음성인식 보안 취약점 개선방안에 대한 연구

김연정, 윤혜민
서울여자대학교 정보보호학과
email : hyemin3307@naver.com

A Study on the Improvement Plan of Voice Recognition Security Vulnerability

YeonJeong Kim, HyeMin Yun
Seoul Women's University, Information Security
email : hyemin3307@naver.com

요 약

음성인식을 사용하는 이용자가 많아지는 요즘, 이를 악용하여 개인정보를 탈취하고, 휴대폰을 해킹하는 등 정보보호 상의 문제점이 많아지고 있다.

이 논문에서는 음성인식 중에서도 IoT 기기의 음성비서를 이용하는 사용자들의 개인정보보호를 위해 음성인식의 보안 정도를 높이고, 본인인증을 더 확실히 할 수 있는 방안을 제안한다.

1. 서론

음성인식 기능은 인공지능이 발달함에 따라 음성비서로 발전하였고 현재는 일상적인 대화 및 감정적인 교류 등 기능의 폭이 확장되고 있다. 이로써 일상생활 속에서 사용하는 IoT 기기들에서도 손쉽게 음성인식 기능을 만나볼 수 있으며 중요한 위치를 차지하고 있다. 또한 음성인식은 다른 신체 인증과는 달리 원격으로 인증이 가능하기 때문에 차세대 인증 서비스로 손꼽히고 있다.

하지만 음성인식의 역할이 세분화되고 응용분야가 넓어짐에 따라 보안 문제점은 많아지고 이에 대한 우려의 목소리는 높아지고 있다. 2015년 한 매체[1]에 의하면, 아이폰 음성비서인 시리를 우회하여 기기 내의 개인정보 탈취가 가능하다는 것이 발견되었다. 이에 대해 애플사는 보안 패치를 선보였지만, 아직까지도 같은 취약점에 있어서 다른 경로로 접근한 공격들이 지속적으로 나타나고 있다. 이처럼 보안 패치를 제공하였는데, 동일한 취약점이 보인다는 것은 근본적인 원인 파악이 부족했음을 의미한다.

이렇듯 취약점이 발견될 때마다 일시적인 대안을 제공하는 것은 바람직하지 않다. 그러므로 근본적인 원인을 찾는 것이 중요하며 우리는 그 원인을 분석해본 결과, 음성인식이 불특정 다수를 받아들인다는 점이 문제임을 파악하였다. 그 이유는 '불특정 다수'가 대상이라는 점이 공격자에게는 악용하기 좋은 보안 틈새이기 때문이다. 그리고 이 틈새를 노린 공격은 범위가 넓고 다양하여 예상치 못한 공격이 행해질 가능성이 높다

반면에, 만약 음성비서가 특정 인물을 인지하는 '화자인식'을 한다면 본래 명령을 하는 시점에서부터 보안을 할 수 있기에 화자인식을 음성비서에 적용함을 제안하고자 한다.

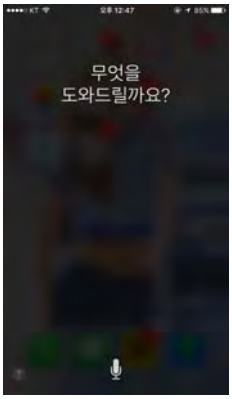
2. 음성인식의 보안 취약점

음성인식 기술력이 높아지면서 음성인식을 통한 공격은 더욱 치밀한 방법으로 이루어지고 있다. 특정한 한 가지 수단을 통해서 공격하기 보다는 여러 단계를 거쳐서 공격하는 경우가 더 많다. 그렇기 때문에 음성인식의 보안 취약점에 있어서 공격이 전반적으로 어떻게 이루어지는지 확인할 필요가 있다.

