情報保護學會論文誌
第 22 卷 第 6 號, 2012. 12

STM-GOMS 모델: 모바일 스마트 기기 환경의 인증 기법을 위한 안전성 분석 모델*

신 수 연,† 권 태 경‡
세종대학교

STM-GOMS Model: A Security Model for Authentication Schemes in Mobile Smart Device Environments*

Sooyeon Shin,† Taekyoung Kwon‡
Sejong University

요 약

최근 모바일 스마트 기기의 보편화로 인하여 사용자 인터페이스로부터 개인 정보를 직접 획득하는 유형의 공격(숄더 서핑 공격, 레코딩 공격 등) 위협이 크게 증가하고 있다. 이러한 공격 가능성 및 안전성에 대한 체계적 평가를 위해 정형화된 안전성 분석 모델이 필요하지만, 이에 적합한 모델이 존재하지 않는다. 본 논문에서는 모바일 스마트 기기 환경의 안전성 및 사용성 분석 모델인 STM-GOMS 모델을 제안한다. STM-GOMS 모델은 HCI 인지 모델을 안전성 분석에 처음으로 활용한 이전 연구 사례를 메모리 한계 관점에서 개선한 GOMS 기반 모델로 인증 기법의 사용성과 안전성 평가가 가능하다. 본 논문에서는 현재 스마트 기기에서 사용 중인 패스워드 입력 기법을 STM-GOMS 모델로 분석하여 사용성과 숄더 서핑 공격에 취약함을 보이고 이를 실험을 통해 검증한다.

ABSTRACT

Due to the widespread use of smart devices, threats of direct observation attacks such as shoulder surfing and recording attacks, by which user secrets can be stolen at user interfaces, are increasing greatly. Although formal security models are necessary to evaluate the possibility of and security against those attacks, such a model does not exist. In this paper, based on the previous work in which a HCI cognitive model was firstly utilized for analyzing security, we propose STM-GOMS model as an improvement of GOMS-based model with regard to memory limitations. We then apply STM-GOMS model for analyzing usability and security of a password entry scheme commonly used in smart devices and show the scheme is vulnerable to the shoulder-surfing attack. We finally conduct user experiments to show the results that support the validity of STM-GOMS modeling and analysis.

Keywords: Security model, GOMS model, Smart devices, Shoulder-surfing attack, Usability and Security Analysis

접수일(2012년 4월 5일), 수정일(2012년 9월 19일), 게재확정일(2012년 10월 17일)
* 본 연구는 지식경제부 및 한국산업기술평가관리원의 산업융합원천기술개발사업(정보통신)의 일환으로 수행하였음. [10039180, 모바일 환경하에서 모바일 인증과 보안 강화를 위해 직관적이며 사용하기 편하고 안전한 인간-컴퓨터 상호작용(HCI) 기반 Usable Security 원천기술 개발]
† 주저자, shinsy80@sju.ac.kr
‡ 교신저자, tkwon@sejong.ac.kr

I. 서 론

최근 모바일 스마트 기기가 보편화되면서, 이를 통한 개인 정보, 업무 관련 정보, 금융 정보 등 민감한 정보 처리가 크게 늘어나고 있다. 개방된 장소에서 스마트 기기를 통한 민감한 정보 입력은 사용자 인터페이스를 직접 어깨너머로 관찰하여 개인 정보를 획득하는 공격인 숄더 서핑 공격[9] 및 숨겨진 카메라 혹은

스마트 기기의 카메라를 이용하여 관찰을 시도하는 레코딩 공격에 대한 위협을 증가시킨다. 이와 같은 공격의 가능성 및 안전성을 체계적으로 평가할 수 있는 정형화된 안전성 분석 모델이 필요하지만, 이에 적합한 모델이 존재하지 않는다.

