캡차의 개념과 안전성 분석 사례

김 웅 희
ETRI 부설연구소

지 성 택
ETRI 부설연구소

Ⅰ. 서 론

인터넷이 보급됨에 따라 포털사이트, 무료이메일, 인터넷 커뮤니티, 블로그 등과 같은 다양한 인터넷 서비스가 등장했고 이제는 실생활에 많은 영향을 미치고 있다. 이러한 서비스가 대중화됨에 따라서 이것을 악용하거나 방해하고자 하는 시도가 있었다. 예를 들어서, 불특정 다수의 블로그에 악성, 광고 댓글을 작성하거나 광고 게시물을 다수의 인터넷 커뮤니티에 게시하여 사람들에게 피해를 주는 것이 대표적인 사례들이다. 또한, 간단한 정보만으로 무료 이메일 계정을 만들 수 있는 서비스의 경우는 다수의 계정을 생성하여 스팸메일을 보내는데 사용될 수도 있다. 이러한 악의적인 시도 중에서 사람이 아니라 자동화된 프로그램(봇, bot)을 이용하는 경우 단시간 내 광범위하게 피해를 끼칠 수 있다. 자동화된 기계적 방법으로 이러한 서비스를 악용하고자 하는 시도는 근본적으로 서비스를 제공하는 측에서 사용자가 기계인지 사람인지 구분할 수 없기 때문에 발생한다고 볼 수 있다. 만약, 서비스 제공자가 사용자를 사람과 기계로 구분할 수 있다면 자동화된 도구를 이용한 악의적인 시도는 차단될 수 있을 것이다. 본 고에서 소개하는 CAPTCHA(이하 캡차)가 이러한 목적으로 제안되었고, 현재 많은 분야에서 다양하게 활용되고 있다.

CAPTCHA는 컴퓨터와 사람을 구분할 수 있게 해 주는 완전 자동화된 공개 튜링 테스트를 의미

CAPTCHA는 "Completely Automated Public Turing test to tell Computers and Humans Apart"의 줄임말로써, 그 이름이 의미하듯이 컴퓨터와 사람을 구분할 수 있게 해 주는 완전 자동화된

〈그림 1〉 텍스트 기반 캡차의 예(reCAPTCHA)

공개 튜링 테스트를 의미하고 있다[1]. 즉, 캡차가 제시하는 문제는 사람에게는 해결하기 쉬운 문제이나 기계가 자동화된 방법으로는 해결하기 어려운 문제이다. 주로 신호처리 기술, 인공 지능 관련 기술들이 캡차의 공격 시 활용된다. 〈그림 1〉은 대표적인 텍스트 기반의 캡차의 예를 보여주고 있는데, 이러한 캡차는 웹사이트 회원 등록 과정에서 보안 강화, 스팸성 블로그 댓글 방지 등과 같은 용도로 현재 많이 이용되고 있다.

역사적으로는 캡차는 1996년 Moni Naor[2]에 의해서 이론적으로 처음 제안된 것으로 보인다[3]. 캡차를 공개적으로 처음 활용한 사례는 Alta-Vista의 웹 검색 엔진이다[3-4]. Alta-Vista는 악의적인 사용자가 그들의 검색 엔진에 URL(Uniform Resource Locator)을 자동화된 방식으로 반복적으로 제출하여 검색 엔진 상 검색어 순위에 영향을 미치는 문제점을 발견하였고, Broder[4]는 이 문제를 해결하기 위해서 텍스트 기반의 캡차를 사용하였다. 이와 유사한 악의적인 서비스 이용은 인터넷 검색 서비스를 제공하는 업체가 공통적으로 겪고 있는 문제이다. 또한, Yahoo는 채팅 서비스를 제공하고 있었는데, 봇이 채팅룸으로 들어와서 사용자들에게 특정 사이트를 광고하는 문제가 발생하였다. 이 문제를 해결하기 위해서 Ahn[5]은 캡차를 사용하였고, 캡차의 구체적인 개념과 정형화도 Ahn에 의해서 정립되었다[1]. 캡차는 문서 암호화, 보안 통신과 같은 높은 수준의 보안을 요구하는 분야에서 활용되는 것이 아니다. 캡차는 사람인 사용자와 악의적인 자동화된 공격을 구분하고, 악의적인 방법으로 캡차의 문제를 해결하는 데 있어서 높은 비용이 수반될 때, 그 비용 대비 효율이 높은 장점을 활용하고자 하는 것이다.

