情 報 保 護 學 會 誌
第21卷 第7號, 2011. 11

보색을 이용한 거래연동 OTP

맹 영 재*, 양 대 헌**

요 약

악성 프로그램으로 인한 거래정보 변조공격은 국내에서는 아직 대응책이 마련되지 않은 보안위협이다. 거래정보 변조공격에 대응하기 위해 제안된 기법들은 아직 그 종류나 수가 많지 않고 새로이 제안되는 기법은 적용성, 편의성, 보안성을 동시에 충족시킬 수 있어야하기 때문에 접근이 쉽지 않다. 이 논문에서는 다양한 형태로 발생할 수 있는 거래정보 변조공격에 대해 알아보고 그에 대응하기 위한 새로운 접근방법인 보색을 이용한 거래연동 OTP를 소개한다. 제안하는 기법은 전자기기를 이용하지 않고 정적인 형태의 반투명한 재료로 구현될 수 있다는 점이 특징이다.

Ⅰ. 서 론

인터넷뱅킹은 우리생활에 필수적인 금융서비스이고 스마트폰, 태블릿PC와 같이 모바일뱅킹이 가능한 이동통신기기의 보급이 확대됨에 따라 접근성이 보다 편리한 금융시스템으로 발전하고 있다. 한국은행의 2011년 2/4분기 국내 인터넷뱅킹서비스 이용현황 보도자료[5]에 따르면 모바일뱅킹 이용건수는 일평균 715만건, 6,100억원을 기록하였고, 이 중에서 특히 스마트폰 기반의 모바일뱅킹서비스는 512만건, 2,989억원으로 전 분기 대비 31.5%, 37.1% 증가한 것으로 조사되었다. 인터넷뱅킹의 전체의 이용건수 및 금액은 일평균 3,893만건, 31조 3,263억원으로 조사되었다.

금융관련 서비스와 그에 관련된 정보는 매우 민감하기 때문에 무엇보다 보안이 필수적이다. 보안서비스는 인증, 무결성, 기밀성, 부인방지, 가용성으로 나뉘고 이 중 어느 하나라도 충족되지 않으면 인터넷뱅킹 서비스의 신뢰도에 적지 않은 영향을 미친다. 공개된 네트워크에서 사용자의 개인단말기를 통해 서비스되는 인터넷뱅킹은 공격자가 접근하기가 어렵지 않은 만큼 다양한 형태의 보안위협에 철저히 대비해야 한다. 인터넷뱅킹에 대한 공격들 중에서 공격자가 악성 프로그램을 동원한 거래정보 변조 공격은 국내외에서 심각한 보안위협으로 떠오르고 있으며 그에 따라 적용성, 편의성, 보안성을 만족하는 다양한 보안 솔루션이 요구되고 있다.

이 논문에서는 거래정보 변조 공격에 대응하기 위한 새로운 방법인 보색을 이용한 거래연동 OTP를 소개한다. 이 논문의 2장에서는 다양한 형태로 존재할 수 있는 거래정보 변조공격과 거래연동 OTP의 필요성을, 3장에서는 관련연구와 동향을, 4장에서는 이 논문에서 제안하는 보색을 이용한 거래연동 OTP를, 5장에서는 다른 기법들과의 비교를 보이고 6장에서는 결론을 담는다.

Ⅱ. 거래정보 변조공격 및 거래연동 OTP의 필요성

네트워크 수준의 공격에 대응하기 위한 암호 프로토콜은 통신하고자 하는 두 단말이 안전하다 가정하고 공유된 키를 이용하여 통신을 보호한다. 이와는 다르게 악성 프로그램이 단말 내에 존재하는 경우에는 안전하다고 가정할 장치가 마련되지 않아 암호학적인 방법의 접근이 쉽지 않다. 그렇기 때문에 백신과 같은 보안 프로그램을 통해 악성 프로그램을 탐지하는 방법이 적용되고 있다. 하지만 보안 프로그램과 동일한 권한을 가지는 악성 프로그램은 보안 프로그램을 우회하도록 작성되기도 하여 보안 프로그램이 언제나 모든 악성 프로그램을 잡아낼 수 있다고 단정하는 것은 무리가 있다.

악성 프로그램을 탐지하는 방법으로는 백신 외에도 단말에 악성코드의 존재여부를 확인하는 방법의 예로

이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임니다.(2011-0004565)
* 인하대학교 컴퓨터정보공학과 정보보호연구실 (brendig@isrl.kr)
** 인하대학교 컴퓨터정보공학과 정보보호연구실 (nyang@inha.ac.kr)

코드-검증기법(Code Attestation)이 있다. 코드검증기법은 센서네트워크에서 센서노드의 메모리영역에 대해 실행한 코드검증 알고리즘의 결과가 서버에 지정된 시간 내에 도착하였고 전달된 결과에 이상이 없다면 해당 센서노드에는 악성코드가 존재하지 않는다고 판단한다. 하지만 이러한 방법을 인터넷뱅킹에 적용하려면 서버에서 단말의 실행코드를 사전에 알고 있어야 하는데 개인사용자의 PC나 스마트폰은 서로 다른 시스템과 OS를 사용하여 실행 중인 프로그램 코드가 모두 다르고 또 이를 모으는 것도 민감한 일이 될 수 있기 때문에 현실적으로 쉽지 않은 접근 방법이다.

이렇게 악성 프로그램을 배재하기 쉽지 않은 환경에서 사용자의 단말이 악성 프로그램에 감염된 경우에는 세션인증이 큰 의미를 가지지 못한다. 악성 프로그램이 사용자의 비밀(ID/PW, 공인인증서, 공인인증서 패스워드)을 가지지 않아도 사용자가 로그인한 세션을 악용하여 스스로 조회하여 볼 수 있기 때문이다. 서비스 요청이 암호화 된 것이라 하여도 그러한 요청은 입력장치가 호출한 이벤트로부터 발생되는데 악성 프로그램에서도 그러한 이벤트를 호출할 수 있다. 다시 말하면, 악성 프로그램을 가정한 경우에서의 사용자인증은 정확히는 "비밀이 입력된 단말"임을 확인한 것이고, 이어지는 세션인증은 "비밀이 입력되었던 단말에서의 서비스 요청"을 의미한 것이지 "사용자의 서비스 요청"을 의미하지는 않는다. 문제는 이러한 인증의 취약점이 거래인증에까지 이어진다는 것이다. 예로, 계좌이체 요청과 함께 제공된 사용자 인증(보안카드 또는 One Time Password, 공인인증서 전자서명)이 사용자로부터 발생된 것이라 할지라도 계좌이체 정보가 사용자가 의도했던 것인지 여부는 위와 같은 사용자 인증 기법으로는 확인하지 못한다.

공격자가 거래정보를 변조하는 공격은 2005년 Augusto에 의해 소개[17]되었고 2007년 Philipp에 의해 MITB(Man In The Browser)[9]라는 이름이 붙었으나, 2009년 Oppliger등의 논문[21]에서 MITB는 컴퓨터내부에서 이루어지는 MITM(Man In The Middle)이기 때문에 MITB와 같은 새로운 용어는 부적절하다고 지적한 바 있다. 사실, 사용자의 클라이언트 내에서 이루어지는 거래정보 변조 공격은 다음와 같이 다양한 방법으로 이루어 질 수 있다.

2.1. 인터넷뱅킹 프로그램 변조

공격자는 인터넷뱅킹 프로그램을 자신이 원하는 대로 동작하도록 변조할 수 있다. 인터넷뱅킹의 경우 웹문서(HTML, SCRIPT 등) 그리고 ActiveX와 같은 보조 프로그램, 모바일뱅킹의 경우 앱(APP)이 그 대상이 된다. 이들 프로그램은 한번 정해진 결과물이 반복되어 사용되기 때문에 발견된 취약점이 보완된 프로그램으로 갱신되기 전까지는 공격자가 변조하여놓은 프로그램으로도 인터넷뱅킹이 가능하다. 거래변조 공격에는 공격자의 인터넷뱅킹 프로그램 분석이 선행된다는 점에서, 서버는 인터넷뱅킹 프로그램을 자주 갱신하여 공격자에게 프로그램을 변조하고 배포할 시간적 여유를 주지 않는 것이 하나의 방법이 될 수 있다. 하지만 인터넷뱅킹 서버와의 통신은 은행 홈페이지에서 제공하는 인터넷뱅킹 프로그램만이 가능한 것은 아니다.

