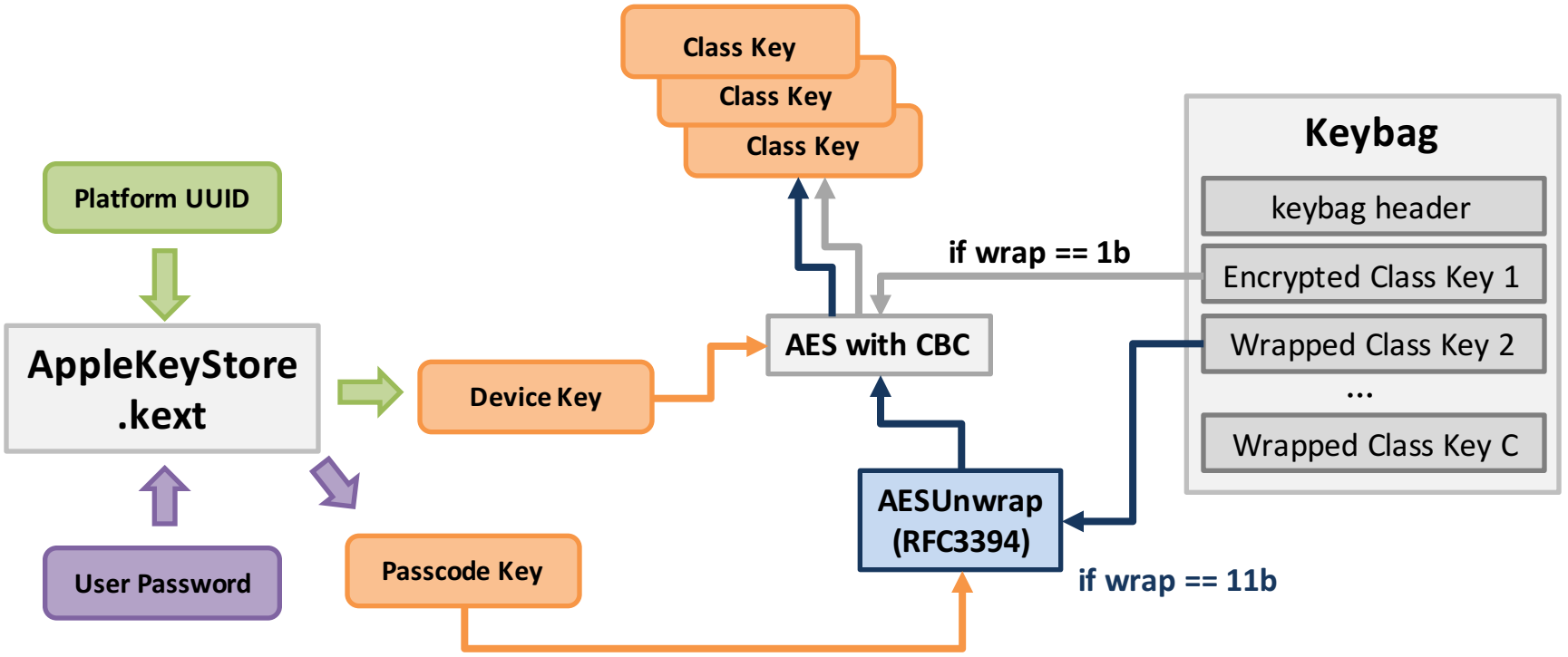


Passcode Key Generation

키백(Keybag) 분석

- iOS의 키백과 동일한 구조
  - Big-Endian, TLV(Type-Length-Value) 구조
  - 시스템 키백, 버전 4
- 키백 헤더 : Passcode Key **생성**과 Device Key **검증**에 사용
- 클래스 키
  - 키체인 레코드 및 파일 암호화에 사용되는 키
    - ✓ 파일 암호화 키 : 클래스 번호 1~5, OS X에서 사용되지 않음
    - ✓ 키체인 암호화 키 : 클래스 번호 6~12, 키체인 암호화에 사용
  - WRAP 설정에 따라 복호화 방법이 다름
    - ✓ WRAP이 1이면 **Device Key** 로 AES with CBC 복호화.
    - ✓ WRAP이 3이면, **Passcode Key**로 AESUnwrap(RFC3394)후, **Device Key**로 AES with CBC 복호화

