Journal of The Korea Institute of Information Security & Cryptology(JKIISC) ISSN 1598-3986(Print)
VOL.23, NO.5, October 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.5.825

CA Arcot VPS의 취약점 분석*

이 상 호,[1†] 김 성 호,[1] 양 대 헌,[1] 이 경 희[2‡]
[1]인하대학교, [2]수원대학교

The Vulnerability Analysis of CA Arcot VPS*

Sang-ho Lee,[1†] Sung-ho Kim,[1] Dea-hun Nyang,[1] Kyung-hee Lee[2‡]
[1]INHA University, [2]The University of Suwon

요 약

미국의 Arcot사는 가상 세션을 이용하여 트랜잭션 변경 사항을 표시하는 안전한 온라인 금융 거래 서비스 솔루션을 판매 중이며, 해당 기술의 특허를 출원 중이다. 하지만 VPS(Virtual Private Session)가 제공하는 캡챠의 구성 방식에 의해 취약점을 갖는다. VPS가 제공하는 캡챠는 색상정보를 이용한 공격이 가능함을 보였고, 이는 VPS 또한 안전성을 확신할 수 없음을 시사한다. 이 논문에서는 VPS의 공격 방법을 제시하고 유사 VPS를 만들어 앞서 제시한 방법으로 모의 공격을 통한 취약점을 알아본다.

ABSTRACT

CA Arcot corporation in U.S.A has secure on-line financial trade solution and patent that verify whether transaction had change using virtual session. But, VPS(Virtual Private Session) has another vulnerability by way to construct CAPTCHA. We can't fully trust safety of VPS, Cause it could be attacked by using color information of CAPTCHA. In this paper, We suggest the method of attack VPS, and also point out the vulnerability of VPS though simulation.

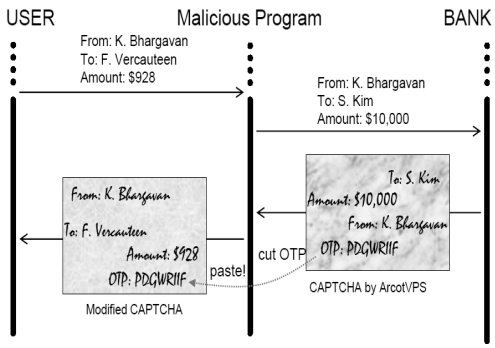
Keywords: CAPTCHA, MITB, VPS

I. 서 론

CA Arcot에서는 MITB[1] 공격에 대응하기 위해 VPS[2][3]를 고안하였다. VPS는 브라우저에서 브라우저 도우미 개체(BHO)로 인한 트랜잭션 변경 사항을 사용자에게 제공함으로서 MITB와 같은 공격을 막는 방식이다. 사용자는 VPS가 제공하는 캡챠[4]를 읽고 확인코드를 입력하면 된다. [그림 1]은 VPS를 인터넷 뱅킹 계좌 이체 승인 페이지에 사용한 예를 보여준다. 사용자와 서버 사이에 MITB 공격으로 트랜잭션이 변경된 경우, 사용자는 입력한 내용과 VPS가 제시한 캡챠를 비교함으로써 트랜잭션을 중지할 수 있다. 하지만 은행이 사용자에게 제시하는 캡챠 또한 변조되었다면 공격자는 사용자의 눈을 속여 악의적인 계좌 이체를 수행할 수 있다. 이는 캡챠의 색상정보를 이용해 가능함을 보였으며, 공격자가 MITB 공격에 이어 캡챠를 재생산해 사용자에게 제시한다면 VPS는 무용지물일 뿐이다[5][6]. 더불어 공격자는 VPS 원본 캡챠에서 필요한 정보를 추출한 후 이를 이용해 캡챠를 재생산하고 사용자에게 노출하는 과정이 캡챠의 난이도에 전혀 영향을 받지 않는다. 결국 VPS 또한 변조가 가능하며 VPS의 무결성을 확신할 수 없다.

접수일(2013년 6월 3일), 게재확정일(2013년 7월 24일)
* 이 논문은 인하대학교의 지원에 의하여 연구되었음.
† 주저자, 181cm76kg245@gmail.com
‡ 교신저자, khlee@suwon.ac.kr(Corresponding author)

〔그림 1〕 계좌 이체 승인 페이지에 사용한 CA Arcot VPS



〔그림 2〕 VPS 이체 승인 페이지 변조

II. VPS의 보안성 고찰

〔그림 1〕과 같이 캡챠의 문자열과 배경이 다른 색으로 구성된 경우, 색상정보를 이용하여 배경과 문자열을 분리해 낼 수 있다. 캡챠 이미지를 군집화 알고리즘을 이용하여 픽셀을 세 군집으로 분리한 후, 군집의 개수가 가장 적은 군집을 선택하여 문자열만 캡챠에서 추출한다.

