특집 02

실제 사용자 인증을 위한 CAPTCHA와 reCAPTCHA: 보안의 한계와 대응 전략

박보경 (강원대학교), 하소희 (영남이공대학교), 한성수 (강원대학교)

목 차

1. 서 론

1990년대 말에 등장하여 현재까지 많이 사용되는 CAPTCHA는 웹 사이트에 사람이 접근하는 것인지 봇이 접근하는 것인지 판단하기 위해 사용된다. 현재 CAPTCHA, reCAPTCHA v2, reCAPTCHA v3이 있다. CAPTCHA는 Carnegie Mellon University의 연구원들이 개발하여 사용되다가, 구글에 인수되었다. 이후 구글에서 후속 버전인 reCAPTCHA v2와 reCAPTCHA v3을 개발하였다. CAPTCHA는 웹 사이트와 서비스를 이용하는 사용자가 사람인지, 봇인지 파악하고 컴퓨터로 인해 발생할 수 있는 다양한 문제를 방지하는 데 중요한 역할을 한다. 하지만, CAPTCHA와 reCAPTCHA의 새로운 테스트 방식이 나올 때마다 봇은 지속적으로 진화하여 CAPTCHA와 reCAPTCHA 만으로 완벽한 차단은 힘들어졌다. 따라서, CAPTCHA와 reCAPTCHA의 인증 방식, 문제점, 보안 필요성을 조사하고, CAPTCHA와 reCAPTCHA의 대응 전략에 대해 연구를 해보고자 한다.

2. CAPTCHA와 reCAPTCHA

Completely Automated Public Turing Test to tell Computers and Humans Apart의 약자인 CAPTCHA는 온라인 사용자가 봇이 아닌 진짜 사람인지를 판단하기 위한 공개 튜링 테스트이다[1]. CAPTCHA는 봇을 이용하여 악의적 목적으로 웹 양식을 작성하지 못하도록 한다. 대표적인 사례로는 거짓 등록 방지, 의심스러운 거래로부터 보호, 온라인 여론조사의 질 보호, 댓글 및 제품 후기 스팸 방지, 무차별 대입 공격 및 사전 공격 방어 등이 있다.

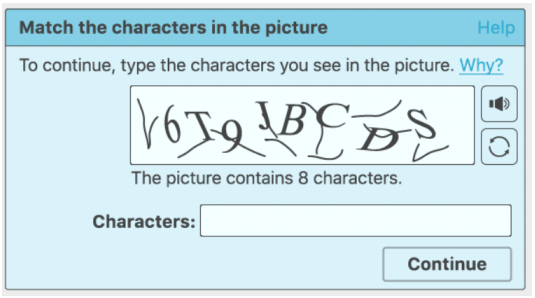
2.1 CAPTCHA와 reCAPTCHA 인증방식

CAPTCHA는 출력된 숫자나 글자를 있는 그대로 입력란에 입력하고 확인하면 끝나는 방식으로, 매우 단순하다. 유동적으로 사고할 수 있는 사람만이 할 수 있어 사람인지 봇인지 판별하는데 유용하게 사용된다. 화면상 텍스트가 폰트를 그대로 사용하면 봇도 당연히 맞힐 수 있기에 글자를 휘

거나 가로 획을 이어 버린다는 등 변형을 준다. CAPTCHA는 광학적 문자 인식 기술인 OCR 기술(Optical Character Recognition)이 사용되어, 봇은 왜곡된 텍스트를 해독하는 데 어려움을 겪어 통과하지 못하였다. 하지만 상용 프로그램을 사용하면 CAPTCHA는 10~20% 확률로 뚫리게 된다.

