모바일 소셜 앱의 IAP 컨텐츠 보호를 위한 메커니즘

조응준 홍충선*
경희대학교 컴퓨터공학과
ejcho@networking@khu.ac.kr, cshong@khu.ac.kr

An IAP Contents Protection Mechanism for Mobile Social Apps

Eung Jun Cho Choong Seon Hong*
Department of Computer Engineering, Kyung Hee University

요 약

IAP (In App Purchase) 컨텐츠는 스마트 기기의 앱 내부에서 진행되는 컨텐츠 구매로 최근 앱 스토어의 주요 수입원으로 떠오르고 있다. 많은 앱 개발사들이 사용자들이 쉽게 앱을 접할 수 있도록 앱 자체는 무료로 판매하고 주요한 기능이나 추가적인 기능을 IAP를 통해서만 구입하여 사용할 수 있도록 유도하고 있다. 이런 방식을 통해 사용자가 불법으로 앱을 다운로드 하더라도 추가적인 기능이나 컨텐츠를 이용하기 위해서는 IAP를 사용하여 대가를 지불하도록 유도하는 것이다. 그러나 앱 자체가 클라이언트 기능만을 수행하는 경우는 문제가 없지만 full-time으로 서버와 동기화를 해가며 동작하는 방식이 아닌 앱의 경우 IAP를 불법적으로 해킹하여 취득하는 것이 가능하다. 본 논문에서는 이러한 불법적인 IAP 컨텐츠 획득을 방지하기 위하여 full-time으로 서버와 동기화를 하지 않으면서도 IAP 컨텐츠를 보호하기 위한 메커니즘을 제안한다.

1. 서 론

애플의 아이폰의 등장과 함께 앱 스토어는 그동안 소프트웨어가 유통되던 생태계를 완전히 바꿔놓았다. 특히 판매 금액의 70%를 개발자에게 배분해주는 정책으로 수많은 개발자들이 앱 스토어에 앱을 등록하였다. 2012년 4월 애플의 앱 스토어 기준으로 약 79만개의 앱이 등록되어있으며 항목별로는 게임이 17%로 가장 높은 비율을 차지하고 있으며 그다음이 책, 엔터테인먼트, 교육분야의 앱이 차지하고 있다[1]. 2011년 8월 정보통신산업진흥원에서 발간한 최신 IT 동향 중 '모바일 플랫폼 중심으로 변화하는 게임 산업'[2]에서는 애플 앱 스토어의 상위 100대 게임의 매출의 비중 중 65%가 IAP를 통해 이루어지는 것으로 나타나 있다. 초창기 앱의 판매 금액이 주요 수입원이었던 구조에서 IAP가 큰 수입원으로 떠오르고 있다. 이런 서비스 형태는 앱의 불법적인 다운으로 인한 손해를 감소시키고 사용자들에게 앱을 보다 효율적으로 광고를 할 수 있어 이상적인 비즈니스 모델로 평가되고 있다.

그러나 몇몇 앱에서는 이런 IAP 컨텐츠를 간단한 해킹을 통하여 획득하고 그 권리를 온라인 상에서 행사할 수 있는 것으로 나타나 피해가 우려되고 있다. 실제 안드로이드 뿐만이 아니라 애플의 iOS 계열의 장치의 데이터를 아무런 위협 없이 수정할 수 있는 프로그램도 존재한다[3, 4]. 특히 클라이언트 기반의 앱에서 이런 문제가 심각한 상태이며 이는 개발자의 수입에 직접적인 영향을 주고 있는 것으로 그 심각성이 매우 높다고 할 수 있다. 이런 문제를 해결하기 위하여 본 논문에서는 서버에 접속하지 않은 상태에서도 플레이가 가능하며 IAP 컨텐츠를 보호할 수 있는 메커니즘을 제안하고자 한다.

2. IAP를 사용하는 앱의 유형 분석 및 문제점

IAP를 사용하는 게임 앱의 유형은 크게 두 가지로 구분이 된다. 하나는 추가적인 컨텐츠를 사용할 수 있도록 허가해주는 것이고 다른 하나는 게임 내에서 사용가능한 컨텐츠를 구매하는 것이다. 여기서 문제가 되는 것은 게임 내에서 사용 가능한 컨텐츠를 구입하는 경우가 된다. 최근 IAP기반의 무료 게임의 경우 대부분이 두 가지의 화폐 시스템을 두고 있다. 하나는 게임 내에서 쉽게 획득이 가능한 화폐이고 다른 하나는 게임 내에서 어렵게 획득 가능하거나 IAP를 통해 구매할 수 있는 화폐이다. 현재 애플의 한국 앱 스토어 매출 순위 상위 10개의 앱을 분석해보면 앱 내 최고 IAP 컨텐츠는 모두 앱내에서 사용할 수 있는 화폐로 나타나고 있다. 이처럼 사용자들이 실제 돈을 주고 구입한 컨텐츠가 손쉽게 해킹이 된다

본 연구는 지식경제부 및 한국산업평가관리원의 산업원천기술개발사업의 일환으로 수행되었음. [과제관리번호 : KI002164, 센싱기반 감성서비스 모바일 단말 기술개발] *Dr. CS Hong is corresponding author.