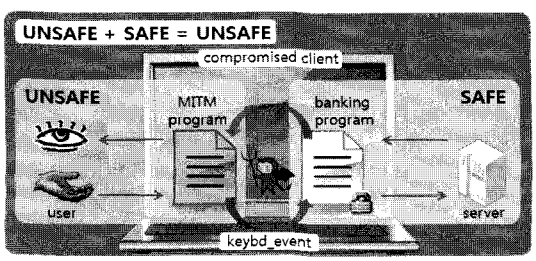
2.2. 가짜 인터넷뱅킹 프로그램 제작

인터넷뱅킹 프로그램의 갱신주기가 단축됨으로 인해 프로그램 변조와 배포에 시간적인 여유가 없는 공격자는 인터넷뱅킹 프로그램을 참고하고 분석하여 가짜 인터넷뱅킹 프로그램을 작성하고, 사용자가 인터넷뱅킹을 실행할 때 준비해놓은 가짜 인터넷뱅킹 프로그램이 실행되도록 할 수 있다. 서버는 수신된 서비스 요청이 암호 프로토콜의 규격에 맞는지 그리고 세션인증 값이 올바른지를 확인하고 클라이언트에 요청된 서비스를 응답한다. 그리고 클라이언트에서 정상적인 프로그램이 실행되고 있는지 여부를 확인하는 것은 암호 프로토콜과는 독립된 다른 보안 프로그램이 담당한다. 앞서 언급하였듯이 악성 프로그램을 가정하였을 때 암호 프로토콜을 이용한 세션인증은 큰 의미가 없고 공격자는 보안 프로그램을 우회하는 것만이 목표가 된다. 일반적으로 보안 프로그램은 사용자의 컴퓨터에서 실행되는 모든 프로그램을 통제하기가 쉽지 않아 공격자가 작성한 프로그램이 보안 프로그램을 우회하기 위해 다양한 방법을 동원할 수 있다. 예로, 보안 프로그램이 인터넷뱅킹 프로그램의 검사 결과를 서버에 전송하지 않는 경우에는 그 보안 프로그램이 호출되지 않도록 가짜 인터넷뱅킹 프로그램을 작성할 수 있다. 검사 결과를 서버에 전송하고 그 전송값이 스스로 생성해낼 수 있는 정도의

것이라면 검사결과를 가짜로 만들어서 서버에 전송할 수 있다. 검사결과를 스스로 만들어내기 힘든 경우라면 가짜 인터넷뱅킹 프로그램이 서버에 전송할 검사결과를 얻어낼 목적으로 인터넷뱅킹 프로그램을 실행시켜 보안 프로그램이 실행되도록 하고 검사결과가 서버에 전송되도록 한 뒤에 연결된 보안세션을 이용할 수 있다. 이러한 공격은 암호 프로토콜과 보안 프로그램이 서로 연결되어있는 형태가 아니고 서버의 입장에서 분리된 형태로 운영된다는 점을 악용한 것이다.

2.3. HCI수준에서의 MITM

MITM은 서버와 사용자를 동시에 속이는 공격이다. MITM을 실행하는 위치는 서버와 사용자사이의 구간 어디든 될 수 있으며 공격자가 악성 프로그램을 동원할 수 있는 경우에는 사용자와 가장 가까운 위치 즉, HCI(Human-Computer Interaction)수준에서 MITM을 할 수 있다. 이러한 관점에서 공격자는 인터넷뱅킹 프로그램을 변조하거나 서버와 직접 통신하는 가짜 인터넷뱅킹 프로그램을 작성하지 않아도 거래변조 공격이 가능한 MITM 프로그램을 제작할 수 있다. 이 MITM 프로그램은 인터넷뱅킹 프로그램을 정상적으로 실행시키되 사용자와 컴퓨터 사이에서 발생하는 HCI데이터는 MITM 프로그램을 통하도록 한 것이다. 컴퓨터에서 HCI는 사용자에게 정보를 전달하는 출력장치(주로 디스플레이 장치)와 사용자가 입력하는 정보를 입력받는 입력장치(주로 키보드, 마우스)로 나뉜다. 디스플레이 장치에 출력되는 정보를 조작하는 것은 곧 사용자를 속이는 것으로 이어지며 출력되는 정보를 조작하는 방법의 예로는 맹영재 등의 논문[3]에서 언급된 문서수준에서의 조작이 있고, MITM프로그램이 인터넷뱅킹 프로그램보다 더 높은 화면출력 우선순위를 가지도록 하는 방법도 가능하다. 보다 안전한 화면출력을 위해 비디오



〔그림 1〕 HCI수준에서의 MITM

오버레이를 사용한 보안 프로그램도 존재하지만 악성 프로그램이 비디오 오버레이에 접근이 불가능한 것은 아니다. HCI와 관련하여 서버를 속이는 방법은 입력장치의 이벤트를 이용하는 것이다. 예로, 공격자는 가상키보드(또는 원격데스크톱)에서 사용되는 키 이벤트 함수를 이용하여 사용자가 입력한 데이터인척 위장하여 단말에 키를 입력할 수 있다. 이러한 키 입력은 사용자가 키를 입력하였을 때와 동일한 이벤트 함수를 사용하는 것이 목적이기 때문에 키보드 암호가 단 대 단으로 동작한다하여도 사용자의 입력과 악성 프로그램으로 인한 입력을 구분할 수 없다. 그러한 이벤트를 사용하지 못하도록 하는 것은 가상키보드, 원격 데스크톱 또한 사용하지 못하도록 한 것이고 또, 태블릿 PC나 스마트폰에서 키 입력을 지원하지 않는 것이라고도 할 수 있다. 더해서 인터넷뱅킹 프로그램에서 자체적으로 동작하는 가상키보드 또한 사용자가 입력한 것과 악성 프로그램이 입력한 것을 구별하지 못하는 이상 공격으로부터 자유로울 수는 없다. 악성 프로그램을 가정할 때 사용자의 키 입력과 악성 프로그램의 키 입력을 구분하는 것은 쉽지 않은 일이기 때문이다.

금융감독원의 전자금융거래 인증방법의 안전성 세부기술평가기준[1]에는 전자금융거래에 도입되는 인증방법에 대한 보안 고려사항이 정리되어 있다. 보안 3등급 요구사항에는 전자금융 거래내역의 무결성 기능이 포함되어 있으며 이는 금융기관에서 전자금융 거래내역의 위·변조 발생여부를 확인할 수 있어야 함을 의미한다.

하지만 신뢰할 수 없는 단말이 이용되는 현재의 인터넷뱅킹 환경에서 2.1장, 2.2장 그리고 2.3장에서 소개한 공격방법들을 고려하면 그러한 요구사항을 만족시키기란 쉽지 않아 보인다. 현재 인터넷뱅킹에서 사용되는 비밀은 모두 사용자 인증기법에서 유래한 것이고 거래정보 변조공격을 고려하지 않은 것이기 때문이다. 사용자 인증 프로토콜은 서버와 공유되어 있는 사용자 비밀을 확인하는 과정이고 2.2장에서 언급하였듯이 사용자에게 거래정보를 확인시켜주는 것은 악성 프로그램으로부터 취약할 수도 있는 보안 프로그램이 담당한다. 거래정보 변조공격에 대응하는 방법은 사용자 인증과 거래 인증을 서로 분리된 프로토콜이 아닌 하나의 프로토콜로 해결하도록 하는 것이다. 사용자 인증과 거래 인증을 동시에 수행하는 프로토콜의 고려사항은 다음과 같다.

1) 서버에서 생성된 정보가 사용자에게 전달되기까

지 공격자가 원하는 형태로 조작될 수 있어서는 안 된다.

2) 서버에서 생성된 정보를 확인한 사용자는 그에 대한 응답을 서버에 전송해야 하고, 이 응답은 해당 거래를 승인하는 데만 사용되어야하며 공격자가 흉내 낼 수 없는 것이어야 한다.

위의 두 고려사항은 HCI 보안성을 강화시키기 위한 것임을 알 수 있다. 사용자의 단말이 악성 프로그램으로 인해 신뢰할 수 없는 상태를 가정하기 때문에 클라이언트와 서버가 아닌 사용자와 서버 사이의 통신을 보호하기 위한 것이다. 3장에서는 거래정보 변조방지기법과 관련한 연구들을 소개한다.

Ⅲ. 관련연구 및 동향

거래정보 변조공격을 방지하기 위한 연구는 크게 두 방향으로 나누어 볼 수 있다. 첫 번째로는 디스플레이가 가능한 추가 보안장치를 발급하여 이를 통해 거래정보를 확인하고 승인요청을 하도록 하는 방법이 있다. 두 번째로는 거래정보 변조 공격을 자동화된 공격으로 보고 자동화된 공격을 방지하기 위해 CAPTCHA를 응용하는 방법이 있다. 세 번째로는 아직 시도된 적이 없는 Visual Cryptography Scheme이 있다. 이 장에서는 위의 세 가지 방법과 거래연동 OTP를 위한 고려사항을 소개한다.

3.1. 추가적인 보안장치를 이용한 대응방법

신뢰할 수 없는 사용자의 단말 대신에 서버와의 안전한 채널을 확보하기 위해 추가적인 보안장치가 사용될 수 있다. 추가 보안장치를 사용한 방법에는 거래서명 인증기술과 ZTIC, 그리고 스마트폰을 활용한 방법이 있다. 거래서명 인증기술은 Hiltgen등의 논문[6]에 소개되어 있으며 실례로는 CAP(Chip Authentication Program)이 있다[2]. 거래서명 인증기술은 보안성은 뛰어나지만 사용자 편의성을 떨어뜨리기가 쉽다는 단점이 있다. 사용자 단말에 입력한 거래정보를 MAC(Message Authentication Code)생성을 위해 발급된 보안장치에 다시 입력해야 하거나, 최악의 경우 요청할 거래의 개수만큼 발급된 보안장치에 입력해야 하기 때문이다. ZTIC(Zone Trusted Information Channel)은 Weigold 등의 논문[23]에 소개되어 있다. ZTIC은 사용자의 컴퓨터와 USB로 연결되어 동작하여 사용자가 거래정보를 추가로 입력할 필요가 없고 거래정보 확인과정도 버튼 두 개 중에서 선택하도록 되어있기 때문에 사용자 편의성이 좋다. 하지만 USB를 연결할 수 있는 장치에서만 동작하여 호환성은 낮다. 스마트폰을 활용한 거래정보 확인방법[8]도 존재하지만 스마트폰 또한 사용자의 임의적인 앱 설치가 가능하다는 점에서 보안성을 보장하기 힘들다는 단점이 있다. 공격자의 입장에서 사용자의 컴퓨터와 스마트폰 두 단말을 모두 공격해야 한다는 점은 부담이 되지만 두 단말은 서로 연결되는 환경에 놓여있기 때문에 공격에 안전하다고는 볼 수 없다.