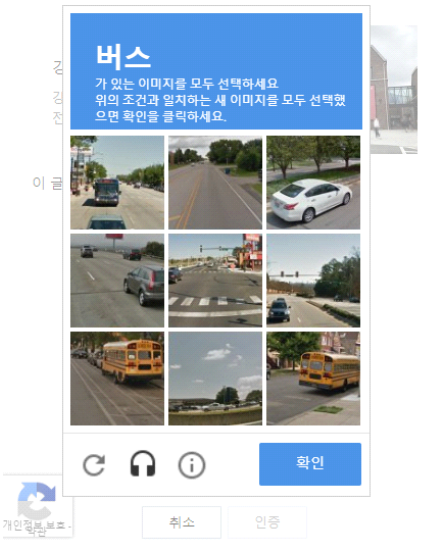
CAPTCHA의 한계를 보완하기 위해 reCAPTCHA는 문자 인식뿐만 아니라 다양한 방식으로 사용자를 판단한다. reCAPTCHA v2는 현재 가장 많이 사용하고 있는 방식이다. 기존 CAPTCHA는 사람조차 알아보기 힘들었지만, 체크박스를 체크해서 통과하는 'I'm not a robot'과 'Invisible'이 있다. 또는 체크를 클릭하는 방식과 유사하지만, 이미지 선택 창이 뜨며 사물을 선택해 통과하는 것도 있다. reCAPTCHA는 문자 인식 테스트, 이미지 인식 테스트, 체크박스 테스트, 사용자 행동 분석 테스트 방식이 있다[2].

문자 인식 테스트는 여러 단어로 구성된 문자가 표시되며, 문자를 흐리게 처리하는 것과 같은 효과를 통해 컴퓨터의 문자 인식을 어렵게 하는 장치가 마련되어 있다. CAPTCHA와 다르게 책, 신문과 같은 실제 문자 인식 이미지를 제공해 테스트의 신뢰도를 높이고 있다.



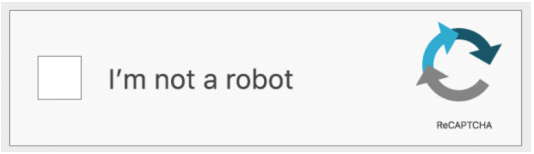
(그림 1) CAPTCHA 방식[1]

이미지 인식 테스트는 임의의 사진이 제공되는데, 사용자는 제공된 사진에서 임의의 물체가 포함된 타일을 찾아 클릭해야 한다. 사용자가 선택한 답이 다른 사용자의 답변과 유사하면 정답으로 간주된다. 문자 인식 테스트보다 기술이 필요하기에 성능이 보다 높다.



(그림 2) reCAPTCHA v2 이미지 인식 테스트 [3]

체크박스 테스트는 체크박스를 클릭했는지가 중요한 것이 아니라 어떻게 체크박스를 클릭했는지가 중요하다. 체크박스를 클릭하는 과정을 감지해 사용자가 인간인지, 컴퓨터인지 파악한다. 이 방식으로 판단이 불가능할 경우, 문자 인식 테스트와 이미지 인식 테스트를 다시 진행하기도 한다.



(그림 3) reCAPTCHA v2 체크박스 테스트 [1]

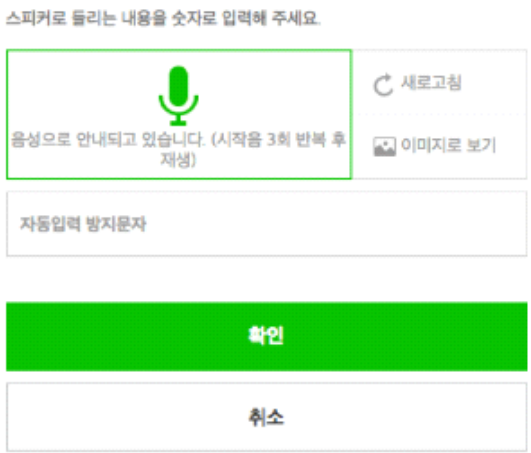
사용자 행동 분석 테스트는 사용자 화면에 표시되지 않는다. reCAPTCHA가 자동으로 파악하여 컴퓨터라고 의심될 때 서비스 이용을 제한한다.

웹 사이트를 이용할 때, 검색어를 반복해서 여러 번 입력하거나 많은 링크를 한 번에 클릭할 때 이용이 제한된다. 이때 reCAPTCHA의 사용자 행동 분석 테스트에서 비정상적인 행동을 감지되었기 때문에 제한하는 것이다. 일반적인 CAPTCHA 패턴일 때, 사람은 쉽게 알아볼 수 있지만, AI 봇은 인식할 수 없어, 스팸을 차단하는 효과를 본다. 이는 reCAPTCHA v2에 들어가는 연산의 대부분이 비가역적 연산이기 때문이다. 비가역적 연산은 연산의 대부분이 실행된 뒤에 되돌릴 수 없다. reCAPTCHA v2는 글자를 비틀거나 회전시키는 역연산이 존재하지 않는 방법을 이용해 글자를 왜곡하고, jpeg로 저장된 이미지를 완벽하게 복원하는 것이 불가능하다.