〔그림 1〕의 VPS의 경우 계좌 이체 정보와 OTP 문자열에 각각 일정하지 않은 폰트와 필터가 적용되어 있다. 또한 OTP 문자열의 위치가 고정되어 있지 않기 때문에 OTP 값을 추출해내기는 어려워 보인다. 하지만 계좌 이체 정보의 요소들(송신자, 수신자, 금액, OTP)이 캡챠 내에 일정한 거리를 두고 있으므로 이러한 특징을 이용하여 각각의 요소를 분리한다면 OTP 문자열을 추출하는 문제는 분리된 개별 요소 중에서 OTP를 선택하는 문제로 바뀌게 된다. 더불어 OTP 문자열의 평균 길이 정보를 이용한다면 OTP 추출의 확률을 높일 수 있다.

이 논문에서는 〔그림 2〕의 공격 시나리오를 고려한다.

은행은 사용자에게 〔그림 1〕과 같은 계좌 이체 승인 페이지를 제공한다는 가정 하에 사용자는 인터넷 뱅킹 서비스를 이용한다. 이때 MITB 공격에 의해 금액과 수신자가 변조된다. 은행은 계좌 이체 내용을 VPS를 통해 문자열 기반 캡챠의 형식으로 사용자에게 제시한다. 만약 은행이 제공하는 캡챠가 그대로 사용자에게 노출된다면 사용자는 변조된 계좌 이체 내용을 확인, 계좌 이체를 중단할 수 있다. 때문에 공격자는 캡챠를 재구성해야 할 필요가 있다. 공격자는 사용자가 입력한 정보(송신자, 수신자, 금액)로 새로운 캡챠를 만들고 이에 은행이 제공하는 캡챠를 가로채 OTP를 추출하여 공격자가 생성한 캡챠에 오버레이 한 후 사용자에게 제시하면 사용자는 계좌 이체의 내용을 확인한 후 OTP를 입력하여 계좌 이체를 완료한다.

공격자는 VPS에서 OTP를 추출하고 변조하는 일련의 과정을 자동화하여 공격의 범위를 넓힘과 동시에 수행시간을 단축시킴으로서 사용자로 하여금 공격의 대상이 되고 있다는 사실을 눈치 챌 수 없도록 할 수 있다.

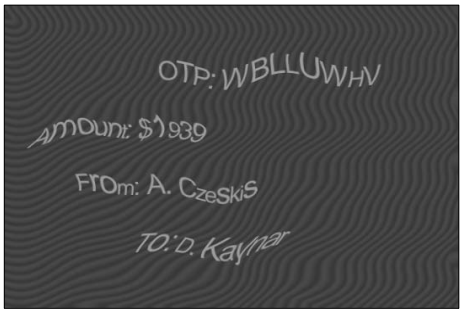
색상과 문자열 길이 정보를 이용해 OTP 문자열을 얼마나 효과적으로 추출할 수 있는지는 VPS 모의 공격을 통해 살펴보도록 한다.

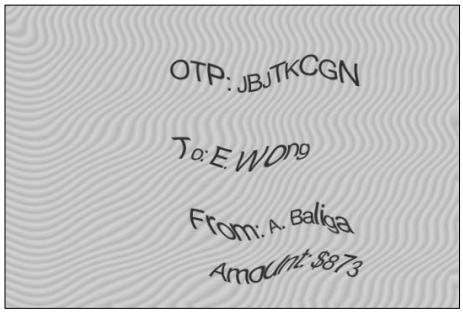
III. VPS 모의 공격

3.1 VPS 승인 페이지 생성

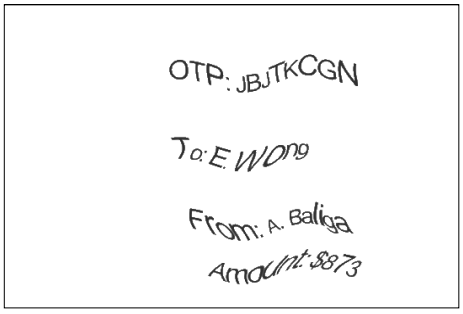
앞서 설명한 공격 방법의 성공률을 실험해 보기 위해 〔그림 3〕과 같은 유사 VPS를 제작하였다. 해당 캡챠는 다음과 같은 기준을 두고 제작하였다.