먼저 음성비서의 작동원리를 본다면, 사용자의 음성을 전파로 전환하고 이를 분석한 결과를 토대로 사용자의 말을 이해한다. 보안 취약점은 주로 이 과정 중 전파를 보내는 단계에서 나타나는데, 악성코드를 주입하거나 멀웨어 설치를 명령하는 등의 공격이 이에 해당된다. 위와 같은 공격이 실행되면 공격자는 사용자의 음성인식에 대한 권한을 갖게 되고, 이에 따라 사용자가 누구와 대화를 나누는지 알 수 있으며 대화의 도청 및 감청이 가능해진다. 그리고 탈취당한 정보는 스팸 문자 및 메일을 임의로 보내는 데에 도용될 가능성이 높아진다.

이러한 공격들은 네트워크 및 서버, 소프트웨어 등의 취약점을 가지고 나타나기도 하지만, 물리적인 취약점으로 인해 발생하기도 한다. 휴대폰 기기에 연결된 이어폰을 안테나로 이용하여 전파를 보내게 되면 기기에서 음성명령으로 변경하는 것이 하나의 예시이다[2]. 음성 비서가 음성을 디지털 신호로 변환하는 과정을 외부에서 전자파로 조작 및 재현하는 구조로 만들어 음성 비서가 음성으로 입력한 것과 같은 작업을 수행하도록 만든 것이다. 더불어 2015년 기사[3]에 의하면 음성명령 변경 장치가 가방에 들

어갈 크기라면 2m 내외까지 전파를 전송할 수 있고, 더 큰 장치를 이용한다면 최대 5m까지 보낼 수 있다고 한다. 이를 통해 공격이 사용자가 모르는 사이에, 먼 거리에서도 이루어질 수 있음을 보여준다.



그림[1] iPhone Siri 실행화면

하지만 먼 거리가 아닌, 공격자가 직접적으로 음성비서와 대치할 경우에도 문제는 발생한다. 예를 들어 그림[1]의 아이폰 시리 같은 경우 이중 비밀번호로 잠금이 되어 있지만 홈 버튼만 길게 누른다면 음성비서가 활성화되기 때문에 사용자의 개인정보를 포함하여 최근 통화목록 등에 대해서도 알 수 있다[4].

현재 개인정보에 대한 직접적인 접근 명령은 불가능하게 보안을 강화하였지만 완벽한 해결책이라고 할 수 없다. 2016년 기사[5]에 따르면, 비밀번호 잠금을 우회하여 개인정보를 훔치는 것도 가능하다고 보도한다. 구체적인 방법은 음성비서에게 특정 어플리케이션 검색을 명령하고 검색결과를 통해서 개인정보에 접근하는 것이다. 여기서 사용되는 어플리케이션은 '트위터', '왓츠앱', '유투브', '인스타그램' 등으로 익히 들어본 어플리케이션들을 통해서 우회 가능하다. 이에 대해 휴대폰 사용자가 설정하여 각 어플리케이션을 수동으로 제어할 수 있지만 이는 일시적인 보안 대책일 뿐이며, 사용자의 편의성이 떨어진다.

다른 공격으로는 돌핀어택이 있다. 이 공격은 사람이 들을 수 있는 영역을 벗어나 20,000hz 이상의 초음파를 사용하는 방법이다. 최근 기사[6]에 의하면 중국 즈장대 연구팀은 음성 명령 파일을 초음파 대역의 파일로 변환하고 휴대폰에 앰프와 스피커를 연결하여 초음파 대역 파일을 틀어 실험을 하였다. 결과적으로 음성비서를 불러내는 명령어로 쉽게 이용할 수 있으며 다양한 명령어를 통해 음성 명령과 같은 일을 수행할 수 있는 것을 알 수 있었다. 이 취약점은 대부분의 음성 인식 기기에 해당된다. 일시적인 대책으로 초음파 대역의 명령을 수행하지 않도록 펌웨어 업그레이드를 하거나 마이크에서 필터링을 하면 되지만 이 역시 사용성이 떨어진다.

3. 제안방안

보안 업데이트를 하더라도 해결이 안 되는 보안 취약점이 계속해서 발견되고 있으며, 현재 음성인식 인공지능으로는 일일이 문제점에 대응하기는 어려운 것으로 보인다. 하지만 음성비서에 특정 음성을 인식하여 개인을 식별하는 화자인식이 적용된다면, 앞서 취약점들은 전면 보안 가능하다. 어떻게 보안할 수 있는지는 공격이 간접적으로 이루어지는지 혹은 직접적으로 이루어지는지에 따라 서술 가능하다.