reCAPTCHA v3는 reCAPTCHA v2와는 다르게 직접 인증할 필요 없이, 웹 사이트에서의 상호작용으로 악성 트래픽을 감지할 수 있다. 보안 문자 챌린지를 표시하는 대신 점수를 반환하므로 웹 사이트에 가장 적절한 액션을 선택할 수 있다. 앞서 말한 상호작용은 ARAE(Adaptive Risk Analysis Engine)를 기반으로 Good Interaction과 Interaction으로 나뉘는데, Good Interaction은 1.0, Interaction은 0.0을 준다. 1,0과 0.0은 사용자의 행동을 봇일 가능성이 큼(0.0)부터 인간일 가능성이 큼(1.0)의 척도로 점수를 매긴다[4].

2.2 CAPTCHA와 reCAPTCHA 문제점

CAPTCHA와 reCAPTCHA는 여러 문제점을 수정하여 발전하고 있지만, 사용자 저해, 접근 불가능성, 봇 AI 진화 등 공통된 문제점이 있다. CAPTCHA 테스트는 사용자가 원하는 작업의 흐름을 막아, 웹 자산에 대한 경험에 부정적으로 작용되고 사용자가 아예 웹페이지 자체를 포기하는 경우도 있다. CAPTCHA의 복잡성이 증가하는 만큼 난이도가 높아진다. 텍스트 및 이미지 기반 CAPTCHA는 시각 장애인들에게 매우 어렵다. CAPTCHA 테스트는 기계가 읽을 수 없도록 설계되었기에, 스크린 리더가 대부분의 CAPTCHA 과제를 읽지 못하는 문제가 있다. 이를 해결하기 위해 오디오 해독을 요구하는 오디오 CAPTCHA가 있지만, 풀기가 어렵다.



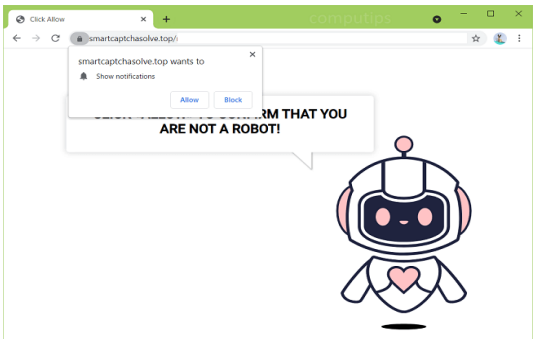
(그림 4) 오디오 CAPTCHA [5]

새 CAPTCHA 과제가 등장할 때마다 이를 이기기 위해 봇이 지속적으로 진화해왔기 때문에 CAPTCHA 기술은 시작된 이래 매우 여러 번 변경되었다. CAPTCHA는 봇 AI를 막기 위해 해결되지 않은 AI 문제에 의존하므로 CAPTCHA 기술의 구조 자체가 약화된다[6].

3. CAPTCHA와 reCAPTCHA 보안

문자 인식 테스트를 통과할 수 있는 봇이 존재하며, 이미지 인식 테스트와 체크박스 테스트도 기술이 발전함에 따라 완벽한 차단 성능을 보장하기가 어려워졌다. 특히 봇이 아니라 여러 명의 사람을 고용해 악의적인 행위를 하는 경우에는 CAPTCHA와 reCAPTCHA가 도움이 되지 않으며, 콘텐츠 스크랩 봇, 자격 증명 스터핑 봇, 스팸

봇을 차단할 수 없다는 단점이 있다. 또한, 웹 사이트나 서비스가 CAPTCHA와 reCAPTCHA를 활용하고 있는 경우에도 악의적인 공격이 발생할 수 있다는 사실을 알고 있어야 한다.