- 배경은 2가지 색상을 사용하고 문자열은 배경과 다른 색상을 사용하였다.
- 배경이 어두운 색상을 띄면 문자열은 밝은 색상을 사용, 반대로 배경이 밝은 색상을 띄면 문자열은 어두운 색상을 사용하였다.
- 문자열(계좌 이체 정보) 각각의 위치는 무작위로 지정하였다.
- 문자열에는 문자 왜곡 필터를 적용시켰고 OTP는 8자리 대문자, 이체 액수는 $10~2,000, 송·수신자의 이름은 ACM CCS 2008의 저자 목록

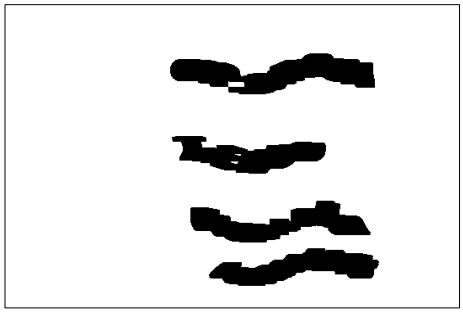




〔그림 3〕 CA Arcot VPS와 유사하게 제작한 캡챠



(a) 원본에서 추출한 문자열 이미지



(b) 추출된 문자열 이미지를 마스크한 이미지

〔그림 4〕 OTP 문자열을 선택하기 위해 생성한 이미지

(200명)에서 무작위로 선택하였다.

- 문자 크기는 각 문자별 25 ~ 40픽셀 중 무작위로 선택하였다.

3.2 VPS의 OTP 문자열 추출

이 절에서는 OTP 문자열을 추출하기 위한 과정을 설명한다.

3.2.1 배경색과 문자열 분리

〔그림 3〕을 살펴보면, 해당 이미지에는 3가지의 대표색이 존재하고 배경 색상 보다는 문자열을 나타내는 색상이 더 적게 사용된 것을 알 수 있다. 문자열을 분리해내기 위해 군집화 알고리즘 K-means++〔7〕을 사용하였다. 먼저 캡챠의 픽셀을 3가지 군집으로 나눈 후 나누어진 군집 중에서 픽셀 수가 가장 적은 군집을 선택하였다. 선택된 군집의 픽셀 위치 정보를 이용하여 〔그림 4-a〕와 같은 이미지를 생성하였다.

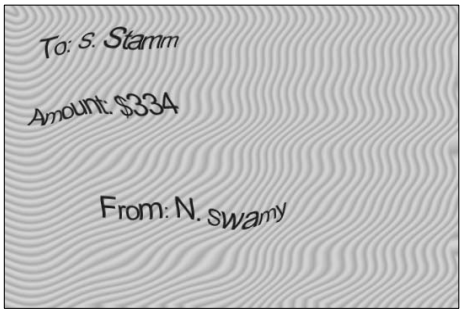
Input:
$I = \{i_1, \cdots, i_k\}$ (Instances to be clustered)
n (Number of clusters)
Output:
$C = \{c_1, \cdots c_n\}$ (Cluster centroids)

Foreach w **in** width
  Foreach h **in** height
    get pixel(w, h) **into** I
  End
End
C = **K-Means++**(I, n)
search Minimum a number of cluster in C

〔그림 5〕 문자열 분리 의사코드

3.2.2 배경과 분리된 문자열의 구별 및 OTP 선택

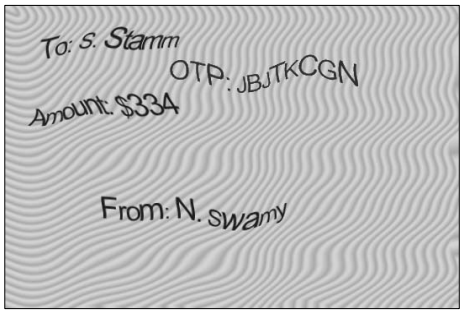
캡챠의 계좌 이체 정보(송신자, 수신자, 금액, OTP)를 담고 있는 픽셀들은 서로 근접한 위치에 있지만 각각의 성분은 일정한 간격을 두고 있다. 추출한 문자열 이미지를 순차적으로 검색하여 문자열에 해당