면 사용자들의 구매 욕구를 감소시킬 뿐만 아니라 돈을 주고 컨텐츠를 구매한 사용자들에게 상대적인 박탈감을 줄 수 있다.

IAP 컨텐츠를 제공하는 앱은 서버 기반과 비 서버기반으로 구분할 수 있다. 유료 아이템을 구매하기 위해서는 반드시 앱 스토어 계정을 통해 결제가 이루어져 이 과정은 보안상에 문제가 없지만 이렇게 구매된 아이템이 사용되는 부분은 앱 개발자의 역량에 맡기고 있는 것이다. 이 부분에서 항상 온라인 서버에 접속을 하여 진행되는 앱의 경우에는 큰 문제가 없지만 오프라인 상에서도 플레이가 가능한 게임은 문제가 발생한다. 즉, 모든 사용자의 데이터가 사용자 기기에 저장되어 있고 게임 내 컨텐츠 구입도 로컬에서 이루어지는 경우 사용자가 임의로 데이터 조작을 통해 IAP 컨텐츠를 획득할 수 있다. 모든 컨텐츠가 온라인 서버를 두고 인증이 이루어지는 것이 가장 이상적인 방법이지만 정확한 수익을 예측할 수 없는 IAP 기반 앱의 특성상 서버를 충분히 확장하는 것도 힘든 일이다. 따라서 사용자가 서버에 접속하지 않더라도 사용이 가능하며 임의로 해킹이 불가능한 IAP 컨텐츠를 보호할 수 있는 기술이 필요하다.

3. 비 서버 기반의 IAP 컨텐츠 보호 메커니즘

본 논문에서는 사용자가 통신이 되지 않는 상태에서도 앱과 사전에 구매한 IAP 컨텐츠를 사용할 수 있는 보호 메커니즘을 제안하고자 한다. IAP 컨텐츠를 보호하기위해 필요한 조건은 다음과 같다.

- 서버와 접속되지 않은 상태에서 사용되거나 획득한 컨텐츠의 무결성 보장
- 사용자에 의해 조작된 컨텐츠에 대한 탐지 가능

위 조건을 만족하기 위해 본 논문에서는 공개키 기반의 서명 기법을 사용하여 컨텐츠의 무결성을 보장하고자 한다. 서버에 접속되지 않은 상태에서 사용자의 행위에 대한 무결성을 보장하기위해서는 우선 무결성을 보장할 대상의 범위를 한정해야 한다. 본 논문에서는 IAP로 구입 가능한 컨텐츠 및 해당 컨텐츠를 소모하는 행위, 그리고 해당 컨텐츠를 앱 내부에서 생산하는 행위를 그 대상으로 한다.

모바일 소셜 게임에서 IAP로 구매한 화폐의 사용은 크게 세 가지로 구분된다. 첫 번째는 특정 아이템구매, 두 번째는 권한 획득, 마지막으로 시간 제약해제이다. 컨텐츠 인증을 위해 사용자가 서버에 접속하지 않은 상태에서 플레이 시 사용자의 행동에 대한 로그를 기록한다. 해당 로그를 기반으로 다음번 서버에 접속을 할 때 서버에 저장되어 있던 이전 정보와 클라이언트에 저장되어 있는 정보를 비교, 로그에 대한 인증을 통하여 컨텐츠에 임의적인 조작이 없었는지를 검사한다. 다음 그림은 컨텐츠의 무결성 검증을 위한 일반적인 절차이다.

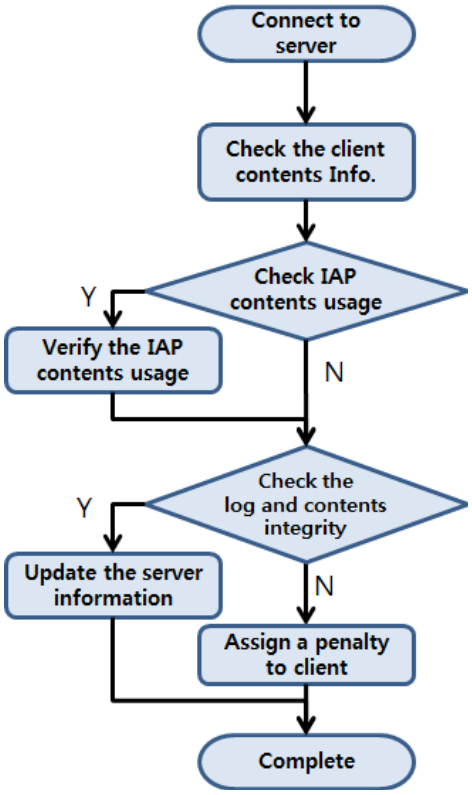

그림 1. 컨텐츠의 무결성 검증을 위한 절차

4. IAP 컨텐츠 보호 메커니즘의 동작 예시

제안된 메커니즘의 구체적인 설명을 위하여 다음과 같은 게임 시나리오를 가정한다.