첫 번째로, 공격자가 간접적으로 음성비서에 접근하는 경우이다. 일반적으로 간접 공격은 물리적인 도구를 사용하여 악의적인 전파를 음성비서에게 보내는 것이 대표적이다. 이어폰, 헤드폰 등이 전파를 보내는 매개체로 사용되고 음성명령 장치가 공격의 보조 역할을 하여 공격 범위를 넓이거나 정밀도를 높이는 데에 사용된다. 이러한 상황에서 음성비서가 화자인식을 한다면, 어떠한 악의적인 보조 장치를 사용하던지 상관없이 음성비서가 자체적으로 접근을 허용한 개인 외에는 모두 차단한다. 화자인식이란 저장되어 있는 음성 데이터와 음성 명령으로 입력한 음성 데이터를 비교하여 사용자가 누구인지 식별하는 기술이다. 휴대폰 사용자의 음성을 데이터베이스에 등록만 해 놓는다면, 다른 음성으로 명령을 하였을 때 실행하는 일을 방지 할 수 있다.

이는 최근 초음파를 이용한 음성인식 취약점인 돌핀어택(Dolphin Attack)의 보안 대책으로도 사용될 수 있으며, 다음과 아래와 같다. 위 취약점이 현재 iOS와 안드로이드 기기에 모두 나타난다는 점에서 전파의 허용 범위가 넓다는 것을 알 수 있다. 하지만 대안으로 전파의 허용 범위를 구체화시킨다는 것만으로는 개인과 타인의 식별에 있어서 오차율의 문제가 생길 수 있다. 반면에 화자인식으로 변경한다면, 전파의 허용 범위가 사용자 개인에게 맞춰지기 때문에 초음파와 같은 공격은 무력화되고 결과적으로 보안이 강화된다.

두 번째로, 직접적으로 음성비서에 접근하는 경우 이다. 직접적인 접근에서도 화자인식을 사용하면 보안 문제점을 해결할 수 있음을 보여준다.

예를 들어 아이폰의 경우, 휴대폰 잠금 상태 에서 음성비서가 작동되는 방법은 네 가지로 나눌 수 있다. 먼저, 지문과 음성이 모두 본인일 경우와 타인일 경우는 개인정보 접근을 허용하고 차단하는 오차율이 낮다. 하지만 본인 지문과 타인음성 혹은 타인 지문과 본인 음성이 사용될 경우, 시리의 판단 기준은 지문이 된다. 여기서 지문이 무용지물이 된다면 공격자는 지문과 음성의 매칭에서 틈새를 노리고 공격을 실행할 수 있다. 이를 보안하기 위해서는 지문이 사용자 개인을 인식하듯 음성을 통해 사용자를 인식하는 화자인식이 필요하다.

이렇듯 음성비서는 모든 사람의 음성을 인식하기 때문에 위험성이 다분하며, 화자인식만이 추가적인 임의 공격을 막는 최선의 방법이다.

4. 필요성

최신 기술 경향은 사용자 맞춤형 서비스에 초점이 맞춰져 있고, 이에 따라 개인정보 보안의 필요성은 더욱 강조되고 있다. 하지만 일반 사용자의 경우, 보안에 대해 제대로 인지하지 못하는 경우가 상당하며 보안을 일반적으로 어려워한다. 그렇기 때문에 IoT 업체들은 사용자가 다루기 어려워하는 보안보다는 쉽게 조작 가능하지만 보안은 강력한 기술을 선호한다. 이러한 경향에 따르면 화자인식은 '사용 가능한 보안'[7]에 가장 적합한 기술이다.