3.2. 자동화된 공격을 방지하기 위한 CAPTCHA의 응용

거래정보 변조공격에서 사용자와 서버를 동시에 실시간으로 속이기 위해서는 자동화된 프로그램이 필요하다. 자동화된 공격을 막는 것으로 거래정보 변조공격에 대응하기 위해 CAPTCHA를 사용하거나 또는 CAPTCHA를 응용한 방법들이 제안되었다. 주의해야 할 점은, 거래정보 변조공격에 대응하기 위해 일반적으로 사용되는 CAPTCHA을 그대로 적용하면 효과를 볼 수 없다는 것이다. CAPTCHA가 자동화된 공격을 방지해주는 것은 맞지만 MITM공격에서는 CAPTCHA 또한 사용자가 해결하도록 전달될 수 있기 때문이다. CAPTCHA를 응용한 방법의 예로는 ArcotVPS[19]가 있다. 이 기법은 배경과 문자열을 분리가 가능하고 문자열을 읽을 수 없더라도 1/4의 확률로 공격이 가능한 것으로 알려졌다[3]. 맹영재 등이 제안한 퍼즐[4] 있으며, 이 기법에서는 사용자에게 소유한 비밀을 거래정보에 해당하는 CAPTCHA에 위치시키도록 하여 거래정보 변조공격을 방지하였다.

3.3. Visual Cryptography Scheme

1994년 Naor와 Shamir에 의해 처음 소개된 Visual Cryptography Scheme(이하 VCS)은 2개로 나누어진 이미지에(이하 share)에 비밀 이미지를 암호화하고 컴퓨터의 도움 없이 사람의 시각만으로 복호화가 가능하도록 만들어진 암호기법이다[16]. 이 논문을 시작으로 많은 연구가 진행되었으며 기법을 적용할 환경에 따라

픽셀 확장, 명암 대비, 보안성, 명확도, 연산 복잡도, 이미지 포맷(흑백, 그레이, 컬러), 다수의 비밀 저장 가능 여부, share의 개수와 같이 적지 않은 고려사항이 존재한다. 그러한 고려사항을 모두 동시에 만족하기가 쉽지 않음에 따라 각각의 기법들은 위의 고려사항을 선택적으로 만족하고 있으며, 어떤 시스템에 VCS기법을 적용할 때는 그 환경에 맞는 기법을 선택하면 된다[18]. 예로, 픽셀 확장을 요구하지 않는 상황에서는 [25, 26, 27, 14]를 선택하면 되고, 픽셀 확장이 불가피하지만 비교적 높은 보안성 요구되는 경우에는 [11, 10, 12, 13]을, 그리고 색상 지원이 요구되는 경우에는 [11, [10, 12, 13, 20]을, 저장 공간 및 전송량의 효율이 요구될 때는 [22, 15, 24]을 선택하면 된다.

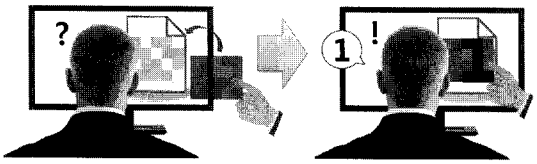
하지만 이 논문에서의 거래연동을 위한 VCS는 기존의 VCS의 고려사항과는 많은 부분이 다른 것으로 보인다. 아래에서 거래연동을 위한 VCS의 고려사항을 정리하여 보았다.

1) 연산을 사용할 수 없음: 몇몇 연구들은 높은 보안성과 이미지 품질을 제공하기 위해 XOR등의 간단한 연산을 도입하여 VCS를 구현하기도 하였다. 그러한 연산은 사람의 시각능력으로는 불가능한 것이기 때문에 간단한 연산이라도 컴퓨터가 필요하게 된다. 하지만 컴퓨터를 사용할 수 있는 환경에서는 VCS대신에 잘 알려진 다른 암호기법(예로, 대칭키 암호기법)등을 이용하여 이미지를 암호화할 수 있고, 컴퓨터 내부에 존재하는 비밀은 악성 프로그램으로부터의 안전을 보장할 수 없기 때문에 연산이 필요한 VCS는 거래연동을 위한 VCS에 적합하지 않는 것으로 보인다. 따라서 거래연동을 위한 VCS는 사용자 단말의 디스플레이 장치와 사용자에게 발급된 share가 포개지는 과정에서 자연히 발생하는 현상(예로, 색의 감산혼합)만이 이용되어야 한다.
2) 복수의 사용에 대한 보안성: 거래연동을 위한 VCS는 복수의 사용에 대해 안전해야 한다. 기존의 VCS는 특정 수 이상의 공유이미지가 모여야 비밀 이미지를 확인할 수 있도록 한 k-out-of-n기법이나, 다수의 이미지를 share에 표현한 기법도 존재한다. 하지만 기존의 VCS에서 복수의 사용과 관련한 기법은 찾아볼 수 없었다.
3) 그림이 아닌 문자의 표현: 비밀이미지를 share에 표현하는 것이 목표인 기존의 VCS는 이미지의 품질을 위해서 이미지 포맷이나 명암대비, 명확도 등을 고려해야 하는데, 그러한 고려사항은 연산을 사용하지 않고 복수의 사용을 고려해야 하는 VCS에서 share 정보의 은폐를 어렵게 만든다. 이와는 다르게 거래연동을 위한 VCS에 표시할 내용은 거래정보와 같은 문자로 이루어진 정보이고 문자정보는 단색으로만 표현되어도 인식이 가능하기 때문에 위의 고려사항은 해당되지 않는다. 자연적인 현상만이 사용되는 VCS에서 이미지 품질과 관련한 고려사항은 픽셀정보가 높은 Entropy를 가지도록 하여 예측이 쉬워지는 반면에 거래연동을 위한 VCS는 단색의 문자 정보만을 표시하면 되기 때문에 픽셀정보의 Entropy가 낮아져 share의 예측을 어렵도록 만들 수 있다.
4) 픽셀 확장이 쉽지 않음: 위의 고려사항 1에서 언급하였듯이 share는 사용자에게 물리적으로 발급된 것이기 때문에 share를 사용자가 직접 디스플레이 장치에 포개는 방법으로 사용된다. 따라서 두 개 이상의 share를 사용하면 사용자 편의성이 떨어질 수 있고, share의 픽셀크기는 사용자 편의성을 고려하여 정해져야 한다. 더해서 모바일뱅킹 단말기에 대한 호환성과 휴대성을 고려하면 share는 일반 카드크기가 적합한 것으로 보인다. 일반 카드와 같은 크기에 사용자 편의성을 고려한 픽셀 크기는 사용가능한 해상도의 크기에도 제한을 준다. 이는 픽셀을 확장한 기법을 적용하기 힘들다는 것을 의미하며 대다수의 기존 VCS는 픽셀확장을 이용하고 있기 때문에 고려사항 3을 고려하여 픽셀확장이 필요하지 않은 새로운 VCS가 요구됨을 의미한다.

조사결과 위의 거래연동을 위한 VCS 고려사항을 동시에 만족하는 VCS는 찾아볼 수 없었다. 4장에서는 VCS의 새로운 응용환경인 보색을 이용한 거래연동 OTP를 소개한다.

Ⅳ. 보색을 이용한 거래연동 OTP

이 장에서는 거래연동을 위한 VCS의 고려사항을 참고하여 보색을 이용한 거래연동 OTP를 소개한다. 제안하는 기법은 사용자가 어떤 거래를 하고자 할 때 발급



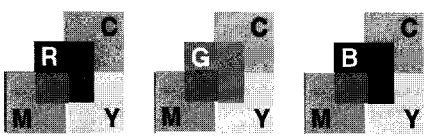
〔그림 2〕 보색을 이용한 안전한 정보전달

받은 거래연동 OTP카드(이하 OTP_C)를 디스플레이 장치의 OTP영역(이하 OTP_A)에 포개는 방법으로 사용된다. 거래연동 OTP_C는 빛의 삼원색(Red, Green, Blue, 이하 RGB)으로 구성된 불투명한 카드(8.5cm * 5.4cm)이고 디스플레이 장치에 출력되는 OTP_A은 색의 삼원색(Cyan, Magenta, Yellow, 이하 CMY)으로 이루어지며, RGB와 CMY가 서로 포개어졌을 때 보색에 해당되는 경우에만 검은색에 가까운 색이 나타나는 원리를 이용하여 거래정보 및 OTP가 표시되도록 하였다(참고로, OTP_C의 RGB와 OTP_A의 CMY는 서로 바뀌어도 무방하다).

4.1장에서는 감산혼합과 보색관계에 대해 알아보고 4.2장에서는 보색을 이용한 거래연동 OTP 프로토콜을 소개한다. 4.3장에서는 보안성에 대해 분석하여보고 4.4장에서는 보색을 이용한 거래연동 OTP의 구현을 소개한다.