숄더 서핑 공격자도 사용자와 마찬가지로 인간이라는 관점에서 인간으로써 가지는 지각 및 인지 능력의 한계에 기반하여 사용자 뿐 만 아니라 공격자를 모델링한 연구 사례가 있다[8]. 해당 연구에서는 널리 알려진 CPM-GOMS 모델을 활용하여 Roth 등이 제안한 블랙 앤 화이트 인증 기법[10]을 공격 및 분석하였다. 하지만 CPM-GOMS 모델을 포함한 기존 GOMS 모델은 사용성 및 안전성 분석에 중요한 메모리 관리에 대한 고려가 부족하다. 따라서 본 논문에서는 이전 연구를 확장하여 정형화시킨 STM-GOMS 모델을 제안한다. 현재 스마트 뱅킹에 사용 중인 랜덤 공백 키보드 기법을 예로 들어 STM-GOMS 모델링에 대해 설명하고 해당 기법이 숄더 서핑 공격에 취약함을 보인다. 또한 실제 실험을 통해 이를 검증한다. 랜덤 공백 키보드 기법 이외에도 다른 인증 기법에 대한 사용성 및 안전성 분석 결과를 보인 선행 연구가 있다[8,11-13]. ATM 및 스마트 뱅킹에서 널리 사용 중인 일반 PIN 입력 기법이 숄더 서핑 공격에 안전하지 않음을 STM-GOMS 모델을 통해 보이고[12], 간단한 확장 버전을 제안하여 해당 버전이 숄더 서핑 공격에 안전함을 보였다[11]. 2010년 De Luca 등이 제안한 ColorPIN 기법[4]이 숄더 서핑 공격에 안전함 또한 보였다[13]. 본 논문은 STM- GOMS 모델 자체에 초점을 두고 사용성 및 안전성 분석을 위한 수행 단계 및 방법을 포함한다.

II. 관련 연구

2.1 GOMS 모델

GOMS (Goals, Operators, Methods, and Selection Rules) 모델은 인간 정보처리 과정에 대한 이론인 인지 복잡도 이론과 MHP (Model Human Process)[2]에 근거한 과학적이면서도 실용적인 사용성 평가방법이다. MHP는 인간의 정보 처리 시스템을 설명하기 위해 프로세서 간의 상호 연결과 일반적인 연산의 원리를 기술한 것으로 인간의 정보 처리 시스템을 지각, 인지, 동작 프로세서와 저장 시스템의 집합으로 표현한다. GOMS 모델의 변형으로는 CMN-GOMS [2], KLM (Keystroke -Level Model)[1,2], NGOMSL (Natural GOMS Language) [7], CPM (Critical Path Method)-GOMS[6] 등이 있다.

CMN-GOMS 모델은 GOMS 모델 자체를 의미하며, 작업 분석과 사용자 인터페이스 모델링을 위해 의사코드 형식으로 표현 가능하다. CPM-GOMS 모델은 병렬로 수행 가능한 지각(perceptual), 인지(cognitive), 동작(motor) 조작들을 가정하며, 작업을 스케줄 차트로 자세하게 기술하고 주요 경로(critical path)를 선택하여 실행 시간을 예측한다.

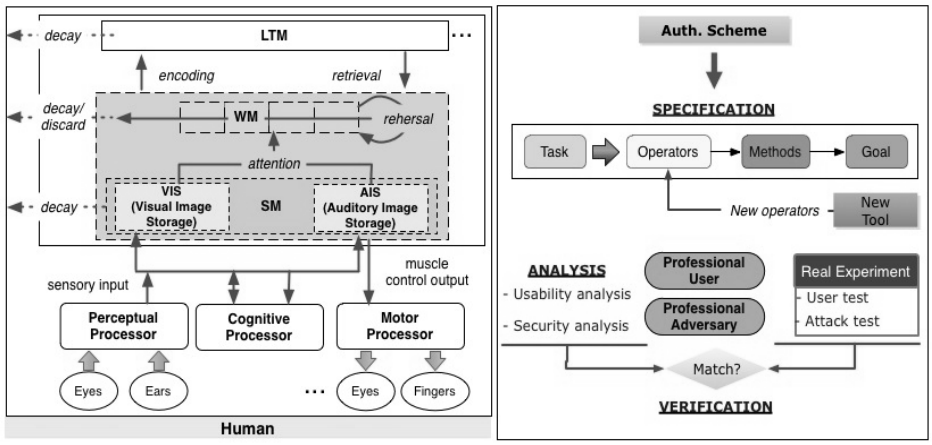
2.2 랜덤 공백 키보드 기법

랜덤 공백 키보드 기법은 현재 ATM 기기, 스마트 뱅킹 등 인증서 패스워드 입력을 위해 널리 사용되는 방법으로 임의의 공백이나 특수문자가 함께 배열된 키보드를 이용하여 패스워드를 입력한다. 랜덤 공백 키보드 기법은 가상 키보드 모든 키 값을 이미지로 표현하고 같은 좌표 값이더라도 매번 다른 숫자 또는 문자와 매치되도록 하여, 값 유추가 매우 힘들며 암호화되어 있으므로 메모리 해킹, 스파이웨어에 강한 저항성을 가진 것으로 알려져 있다. 하지만 키보드의 키를 누를 때 해당 키의 문자가 크게 확대될 뿐만 아니라 입력 창에 해당 문자가 직접 보인 후 별 문자로 변경되므로 숄더 서핑 공격에 취약하다.