우선 사용성이 높은 기술로 평가한 이유는 화자인식이 사용자 인증 기술로써 밝은 미래를 가지고 있기 때문이다. 화자인식은 현존하는 생채 인증 기술들과 달리 비교적 먼 거리에서도 인식 가능하다는 장점을 가진다. 게다가 기존 음성비서의 경우 인증기술로써 사용되지 않기 때문에 다른 인증 기술에 의존하여 얼마나 정보를 제공할지 결정하는데, 이 또한 해결된다. 다시 말해서, 다른 생체 인증 기술을 거칠 필요가 없어졌기에 인증 과정이 간단하게 바뀐다. 이로써 사용자는 더 이상 직접적으로 기기에 신체를 접촉하거나 가까이 하지 않고 음성만으로도 본인 인증이 가능해진다.

그렇지만 기술의 사용성이 높다고 하더라도 보안성이 떨어지면 무용지물이 되므로, 보안 측면에서 보더라도 화자인식은 필히 요구된다. 현재 음성비서는 악의적인 명령의 전파를 흘려보내는 것만으로도 개인 정보 탈취 및 스팸공격 등이 가능하고 이는 보안성이 떨어진다는 것을 의미한다. 이 보안 문제의 근본적인 원인은 대상이 '불특정 다수'라는 점이므로 대상의 범위를 줄여야만 보안을 높일 수 있으며 이에 해당하는 대안으로는 화자인식이 적격이다.

물론 화자인식을 사용하더라도 사용자의 음성이 변조되었을 때 방어를 할 수 없다는 취약점을 가지지만, 어떠한 음성인식 기술에서도 이는 항상 주의해야할 부분이다. 하지만 모든 음성을 받아들이는 기존의 음성인식이 화자인식으로 바뀌어야만 보안을 높일 수 있다는 점은 변하지 않는다.

5. 결론

우리는 이 논문에서 음성비서의 취약점과 가해질 수 있는 공격을 서술하였고 음성비서에서 화자인식을 사용하게 된다면 전파를 이용한 직접적인 혹은 간접적인 공격이 무력화된다는 점을 증명하였다. 이를 바탕으로 음성인식에 보안 취약점이 생기는 궁극적인 이유는 화자인식을 사용하고 있지 않기 때문임을 확인하였고 해결방안으로써 화자인식이 가장 적절한 방법임을 표명하였다. 결론적으로, 음성비서를 사용하는 IoT기기에 화자인식 기능은 반드시 필요한 존재임을 주장한다.

화자인식은 다른 생채 인증 기술들 중에서도 비교적 먼 거리에서 인증이 가능한 방법으로 유일하고 본인의 목소리를 사용하여 증명하는 수단이기 때문에 어떤 보안 방법보다 강해야하고 공격에 쉽게 당해선 안 된다.

허나 화자의 목소리를 변조하거나 위조하였을 때의 대비책이 마련되어있지 않은 큰 문제점이 남아있기 때문에 우리가 제안한 방안으로 모든 공격을 막을 수 있는 것은 아니라는 점을 설명한다. 이와 같은 잠재적인 문제점은 추후에 추가적인 연구를 통해 해결 방안을 계속 모색해 나갈 예정이다.

6. 참고문헌

[1]보안뉴스, "음성인식"
http://www.boannews.com/media/view.asp?idx=48597 ,(2017.09.06.)
[2]연합뉴스, "음성인식 해킹"
http://www.yonhapnews.co.kr/bulletin/2015/10/16/0200000000AKR20151016028100091.HTML ,(2017.09.06.)
[3]iPnomics "음성인식 해킹"
http://www.ipnomics.co.kr/?p=29292 ,(2017.09.06.)
[4]환경부. "음성비서"
https://www.me.go.kr/home/web/board/read.do?menuId=10392&boardMasterId=713&boardId=804510
, (2017.09.06.)
[5]전자뉴스. "siri 취약점"
http://www.etnews.com/20160405000341 ,(2017.09.06.)
[6]The hacker news, "음성인식 공격"
http://thehackernews.com/2017/09/ai-digital-voice-assistants.html , (2017.09.07.)
[7]Jendricke, Uwe, and D. Gerd tom Markotten. "Usability meets security-the Identity-Manager as your personal security assistant for the Internet." Computer Security Applications, 2000. ACSAC'00. 16th Annual Conference. IEEE, 2000.