(그림 5) 푸시 알림 시스템 악용 사이트 [7]

이 웹사이트는 외관상 reCAPTCHA v2로 보이지만, 사실은 사용자의 장치에 스팸 팝업 광고를 표시하기 위해 브라우저의 내장 푸시 알림 시스템을 악용하는 사이트이다. Totalrecaptcha.top는 일반적인 CAPTCHA 서비스처럼 보이며, “로봇이 아니라는 것을 확인하려면 <<ALLOW>>를 클릭하세요!”라는 메시지와 함께 “totalrecaptcha.top에서 다음 권한을 요청합니다.”라는 메시지가 담긴 푸시 알림을 보낸다. 이러한 메시지는 사용자를 속이고 푸시 알림에 있는 버튼을 클릭하도록 유도한다. 사용자가 푸시 알림을 구독하면 브라우저가 닫혀 있어도 사용자의 장치에서 직접 스팸 팝업을 받게 된다. 이는 사용자에게 불편과 스팸 광고로 인한 피해를 입힐 수 있다.

사용자가 악성 웹 페이지에서 링크를 실수로 클릭할 때 totalrecaptcha.top/robot4/ 또는 totalrecaptcha.top/robot37/에서 랜딩 페이지에 도달한다[8].

3.1 보안 대책 필요성

CAPTCHA는 일그러진 숫자나 글자를 인식하여 사용자로부터 입력을 받는 방식으로 인증을 수행한다. 사용자는 보이는 일련의 숫자나 글자를 정확하게 입력하여 인증을 완료해야 한다. 이는 기계가 정확하게 인식하기 어렵게 디자인되어 있어, 사용자가 인간임을 확인하는 역할을 한다.

reCAPTCHA는 다양한 인증 수준과 기능을 제공하는 Google의 보안 서비스이다. ReCAPTCHA v2에서는 사용자가 직접 체크 박스를 체크하거나 이미지 인증을 수행하여 인증을 완료해야 한다. 사용자가 로봇이 아닌 실제 사용자임을 증명하는 데에 사용된다.

reCAPTCHA v3는 사용자의 웹 사이트 상의 동작 패턴과 상호 작용을 분석하여 실제 사용자를 판별하는 ARAE(Adaptive Risk Analysis Engine)를 기반으로 한다. 사용자가 직접적인 CAPTCHA 작업을 수행하지 않고, 점수를 기반으로 인증 여부가 결정된다. 이는 웹 사이트 개발자가 웹 사이트 상에서 사용자의 신뢰도를 파악하고, 악성 로봇이나 스팸 봇으로부터 보호하기 위해 사용된다.

이러한 CAPTCHA와 reCAPTCHA의 작동 방식은 사용자가 로봇이 아닌 실제 사용자임을 확인하고 인증하는 데에 도움을 주지만, 최근의 기술 발전으로 인해 그 효과에 제한이 발생할 수 있음을 고려해야 한다. 악의적인 개체들은 커서 동작, 쿠키, 기기 이력 등의 정보를 활용하여 CAPTCHA와 reCAPTCHA를 우회하거나 피해를 입힐 수 있다. 따라서, CAPTCHA와 reCAPTCHA 만으로 완벽한 보안을 제공하기는 어려울 수 있으며, 추가적인 보안 대책과 방어 전략의 필요성이 요구된다.

3.2 reCAPTCHA의 제한된 효과에 대한 고려

CAPTCHA와 reCAPTCHA의 제한된 효과에 대해 고려해야 할 점이 있다. 지금까지 우리는 CAPTCHA와 reCAPTCHA라는 보안 도구를 통

해 인터넷상의 악의적인 행위로부터 보호되어 왔다. 그러나 최근의 기술 발전은 우리가 직면한 보안 도전에 새로운 시각을 제시하고 있다. 문자 인식, 이미지 인식, 체크박스 테스트 등 다양한 방식의 CAPTCHA를 통과하는 봇이 등장하고 있다. 이로 인해 우리는 CAPTCHA와 reCAPTCHA를 통해 완벽한 차단을 보장하기가 어려워지고 있는 실정이다.

또한 악의적인 행위를 위해 여러 명의 인력을 동원하는 경우에는 CAPTCHA와 reCAPTCHA가 그 효과를 제대로 발휘하지 못한다는 한계가 있다. 콘텐츠 스크랩 봇, 자격 증명 스터핑 봇, 스팸 봇과 같은 악성 행위를 저지하기 위해서는 더 강력하고 진보된 방어 체계가 필요하다.