III. STM-GOMS 모델

3.1 STM-GOMS 모델의 개념

다양한 센서를 가지고, 화면 터치가 가능하며, 이동성을 제공하는 모바일 스마트 기기 환경의 인증 기법에 대한 안전성 및 사용성 분석 모델인 STM-GOMS 모델을 제안한다. STM은 Security and Threat Model, Sensor-Touch-Mobile, Smart Technology Model의 약어로 안전성 분석 모델의 의미와 모바일 스마트 기기 환경을 위한 모델의 의미를 포함한다. STM-GOMS 모델은 이전 연구 사례를 바탕으로 [그림 1]과 같이, 공격자도 사용자와 마찬가지로 인간이라는 관점에서 사용자와 공격자를 모델링하며, 인간의 지각 및 인지 능력 한계 뿐 만 아니라 메모리 한계 또한 고려한다. 인간의 메모리를 MHP와 마찬가지로 크게 감각 기억(SM: Sensory Memory),



〔그림 1〕 STM-GOMS 모델 개념

작업 기억(WM: Working Memory), 장기 기억(LTM: Long-Term Memory)로 나누어 고려한다. 인간이 감각 기관을 통해 지각한 정보는 SM에 잠시 저장되어 주의(attention)을 통해 WM으로 전달된다. WM에 저장된 정보는 반복(rehersal) 혹은 암송을 통해 LTM으로 전달되고 그렇지 못한 정보는 망각(decay)된다. 인간의 WM은 처리 용량이 제한되어 있기 때문에 한 번에 활성화될 수 있는 정보의 양이나 한 번에 처리될 수 있는 인지 과정의 수가 제한되어 있다. STM-GOMS 모델에서는 Cowan의 주장[4]에 기반하여 인간의 WM 처리 용량을 4개의 묶음(chunk)으로 가정한다. 묶음의 크기는 개개인이 정보를 어떻게 나누는지와 정보의 유형에 따라 달라질 수 있으므로, STM-GOMS 모델에서는 인증 기법에서 주어지는 정보에 맞게 묶음의 크기 및 그룹화 방법을 가정하여 사용성 및 안전성 분석에 활용한다.

STM-GOMS 모델은 사용자와 공격자의 작업 목표와 수행하기 위해 필요한 조작들은 CMN-GOMS 모델과 CPM - GOMS 모델을 확장한 의사코드와 스케줄 차트로 서술된다. 서술된 사용자의 스케줄 차트를 바탕으로 인증 기법의 사용성을 분석한다.

공격자는 스마트 장치와 스파이웨어 같은 소프트웨어를 추가적으로 활용 가능하지만, 본 논문에서는 인간으로서 가지는 인지, 지각, 메모리 능력을 기반으로 근거리에서 직접적인 관찰을 통해 공격을 시도하는 숄더 서핑 공격자만을 고려한다. 숄더 서핑 공격은 직접적인 관찰, 즉 눈을 통한 지각과 짧은 시간 내에 정보를 처리하고 저장하는 WM의 능력을 가지고 이루어지는 공격이다. 인간이 가지는 VIS (Visual Image Storage)는 짧은 시간 내에 지각할 수 있는 정보의 양이 정해져 있으며, 지각한 정보를 처리하는 WM의 경우에도 처리 용량에 한계를 가지므로 숄더 서핑 공격의 성공 여부는 주어진 시간 내에 지각할 수 있는 능력, 지각 프로세서와 연결된 SM의 한계, 지각한 정보의 저장을 위한 WM의 한계에 의해 결정된다. 그러므로 STM-GOMS 모델은 사용자와 공격자의 실행 시간을 동기화하고 비교하여 공격자에게 주어진 시간이 공격 수행을 위해 충분한지를 판단하고 공격자의 지각 정보 비율을 예측하여 공격의 성공/실패 여부를 판단한다.