본 고에서는 캡차의 개념과 종류와 활용 사례를 소개하고, 캡차의 취약성과 안전성 분석에 대해서 정리하고자 한다. 2장에서는 캡차의 개념 및 분류에 대해서 살펴보고, 3장에서는 캡차의 활용 가능 분야와 실제 활용 사례들을 소개한다. 4장에서는 현재 가장 많이 활용되고 있는 텍스트 기반 캡차의 취약성을 이용한 공격 방법에 대해서 살펴보고, 캡차 설계 시 고려해야 할 사항들을 제시하고, 5장에서 본 고를 요약하고 마무리한다.

Ⅱ. 캡차의 개념 및 분류

캡차는 1절에서 기술한 바와 같이 사람은 높은 확률로 해결할 수 있으며 현재의 컴퓨터 프로그램은 쉽게 풀 수 없는 문제를 의미한다[1,5]. 이 조건을 만족시키는 문제는 캡차로써 활용될 수 있는데, 대표적인 경우가 인공 지능의 문자 인식 문제에 기반을 둔 텍스트 기반의 캡차이고, 텍스트 기반의 캡차의 취약성과 단점을 보완하기 위해서 음성, 정지 영상, 동영상 기반의 캡차가 개발되고 있다.

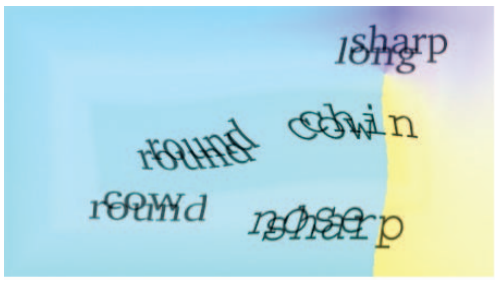
1. 텍스트 기반 캡차

텍스트 기반의 캡차는 인터넷 서비스를 이용하면서 가장 흔하게 접할 수 있는 고전적인 캡차이다. 텍스트 기반의 캡차는 무작위로 문자들을 선택하여 잡음이 첨가된 배경에 선택된 문자의 외형을 왜곡시켜 이미지의 형태로 제시하고 사용자로 하여금 제시된 문자를 답하게 하는 방식이다. 〈그림 1〉은 텍스트 기반의 대표적인 예인 reCAPTCHA를 보여주고 있다.

텍스트 기반의 캡차는 사람은 높은 확률로 제시된 문자를 유추할 수 있으나 컴퓨터로는 인식하기 어렵다는 동기에서 개발되었다. 예를 들어서, 텍스트 기반의 캡차를 컴퓨터가 자동으로 풀기 위해 가장 간단히 사용할 수 있는 방식은 기존의 OCR(Optical Character Recognition) 기술을 활용하여 문자를 인식하는 방식인데, 이 경우 문자 인식을 위한 특징점이 왜곡된 문자 외형에서는 정형화된 경우와는 상이하게 추출되어 인식에 어려움이 있을 수 있다.

고전적인 텍스트 기반의 캡차로 Gimpy, EZ-Gimpy, Gimpy-R 등이 여기에 해당된다. Gimpy,

〈그림 2〉 EZ-Gimpy 캡차의 예



〈그림 3〉 Gimpy 캡차의 예

EZ-Gimpy는 소규모 사전 데이터에서 단어를 선택하여 그 단어의 외형을 왜곡시키고 그 모습을 이미지로 형상화한 후, 잡음이 첨가된 배경에 위치시켜 사용자에게 제시하는 방법이다. Gimpy-r은 무작위로 문자로 선택하여 마찬가지로 외형을 왜곡시킨 후, 잡음이 있는 배경과 함께 사용자에게 제시하는 유형의 캡차이다. 〈그림 2, 3〉은 각각 EZ-Gimpy, Gimpy 캡차의 예[1]를 보여주고 있다.