게다가 Totalrecaptcha.top과 같은 악성 웹 사이트의 등장으로 인해 CAPTCHA와 reCAPTCHA의 효용성에 대한 의문이 제기되고 있다. Totalrecaptcha.top은 외부에서는 일반적인 reCAPTCHA v2로 보이지만, 실제로는 브라우저의 내장 푸시 알림 시스템을 악용하여 피해자의 장치에 스팸 팝업 광고를 표시하는 사이트이다. 이로 인해 사용자는 CAPTCHA와 reCAPTCHA를 통해 보안을 강화하고자 하더라도 악의적인 공격에 취약할 수 있다는 문제가 발생한다.

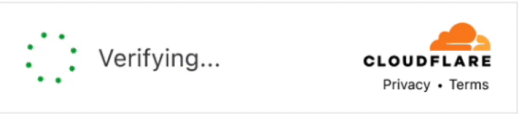
위와 같은 상황에서 우리는 새로운 시대에 맞는 보안 전략을 개발하고 도입해야 한다, CAPTCHA와 reCAPTCHA 외에도 다양한 보안 대책과 방어 전략을 고려해야 하며, 최신 기술과 연구를 통해 악의적인 행위에 대응할 수 있는 방법을 탐구해야 한다. 우리는 보안의 중요성을 깨닫고, 지속적인 노력과 혁신을 통해 인터넷 환경을 안전하고 신뢰할 수 있는 공간으로 만들어 나가야 한다[2].

4. 대응 전략

우리는 새로운 시대에 맞는 보안 전략을 개발하고 도입해야 한다. CAPTCHA와 reCAPTCHA 외에도 다양한 보안 대책과 방어 전략을 고려해야 하며, 최신 기술과 연구를 통해 악의적인 행위에 대응할 수 있는 방법을 탐구해야 한다. 우리는 보안의 중요성을 깨닫고, 지속적인 노력과 혁신을 통해 인터넷 환경을 안전하고 신뢰할 수 있는 공간으로 만들어 나가야 한다.

CAPTCHA와 reCAPTCHA의 제한된 효과에 대응하기 위해 다양한 전략들을 제시하고자 한다. 실시간 모니터링 및 대응 시스템을 구축함으로써 악의적인 행위를 실시간으로 감지하고 대응할 필요가 있다. 웹 사이트나 애플리케이션에서 발생하는 악의적인 행위를 모니터링하고 적절한 조치를 취함으로써 신속하게 악성 로봇이나 스팸 봇을 차단할 수 있다. reCAPTCHA의 제한된 효과를 보완하여 사용자 인증의 강도와 보안 수준을 향상시킬 수 있는 방안으로 고려된다.

CAPTCHA나 reCAPTCHA 외에 사용자 인증을 위한 다른 보안 기능을 추가하는 방법이 있다. CloudFlare CAPTCHA는 이미 CAPTCHA와 reCAPTCHA를 대체하는 보안 도구로 도입된 예시이다. CloudFlare CAPTCHA는 CloudFlare의 네트워크를 통해 분산되어 서비스되므로 대규모의 트래픽에 대한 처리 능력과 보안성을 제공한다. 이는 웹사이트의 성능 저하 없이 효과적인 보안 인증을 가능하게 한다.



(그림 6) CloudFlare CAPTCHA [9]

4.1 생체 인식 모바일 CAPTCHA 인증

모바일 CAPTCHA 인증 방식으로 생체 인증을 도입하는 것을 고려해 볼 수 있다. 생체 인증은

개인의 고유한 신체적인 특징을 활용하여 신원을 확인하는 방법으로, 지문 인식은 그중에서도 안정성과 정확성이 검증되어 있어 많은 관심을 받고 있다[10]. 이를 통해 모바일 디바이스에 저장된 생체 인증 정보를 활용하여 사용자가 봇이 아닌 실제 사용자인지를 체크하는 방식을 제안하고자 한다.

지문 인식을 통해 사용자가 봇이 아닌 실제 사용자인지 체크하는 방식은 새로운 모바일 CAPTCHA 인증 방식으로 매우 효과적일 것으로 예상된다. 이를 통해 기존의 CAPTCHA 인증 방식과 비교했을 때, 보안성을 더욱 강화하면서 사용자 편의성을 높일 수 있다.

