모바일 클라우드 서비스 환경에서 단말 내 키로깅 위협 방지를 위한 가상키보드 제공방안

안성환*, 한선희*, 정성민*, 정태명**
성균관대학교 전자전기컴퓨터공학과*
성균관대학교 정보통신대학**
e-mail : {shahn, shhan, smjung}@imtl.skku.ac.kr*, tmchung@ece.skku.ac.kr**

The Idea of Virtual Keyboard to Prevent Device Keylogging in Mobile Cloud Service

Sung-Hwan Ahn*, Sun-Hee Han*,Sung-Min Jung*, Tai-Myoung Chung**
Dept. Electrical and Computer Engineering, Sungkyunkwan Univ.*
College of Information and Communication Engineering, Sungkyunkwan Univ.**

요 약

최근 많은 스마트 디바이스의 보급으로 언제 어디서든지 모바일 네트워크를 통해 인터넷을 사용할 수 있게 되었으며, 단말이 가지는 자원 및 컴퓨팅 파워의 한계에 따라 모바일 클라우드 서비스에 대한 관심이 폭발적으로 증가하고 있다. 하지만 모바일 클라우드 서비스는 그 환경에 따라 사용자 단말에서 나타나는 보안위협과 클라우드 환경에서의 보안위협이 복합적으로 나타나게 된다. 모바일 클라우드 환경에서의 보안위협 중 사용자 단말 영역에서의 키로깅 공격으로부터 사용자 입력정보를 보호하기 위한 기존의 가상키보드를 비교·분석하였다. 본 논문에서는 기존에 사용되고 있는 가상키보드의 확률적 분석을 통한 키 유추 가능성을 보완하기 위해 보안성이 강화된 새로운 형태의 가상키보드를 제안한다.

1. 서론

클라우드 컴퓨팅은 인터넷을 통해 물리적으로 다른 위치에 존재하는 각종 컴퓨터 자원(네트워크, 서버, 스토리지, 소프트웨어, 서비스 등)을 이용자가 필요한 만큼 빌려서 사용하고, 부하 발생에 따라 실시간 확장성을 보장 받을 수 있는 컴퓨팅 방법이다[1]. 특히, 최근 언제 어디서나 인터넷에 접속하여 서비스를 이용할 수 있는 스마트폰, 태블릿PC 등 스마트 디바이스의 이용이 급격하게 증가함에 따라 처리성능, 저장공간 등의 자원이 제한적인 스마트 디바이스의 한계를 극복하며 지속적인 서비스를 제공할 수 있는 모바일 클라우드 서비스가 주목 받고 있다.

기존의 컴퓨팅 환경에서는 이용자가 직접 데이터 및 컴퓨팅 자원들에 대해 관리를 해야 했지만 모바일 클라우드 서비스 환경에서는 데이터 및 컴퓨팅 자원들을 클라우드 서비스 제공자에게 위탁하여 통합적으로 관리하고 스마트 디바이스를 통해 모바일 네트워크 환경에서 실시간 서비스를 제공 받을 수 있다. 이런 특징에 따라 스마트 디바이스의 분실로 인한 정보유출, 가상화 취약성을 이용한 공격, 자원 집중이 되어있는 상황에서 서비스 거부 공격으로 인한 장애, 스마트 디바이스 키로깅을 통한 사용자 입력정보 탈취 등 모바일 및 클라우드 환경에서의 보안위협이 복합적으로 나타나게 되어 이에 대한 보안이 새로운 관심사로 나타나고 있다.

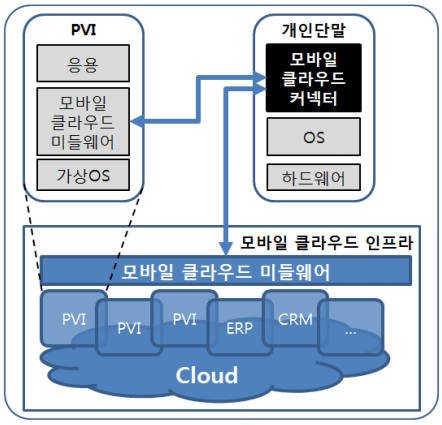
본 논문에서는 많은 보안위협 중 사용자 단말 영역에서의 보안위협을 알아보고 특히 키로깅 공격을 통해 사용자 입력정보 탈취를 방지하는 가상키보드에 대해서 다루고자 한다. 새로운 가상키보드 제안을 위하여 관련연구로 2장에서 모바일 클라우드 서비스와 사용자 단말 영역에서의 보안위협을 살펴보고, 사용자 단말 영역에서의 보안 요구사항을 알아본다. 이후 3장에서 기존에 알려진 가상키보드의 대표적인 형태에 대해서 비교 분석한 후 4장에서 키로깅에 대해 더욱 안전한 가상키보드에 대해서 제안한다. 5장에서는 결론 및 향후 연구에 대해 설명한다.