기존의 인지 모델들은 대부분 데스크탑 환경에 초점을 두었으므로, 모바일 스마트 기기 환경의 인증 기법에 대한 사용성 및 안전성 분석을 위해서는 새로운 조작의 정의와 시간 평가가 필요하다. STM-GOMS 모델은 기존 모델에 포함되어 있지 않은 모바일 스마트 기기에서 많이 사용되는 손가락 이동([Finger-Move]) 및 터치([Finger-Touch])를 포함하도록 한다. 전문 사용자를 가정하여 해당 동작 조작의 시간을 평가하기 위해, 평균 나이가 28.7세인 컴퓨터 공학 전공의 스마트 기기에 능숙(평균 휴대폰 사용 기간: 12년, 평균 스마트폰 사용 기간: 2.5년)한 대학생 및 대학원 생 12명(남: 8명, 여: 4명)이 참여하였다. 삼성 갤럭시 S2를 스마트 기기로 하여 실험용 프로그램을 제작하였다. 기존 GOMS 모델과 달리 타겟의 크기 및 거리에 따라 이동 평가 시간이 달라진다는 Fitt 법칙[3]을 적용하는 대신, 일반화를 위해 버튼의 크기와 버튼 사이의 거리를 달리하여 측정한 후 평균을 계산하였다. 〔표 1〕은 손가락 이동 및 터치 사용자 실험 결과

를 정리한 표이며, 〔표 2〕는 STM-GOMS 모델에서 사용될 기존 CPM-GOMS 모델에서 정의한 조작과 평가 시간을 포함한다.

〔표 1〕 손가락 이동 및 터치 조작 평가 시간
(단위: 밀리초)

조작	최소	최대	평균	표준편차
Finger-Move	67	1248	250 (249.76)	122 (121.95)
Finger-Touch	40	307	110 (110.17)	47 (47.04)

〔표 2〕 CPM-GOMS 모델 조작 평가 시간
(단위: 밀리초)

	조작	시간(밀리초)
Perception (지각)	Visual	simple: 100 complex: 290
	Audio	100
Cognition (인지)	Init. motor	50
	Attend info.	
	Verify	
Motor (동작)	Eye-Move	30

3.2 STM-GOMS 모델의 기능

STM-GOMS 모델은 사용자 측면과 공격자 측면에서 심볼릭 형식의 절차를 분석하고, 계량 형식의 사용성 분석을 제공한다. 〔표 3〕은 사용성 분석 평가 항목과 설명을 포함한다. 사용자 실행 시간은 스케줄 차트로 표현된 사용자의 전체 작업 주요 경로 시간을 통해 측정한다. 인증 기법을 사용 시, 많은 정보를 기억해야하거나 오랜 시간 동안 정보를 기억해야 하는 경우 해당 기법을 불편하게 느낄 수 있다는 점을 고려하여 LTM 복잡도와 WM 복잡도를 이용하여 메모리 복잡도를 측정한다. LTM 복잡도는 요구되는 LTM 처리 항목의 수로 패스워드 길이 혹은 PIN 길이를 고려하여 측정한다. WM 복잡도는 지각하여 WM에 저장해야 할 그룹화된 정보 수(단순 위치 정보, 동작 확인을 위한 지각은 제외)인 요구되는 WM 처리 묶음 수와 지각한 정보가 WM에 유지되어야 하는 시간인 WM 사용 지속 시간으로 측정한다. 또한 인터페이스가 자주 바뀐다거나 단일 인터페이스에서 많은 동작을 해야 하는 경우에도 불편함을 느낄 수 있으므로, 인터페이스 복잡도를 실행동안 디스플레이되는 화면 수와 실행동안 요구되는 눈, 손가락 움직임의 수를 합산하여 측정한다.