4.1. 감산혼합과 보색관계

색을 혼합하는 방법에는 가산혼합과 감산혼합 두 가지가 있다. 가산혼합은 빛의 삼원색으로 색을 만드는 방식이며 RGB혼합, 색광혼합이라고도 불린다. 광원이 있는 텔레비전이나 모니터와 같은 출력장치 등에서 사용된다. 감산혼합은 CMYK(Cyan, Magneta, Yellow, Black)을 혼합하는 방식이며 색상을 실제 출력물에 표현할 때에 사용된다. 이론상으로는 CMY만으로 모든 색상을 표현할 수 있어야 하지만 현실에서는 CMY가 순수한 색이 아니거나 농도 등이 완전치 못하여 짙은 갈색, 짙은 녹색 정도로 인쇄되기 때문에 이를 보완하기 위해 검정(K)이 사용된다.



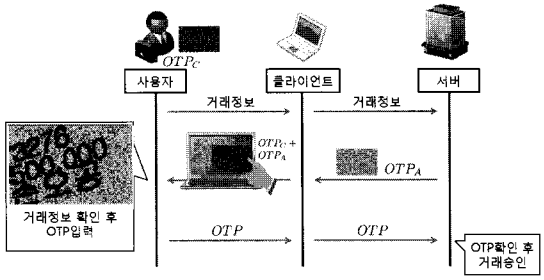
〔그림 3〕 감산혼합과 보색

흥미로운 점은 감산혼합에서 사용하는 색 CMY 중 어느 두 색을 섞으면 그 결과로 RGB 중 하나가 된다는 것이다. RGB는 CMY 중 어느 두 색이 혼합하여 만들어진 것이고 CMY 세 가지를 모두 혼합하면 검은색에 가까운 색(이하 검은색)이 되므로, RGB에 보색(Complementary Color)에 해당하는 CMY 하나를 혼합하면 검은색이 되는 셈이다. 예로, R은 M+Y이므로 C, G(C+Y)의 경우에는 M, B(C+M)의 경우에는 Y가 보색이 된다. RGB에 보색이 아닌 CMY가 섞이는 경우에는, 그 CMY가 RGB에 이미 포함되어 있는 색이기 때문에 RGB에 가까운 색을 유지한다.

요약하면, RGB에 CMY를 혼합하는 경우 1/3의 확률로 검은색(보색이 혼합되는 경우)이 되고 2/3의 확률로 자신의 색을 유지한다. 이러한 보색 관계를 이용하면 색상과 패턴이 임의적인 것으로 보이는 RGB계층과 CMY계층을 결합하였을 때 사전에 지정해 놓은 위치에만 검은색이 출력되도록 하여 특정한 정보가 표시되도록 할 수 있다.

4.2. 보색을 이용한 거래연동 OTP 프로토콜

이 장에서는 4.1장에서 소개한 보색관계를 이용한 거래연동 OTP 프로토콜을 소개한다. 2.4장에서 소개한 거래연동 OTP 고려사항에서와 같이 거래연동 OTP를 통해 표시할 내용(이하 T)은 두 종류로, 사용자가 확인해야 할 거래정보와 사용자가 그 거래정보를 확인하였다는 증거로 단말에 입력할 OTP이다. 거래정보는 사용자가 이미 알고 있는 정보이므로 자신이 입력한 거래정보가 맞는지를 구분할 수 있는 정도로 표시하면 되고, OTP는 사용자가 문자를 인식하고 단말에 입력해야 하므로 가시성이 나쁘지 않도록 표시해야 한다. 보색을 이



〔그림 4〕 보색을 이용한 거래정보 확인 프로토콜

용한 거래연동 OTP 프로토콜은 다음과 같다.

1) 금융기관은 임의적인 RGB로 채워진 OTP_C를 사용자에게 발급한다.
2) 사용자가 서버에 어떤 거래를 요청하면 서버는 T(요청된 거래정보와 이 거래에 대한 OTP)를 OTP_C의 보색을 고려하여 OTP_A를 작성하고 클라이언트에 전송한다. T는 계좌이체의 경우 수신자명, 이체금액, OTP가 되며 OTP_A를 작성할 때 이들의 배치는 임의적으로 설정한다. T를 임의적으로 배치하지 않을 경우 공격자는 OTP_C를 알지 못해도 거래변조 공격이 가능하기 때문인데 이에 대해서는 4.3.4장에서 더욱 자세히 알아보도록 한다.
3) 사용자는 디스플레이에 출력된 OTP_A에 발급받은 OTP_C를 포개어 거래정보를 확인하고 그에 대한 응답으로 단말에 OTP를 입력한다.
4) 서버는 OTP를 확인하고 거래승인 여부를 결정한다.

보색을 이용한 거래연동 OTP는 특별한 사전교육이 필요하지 않기 때문에 사용자 편의성이 비교적 높고 소유하는 형태의 비밀인 OTP_C는 사용자의 단말과 물리적으로 분리되어있기 때문에 악성 프로그램으로부터 안전하다. 사용자 단말을 통해 서버에 전달되는 OTP는 변조될 수는 있지만 그렇다고 공격자가 원하는 거래를 성사시킬 수 있는 것은 아니다. 사용자가 거래정보를 확인한 뒤에 입력한 OTP는 해당 거래에만 유효하기 때문이다. OTP_C에 대한 접근이 불가능한 공격자는 서버에서 전송된 OTP_A정보를 토대로 OTP_C를 복구하거나 OTP_A를 자신이 원하는 형태로 바꾸려는 공격을 시도할 수 있다. 4.3장에서는 OTP_A의 분석을 통한 무차별 공격과 패턴(윤곽선) 추출공격, MITM공격에 대해 소개하고, 대응방법 또한 알아본다.

4.3. 보안성 분석

4.3.1. 무차별 공격에 대한 보안성

공격자는 OTP_C 복구를 무차별적으로 시도할 수 있다. 어느 한 픽셀의 색을 유추하여 맞출 확률은 1/3이고 OTP카드에서 가로 블록의 개수를 w, 세로 블록 의개수를 h라고 했을 때, OTP_C의 모든 픽셀의 색을 무차별 공격을 통해 맞출 확률은 $(1/3)^{w*h}$가 된다. 예로, 일반적인 카드의 크기(8.5cm * 5.4cm)를 고려하고 한 픽셀의 크기를 0.79cm로 설정한 OTP_C의 w는 107(8.453cm), h는 68(5.372cm)이 되며, 이 OTP_C를 무차별공격을 통해 복구시키기 위한 확률은 $(1/3)^{7276}$이 된다.

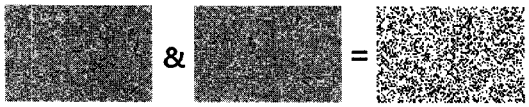
4.3.2. 통계를 사용한 공격과 그에 대한 대응방법

T가 차지하는 비율이(보색이 차지하는 영역)이 OTP_A의 1/3이 아니라면 공격자는 이 정보를 바탕으로 OTP_C의 복구를 시도할 수 있다. 예로, T가 차지하는 영역이 평균 약 1/6이 되도록 설정되어 있다면, 각각의 OTP_A에서 보색이 아닌 다른 색이 차지할 확률은 약 85%가 된다. 이는 하나의 OTP_A에서는 의미가 없지만 공격자가 다수의 OTP_A을 얻어낸 경우에는 각 픽셀에 대해 표현된 색의 통계를 구하고 출현빈도가 약 15%가 되는 색(또는 출현 비율이 가장 낮은 색)을 찾아 보색을 추측해낼 수 있다.

이렇게 통계를 사용한 공격을 방지하는 방법은 보색이 차지하는 비율이 OTP_A의 1/3이 되도록 T의 폰트 크기 등을 조절하거나 노이즈를 추가하는 것이다. 노이즈는 T가 정해진 이후에 T와 노이즈를 포함한 보색이 OTP_A의 1/3이 되도록 OTP_A 안에 위치시킨다. 노이즈는 T와 함께 사용자에게 노출되기 때문에 사용자가 T를 읽는데 지장이 없도록 위치시켜야 한다. 또한 노이즈는 임의적인 형태 보다는 T에 사용된 문자의 일부분을 추가하는 것이 공격자에게 패턴을 분석하기 어렵도록 하는데 도움을 주고, OTP가까이에 선을 추가하면 MITM에 대한 내성을 더욱 강화시킬 수 있다. OTP근처에 위치하는 선에 관해서는 4.3.4 장에서 자세히 설명하도록 한다.

4.3.3. 교차공격과 그에 대한 대응방법

Hou등은 확장된 픽셀과 4개의 share(black mask와 3개의 CMY share)이용한 Color VCS[28]을 제안하였다. 이 기법에 대해 Leung등은 이미지의 경우 윤곽선만

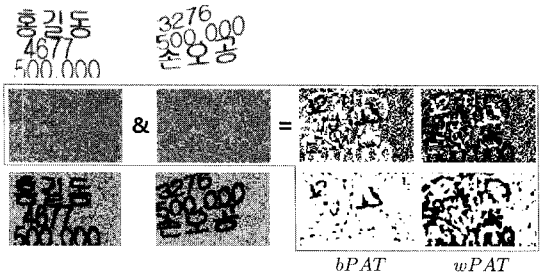


〔그림 5〕 임의의 CMY 비교결과

알아볼 수 있어도 인식이 가능하다는 점에 착안하여, black mask없이 2개 또는 3개의 share만 가지고도 원본 이미지에 표현된 색상 수에 따라 윤곽선 추출이 가능하다는 취약점을 분석하였다[7]. 제안하는 기법은 3.3장에서 언급한대로 픽셀확장이나 다수의 share를 사용하지 않았기 때문에 그러한 분석이 적용되지는 않는다. 하지만 다음과 같이 복수의 OTP_A를 비교 및 분석하여 OTP_C 복구를 시도할 수 있다.