2. 관련연구

2.1 모바일 클라우드 서비스

모바일 클라우드 서비스는 스마트 디바이스에서 처리해야 할 작업 및 데이터 저장의 일부를 클라우드 내 가상 단말에 접속하여 클라우드 컴퓨팅 환경에서 처리를 하고 스마트 디바이스에서 처리결과를 보여주는 애플리케이션이다[2].

(그림 1)은 모바일 클라우드의 전체 아키텍처를 나타낸다. 모바일 클라우드 인프라는 모바일 클라우드 미들웨어, PVI(Private Virtual Instance : 가상 단말), 모바일 클라우드를 전체적으로 관리하는 관리시스템 등으로 나눌 수 있다[3].



(그림 1) 모바일 클라우드 아키텍처

모바일 클라우드 서비스에서 사용자는 모바일 클라우드 커넥터를 이용해 모바일 클라우드 인프라의 가상 단말로 접속하게 되며, 데이터의 전달은 모바일 클라우드 미들웨어와 모바일 클라우드 커넥터 사이에 일어나게 된다. 사용자가 모바일 클라우드 서비스를 이용할 때 단말을 통해 입력하는 중요정보들은 타인에게 노출되지 않도록 보호되어야 하며, 모바일 클라우드 서비스에서도 기존 모바일 서비스와 마찬가지로 사용자 단말 영역에서 사용자 입력정보를 보호하기 위한 가상키보드가 필요하다.

2.2 사용자 단말 영역에서 보안위협과 보안요구사항

한국정보통신기술협회(TTA:Telecommunications Technology Association)는 모바일에서 사용되는 가상키보드의 주요 보안 위협에 대해 네트워크 계층, 가상키보드 모듈, 단말 영역 환경으로 구분했고 그 중 사용자 단말 영역 환경에 의한 입력정보 절취 또는 위·변조에 대해 <표 1>과 같이 정의했다[4].

<표 1> 단말 영역 환경에서의 보안위협

보안위협	세 부 내 용
메모리 해킹	애플리케이션 동작에 필요한 메모리 정보를 열람하여 위·변조 할 수 있는 위협을 가하는 행위
화면 캡쳐 데이터 노출	가상키보드에서 입력하는 내용이 사용자 모니터에 표시됨으로써 가상키보드 이용 시 공격자가 가상키보드 화면 내용을 가로채는 행위
키보드 이벤트 내용 절취	운영체제 상에서 처리하는 키보드 이벤트를 통해 가상키보드에 입력하는 사용자 입력 정보를 스니핑하는 행위

또한, TTA는 <표 1>에 정의된 보안위협에 대응할 수 있도록 사용자의 단말 영역에서 가상키보드에 대한 보안요구사항을 보안프로그램 영역, 프로세스 영역, 데이터 전송영역으로 나누었고 프로세스 영역에서 제시한 보안 요구사항은 다음과 같다.

- 보안 키보드 모듈 영역에 할당된 메모리 영역에서 비밀정보에 대한 유출이 없어야 한다.
- 가상키보드 이용 시 키보드 메시지 후킹 위협에 안전하게 보호되어야 한다.

메모리영역에서의 비밀정보는 사용자 입력정보를 공인된 암호화 방식을 통해 암호화 하여 전달하게 되어 공격자가 메모리정보를 열람하여 정보를 취득하더라도 복호화를 할 수 없기 때문에 내용을 알아볼 수 없다.

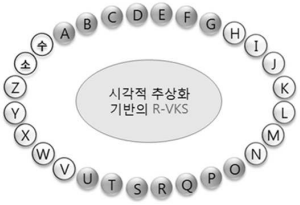
모바일 단말에서는 메시지 후킹 혹은 키로깅으로 알려진 공격방식으로 인해 탈취된 가상키보드의 좌표를 통해 입력키를 알아내는 위협에 대비해야 한다.