〈그림 1〉은 reCAPTCHA를 보여주며, reCAPTCHA는 왜곡된 문자의 외형에 긴 선을 덧붙여 캡차를 생성한다. reCAPTCHA의 경우, 캡차를 OCR의 한계를 극복하는데 활용되고 있다. 오래된 서적을 디지털화하는 경우 문자 인식을 위해 대부분의 경우와 마찬가지로 OCR기술을 이용하게 되는데, 문자가 얼룩이나 낙서 등으로 인해 OCR을 이용해 인식이 불가능한 경우가 발생하는 경우가 있다. 이 문제는 대부분 사람이 수작업으로 확인하여 정확한 문자를 입력해야 하는데 이 작업은 많은 비용과 시간을 요구한다. reCAPTCHA는 이런 경우에 활용되고 있다. reCAPTCHA는 두 개의 문자 기반의 캡차를 제시한다. 둘 중 하나는 캡차를 풀고 있는 대상이 사람이며 캡차를 풀 수 있을 정도의 능력이 있는지 확인하는 것으로써 캡차를 제시하는 컴퓨터가 그 답을 알고 경우이다. 제시된 다른 하나의 캡차는 오래된 서적을 디지털화하는 과정의 OCR과정에서 실패한 단어로써, 만약 컴퓨터가 만든 캡차를 통과한 사용자에 한해서 이 캡차의 답을 저장한다. 저장된 데이터 중에서 높은 비율로 나온 단어가 OCR 단계에서 실패했던 단어를 디지털화하는데 사용된다.

텍스트 기반의 캡차는 구현이 용이하고, 적은 양의 기본 데이터로 다양한 경우의 문제를 생성할 수 있는 장점이 있다. 예를 들어서, 알파벳 대소문자로 4자리 텍스트 기반 캡차를 만드는 경우, 52개의 기본 정보만으로 52^4(약 730만) 조합을 생성할 수 있다. 하지만, 텍스트 기반의 캡차는 컴퓨터 비전과 영상처리 분야의 기술들을 이용하여 무력화 될 수 있다[6]. 반면, 이러한 공격에 대비하기 위해서 텍스트 기반의 캡차의 문제를 복잡하게 만들 경우, 사람조차도 문제를 쉽게 답을 할 수 없는 경우가 발생할 수 있는 단점이 존재한다.

2. 이미지 기반 캡차

텍스트 기반의 캡차는 인공지능 기술과 영상처리 기술을 이용하여 공격하여 무력화시킬 수 있어 안전성을 강화하기 위해 텍스트 기반 캡차의 대안으로 이미지 기반의 캡차가 활용되고 있다. 이미지 기반 캡차는 사진이나 그림, 이미지 등을 이용하여 문제를 만들어 사용자에게 제시하고 사용자로 하여금 문제를 풀게 하는 캡차이다. 예를 들어서, 특정 사물의 그림을 보여주고 그 이름을 입력하게 하거나 같은 종류의 물체를 이미지에서 선택하는 캡차 등이 여기에 포함된다.

안전성을 강화하기 위해 텍스트 기반 캡차의 대안으로 이미지 기반의 캡차가 활용되어 있어

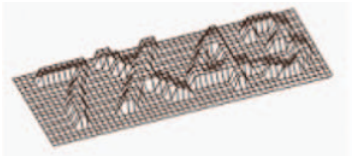
Chew[7]는 "naming images Captcha", "distinguishing images Captcha", "identifying anomalies Captcha"와 같은 이미지기반의 캡차를 제안하였다. "naming Images Captcha"는 제시된 이미지들을 모두 표현할 수 있는 단어를 입력하는 것이며, "distinguishing images Captcha"는 두 개의 이미지 집합이 주어지고, 각 집합은 동 수의 이미지를 포함하