만약 OTP_A가 임의의 CMY로 구성되어있고 그러한 두 OTP_A에 대해 동일한 색이 표현된 픽셀만이 출력되도록 하면 모든 픽셀이 1/3의 확률로 표현되고 특정한 패턴을 찾기 힘든 결과가 나온다([그림 5]: 구분이 쉽도록 검은색으로 표시하였다). 하지만 RGB가 고정되어있는 OTP_C를 고려하여 T가 표시되도록 하면 OTP_A에서 T가 표현될 픽셀들은 보색이 연속된 집단을 형성하게 된다. 높지 않은 해상도에서 1/3을 차지하는 픽셀이 보색이 되기 때문에 서로 다른 OTP_A에서 이 보색이 겹칠 확률은 언제나 존재한다. 노출되는 패턴의 크기는 문자의 종류, 크기, 배치, 기울기 등에 따라 조절될 수는 있지만 다수의 OTP_A들에서 패턴이 나타나는 것은 피할 수 없다.

[그림 6]은 두 개의 OTP_A에 대해 동일한 색을 가진 픽셀만을 검은색으로 표시하여 본 결과이다. 검은색으로 연속된 픽셀(이하 $bPAT$)은 두 OTP_A에서 T가 겹쳐진 부분이고 보색이 노출되었다는 것을 의미한다. 하얀색으로 연속된 픽셀(이하 $wPAT$)은 OTP_A 둘 중 한

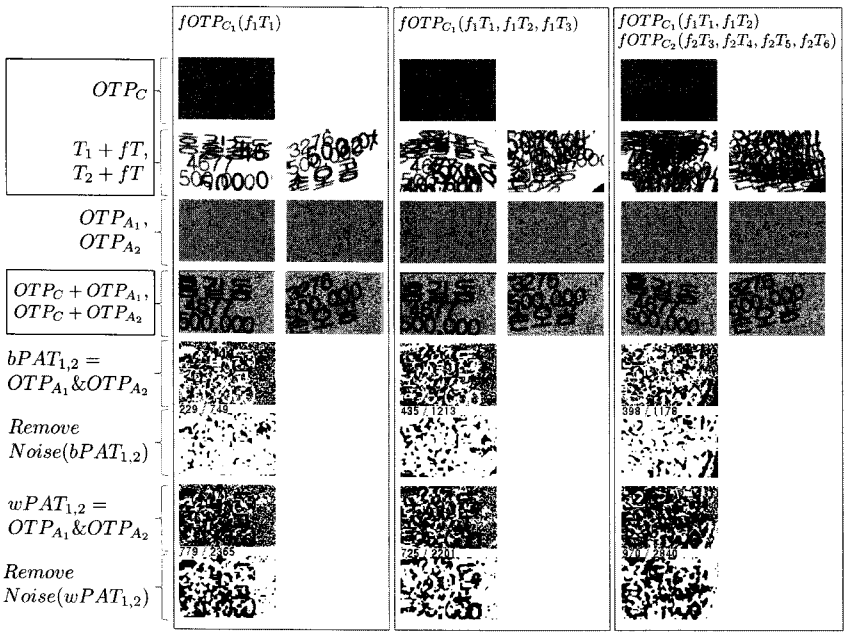


〔그림 6〕 두 OTP_A의 비교분석

곳에서 T가 표현되었던 부분이라는 것을 의미하기 때문에 1/2의 확률로 보색이 노출된 것이라 볼 수 있다. $wPAT$가 나타나는 이유는 보색과 그 외의 색이 서로 겹치지 않기 때문이다. 공격자는 이렇게 얻어낸 패턴을 이용하여 OTP_C 복원을 시도할 수 있다.

두 OTP_A을 비교하였을 때 나타나는 패턴은 보색을 유추하는데 결정적인 역할을 하고, 고정된 OTP_C에서 그러한 패턴이 나타나지 하지 않도록 하는 것은 불가능하다. 하지만 공격자가 동일한 패턴의 연속된 픽셀을 참고한다는 점에서, 서버는 가짜패턴(이하 $fPAT$)을 추가하여 패턴분석을 어렵도록 만들 수 있다. 서버가 사전에 각 사용자를 위한 가짜 OTP_C(이하 $fOTP_C$)를 준비하여 놓고 OTP_A에 T를 작성할 때 T와 동일한 내용의 fT를 T와 다른 위치에 $fOTP_C$를 이용하여 추가되도록 하면, 공격자가 패턴을 분석할 때 $fPAT$ 또한 나타나게 되는 것이다. $fOTP_C$가 보색으로 구성되면 fT가 T와 뒤섞여 구분이 힘들어질 수 있기 때문에 $fOTP_C$는 보색이 아닌 다른 두 색 중에서 임의적으로 구성하도록 한다. 또, T와 같은 내용으로 fT를 작성하는 것은 공격자가 어느 정도 복구에 성공하였다 하더라도 그것이 T인지 fT인지를 구별하기 힘들게 하도록 위함이다. 4.3.2장의 통계를 이용한 공격을 고려하면 복수의 OTP_A에서 CMY세 가지 색이 골고루 표시되도록, RGB가 서로 겹치지 않는 $fOTP_C$ 2개를 준비하는 것이 좋으며 fT를 서로 다른 위치에 여러 번 생성하는 것은 $fPAT$의 출현률을 높여 긍정적인 영향을 준다. f_1T는 $fOTP_{C_1}$을 통해 생성된 fT를 뜻하고 f_2T는 $fOTP_{C_2}$을 통해 생성된 fT를 뜻한다.

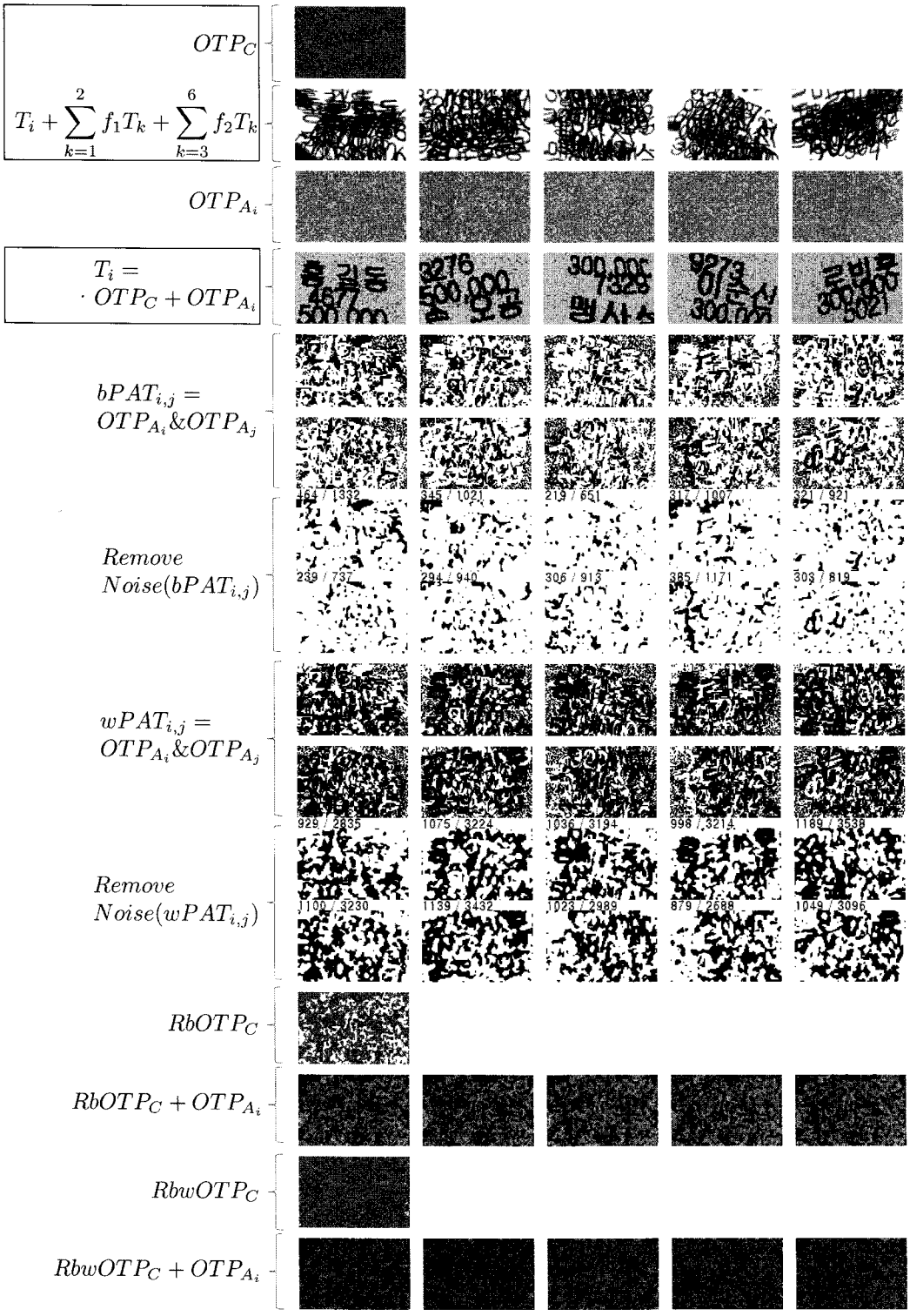
[그림 7]에서 추출된 패턴에는 T가 만들어낸 패턴과 fT가 만들어낸 패턴이 모두 표현되어 있다는 것을 알 수 있다. 각각의 패턴이 T로부터 만들어진 것 또는 fT로부터 만들어진 것으로 양분되어 있다면 공격자는 각각의 패턴에 대한 모든 경우의 수를 조합하여 OTP_C를 추측하려 할 수도 있을 것이다. 하지만 공격자의 패턴분석을 어렵게 만드는 것은 T가 만들어낸 패턴과 fT가 만들어낸 패턴이 어우러져 나타나는 경우이다. 이렇게 두 패턴이 더해져있는 경우 때문에 패턴이 조각나는 상황을 만들고, 조각난 패턴 분석은 결국 픽셀 수준의 통계분석으로 이어지게 된다.