3. 기존의 가상키보드

기존에 알려진 가상키보드의 형태는 첫째, (그림 2)와 같이 가상키보드에 배치된 키의 위치를 무작위하게 바꾸는 방법과 둘째, (그림 3)과 같이 가상키보드 내에 임의의 공백을 삽입하여 키를 배치하는 방법으로 키로깅을 통해 키에 대한 좌표를 알아내더라도 해당 좌표의 입력 값에 대해 정확히 알 수 없도록 만드는 방법이다. 셋째, (그림 4)와 같이 가상키보드의 형태를 기존에 사용하는 키보드의 배치와 다른 형태로 만들고 한 키가 선택되면 회전되어 어떤 키가 선택되었는지 알 수 없도록 만드는 방법이 대표적이다[5].

(그림 2) 키 배치를 랜덤하게 바꾸는 방법

(그림 3) 키 사이에 랜덤한 공백을 삽입하는 방법



(그림 4) 키보드의 모양을 변형하는 방법[5]

(그림 2)와 (그림 4)의 방법은 키의 위치가 임의로 섞여 키 배치의 무작위성이 높고, 공격자가 좌표 획득 시 대응되

는 키의 유추가능성이 낮은 장점이 있으나 기존에 사용되는 키보드 배치와는 전혀 다른 키 배치를 가지게 되므로 친밀성이 낮고 키가 무작위로 섞이게 되어 선택하고자 하는 키를 찾아야하는 불편을 초래하게 되어 사용자 편의성이 낮은 단점이 있다.

(그림 3)의 경우 키 배치는 기존의 PC키보드와 같아 사용자가 쉽게 키를 선택할 수 있어 편의성과 친밀성은 높지만 키의 무작위성이 적어 다른 두 방법보다 입력키를 유추하기가 쉬운 단점이 있다.

기존에 알려진 대표적인 가상키보드에 대한 특징들에 대해 <표 2>와 같이 나타낼 수 있다.

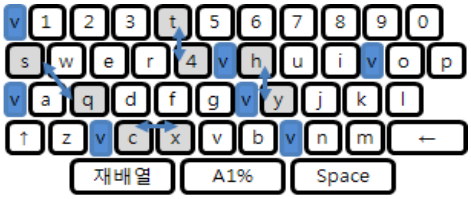
<표 2> 기존 가상키보드의 특징

가상키보드	무작위성	친밀성	편의성	유추가능성
그림 2	높음	높음	낮음	낮음
그림 3	낮음	높음	높음	높음
그림 4	높음	낮음	낮음	낮음

기존의 모바일 서비스는 모바일 결제, 뱅킹, 증권거래 이용 시에 알려진 가상키보드 방법 중 키보드의 각 행에 임의의 공백을 삽입하는 방법(그림 2)을 이용하고 있다. 하지만, 이런 가상키보드는 키로깅 공격을 통한 가상키보드의 X,Y 좌표를 얻어 확률적 분석을 통해 키 유추가 가능하다는 사실이 알려져 있다. 특히 공격자가 입력되는 좌표를 지속적으로 감시하는 경우에는 이에 대응하는 키에 대한 유추한 결과 95% 이상 일치한다[6]. 따라서 기존의 가상키보드보다 사용자 편의성을 최소한으로 훼손하는 범위에서 키 배열의 무작위성을 증가시키는 더욱 안전한 가상키보드가 필요하다.

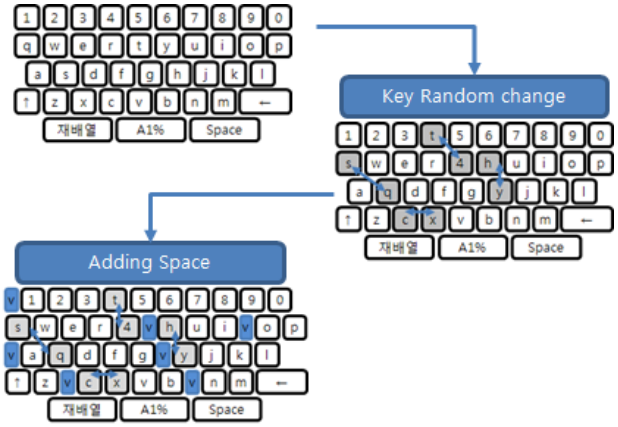
4. 향상된 보안성을 가지는 가상키보드 제안

본 논문에서는 기존 가상키보드의 문제점을 보완할 수 있는 새로운 형태의 가상키보드를 다음과 같이 제안하고자 한다.