(a) 공격자가 사용자 계좌 이체 정보로 생성한 캡챠

(b) 문자열 길이 정보를 이용해 추출한 OTP

〔그림 6〕 승인 페이지를 변조하기 위해 생성한 캡챠



〔그림 7〕 공격자에 의해 변조된 승인 페이지

하는 픽셀이 검색되었을 때 왼쪽에서 오른쪽 방향으로 고정 길이의 픽셀을 추가한다면 〔그림 4-b〕와 같은 마스크 이미지를 생성 할 수 있다. 마스크 이미지에서 픽셀의 연결 요소의 특징을 이용하여 다시 4개의 성분으로 분리하면 1/4 확률로 OTP 문자열을 찾아낼 수 있다.

3.2.3 문자열 길이 정보를 이용한 OTP 선택

추출한 문자열 중 OTP 문자열만이 가지는 정보를 이용한다면 더 높은 확률로 OTP 문자열을 추출해 낼 수 있다. 공격자는 8자리 대문자로 이루어진 OTP 문자열의 길이를 가늠하여 OTP 문자열을 추출할 수 있다.

```
Foreach text in strings
   If( text.length is similar to average O
   TP length the most)
      return text
End
```

〔그림 8〕 문자열 길이를 이용한 OTP선택 의사코드

3.3 OTP 추출 실험

앞서 설명한 방법으로 OTP 문자열 추출의 성공률을 알아보기 위해 중복 없는 3006개의 캡챠를 실험에 사용하였다. 배경과 문자열을 분리하는 과정은 3006회 모두 성공 하였다. 분리한 문자열 중 각각의 요소(계좌 이체 정보)를 분리하는 과정 역시 3006회 모두 성공하였다. 〔표 1〕에는 OTP 문자열 추출에 관한 실험의 결과를 정리하였다.

〔표 1〕 유사 VPS의 OTP 추출 실험 결과

	사용한 캡챠 수	문자열 분리 성공	OTP 추출 성공	OTP 추출 성공 확률
실험 1	1000	1000	823	82.3 %
실험 2	1001	1001	837	83.6 %
실험 3	1005	1005	823	81.9 %

첫 번째 실험에서 실험자는 OTP 문자열의 길이를 알고 있으며 계좌 이체 정보가 렌더링 되었다고 가정했을 때 길이를 계산하여 OTP 문자열의 길이와 가장 가까운 성분을 추출 하였다. 실험 1에서 사용된 캡챠 1000개의 OTP 문자열 평균 길이는 159픽셀이었다. 두 번째 및 세 번째 실험에서는 첫 번째 실험의 OTP 문자열 평균 길이와 가장 근사한 값을 갖는 문자열을 추출하였다. 유사 VPS에 대한 공격 결과 OTP 문자열을 80%이상의 확률로 추출하였다.

3.4 VPS 승인 페이지 변조

〔그림 2〕의 시나리오에서 MITB 공격에 의해 계좌 이체 정보가 조작 되었다면 사용자는 승인 페이지를 통해 트랜잭션이 변경되었음을 알고 계좌 이체를 중지

할 수 있다. 〔그림 2〕의 시나리오를 완벽히 수행하기 위해서는 은행이 제공하는 승인 페이지를 한 번 더 변조해야 한다.

〔그림 6-a〕와 같이 사용자가 입력한 정보(송신자, 수신자, 금액)를 이용해 공격자는 캡챠를 새로 생성한다. 은행이 제공하는 캡챠에서 추출한 OTP〔그림 6-b〕를 오버레이하여 캡챠를 생성하고 사용자에게 제시한다. 공격자가 최종적으로 생성한 캡챠는 〔그림 7〕과 같다. 사용자는 자신이 입력한 정보를 확인하고 OTP를 입력하여 계좌 이체를 계속 진행하지만 실질적으로 계좌 이체는 공격자가 변조한 내용으로 이루어지며 사용자에게 제시된 정보만으로는 사용자는 악의적인 계좌 이체인지 정상적인 계좌 이체인지 판단 할 수 없다.

이는 캡챠의 색상정보를 이용한 공격으로서 색상정보를 이용한 OTP 추출, 변조 공격이므로 캡챠의 난이도를 어렵게 하여도 색상정보를 이용한 공격은 성공할 것이다.