〔표 3〕 사용성 평가 항목

평가항목		의미
T_U		사용자 실행 시간(ms)
C_{MEM}	$[R_{LTM} : R_{WM}(D_{WM})]$	메모리 복잡도
	R_{LTM}	요구되는 LTM 처리 항목 수
	R_{WM}	요구되는 WM 처리 묶음 수
	D_{WM}	WM 사용 지속 시간(ms)
C_{IF}	$[N_{DS}, R_M]$	인터페이스 복잡도
	N_{DS}	디스플레이 화면 수
	R_M	요구되는 동작 수

사용자와 공격자의 절차와 공격 시점 동기화 및 공격자의 메모리 한계를 고려하여 숄더 서핑 공격에 대한 안전성을 분석한다. 〔표 4〕는 안전성 분석 평가 항목과 설명을 포함한다. 숄더 서핑 공격은 사용자의 특정 조작을 관찰하여 이루어지는 공격으로 특정 조작 이후에 이루어져야 하는 공격자 조작의 시간을 동기화한다. 그 다음, 시간 동기화를 통해 공격자의 대기 시간(w)를 측정한다. 동기화 시점에서 사용자의 실행 시간보다 공격자의 실행 시간이 더 짧으면 동기화한 특정 조작까지 여유 시간($w \geq 0$)을 가지게 된다. 반대로 공격자의 실행 시간이 더 길다면 공격 시간이 부족한 상황($w < 0$)이 발생한다. 공격 실행 시간은 대기 시간과 사용자와 공격자의 전체 동기화 이후 종료 시간 차이(x), 사용자 실행 시간을 이용하여 측정한다. 만약 공격자 실행 시간이 사용자 실행 시간 보다 짧다면 공격 성공 가능성이 존재한다.

공격 실행 시간이 실시간으로 이루어지는 숄더 서핑 공격의 성공/실패 여부 판단을 위해 중요한 평가 항목이기는 하지만 실행 시간만으로 공격의 성공/실패 여부를 판단하는 것은 한계가 있다. 따라서 STM-GOMS 모델은 실행 시간 비교뿐 만 아니라 메모리 한계도 고

〔표 4〕 안전성 평가 항목

평가 항목		의미
T_A	$T_U - w + x$	공격 실행 시간(ms)
I_P	I_{CP}/I_{HP}*100	지각 정보 비율(%)
	I_{CP}	지각할 수 있는 정보량
	I_{HP}	지각해야하는 정보량

려한다. 숄더 서핑 공격자는 사용자의 입력을 관찰하여 비밀 정보를 획득하고자 한다. 이 때 공격자의 관찰은 지각 조작을 의미하며 공격자가 공격 성공을 위해 그 순간 지각해야만 하는 정보가 존재한다. 이러한 원리를 바탕으로 숄더 서핑 공격자의 지각 정보 비율을 측정한다. 지각 정보 비율은 공격자가 주어진 시간 내에 지각 조작을 통해 지각할 수 있는 정보의 양과 공격 성공을 위해 지각 해야만 하는 정보의 양을 통해 계산된다. 만약 지각 저보 비율이 100%라면 주어진 시간 내에 지각해야만 하는 정보를 모두 지각한 것이므로 공격 성공 가능성이 존재한다. 반대로 지각해야만 하는 정보에 비해 지각 할 수 있는 정보의 양이 적은 경우(e.g., 시간 부족) 공격 성공이 불가능하다. 따라서 숄더 서핑 공격이 완전히 성공하려면 공격 실행 시간이 사용자 실행 시간보다 작거나 같아야 하며, 지각 정보 비율이 100%가 되어야 한다.

IV. STM-GOMS 모델의 수행 단계

4.1 서술

인증 기법을 사용하는 사용자의 작업을 서술하거나 공격을 시도하는 공격자의 작업을 서술하는 단계이다. 먼저 CMN-GOMS 모델에서 사용되는 의사코드 형태를 활용하여 작업을 자세히 목표, 방법, 조작으로 표현한다. STM -GOMS 모델에서는 가독성을 높이기 위해, CMN-GOMS 모델의 의사코드를 확장하여 목표를 최종목표(FGOAL), 부목표(SGOAL), 세부목표(GOAL)로 좀 더 세분화하고 인덱스 (부목표의 인덱스는 알파벳 대문자 이용, 세부목표의 인덱스는 상위 부목표의 인덱스, 숫자와 점(.) 이용)를 활용한다. 또한 선택 규칙인 SELECT 코드 다음에도 인덱스를 붙여 여러 선택 규칙이 존재할 경우 구분 가능하도록 하며, 효율적인 작업 분석을 위해 반복(ITERATE) 부분을 목표 내부에 포함시킨다.