1) http://www.cs.sfu.ca/~mori/research/gimpy/

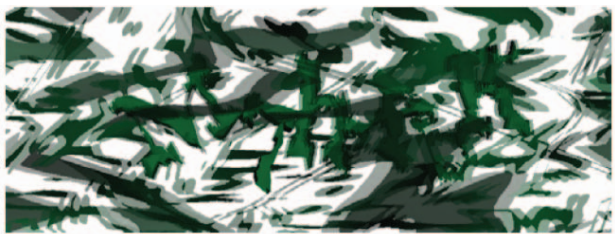
〈그림 4〉 PIX 캡차의 예

고 있으며 두 집합이 같은 주제를 표현하고 있는지 다른 주제를 표현하고 있는지를 물어보는 캡차이다. "identifying anomalies images Captcha"는 6개의 이미지를 제시하는데, 5개는 같은 주제를 표현하고 있지만, 나머지 한 개는 이질적인 주제를 표현하고 있는데, 이질적인 주제를 표현하고 있는 이미지를 선택하는 캡차이다. Ahn[13]은 "ESP game"이라는 게임을 만들고 그것을 이용하여 이미지에 대한 메터데이터를 레이블링하였고, 이렇게 구축된 데이터베이스를 이용하여 "PIX CAPTCHA"에 활용하였다. "PIX CAPTCHA[2]"는 레이블링된 데이터베이스에서 동일한 물체로 분류된 이미지를 무작위로 4개를 선택하여 이미지를 왜곡하여 사용자에게 제시하고 어떤 대상을 제시한 것인지를 사용자에게 물어보는 방식이다. 〈그림 4〉는 PIC 캡차의 한 예[2]를 보여 주고 있는데, "baby"라고 레이블링된 이미지들을 데이터베이스에서 무작위로 4개 선택하여 보여준 것으로, 사용자는 이 이미지 캡차에 "baby"라고 답을 하면 된다.

2차원 정지, 동영상 기반 캡차 뿐만 아니라, 최근에는 인공적으로 3차원 이미지처럼 보이는 원근감을 갖는 이미지를 이용하여 캡차를 개발하는 방법도 제안되고 있다. Teabag 3D 캡차[8]는 3D 효과를 이용한 캡차에 해당되며 〈그림 5〉는 그 한 예를 보여주고 있다. 다른 접근 방법으로 Susilo[9]는 스테레오스코픽



〈그림 5〉 Teabag 3D 캡차의 예[8]

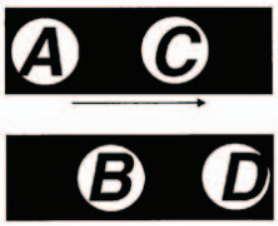


〈그림 6〉 스테레오 이미지를 이용한 캡차(STE-3D CAP)

(Stereoscopic)을 이용한 캡차(STE3D-CAP)도 제안하였는데, 〈그림 6〉은 STE3D-CAP의 한 예를 보여주고 있다. 하지만, 이러한 종류의 캡차는 경우에 따라서 사람인 사용자인 경우에도 사용 편의성, 문제 해결성 측면에서 불편함을 야기시킬 수 있다.

또한, 정지되어 있는 이미지를 이용하는 캡차 뿐만 아니라 움직이는 이미지를 이용한 캡차도 개발되어 활용되고 있다. nuCaptcha[3]는 비디오 스트리밍을 이용한 캡차 방식으로써, 기존의 정지 영상 만을 사용하는 텍스트 기반의 캡차와 유사하지만 텍스트가 정지해 있는 상태가 아니라 문자 자체가 움직임을 갖는 캡차이다. 〈그림 7〉

〈그림 7〉 비디오 스트리밍을 이용한 nuCaptcha



〈그림 8〉 움직이는 전경을 이용한 캡차

2) http://www.captcha.net/captchas/pix/
3) http://www.nucaptcha.com

은 nuCaptcha의 예를 보여 주는데, 문자열 "MAX"에 해당하는 캡차 중 2 프레임을 제시한 것이다. Qvarfordt[10]는 레이어(layer) 개념을 사용한 캡차를 제안하였다. 한 레이어(L1)는 일반적인 캡차 문제를 포함하고 있고, 또 다른 레이어(L2)는 L1의 인식을 방해하는 요소들을 포함시킨다. 예를 들어서 〈그림 8〉에서 L1은 텍스트 캡차 "ABCD"를 가지고 있고, L2는 검정색 배경에 투명한 원형의 패턴을 포함하고 있다. L2가 이동하면서 L1을 부분적으로 가리지만 사람의 경우 잔상과 기억의 효과로 캡차 문제를 해결할 수 있다.

이미지를 이용한 캡차는 텍스트를 이용한 캡차에 비해서 봇의 공격에 강인하고, 사용자에게는 풀기 쉬운 문제가 될 수 있다. 하지만, 이미지 캡차의 경우 텍스트 캡차보다는 문제를 구성하는데 필요한 데이터의 양이 증가하게 되고, 제한된 데이터 양에 의해서 캡차에서 제시할 수 있는 문제의 경우의 수가 줄어들 가능성이 있다. 또한, 이미지를 사전에 저장하기 위해서 텍스트에 비해 많은 저장 공간이 필요하고 이것은 텍스트 기반의 캡차에 비해서 높은 비용이 소요되는 것을 의미한다.