현재 레벨이 5인 사용자는 일반 게임머니를 1000개를 가지고 있고 IAP 컨텐츠인 유료 캐쉬를 50개 가지고 있다. 본 게임에는 일반 게임머니 획득을 위해 다음과 같은 플레이가 가능하다.

표 1. 사용자가 선택가능한 행위의 조건 및 보상

	A	B	C	D	E
필요시간	20분	40분	50분	80분	150분
보상	50	80	100	140	210
조건레벨	-	2	4	10	15

이 사용자가 같은 시간대에 실행할 수 있는 행위의 수는 3개로 제한되어 있다고 가정한다. 정상적인 사용자가 서버에 접속하지 않은 상태에서 B라는 행위를 2번 선택하

고 좀 더 편한 진행을 위해 유료 화폐를 이용하여 D의 조건을 해제한 뒤(조건을 해제하기 위해서는 해당 조건 레벨과 현재 레벨의 차이만큼의 유료 캐쉬가 필요) D라는 행위를 선택하였다. 그리고 45분이 지난 시점에서 서버에 접속을 하였다. 이때 정상적인 로그는 다음과 같이 나타날 수 있다.

```
000224 : Do B H(DB+000224+UID)
000241 : Do B H(DB+000241+UID)
000270 : Unlock D H(UD+000270+UID)
000275 : Do D H(DD+000275+UID)
024224 : Get B H(GB+024224+UID)
024241 : Get B H(GB+024241+UID)
----------------------------------------
H() : Hash function
UID : Unique ID of Device
```

위의 로그는 예시로 영문 및 10진수로 기록이 되어 있지만 기기에 효율적으로 저장하기 위해 비트 형태로 정보가 정의될 수 있다. 로그는 해당 로그가 기록되는 시간이 제일 먼저 기록되며 사용자 행위의 종류(Do, Unlock, Get)이 위치하고 앱 내의 컨텐츠 유형(A, B, C, D, E)가 위치하게 된다. 해당 로그의 재사용 및 임의 조작을 방지하기 위해 각 로그 마다 해쉬함수를 이용한 인증 코드를 부착한다. 해당 인증코드는 사용자 장치의 고유 ID와 시간이 포함되어 무결성 입증에 사용된다.

45분이 지난 시점에 서버에 접속하였을 때 사용자는 1160개의 게임 머니와 45개의 유료 화폐를 가지고 있었다. 이를 입증하는 절차는 다음과 같다.

```
1. 로그 정보 자체의 무결성 검사
   (해쉬코드 연산 비교)
2. 클라이언트의 게임 머니 및 유료 캐쉬, 허용된 아이템 확인
3. 사용된 유료 캐쉬 검증
   000270 : Unlock D H
   D 컨텐츠의 요구 레벨 - 현재 레벨 = 5
4. 획득한 게임 머니 계산
   024224 : 80      024241 : 80
   160 획득
5. 시간 무결성 검증
   현재 시간 - 마지막 저장 시간 ≧ 로그의 마지막 시간
6. 유료 캐쉬 및 게임 머니의 무결성 검사
7. 검증 종료
```

이와 같은 시나리오 상에서는 사용자가 임의로 클라이언트 상의 유료 캐쉬의 값이나 게임 머니의 값을 수정하더라도 이를 탐지할 수 있다. 그리고 사용자가 획득한 골드에 대한 로그 분석이 시간 정보와 함께 기록되기 때문에 사용자가 임의로 로그 정보를 복사할 수도 없다. 또한 로그 무결성 검증에 사용되는 사용자의 UID로 인해 사용자가 다른 사용자의 로그 정보를 악용하는 것을 방지할 수 있다.

5. 결론

본 논문에서 제안한 메커니즘은 서버에 접속하지 않은 사용자가 IAP를 통해 구매한 컨텐츠를 사용하고 정상적으로 앱을 사용할 수 있는 메커니즘을 제안하였다. 이 메커니즘을 통해 사용자의 악의적인 컨텐츠 조작을 막을 수 있고 나아가 IAP 컨텐츠의 보호를 통해 개발사의 이익을 보전할 수 있다. 또한 일시적인 네트워크 혼잡이나 서버의 문제로 접속이 원활하지 않더라도 사용자는 자신이 구매한 앱을 사용할 수 있도록 지원할 수 있다.

참고문헌

[1] Appstore Metric, http://148apps.biz/app-store-metrics/

[2] 모바일 플랫폼 중심으로 변화하는 게임 산업, 정보통신산업진흥원 주간기술동향 1509호, 최신 IT 동향, 2011년 8월 19일

[3] i-FunBox, http://www.i-funbox.com/

[4] iExplorer, http://www.macroplant.com/iexplorer/