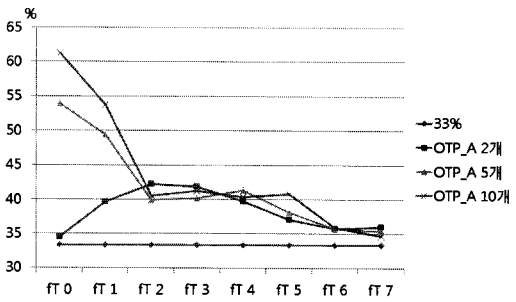
〔그림 7〕 T와 fT가 표현된 두 OTP_A의 비교결과

[그림 8]은 복수의 $\{OTP_{A_i}\}_{i\in[1..5]}$에 대한 패턴분석 및 통계분석의 예를 보인다. [그림 8] 좌측의 네모는 공격자가 모르고 있는 정보이고 공격자는 OTP_{A_i}만을 가지고 분석을 시작한다. 5개의 OTP_A를 서로 비교하면 $bPAT$과 $wPAT$ 각각 ${}_5C_2 = 10$개의 패턴을 얻어낼 수 있다. 여기서의 패턴은 노이즈가 섞여있기 때문에 노이즈를 제거 한 이후에 각 픽셀에 대한 통계를 구해보았다. 통계를 구할 때 $bPAT$의 가중치는 2, $wPAT$의 가중치는 1로 설정하였다($fPAT$가 추가되지 않은 상태에서 $bPAT$는 보색이 그대로 노출되지만 $wPAT$는 1/2의 확률로 보색이 노출된다는 점을 고려하였다). $RbOTP_C$는 $bPAT$의 통계만을 이용하여 OTP_C를 복원시켜 본 것이고 $RbwOTP_C$는 $bPAT$와 $wPAT$통계를 모두 이용하여 OTP_C를 복원시켜 본 것이다. 이렇게 복원한 OTP_C를 이용하여 OTP_{A_i}영역을 포갠 결과는 $RbOTP_C$과 $RbwOTP_C$하단에 표시되어있다. 이 결과에서 나타난 패턴은 $T_{i_{i\in[1..5]}}$와 특별한 관련 없이 나타났고 T_i는 알아볼 수 없었다. 통계에서 PAT와 $fPAT$의 비율이 큰 차이를 보이지 않았기 때문이다. 참고로, [그림 8]의 실험에서 T가 차지하는 픽셀은 평균 28.79%였으며, $fOTP_{C_1}$로 발생된 f_1T는 평균 28.81%, $fOTP_{C_2}$로 발생된 f_2T는 평균 27.49%, 그 외 임의적인 배경은 14.91%였다. 노이즈를 제거한 후의 $bPAT$은 평균 940픽셀, $wPAT$은 평균 3207픽셀이었고 복원해낸 $RbwOTP_C$의 픽셀은 7276픽셀(전체 7276픽셀)이며 이 중에서 복원에 성공한 픽셀은 2525픽셀로 복원한 픽셀 중 34.70%가 보색에 해당하는 것으로 나타났다. 임의로 선택한 RGB를 OTP_C와 비교하여도 약 33%가 보색이 된다는 점을 고려하면 이 수치는 공격에 실패하였다는 쪽에 가깝다는 것을 의미한다.

[그림 8]의 복원 결과에서 보이듯이 복원된 픽셀 중 어느 것이 옳은 것인지는 알기 힘들다. $RbOTP_C + OTP_{A_i}$ 또는 $RbwOTP_C + OTP_{A_i}$에서 나타난 패턴을 활용하려 하여도 그 패턴은 다시 진짜패턴, 거짓패턴, 그리고 그 두 패턴이 섞인 경우로 나뉘기 때문에 활용이 쉽지 않다. 만약 어떤 분석과정을 통해 어떤 문자 조각이 나타났다 하여도 이것이 T인지 또는 fT인지는 다시 한 번 유추해내야 한다. 참고로, 서버에서 OTP_A를 작성할 때 T와 fT가 겹치는 경우 T가 우선권을 가진다. 공격자는 [그림 8]의 분석에 더해서 이 점을 참고하여 보색을 유추하려 할 수 있지만, 그러한 차이는 문자 인식이 가능한 정도로 복구 가능 하였을 때 구별 가능한 것이기 때문에 T와 fT의 우선권 차이를 통해 공격하



〔그림 8〕 5개의 OTP_A에 대한 OTP_C 복원시도 및 OTP_A와의 대입결과



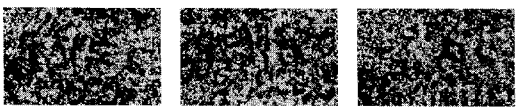
〔그림 9〕 $RbwOTP_C$의 픽셀 추측 성공률
(33%에 가까울수록 얻어낸 정보가 없음을 의미)

는 것은 쉽지 않다. 더해서, 서버에서는 그러한 공격을 예측하여 fT가 가능한 완전한 형태로 노출되도록 OTP_A를 준비해놓을 수도 있다.

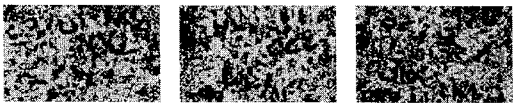
[그림 9]는 공격자가 획득한 OTP_A의 개수와 추가된 fT 개수가 서로 다른 상황에서 $RbwOTP_C$의 픽셀 수 중 옳게 추측한 픽셀의 성공률을 보인다. 참고로, OTP_C를 무차별 적으로 추측했을 때의 성공률은 약 33%이고 이 비율은 보색의 비율을 의미하는 것이며 공격 성공률을 뜻하는 것은 아니다. 따라서, 33%에 가까울수록 OTP_C의 추측에 실패하였다는 것을 의미한다.

fT가 너무 많은 부분을 차지하면 T의 추측이 쉬워

〔그림 11〕 10개의 OTP_A, fT 0의 $RbwOTP_C$(61.26%) + OTP_{A_i}의 예제



〔그림 12〕 10개의 OTP_A, fT 2의 $RbwOTP_C$(40.52%) + OTP_{A_i}의 예제



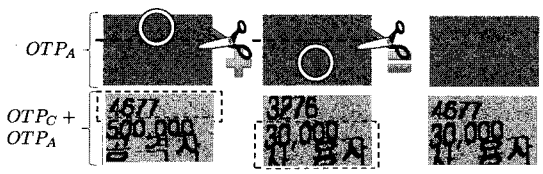
〔그림 13〕 10개의 OTP_A, fT 7의 $RbwOTP_C$(34.7%) + OTP_{A_i}의 예제

질 수 있기 때문에 T와 f_1T, 그리고 f_2T의 비율을 조절하기 위해 fT 두 개까지는 $fOTP_{C_1}$을 통해 작성하였고 3부터 7에 해당하는 fT는 $fOTP_{C_2}$를 통해 작성하도록 하여 출현 비율을 조절한다. fT의 배치는 임의적으로 설정하였다. fT를 추가하지 않은 경우, 획득한 OTP_A가 많을수록 높은 성공률을 보였고 획득한 OTP_A수가 적은 경우 낮은 성공률을 보였다. fT를 추가한 경우에는 OTP_A개수와는 관련 없이 공통적으로 성공률이 낮아졌으며 전체적은 성공률은 fT가 6개 또는 7개일 때 가장 낮게 나타났다. 임의적으로 배치한 fT가 OTP_A에서 고르게 퍼질수록 공격자의 추측 성공률이 낮게 나타난 것이다. $RbwOTP_C$의 추측 성공률이 약 60%인 [그림 10]의 경우 문자의 형태를 알아볼 수 있는 정도로 복구되었으며 $RbwOTP_C$의 추측 성공률이 약 40%인 [그림 11]에서는 이따금 문자의 형태가 보이기도 하지만 알아볼 수 있는 정도는 아니었다. $RbwOTP_C$의 추측 성공률이 약 34%인 [그림 12]에서 역시 문자를 알아볼 수 없었다.