키백(Keybag) 분석

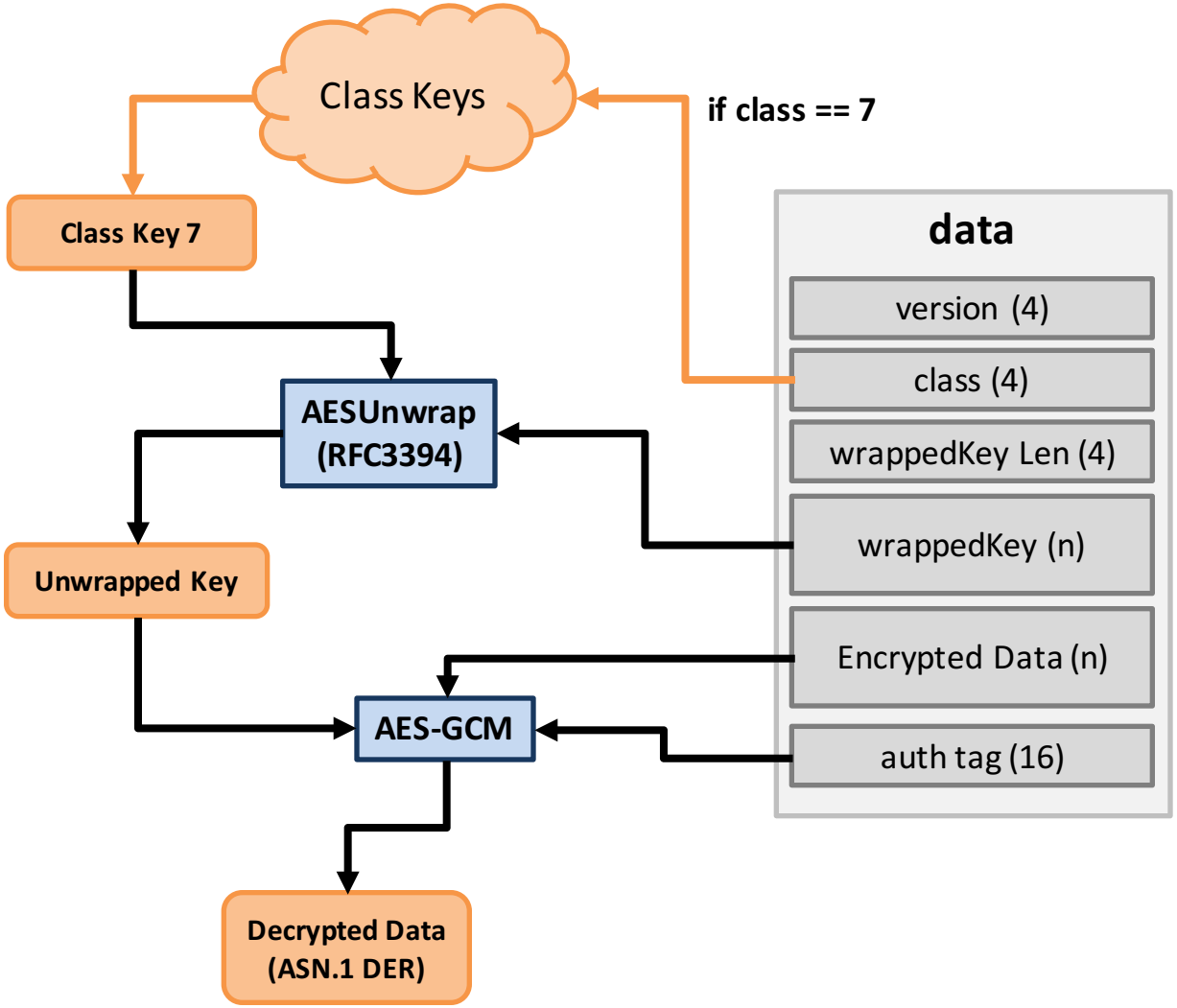

Class Key
Class Key
Class Key
Keybag
keybag header
Encrypted Class Key 1
Wrapped Class Key 2
...
Wrapped Class Key C
if wrap == 1b
Platform UUID
AppleKeyStore
.kext
Device Key
AES with CBC
AESUnwrap
(RFC3394)
if wrap == 11b
User Password
Passcode Key