캡차는 웹사이트 계정을 생성하거나 게시물을 등록할 경우, 사람이 아닌 봇에 의해 악의적인 행위가 발생되는 것을 방지하는데 활용

Ⅲ. 캡차의 활용 사례

캡차는 웹사이트 계정을 생성하거나, 게시물을 등록할 경우, 사람이 아닌 봇에 의해 악의적인 행위가 발생되는 것을 방지하는데 활용될 수 있다. 캡차는 대표적으로 다음과 같은 분야에서 활용될 수 있다[5].

• 사전 공격 방지[11]

비밀번호는 계정을 보호하는 기본적인 보안 장치로써 활용되고 있다. 비밀번호를 이용한 보안 방식은 자동화된 사전 공격에 취약할 수 있는데, 정해진 횟수 비밀번호를 틀렸을 경우 캡차를 이용하게 되면 봇에 의한 사전공격을 방어 할 수 있다. 물론, 정해진 횟수 이상 로그인에 실패하였을 경우, 계정 자체에 접근하는 것을 막는 것도 사전 공격을 방어하기 위한 한 방법이 될 수 있으나, 이 경우 봇이 여러 번 잘못된 비밀번호로 접근하여 의도적으로 계정을 막히게 할 수 있는 가능성이 있다. 캡차는 이러한 문제점을 해결할 수 있는 좋은 방법이 될 수 있다.

• 온라인 투표

1999년 11월, Slashdot[4]은 어떤 학교에서 컴퓨터 공학을 전공하는 것이 가장 좋은지를 묻는 온라인 투표를 실시하였다. 한 사람이 여러 번 투표하는 것을 방지하기 위해서 투표할 당시의 아이피(IP)를 기록하였다. 그러나 카네기 멜론 대학의 한 학생이 카네기 멜론 대학에 중복 투표할 수 있는 프로그램을 제작하여 카네기 멜론 대학의 순위가 상승하게 되었고, 다음 날 MIT 학생들도 유사한 투표 프로그램을 제작하여 투표를 하였다. 결국, 투표는 양 대학에서 만든 봇들의 경쟁이 되었다. 캡차는 이러한 분야에서 사람만이 투표에 참여할 수 있도록 할 수 있게끔 시스템을 보완하는데 활용될 수 있다.

• 자동 계정 생성 방지

현재 많은 포털 사이트, 무료 이메일 제공 사이트가 존재하는데 이러한 서비스 업체들은 가입 시 개인 정보를 특별히 제공하지 않아도 무료 회원으로 등록이 가능하다. 이 경우, 악의적인 목적을 가지고 봇에 의해서 수많은 무료 계정을 생성할 수 있고 스팸 메일을 발송하는데 악용될 수 있다. 이러한 피해를 방지하기 위해서 회원 등록을 하는 과정에서 캡차가 활용될 수 있다.

〈그림 9〉 Naver社의 캡차

4) http://www.slashdot.org

〈그림 10〉 Google社의 캡차

〈그림 11〉 CNN社의 캡차

이것은 사이버 공간의 회원 등록 과정에 공통적으로 적용될 수 있다.

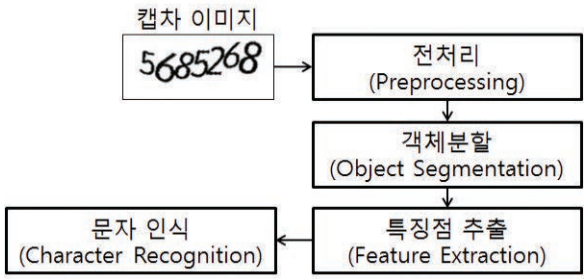
• 광고성 게시물 방지

개인 홈페이지 또는 블로그에 누구나 아무런 절차 없이 댓글이나 게시물을 작성할 수 있는 경우 봇에 의해 무차별적인 광고나 악성 댓글이 등록될 가능성이 높다. 미등록 사용자가 게시물이나 댓글을 작성하고자 할 때, 이에 대한 보완 수단으로 캡차를 활용하게 되면 봇에 의한 공격을 방지할 수 있을 것이다.