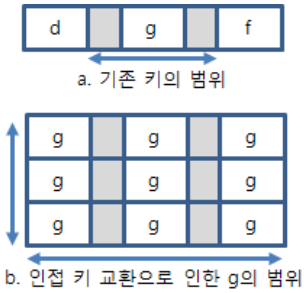
(그림 6) 제안 가상키보드

(그림 6)의 가상키보드는 기존의 공백을 삽입하여 키의 위치가 좌우로 이동 되는 형태의 가상키보드를 기반으로 키를 인접한 키와 무작위로 교환하는 방식을 추가함으로써 보안강도를 높인 가상키보드이다.



(그림 7) 가상키보드 생성과정

(그림 7)은 제안된 방식의 가상키보드의 생성과정을 나타낸다. 기본 키보드 형태에서 키 위치의 무작위성을 높이기 위해 먼저 전체 가상키보드위에서 임의의 개수의 키를 선택하고 선택된 키의 인접 키 중 하나와 무작위하게 자리를 교환한다. 교환된 자리는 사용자가 알아보기 쉽게 하기위해 음영 및 키 색상 변화로 표시 한다. 이후 한 행에 임의의 개수의 공백을 추가하여 가상키보드를 생성한다.

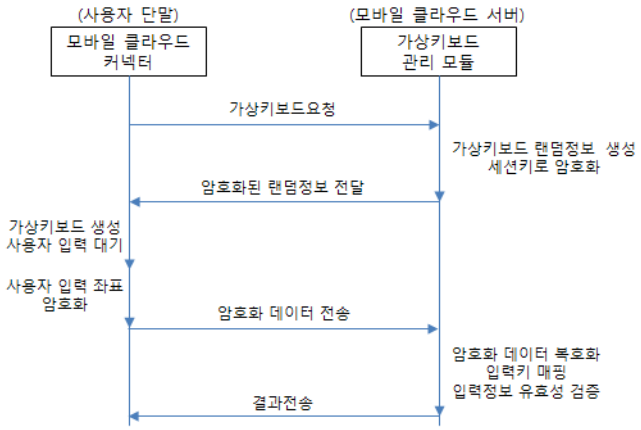


(그림 8) 기존 가상키보드와 제안방식의 비교

보안을 위한 어떠한 방법도 적용되지 않은 가상키보드에서 중앙에 위치하는 키(g)에 대하여 임의의 공간이 키 크기의 절반이고 가상키보드의 각 행에 최대 2개의 임의의 공백 추가 하게 될 경우 키(g)가 존재할 수 있는 공간의 범위가 기존의 방법은 a와 같고 제안된 방법을 사용한 경우에는 키(g)가 존재할 수 있는 공간의 범위가 b로 확장되는 것을 알 수 있다.

따라서 제안된 방법을 사용하게 되면 공격자가 키로깅으로 얻어진 좌표를 확률적 분석을 하게 되더라도 키가 존재할 수 있는 공간이 확장되고, 무작위하게 위치하기 때문에 키 유추가 어려워져 기존 가상키보드 방법이 가졌던 문제점을 보완할 수 있게 된다.

또한 가상키보드 외각의 키 즉, '1','z','m','0' 는 기존의 가상키보드 방법에서 이동범위가 중앙에 위치한 다른 키보다 좁아 확률적 분석에 의해 더 쉽게 유추할 수 있었지만 제안방식을 사용하게 되면 키 공간 확장이 되어 유추하기 어렵게 된다[6].



(그림 9) 가상키보드 흐름도

(그림 9)는 가상키보드의 전체적인 흐름을 나타낸다. 가상키보드 생성에 앞서 세션키는 미리 안전하게 나누어가진 상태이고, 사용자 단말과 서버간의 통신은 안전하다고 가정한다.