키체인 데이터베이스 분석

- **SQLite3 파일 포맷**
  - Journal Mode : Write-Ahead Logging (WAL)
    - ✓ Portable Device일 수록 WAL를 먼저 분석하는 것이 좋음

- **데이터 관리**
  - 테이블 : genp, inet, keys, cert
  - 모든 컬럼의 데이터가 암호화되어 있음
    - ✓ 분석 결과 data 필드만 분석하면 모든 정보를 획득할 수 있음
  - 복호화된 데이터는 **ASN.1** DER(Distinguished Encoding Rules) 포맷을 가짐

키체인 데이터베이스 복호화



키체인 데이터베이스 분석

- 주요 컬럼(FourCharCode) 정보

컬럼	설명
cdat	Creation Date. 해당 레코드의 생성 시간을 말한다. 사용자가 처음으로 애플리케이션 로그인을 수행하거나, 특정 SSID에 최초 연결된 시간 정보를 가진다. **유닉스 타임(Unix Time)** 값을 가진다.
mdat	Modification Date. 해당 레코드의 최종 수정 시간을 말한다. 기 등록된 계정의 패스워드가 변경되는 경우 이 시간이 변경된다. **유닉스 타임(Unix Time)** 값을 가진다.
desc	Description. 해당 레코드에 대한 부가적인 설명을 기록한다. Wi-Fi 정보일 경우 `Airport network password`라는 값이 기록된다.
labl	Label. 말 그래도 표식이며, 파일이 삭제된 경우에는 해당 필드를 제거한다.
acct	Account. 계정 이름을 저장한다.
data	Data. **패스워드**와 같이 사용자가 숨기고자 하는 정보를 저장한다.
srvr	Server. 해당 기밀 정보가 사용되는 서버 주소를 저장한다.
sync	Sync. 해당 레코드를 아이클라우드 키체인으로 동기화할지를 Flag로 설정한다. 사용자가 등록하는 계정 정보는 기본으로 동기화가 활성화되어 있다.
tomb	Tomb. 해당 데이터를 더이상 사용하지 않는지를 Flag로 표시한다. Flag가 활성화(1)되어 있으면, 해당 정보를 더이상 사용하지 않는 것으로 간주한다.

아이클라우드 키체인 분석 도구

- iChainbreaker
  - 언어 : Python 2.7
  - 인자
    - ✓ 키체인 디렉터리 경로
    - ✓ 사용자 패스워드
    - ✓ 복호화된 정보를 저장할 SQLite DB 파일 이름 (Optional)
  - Chainbreaker와 통합될 예정

```
usage: iChainbreaker.py [-h] -p PATH -k KEY [-x EXPORTFILE]

Tool for iCloud Keychain Analysis by @n0fate

optional arguments:
  -h, --help            show this help message and exit
  -p PATH, --path PATH  iCloud Keychain Path(~/Library/Keychains/[UUID]/)
  -k KEY, --key KEY     User Password
  -x EXPORTFILE, --exportfile EXPORTFILE
                        Write a decrypted contents to SQLite file (optional)
```

키체인 데이터베이스 분석 (시간 정보)

- Unix-Time, GMT-0로 설정
  - cdat : 사용자가 최초 정보를 생성한 시점(신규 WiFi AP에 접속했을 경우)
  - mdat : 레코드에 모든 정보가 기록된 시점, 정보 수정 시점

- A 디바이스에서 새로운 레코드를 등록한 경우 B의 시간 정보 설정은?
  - A와 동일하게 설정됨. 즉, 시간 정보도 함께 공유함.