이러한 실험 결과는 통계를 이용한 공격이 성공하기 어렵다는 것을 의미하며, 공격자가 획득한 OTP_A의 개수와는 무관하다는 것을 보여준다. 서버에서 통계를 이용한 공격이 어렵도록 CMY 출현 비율과 T, fT의 배치를 조절할 수 있기 때문이다. 아직 밝혀지지 않은 패턴을 활용한 공격이 있을 수 있으나 이 경우 하나의 패턴에 어우러진 진짜패턴과 가짜패턴을 분류하는 것이 선과제가 될 것이다.

4.3.4. MITM 공격과 그에 대한 대응방법

만약 OTP카드에서 거래정보와 OTP가 비추어지는 위치가 고정되어 있다면 MITM 공격에 취약해진다. [그림 13]은 거래정보와 OTP의 위치가 고정된 OTP_A에 대한 MITM 공격방법을 보인다. 공격방법은 아래와 같다.

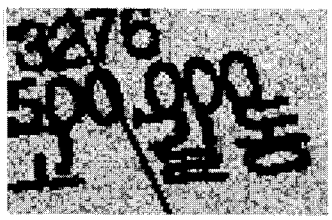


〔그림 14〕 MITM을 통한 거래정보 변조공격

1) 공격자는 사용자가 거래정보를 서버에 요청하면 자신이 원하는 거래 또한 서버에 요청한다.
2) OTP가 상단에 위치한다는 것을 사전에 알고 있는 공격자는 자신이 발생시킨 거래에 대한 OTP_A의 상단(OTP가 위치한 부분)을 잘라내고 사용자가 발생시킨 OTP_A에서는 그 아래 부분(거래정보가 위치한 부분)을 잘래낸 다음, 그 둘을 결합하고 화면에 출력시킨다.
3) 사용자는 거래내용을 확인하고 OTP(공격자의 거래에 해당하는 OTP)를 서버에 전송한다.
4) 서버는 OTP를 확인한 후 공격자가 발생시킨 거래를 처리한다.

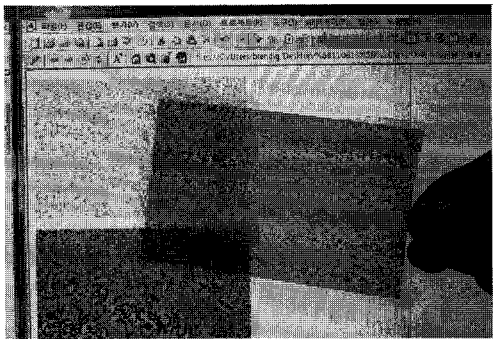
이러한 공격에 대응하는 방법은 T의 위치가 임의적으로 설정되도록 하는 것이다. 공격자가 [그림 13]과 같은 공격을 위해 상중하 세 곳만을 추측한다고 가정하였을 때 하나의 OTP_A에서 OTP만을 정밀하게 잘라내기 위해서는, OTP의 상하 위치에 대한 경우의 수가 20, 회전 20(-10°~ 10°)일 때 3*20*20=1200이라는 경우의 수가 나온다. 공격에 성공하려면 두 OTP_A의 OTP를 동시에 성공적으로 잘라내야 하기 때문에 공격은 더욱 어려워진다. OTP와 거래정보가 부분적으로 겹치는 경우도 존재하여 자르는 위치 및 각도가 정밀하지 않은 경우는 공격에 실패하기 쉽다.

더해서, OTP_A의 OTP근처에 임의적인 직선을 그어 놓으면 공격자가 다른 이미지를 잘라 붙였을 때 직선이 연결되기가 쉽지 않으므로 보안성을 더욱 향상시킬 수 있다. OTP 근처에 직선을 추가한 경우에, 이 직선은 180도의 경우의 수를 가지고 선의 위치가 가지는 경우의 수 또한 적지 않기 때문에 MITM이 성공할 확률은 크게 낮아진다. 선은 직선이나 실선 등이 될 수 있으며 선의 두께나 점선의 빈도 조절 등으로 선의 진행방향을 알 수 있는 경우에는 360도의 경우의 수를 가지게 된다. 참고로, 구현에서 실제 사용한 변수는 상하위치 20, 좌우위치 평균 20(OTP의 경우 30, 수신자명 20, 금액 10~25(액수에 따라 다름)), 회전 20, 이미지 전체에 대한 왜곡은 각 모서리에서 상하좌우 10씩 뒤틀리도록 하였다.

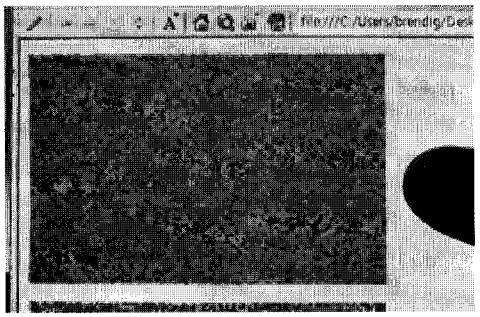


〔그림 15〕 MITM에 대한 보안성 향상을 위해 추가된 선

4.4. 보색을 이용한 거래연동 OTP 구현



〔그림 16〕 OHP 용지에 출력한 OTP_C와 디스플레이에 표현된 OTP_A



〔그림 17〕 OHP 용지에 출력한 OTP_C를 디스플레이의 OTP_A에 포갠 모습
(프린트물에서는 잘 보이지 않음)

실험에는 600dpi급의 컬러레이저프린터를 이용하여 일반 OHP용지에 OTP_C를 출력([그림 15])하고, 모니터에 출력된 OTP_A에 포개어 보았다. OTP_C에 표현된 RGB의 색농도는 60%로 설정하였고 OTP_A의 색농도는 50%로 설정하였다. [그림 16]에서 보이듯이 선명하지는 않았으나 문자 인식이 가능한 수준으로 나타났다. OTP_A와 OTP_C를 포갰을 때의 선명도는 OTP_C의 재료 그리고 RGB와 CMY의 색농도, 채도, 명도 등에 따라 달라진다. 문자는 색농도, 채도, 명도 등의 설정과는 큰 관련 없이 보색이 균일한 색으로 연속되면 인식이

가능한 것으로 보인다. 개인마다 그러한 설정이 다를 수 있기 때문에 문자의 선명도는 다르게 나타날 수 있으나, 평균치를 구하여 보색이 가장 잘 나타나는 값을 사용하고 OHP보다 투과율이 좋은 재료를 사용하면 서로 다른 환경에서도 문자를 표현하는 데는 크게 문제가 없을 것이다.

OTP_C의 크기는 고정되어있는 반면, 디스플레이 장치의 도트 핀치에 따라 OTP_A의 크기가 조금씩 다를 수 있기 때문에 초기에 한번은 사용자가 OTP_A크기를 조절해야 한다. 이후에는 서버에서 그 설정을 참고할 수 있다. 편의성을 위해서는 OTP_C에 손잡이가 있는 것이 좋으며 모니터에 임시로 부착이 가능한 재료를 이용하는 것도 좋은 방법이다. 이 경우 사용자가 설정한 위치에 OTP_A가 노출되도록 할 수 있기 때문에 복수의 거래에 대한 편의성을 높일 수 있다. OTP_C와 OTP_A가 정확하게 겹치는 과정은 사용자가 OTP_C를 직접 조절하도 있지만 OTP_C가 화면에 부착된 상태에서 OTP_A를 마우스나 키보드를 이용하여 위치나 각도를 조절하는 것이 더욱 편리하였다.

V. 다른 기법들과의 비교

이 장에서는 금융보안연구원의 전자금융 新인증기술 연구보고서[2]를 참고하여 거래정보 변조방지 기법들과의 비교를 보인다. 제안하는 기법은 정적인 재료의 불투명한 OTP_C만을 제작하면 되고 추가적인 개발이 요구되지 않으며 플랫폼과 OS에 관련 없이 적용가능하기 때문에 적용 가능성, 적용 비용, 기술 중립성 측면에서 모두 우수하다. 제안하는 기법은 기존에 사용되지 않은 방법이지만 특별한 장비가 요구되지는 않기 때문에 기존 인프라 활용성은 보통이다.

사용자는 OTP_C를 지갑에 소지할 수 있고 1개의 매체로 모든 금융회사에서 공통으로 사용가능하며, 거래내용을 확인하고 OTP를 입력하는 방법에 대해 집중적으로 교육할 필요는 없어 소지 편의성과 관리 편의성, 교육 편의성이 높다. 사용자는 거래내용을 확인 후 OTP를 입력해야 하고 발급 시 1회 대면확인이 요구되어 사용 편의성과 발급 편의성은 보통이다.

제안하는 기법은 전반적으로 보안성이 우수하나 정적인 형태의 재료이기 때문에 어깨너머 훔쳐보기와 같은 물리적인 공격에는 취약하다. 교차공격의 경우 4.3.3장에서 분석하여 보였으나 VCS에서도 처음 시도되는 기법인 만큼 알려지지 않은 공격의 가능성을 배재할 수 없다.