캡차는 구현이 복잡하지 않고, 유지 비용과 효과 측면에서 효율적이기 때문에 현재 많은 인터넷 서비스 업체에서 위와 같은 목적으로 광범위하게 활용되고 있다. 〈그림 9~11〉은 각각 현재 Naver社와 Google社, CNN社가 회원 가입 시 실제 사용하고 있는 캡차의 예를 보여 주고 있다.

Ⅳ. 캡차의 안전성 분석

캡차는 설계와 적용의 과정에서 알 수 있듯이 문서 암호화, 보안 통신과 같이 엄격한 보안이 요구되는 곳에서 활용되는 것이 아니다. 즉, 캡차는 적당한 노력이나 자원이 있을 경우 풀릴 가능성이 항상 존재한다는 것이다. 따라서, 항상 캡차는 자동화된 방법으로 캡차를 푸는데 필요한 비용과 시간을 고려해서 적용하여야 한다. 또한 캡차의 안전성을 위해서 캡차의 문제 자체를 사람조차도 해결하지 못하게끔 만들면 사용자들에게 불편함을 줄 수



〈그림 12〉 텍스트 기반 캡차 공격의 일반적인 절차

있으며 그 활용성이 크게 줄어들 가능성도 있다. 이러한 사항들을 고려하여 컴퓨터에게는 풀기 어렵고 사람은 풀기 쉬운 캡차의 설계가 이루어져야 한다. 본 절에서는 현재 가장 많이 활용되고 있는 텍스트 기반의 캡차의 공격 방법과 사례를 제시하고자 한다.

텍스트 기반의 캡차가 현재 가장 보편적으로 활용되는 캡차인데, 텍스트 기반의 캡차는 다양한 영상처리 기술과 인공 지능 기술(예: Support Vector Machine, K Nearest Neighbors)을 활용하여 무력화될 수 있다. 텍스트 기반 캡차의 안전성을 검증하는 과정에서 많이 활용되는 기술은 객체 분할 기술과 문자 인식 기술이다. 이 두 가지 기술은 영상처리와 컴퓨터 비전 분야에서 중요하게 연구되는 분야이고, 오랜 역사를 가지고 있는 연구 주제이어서, 현재까지 수많은 기술들이 제안되었고 활용되고 있다.

[12]에서도 제안되었지만, 근본적으로 텍스트 기반 캡차의 공격은 문자 인식 문제와 같을 수 있으므로, 공격 절차는 물체 인식 또는 문자 인식의 과정과 동일하다고 할 수 있다. 〈그림 12〉는 텍스트 기반 캡차를 공격하는 일반적인 절차를 보여준다. 전처리 과정에서는 공격하고자 하는 캡차 이미지의 잡음 제거, 이진화, 불필요한 선 제거 등과 같이 객체 분할을 원활하게 하기 위한 여러 가지 처리를 하게 된다. 이후, 객체 분할 단계에서는 각 문자별로 분리하는 과정을 거치게 되고, 이후 분할된 각각의 문자를 이용하여 문자 인식 과정에서 필요한 특징점을 추출하게 된다. 이 때, 홀의 개수나 문자의 폭, 문자의 높이 등과 같은 것들이 특징점으로 추출될 수 있는 것들에 해당된다. 마지막으로 추출된 특징점을 인공 지능 기술에 적용하여 문자 인식으로

과정을 거쳐 자동적으로 캡차 문제를 해결하게 된다. 이러한 공격을 방어하기 위해 객체 분할 단계와 문자 인식 부분에서 대비책을 마련할 수 있는데 Bursztein[6]은 지금까지 기존의 방어책을 다음과 같이 정리하였다.

- 객체 분할 대비
  - 복잡한 배경 화면
  - 별도 라인 추가
  - 문자간 공간 제거
- 문자 인식 대비
  - 다중 폰트 사용
  - 가변 폰트 사이즈
  - 캡차 전반에 대한 왜곡
  - 문자 블러링
  - 다양한 종류의 문자 외형 왜곡(틸팅, 웨이빙)

Bursztein[6]은 "Decaptcha"라고 하는 정형화된 캡차 공격 방법을 제안하였다. 제안된 "Decaptcha"를 이용하여 유명한 15개의 웹사이트에 적용하여 분석하였는데, 15개의 웹사이트 중 13개가 취약하다는 분석 결과를 얻었다. 〈표 1〉은 "Decaptcha"를 이용한 공격 결과를 보여주고 있다. 〈표 1〉에서 알 수 있듯이 각 서비스에서 이용되고 있는 캡차는 객체 분할에 대한 대비책을 이미 가지고 있다. 그럼에도 불구하고 일부 서비스는 높은 확률로 공격이 성공하는 것을 결과를 통해 알 수 있다.