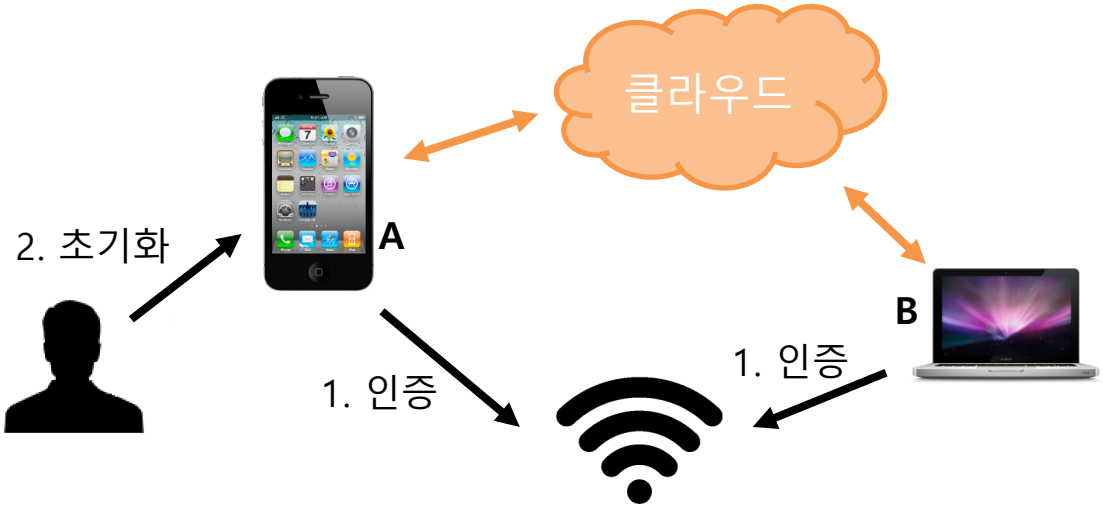
키체인 데이터베이스 분석 (삭제 정보)

- 예) WiFi 정보 A 장치에 등록하여 동기화된 상태에서 A의 WiFi 정보를 삭제하는 경우

- 삭제한 디바이스(A)
  - 키체인 접근(Keychain Access) : 나타나지 않음
  - 데이터베이스 분석 : data, labl, desc 필드 정보만 제거하고 tomb 필드를 1로 설정함
    - ✓ 최종 수정시간이 삭제한 시간으로 변경 (정보 삭제 시점, 해당 AP 최초 접근 시간 확인 가능)
- 연동된 다른 디바이스(B)도 동일함.

키체인 데이터베이스 분석 (삭제 정보) - 다중 디바이스 접속

- 예) A,B 두 장치에 각각 Wi-Fi를 접속 정보를 등록하고, A 장치만 초기화 한 경우
  - A 장치는 초기화되어 복구 불가



- B에는 그 정보를 유지함
  - B의 아이클라우드 키체인에서는 제거된 상태로 표현 (tomb flag => 1)
  - B의 시스템 키체인에는 정보를 유지

결론

- 사용자 기밀 정보를 담고 있는 저장소로 필히 분석이 필요함.
  - 웹브라우저로 접속한 사이트의 계정 정보 확보
  - 키체인 정보 외 숨기고 싶은 정보를 보안 노트 형태로 보관함.
  - SSH, VPN, Cloud 기능을 제공하는 소프트웨어의 대부분이 키체인을 활용함

- **아이클라우드 키체인 분석**
  - 사용자가 접속한 무선 네트워크 정보 수집에 효과적
    - ✓ 최초 접속 시간, 최종 패스워드 변경 시간 확인 가능
  - iOS 장비를 분석하지 않더라도 iOS에 저장한 기밀 정보 확인 가능
    - ✓ 이메일, 신용카드, 웹사이트 Form, 무선 AP 정보 등
  - **메모리에서 키를 추출하는 방법 연구 필요**

Question and Answer