지문 인식은 안정성과 정확성이 높아 사용자의 신원을 확실하게 확인할 수 있다. 또한, 모바일 기기에서 이미 많이 사용되고 있는 인증 방식으로서 사용자들에게 익숙하고 편리한 방법이다. 생체 인증은 비밀번호나 PIN 번호와 같은 기억하기 어려운 정보를 사용하지 않아도 되므로, 사용자들이 비밀번호를 관리하고 기억하는 부담을 줄여준다.

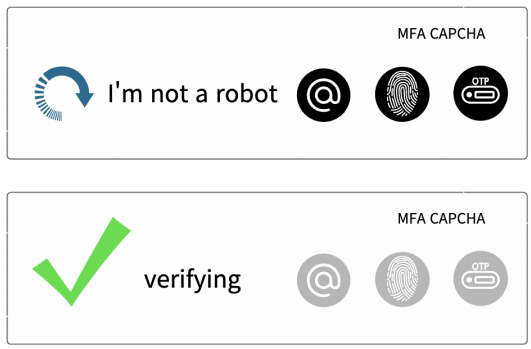
또한, 생체 인증은 사용자의 편의성을 향상시킬 수 있다. 지문 인식은 빠르고 간편하며, 사용자가 따로 입력해야 하는 번거로움을 줄여준다. 이로써 사용자들은 원활하고 빠른 인증 과정을 경험할 수 있다.

(그림 7) 생체인식 모바일 CAPTCHA 인증 방식

따라서, 새로운 모바일 CAPTCHA 인증 방식으로 지문 인식을 도입하는 것은 모바일 보안 분야에 대한 혁신을 이끌어낼 것으로 기대된다.

4.2 Multi-factor authentication

Multi-factor authentication을 도입하는 것을 고려해 볼 수 있다. 이는 기존 인증 방식 외에도 SMS 코드, 보안 키 등 추가적인 인증 요소를 사용하여 사용자를 인증한다. Multi-factor authentication 방식을 도입할 때, 보안 기능이 효과적이고 신속하게 작동하는지 확인할 필요가 있다. 사용자를 신속하게 인증하면서도 악성 행위로부터 보호하는 기능을 개발하여 기술적인 효과성을 갖춘 CAPTCHA를 도입하기 위해 더 연구할 필요가 있다. MFA를 도입할 때 사용자가 편리하게 인증할 수 있는 인증요소 중 OTP, 이메일 인증, SMS 코드 등으로 사용자가 선택할 수 있게 한다.



(그림 8) 사용자가 선택할 수 있게 한 CAPTCHA

5. 결 론

본 논문에서는 CAPTCHA와 reCAPTCHA의 보안의 한계와 대응 전략에 대하여 분석하였다. CAPTCHA와 reCAPTCHA는 과거부터 널리 사용되어 왔지만, 최근 기술의 발전과 공격자들의

더욱 높은 수준의 지능적인 공격으로 인해 보안 수준은 한계에 직면하고 있다.

우선 CAPTCHA의 경우, 기존의 텍스트 기반 인식 방식은 OCR(광학 문자인식) 기술의 발전으로 우회되는 경우가 많다. 이로 인해 자동화된 봇들이 텍스트를 효과적으로 인식하여 보안장치를 우회하는 문제가 발생하였다. 또한 CAPTCHA의 난이도를 적절하게 조절하기 어렵다는 한계도 있다. 난이도가 너무 높으면 일반 사용자도 해결하기 어렵게 되고, 너무 낮으면 공격자가 쉽게 해결할 수 있게 된다.

reCAPTCHA는 CAPTCHA의 한계를 극복하기 위해 도입된 기술로, 사용자들에게 더욱 편리한 인증 방식을 제공하고 있다. 그러나 reCAPTCHA도 보안이 완벽하다고 할 수는 없다. 이는 공격자들이 인간과 구별하기 어려운 패턴을 학습하고 적용하여 reCAPTCHA를 우회하는 공격 기술을 개발해낼 수 있기 때문이다.