먼저 사용자 단말의 모바일 클라우드 커넥터에서 가상키보드가 요청되면 관리모듈은 교환될 키의 개수선택을 위한 정보, 인접키 선택을 위한 정보, 공백을 삽입하기 위한 정보의 랜덤정보를 생성하고 미리 안전하게 나누어가진 세션키로 암호화 하여 전달한다. 사용자 단말은 서버로부터 전송받은 랜덤한 정보들을 이용해 가상키보드를 생성하고 사용자의 입력을 대기하고, 사용자가 디바이스를 터치하게 되면 이벤트는 암호화 되어 서버로 전송하게 된다.

사용자 단말로부터 암호화된 데이터를 수신하면 복호화하여 사용자가 입력한 좌표를 취득하고 키를 매핑한다. 이후 사용자 입력정보의 유효성을 검증하고 결과를 사용자에게 알리기 위하여 모바일 클라우드 커넥터로 전송한다. 이러한 가상키보드 흐름에서 사용자 단말 영역이 처리하는 부분은 사용자 입력 이벤트에 대한 정보만 암호화하여 관리 모듈로 전송하는 역할을 하게 되고 무작위성을 부여하기 위한 랜덤 값의 생성과 키 매핑, 관리는 모두 가상키보드 관리 모듈을 가진 서버측에서 수행하기 때문에 공격자가 단말 영역에서 취득할 수 있는 정보 중에 공격이 용이한 정보는 키로깅으로 얻어지는 터치 이벤트 정보가 유일하다.

앞서 설명한 바와 같이 가상키보드를 생성하고 키를 배치하게 된다면 공격자가 취득한 정보로부터 대응되는 실제 키를 유추하기 어렵기 때문에 사용자 입력정보는 안전하게 보호된다.

5. 결론 및 향후연구

지금까지 모바일 클라우드 서비스 환경에서 사용자 단말에 발생할 수 있는 보안위협과 보안 요구사항에 대해서 살펴보았고, 보안위협 중 하나인 키로깅 공격을 방지하기 위한 기존의 가상키보드들을 비교·분석했다. 이를 통해 새로운 가상키보드를 제안함으로써 키로깅 공격에 대해 더욱 안전하고 사용자 편의성을 최소한으로 훼손하는 범위에서 기존의 방법들을 보완했다.

하지만 제안된 가상키보드를 포함하여 키로깅 공격에 대응하는 다양한 가상키보드들은 공격자가 입력 시에 이벤트 정보, 터치 한 부분의 좌표뿐 아니라 입력당시 가상키보드에 대한 스크린 샷을 실시간으로 취득하게 될 경우 보안성이 상실된다.

따라서 향후 연구에서는 가상키보드에서 정보를 입력할 때 공격자가 스마트 디바이스에서 어떠한 정보를 탈취하더라도 입력키에 대해 유추하거나 입력 키 값을 알아낼 수 없는 방법에 대해서 고안 되어야 할 것이다.

Acknowledgement

본 논문은 지식경제부/산업기술평가관리원에서 지원하는 2012년도 산업원천기술개발사업(KI001810039260, 개인 및 기업 맞춤형 서비스를 위한 개방형 모바일 클라우드용 통합개발환경 및 이기종 단말-서버 간 협업 기술 개발)의 연구수행으로 인한 결과물임을 밝힙니다.

참고문헌

[1] Peter Mell 외 1명, “The NIST Definition of Cloud Computing”, NIST SP 800-145.

[2] F. Samimi 외 2명, "Mobile Service Clouds : A Self-managing Infrastructure for Automatic Mobile Computing Services", Lecture Notes in Computer Science, vol. 3996, pp. 130-141, June 2006.

[3] 김남욱 외 2명, “모바일 클라우드 서비스를 위한 스마트 디바이스 클라이언트 설계”, 제37회 한국정보처리학회 춘계학술대회 논문지 제19권 1호, 2012.4.

[4] 한국정보통신기술협회(TTA : Telecommunication Technology Association), “가상키보드 보안 요구사항”, 정보통신단체표준(TTAS), TTAK.KO-12.0180, 2011.12.

[5] 백금옥 외 2명, “키로깅 방지를 위한 가상키보드 시스템”, 보안공학연구논문지, 제7권 4호, 2010.8.

[6] 이동현 외 5명, “스마트폰을 위한 보안 키패드의 안전성 분석”, 정보보호학회지, 제21권 제7호, 2011.10.