VI. 결론

이 논문에서는 정적인 재료를 이용하여서도 거래정

〔표 1〕 거래정보 변조방지기법들과의 비교

검토항목 \ 기법		CAP[2]		ZTIC[23]		스마트폰[8]		비밀퍼즐[4]		제안기법	
적용성	적용 가능성	우수	우수	보통	보통	보통1	우수	우수	우수	우수	우수
	적용 비용	미흡		보통		보통		우수		우수	
	기술 중립성	우수		미흡		우수		우수		우수	
	기존 인프라 활용성	우수		미흡		우수		우수		보통	
편의성	소지 편의성	미흡	보통	미흡	보통	우수	우수	우수	우수	우수	우수
	사용 편의성	미흡		우수		우수		보통		보통	
	관리 편의성	우수		우수		우수		우수		우수	
	발급 편의성	보통		보통		우수		우수		보통	
	교육 편의성	보통		우수		우수		보통		우수	
보안성	무차별 공격	우수	우수	우수	우수	우수	우수	보통	보통	우수	우수
	훔쳐보기 공격	우수		우수		우수		보통		미흡	
	교차공격	우수		우수		우수		우수		보통3	
	MITM	우수		우수		우수		보통		우수	
	악성 프로그램	우수		우수		보통2		우수		우수	

1: 스마트폰은 소지하는 형태의 비밀로 사용될 수 있으나 포바일뱅킹의 경우 그러한 비밀역할이 불가능 함
2: 스마트폰은 악성 프로그램에 감염될 수 있음. 거래연동 OTP가 악성 프로그램으로부터 안전한 신뢰할 수 있는 채널을 생성하기 위한 접근이라는 점을 고려하면 스마트폰을 이용한 OTP를 신뢰하는 것은 안전하지 않을 수도 있음
3: 교차공격은 4.3.3장에서 분석하였으나 새로운 접근의 기법인 만큼 알려지지 않은 공격이 있을 수 있음

보 변조공격에 대응할 수 있다는 가능성을 보였고 제안하는 보색을 이용한 거래연동 OTP와 다른 기법들을 비교 및 분석하여 보았다. 제안하는 기법은 VCS분야에서도 새로운 접근방법이며 이 연구결과는 앞으로의 다른 연구들에 많은 도움이 될 것으로 기대한다.

보색을 이용한 거래연동 OTP는 휴대가 간편하며 사용방법에 특별한 교육이 요구되지 않아 사용자 편의성이 뛰어나다. 인터넷뱅킹과 모바일뱅킹에 동시에 적용될 수 있어 호환성이 좋으며 플라스틱이나 필름형태로 제작될 수 있기 때문에 적용 비용이 크지 않다는 장점이 있다. 이 기법은 VCS분야에서도 처음 시도된 방법인 만큼 아직 발견되지 않은 공격방법이 존재할 수 있으며 그러한 공격에 대한 연구와 분석은 향후 연구과제로 남는다. 제안하는 접근 방법은 다양한 인터넷뱅킹 환경에서 거래정보 변조 공격에 대응하기 위한 좋은 후보가 될 수 있을 것이라 기대한다.

참고문헌

[1] 금융감독원, "전자금융거래 인증방법의 안전성 세부 기술평가기준", 2011

[2] 금융보안연구원, "전자금융 新인증기술 연구보고서", 2011

[3] 맹영재, 신동오, 김성호, 양대헌, "전자금융거래에서의 문서변조 취약점 분석 및 대응방법 고찰", 한국정보보호학회 학회지, 제 20권 제 6호, pp. 17-27, 2010년 12월.

[4] 맹영재, 양대헌, 이경희, "모바일뱅킹에서 비밀퍼즐을 이용한 비밀증명방법과 거래승인방법", 한국정보보호학회 논문지, 제 21권 제 1호, pp. 187-199, 2011년 2월.

[5] 한국은행, "2011년 2/4분기 국내 인터넷뱅킹서비스 이용현황", http://bok.or.kr/contents/total/ko/boardView.action?boardBean.categorycd=0&boardBean.sdt=&boardBean.edt=&boardBean.searchColumn=title&boardBean.searchValue=&menuNaviId=559&boardBean.menuid=559&boardBean.brdid=81682&boardBean.rnum=1&boardBean.cPage=1, 2011

[6] Alain Hiltgen, Thorsten Kramp and Thomas Weigold, "Secure Internet Banking Authentication", IEEE Security and Privacy, 2006

[7] Bert W. Leung, Felix Y. Ng, and Duncan S. Wong, "On the security of a visual cryptography scheme for color images", Pattern Recognition 42(5): 929-940, 2009

[8] Guenther Starnberger, Lorenz Froihofer and Karl M. Goeschka, "QR-TAN: Secure Mobile Transaction Authentication", 2009 International Conference on Availability, Reliability and Security, pp.578-583, 2009

[9] Gühring Philipp, "Concepts against Man-in-the-Browser Attacks". http://www2.futureware.at/svn/sourcerer/CAcert/SecureClient.pdf, 2007

[10] Chin-Chen Chang, Chwei-Shyong Tsai, and Tung-Shou Chen, "A New Scheme For Sharing Secret Color Images In Computer Network", Proceedings of International Conference on Parallel and Distributed Systems, pp. 21 - 27, 2000.

[11] Chin-Chen Chang, Jun-Chou Chuang, and Pei-Yu Lin, "Sharing A Secret Two-Tone Image In Two Gray-Level Images", Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05), 2005.

[12] Chin-Chen Chang, and Tai-Xing Yu, "Sharing A Secret Gray Image In Multiple Images", Proceedings of the First International Symposium on Cyber Worlds (CW.02), 2002.

[13] Du-Shiau Tsai, Gwoboa Horng, Tzung-Her Chen, and Yao-Te Huang, "A Novel Secret Image Sharing Scheme For True-Color Images With Size Constraint", Information Sciences 179 3247 - 3254 Elsevier, 2009.

[14] Haibo Zhang, Xiaofei Wang, Wanhua Cao, and Youpeng Huang, "Visual Cryptography For General Access Structure By Multi-Pixel Encoding With Variable Block Size", International Symposium on Knowledge Acquisition and Modeling, pp. 340-344, 2008.

[15] Jen-Bang Feng, Hsien-Chu Wu, Chwei-Shyong Tsai, Ya-Fen Chang, and Yen-Ping Chu, "Visual Secret Sharing For Multiple Secrets", Pattern Recognition 41 ,pp. 3572-3581, 2008.

[16] Moni Naor, and Adi Shamir, "Visual cryptography", Advances in Cryptology－EUROCRYPT'94, LNCS, vol. 950, Springer, Berlin, pp.1-12, 1994

[17] Paes de Barros Augusto, "O futuro dos backdoors - o pior dos mundos", http://www.paesdebarros.com.br/backdoors.pdf, 2005

[18] P.S.Revenkar, Anisa Anjum, and W .Z.Gandhare, "Survey of Visual Cryptography Schemes", International Journal of Security and Its Applications, Vol. 4, No. 2, April, 2010

[19] Rajendra A. Gopalakrishna, "Authentication using a turing test to block automated attacks", US 2009/0199272 A1, US Patent, Aug. 2009

[20] R.Youmaran, A. Adler, and A. Miri, "An Improved Visual Cryptography Scheme For Secret Hiding", 23rd Biennial Symposium on Communications, pp. 340-343, 2006.

[21] Rolf Oppliger, Ruedi Rytz, and Thomas Holderegger, "Internet Banking: Client-Side Attacks and Protection Mechanisms", IEEE Computer 42(6): 27-33, 2009

[22] Shyong Jian Shyu, Shih-Yu Huang, Yeuan-Kuen Lee, Ran-Zan Wang, and Kun Chen, "Sharing multiple secrets in visual cryptography", Pattern Recognition, Vol. 40, Issue 12, pp. 3633 - 3651, 2007.

[23] Thomas Weigold, Thorsten Kramp, Reto Hermann, Frank Höring, Peter Buhler, and Michael Baentsch, "The Zurich Trusted Information Channel - An Efficient Defence Against Man-in-the-Middle and Malicious Software Attacks", TRUST 2008: 75-91, 2008

[24] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multi-Secrets Visual Secret Sharing", Proceedings of APCC2008, IEICE, 2008.

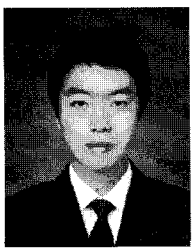
[25] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multiple-Image Encryption By Rotating Random Grids", Eighth International Conference on Intelligent Systems Design and Applications, pp. 252-256, 2008.

[26] Wen-Pinn Fang, "Non-Expansion Visual Secret Sharing In Reversible Style", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.2, February 2009.

[27] Xiao-qing Tan, "Two Kinds Of Ideal Contrast Visual Cryptography. Schemes", International Conference on Signal Processing Systems, pp. 450-453, 2009.

[28] Young-Chang Hou, "Visual cryptography for color images", Pattern Recognition 36(2003) 1619-1629.

〈著者紹介〉



맹 영 재 (YoungJae Maeng)
학생회원

2006년 8월: 인하대학교 컴퓨터 공학과 졸업
2008년 8월: 인하대학교 정보통신대학원 석사
2008년 9월~현재: 인하대학교 정보공학과 박사 과정
<관심분야> 웹 보안, 네트워크 보안, 금융 정보보호

양 대 헌 (DaeHun Nyang)
종신회원

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 정보통신대학원 부교수
<관심분야> 암호이론, 암호프로토콜, 인증프로토콜, 무선 인터넷 보안