이 실험 결과를 바탕으로 [6]에서는 위에서 정리된 일반적인 대비책이 안전하지 않을 수 있고, 각 과정에 캡차 설계 시 고려해야 할 새로운 권고안을 다음과 제시하였는데, 위에서 정리된 일반적으로 받아들여지는 설계 원칙이 분석 결과 문제가 있음을 주장하였다.

- 캡차 설계 기본
  - 정해지지 않은 길이의 캡차 사용
  - 정해지지 않은 폰트 크기 사용
  - 캡차의 문자를 물결처럼 왜곡
- 객체 분할 대비
  - 문자 간 공간 제거 적극 활용
  - 복잡한 배경은 보안 관점에서는 실효성 없음
  - 별도의 선을 사용할 경우 긴 선을 사용
  - 별도의 선을 캡차와 겹치도록 배치
- 문자 인식 대비
  - 복잡하지 않고 혼돈스럽지 않은 문자셋 사용
  - 왜곡 사용 자제
  - 문자 회전은 객체 분할 대비책과 병용

이미지기반 캡차인 경우 아직까지는 기술적 한계가 있으며, 각각의 이미지와 메타데이터를 연결하는 것도 이미지 데이터베이스 크기에 따라 달라지고, 현실적으로 모든 이미지와 메타데이터를 연결하는 것도 불가능

이미지 기반 캡차의 경우 이미지를 인식하거나 이미지에 연결된 메타데이터를 이용하여 공격할 수 있는 방법을 생각할 수 있다. 하지만, 이미지 인식의 경우는 주어지는 이미지기반 캡차의 문제에 따라 요구되는 것이 달라질 수 있고, 기술적으로 아직까지는 한계를 가지고 있다. 또한, 각각의 이미지와 메타데이터를 연결하는 것도 이미지 데이터베이스 크기에 따라서

〈표 1〉 캡차 공격 결과[6]

서비스	정확도	객체 분할 대비책
Authorize	66%	Background confusion
Baidu	5%	Collapsing
Blizzard	70%	Background confusion
Captcha.net	73%	Background confusion
CNN	16%	Line
Digg	20%	Line
eBay	43%	Collapsing
Google	0%	Collapsing
Megaupload	93%	Collapsing
NIH	72%	Background confusion
Recaptcha	0%	Collapsing
Reddit	42%	Background confusion
Skyrock	2%	Background confusion
Slashdot	35%	Lines
Wikipedia	25%	N/A

달라지고 현실적으로 가능한 모든 이미지와 메타데이터를 연결하는 것도 불가능하다.

캡차 자체의 취약성에 기인한 공격과는 다른 종류의 공격도 고려해 볼 수 있다. 캡차 공격 방법 중에서 가장 강력한 것은 인력을 이용한 공격 방법이다. 캡차는 대량 광고 메일을 자동으로 발송하는 업체에게는 커다란 장애물이다. 이 경우, 후진국의 값싼 노동력을 활용해서 캡차를 해결하는 접근 방법을 생각해 볼 수 있다. 실제 다음과 같이 캡차를 풀어주는 서비스가 운영되고 있는 실정이다.

- DEATH by CAPTCHA
  - 주소: http://www.deathbycaptcha.com
  - 비용: 1천개의 캡차 해결에 1.39달러
  - 속도: 1개의 캡차 푸는 속도: 대략 10초
  - 평균 정답률: 약 94%

이와 같이 사람이 중간에 개입되어 캡차를 공격하는 방법은 캡차 방식의 보안이 근본적으로 가지고 있는 문제이고 모든 종류의 캡차에 적용될 수 있는 위협이다.