이러한 CAPTCHA와 reCAPTCHA의 한계에 대응하기 위해서는 신규 보안 기술의 도입이 필요하다. 생체 인증 방식을 도입하기 위해서는 몇 가지 고려 사항이 필요하다. 우선, 생체 인증 정보의 보안 문제에 대한 적절한 대책을 마련해야 한다. 생체 인증 정보의 유출은 심각한 보안 문제를 야기할 수 있으므로, 사용자의 개인정보를 안전하게 보호할 수 있는 방법을 고민해야 한다. Multi-factor authentication 방식을 도입할 때, 보안 기능이 효과적이고 신속하게 작동하는지 확인할 필요가 있다. 사용자를 신속하게 인증하면서도 악성 행위로부터 보호하는 기능을 개발하여 기술적인 효과성을 갖춘 CAPTCHA를 도입하기 위해 더 연구할 필요가 있다.

새로운 CAPTCHA 인증 방식을 도입하기 전에 이러한 고려 사항을 심사숙고하여, 사용자의 보안과 편리성을 동시에 고려하는 최상의 솔루션을 찾는 것이 필요하다. 이러한 연구는 개인의 자산을 지키는데 중요한 발전을 이끌어낼 수 있을 것으로 기대된다.

CAPTCHA를 완전히 폐기하기에는 아직 일부 제약사항이 존재한다. 봇과 인간을 정확히 구분하기 위해서 신뢰할 수 있는 대안이 발전될 필요가 보인다. CAPTCHA 없이도 보안성을 유지할 수 있는 대안이 충분히 검증되어야 한다. 위 논문에서 제시한 방안들은 CAPTCHA를 대체할 수 있는 기술이 충분히 성숙해지기 전까지 사용되기에 충분히 필요한 보안수단이라고 생각한다.

따라서, 본 논문은 CAPTCHA와 reCAPTCHA의 보안 한계를 인식하고, 이를 극복하기 위해 신규 보안 기술의 도입을 제안하였다. 이를 통해 온라인 환경에서의 보안과 개인 정보 보호를 보다 안전하게 유지할 수 있을 것으로 기대한다. 웹 사이트와 앱에서도 사용자 인증을 위한 더 나은 보안 기능을 도입하기 위해 추가적인 연구가 필요하다.

참 고 문 헌

[1] cloudflare, “캡차 작동 원리 | 캡차란?”, cloudflare

[2] Agnė Augustėnė, “캡차란 무엇인가요?”, NordVPN, 2022.6.12.

[3] 임국정, “리캡차, 당신이 모르는 사이 AI 성능 향상에 일조”, IT Chosun, 2022.1.2.

[4] Google, "reCAPTCHA란 무엇인가요?", reCAPTCHA

[5] NAVER CLOUD FLATFORM, “CAPTCHA”, NAVER CLOUD FLATFORM

[6] IBM, "CAPTCHA란?", IBM

[7] Diana N, “How to Remove SmartCaptcha Solve.Top”, CoumpuTips, 2021.9.20.

[8] Stelian Pilici, “Remove TotalRecaptcha.Top Pop-up Ads [Virus Removal Guide]”, MALWARETIPS

[9] Kyle Wiggers, “Cloudflare wants to re-

place CAPTCHAs with Turnstile", TechCrunch, 2022.9.28.
[10] 엄호식, "코로나19 상황에서의 지문인식 안정성과 활용", 보안뉴스, 2020.5.3.

저 자 약 력

박 보 경

이메일 : b.gyung17@gmail.com

- 2020년 대구대학교 정보보호 영재교육원 고등전문B 과정 수료
- 2021년 대구대학교 정보보호 영재교육원 고등전문A 과정 수료
- 2022년 마산여자고등학교 졸업
- 2023년~현재 강원대학교 자유전공학부 재학
- 관심분야 : 웹 개발, 네트워크, 정보보안

하 소 희

이메일 : ihyraxi@gmail.com

- 2020년 대구대학교 정보보호 영재교육원 고등기초심화과정 수료
- 2021년 대구대학교 정보보호 영재교육원 고등전문B과정 수료
- 2022년 수성고등학교 졸업
- 2022년~현재 영남이공대학교 사이버보안스쿨 재학
- 관심분야 : 정보보안, 침해사고, 악성코드 분석, 모의해킹

한 성 수

이메일 : sshan1@kangwon.ac.kr

- 2019년 고려대학교 영상β정보처리학과 (박사)
- 2018년~2019년 순천향대학교 교수
- 2019년~현재 강원대학교 자유전공학부 교수
- 관심분야 : 빅데이터, 분산 병렬 알고리즘, 영상정보처리, 딥러닝