IV. 결 론

인터넷 뱅킹에서 트랜잭션을 검증하지 않는 취약점이 있었고 이를 보안하기 위해 트랜잭션을 검증하는 VPS를 적용한 상황을 가정하였다. 하지만 VPS가 제시하는 캡챠의 구성 방식이 문제점을 낳는다. 앞서 모의 공격을 통해 80% 이상의 확률로 OTP를 추출하고, 추출한 OTP로 승인 페이지를 변조함으로서 VPS가 사용된 인터넷 뱅킹 서비스 환경 역시 MITB 공격에 취약함을 보였다. 또한 색상정보를 이용한 공격이므로 캡챠의 난이도에 영향을 받지 않는다. 이는 캡챠를 구성하는 방식의 문제이기 때문에 캡챠를 구성하는 방법을 재정의함으로서 VPS가 가지는 취약점을 보완 할 수 있을 것으로 보인다.

참고문헌

〔1〕 P. Guhring, "Concepts against man-in-the-browser attacks," http://www2.futureware.at/svn/sourcerer/CAcert/SecureClient.pdf

〔2〕 Arcot Systems, "Protecting Online Customers from Man-in-the-Browser and Man-in-the-Middle Attacks," http://www.ca.com/~/media/Files/whitepapers/protection-from-mitm-mitb-attacks-wp.pdf

〔3〕 R.A. Gopalakrishna, "Authentication using a turing test to block automated attacks," US 2009/0199272 A1, US Patent, Aug. 2009.

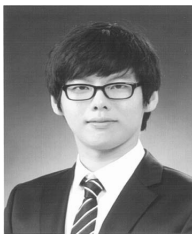
〔4〕 L.V. Ahn, M. Blum, N.J. Hopper, and J. Langford, "CAPTCHA: telling humans and computers apart," Euro-crypt'03, LNCS 2656, pp. 294-311, May. 2003.

〔5〕 S.Y. Huang, Y.K. Lee, G. Bell, and Z.h Ou, "A projection based segmentation algorithm for breaking MSN and YAHOO CAPTCHAs," In Proc. of the 2008 International Conference of Signal and Image Engineering, pp. 727-730, July. 2008.

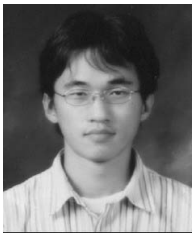
〔6〕 맹영재, 신동오, 김성호, 양대헌, 이문규, "국내 인터넷뱅킹 계좌이체에 대한 MITB 취약점 분석," Internet and Information Security, 1(2), pp. 101-118, 2010년 11월.

〔7〕 D. Arthur and S. Vassilvitskii, "K-means++: the advantages of careful seeding," In Proc. of the eighteenth annual ACM-SIAM symposium on Discrete algorithms, pp. 1027-1035, Jan. 2007.

〈저자소개〉



이 상 호 (Sang-ho Lee) 학생회원
2011년 2월: 공주대학교 정보통신공학과 졸업
2013년 3월~현재: 인하대학교 컴퓨터정보공학과 석사과정
〈관심분야〉 시스템 보안, 웹 보안



김 성 호 (Sung-ho Lee) 학생회원
2009년 2월: 인하대학교 컴퓨터 공학과 졸업
2011년 7월: 인하대학교 정보통신공학과 석사
2011년 8월~현재: 국가보안기술연구소 연구원
〈관심분야〉 시스템 보안, 네트워크 보안

양 대 헌 (Dae-hun Nyang) 정회원
1994년 2월: 한국과학기술원 과학기술 대학 전기 및 전자 공학과 졸업
1996년 2월: 연세대학교 컴퓨터 과학과 석사
2000년 8월: 연세대학교 컴퓨터 과학과 박사
2000년 9월~2003년 2월: 한국전자통신연구원
정보보호연구본부 선임연구원 2003년 2월~현재: 인하대학교 컴퓨터정보공학과 부교수
〈관심분야〉 암호이론, 암호프로토콜, 인증프로토콜, 무선 인터넷 보안

이 경 희 (Kyung-hee Lee) 정회원
1998년 8월: 연세대학교 컴퓨터 과학과 석사
2004년 2월: 연세대학교 컴퓨터 과학과 박사
1993년 1월~1996년 5월: LG소프트(주) 연구원
2000년 12월~2005년 2월: 한국전자통신연구원 선임연구원
2005년 3월~현재: 수원대학교 전기공학과 조교수
〈관심분야〉 바이오인식, 정보보호, 컴퓨터비전, 인공지능, 패턴인식