Ⅴ. 결론

본 고에서는 캡차의 개념과 활용 사례를 정리하였고, 현재 가장 많이 사용되고 있는 텍스트 기반 캡차 방식들의 안전성에 대한 분석 자료를 제시하였다. 캡차는 사람은 쉽게 풀 수 있으나 자동화된 기계는 쉽게 풀 수 없는 문제를 의미한다. 이러한 특징으로 인해 캡차는 온라인 투표, 봇에 의한 악성 댓글 방지, 사전 공격 방어, 무차별 계정 등록 방지 등과 같은 분야에서 광범위하게 활용되고 있다. 캡차는 텍스트 기반, 이미지 기반, 오디오 기반, 지식 기반으로 분류될 수 있으나 현재 가장 많이 사용되고 있는 것은 텍스트 기반의 캡차이고, 그에 따라 다양한 공격 방법이 제안되고 있다. 실제 운용되고 있는 캡차들이 정형화된 공격 방법에 취약하다는 것이 이미 실험적으로 제시되었고, 이에 따른 설계 권고안도 제시되었다. 하지만 캡차에 대한 보안성 평가 기준, 구체적인 설계 권고안, 적용 기준은 아직 정립되지 않고 있는 실정이다. 향후 이러한 분야에 대한 연구가 더 필요할 것으로 판단된다.

참 고 문 헌

[1] L. von Ahn, M. Blum, and J. Langford, "Telling Humans and Computers Apart Automatically," Commun. ACM, vol. 47, no. 2, pp. 56–60, Feb. 2004.

[2] M. Naor, "Verification of a human in the loop or Identification via the Turing Test," http://www.wisdom.weizmann.ac.il/~naor/PAPERS/human.pdf, 1996 [accessed 26.03.2014].

[3] C. J. Hernandez-Castro and A. Ribagorda, "Pitfalls in CAPTCHA design and implementation: The Math CAPTCHA, a case study," Computers & Security, vol. 29, no. 1, pp. 141–157, Feb. 2010.

[4] M. D. Lillibridge, M. Abadi, K. Bharat, and A. Z. Broder, "Method for selectively restricting access to computer systems," US6195698 B127-Feb-2001.

[5] L. V. Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using Hard AI Problems for Security," in Proceedings of the 22Nd International Conference on Theory and Applications of Cryptographic Techniques, Berlin, Heidelberg, 2003, pp. 294–311.

[6] E. Bursztein, M. Martin, and J. Mitchell, "Text-based CAPTCHA Strengths and Weaknesses," in Proceedings of the 18th ACM Conference on Computer and Communications Security, New York, NY, USA, 2011, pp. 125–138.

[7] M. Chew and J. D. Tygar, "Image Recognition CAPTCHAs," in Information Security, K. Zhang and Y. Zheng, Eds. Springer Berlin Heidelberg, 2004, pp. 268–279.

[8] V. D. Nguyen, Y.-W. Chow, and W. Susilo, "Breaking a 3D-Based CAPTCHA Scheme," in Information Security and Cryptology – ICISC 2011, H. Kim, Ed. Springer Berlin Heidelberg, 2012, pp. 391–405.

[9] W. Susilo, Y.-W. Chow, and H.-Y. Zhou, "STE3D-CAP: Stereoscopic 3D CAPTCHA," in Cryptology and Network Security, S.-H. Heng, R. N. Wright, and B.-M. Goi, Eds. Springer Berlin Heidelberg, 2010, pp. 221-240.

[10] P. Qvarfordt, E. G. Rieffel, and D. M. Hilbert, "Motion and interaction based captchas," US20080127302 A129-May-2008.

[11] B. Pinkas and T. Sander, "Securing Passwords Against Dictionary Attacks," in Proceedings of the 9th ACM Conference on Computer and Communications Security, New York, NY, USA, 2002, pp. 161-170.

[12] A. A. Chandavale, A. M. Sapkal, and R. M. Jalnekar, "Algorithm to Break Visual CAPTCHA," in 2009 2nd International Conference on Emerging Trends in Engineering and Technology (ICETET), 2009, pp. 258-262.

[13] L. von Ahn and L. Dabbish, "Labeling Images with a Computer Game," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, New York, NY, USA, 2004, pp. 319-326.

김 웅 희

2000년 2월 고려대학교 전기전자전파공학부 졸업
2002년 2월 한국과학기술원 전기및전자공학과 석사
2002년 1월~2006년 6월 ETRI 부설연구소 연구원
2009년 6월~2011년 11월 KIST 유럽분원 연구원
2012년 12월~현재 ETRI 부설연구소 연구원

지 성 택

1985년 2월 서강대학교 수학과 졸업
1987년 2월 서강대학교 수학과 석사
1999년 2월 고려대학교 수학과 박사
1989년~1999년 12월 ETRI 선임연구원
2000년 1월~현재 ETRI 부설연구소 책임연구원