의사코드로 서술된 사용자와 공격자의 작업을 토대로 방법별로 〔표 1〕과 〔표 2〕의 CPM 조작들을 이용하여 스케줄 차트로 표현한다. 스케줄 차트에 포함된 각 조작의 시작시간과 평가시간을 입력하고 주요 경로를 선택하여 방법의 총 실행시간을 계산한다. 사용자와 공격자의 작업은 방법들의 반복과 집합으로 구성되므로, 방법별로 작성된 스케줄 차트를 이용하여 전체 작업을 쉽게 표현하는 것이 가능하다.

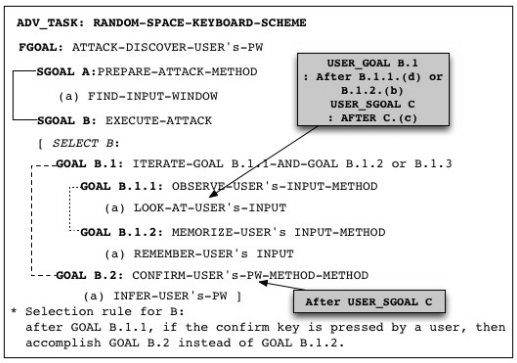
4.1.1 랜덤 공백 키보드 기법의 의사코드 서술

〔그림 2〕는 랜덤 공백 키보드 기법을 사용하는 사용자의 작업을 STM-GOMS 모델의 의사코드로 서술한 것이다. 사용자는 공백이 랜덤하게 배치된 가상 키보드에서 자신의 패스워드를 입력한다.

〔그림 3〕은 사용자의 패스워드가 입력되는 창을 관찰하여 패스워드를 획득하고자하는 숄더 서핑 공격자의 작업을 의사코드로 서술한 것이다. 공격자는 사용자와 해당 기법의 상호작용을 직접 관찰하여 공격을 시도한다. 공격자의 작업은 사용자의 작업에 의존하여 서술되므로 사용자의 특정 조작 이후에 실행되는 목표와 조작을 표시할 필요가 있다. 예를 들어, 공격자는 사용자가 패스워드 각 문자를 입력 한 후에 관찰이 가능하므로 공격자의 ADV_GOAL B.1.1. (a) 조작은 사용자가 가상 키보드 키를 누르는 USER_GOAL B.1.1.(d) 혹은 USER_GOAL B.1.2. (b) 후에 수행되어야만 한다. 또한 공격자는 사용자의 패스워드 입력을 반복적으로 관찰하다가 모든 패스워드 입력이 끝나 사용자가 확인 버튼을 누르면 그 전까지 관찰한 문자들을 가지고 전체 패스워드를 조합하므로 공격자의 ADV_GOAL B.2.(a) 조작은 사용자가 확인 버

```
USER_TASK: RANDOM-SPACE-KEYBOARD-SCHEME
FGOAL: INPUT-PW (|PW|=i)
  SGOAL A: PREPARE-METHOD
     (a) RECALL-PW
  SGOAL B: ITERATE-GOAL B.1-i-TIMES
   [ SELECT B:
    GOAL B.1: INSERT-PW-CH
     [ SELECT B.1:
       GOAL B.1.1: INSERT-NEW-CH-METHOD
          (a) RECALL-PW-CH
          (b) FIND-CH-KEY
          (c) MOVE-HAND-TO-CH-KEY
          (d) PRESS-CH-KEY
       GOAL B.1.2: INSERT-PREVIOUS-CH-METHOD
          (a) RECALL-PW-CH
          (b) PRESS-CH-KEY ]
    GOAL B.2: DELETE-WRONG-CH-METHOD
        (a) FIND-DELETE-KEY
        (b) MOVE-HAND-TO-DELETE-KEY
        (c) PRESS-DELETE-KEY ]
  SGOAL C: CONFIRM-INSERT-PW-METHOD
     (a) FIND-CONFIRM-BUTTON
     (b) MOVE-HAND-TO-CONFIRM-BUTTON
     (c) PRESS-CONFIRM-BUTTON
* Selection rule for B:
  if a wrong character is inserted, then accomplish
  GOAL B.2 instead of GOAL B.1
* Selection rule for B.1:
  if a current character is the same as the previous
  character then accomplish GOAL B.1.2,
  else accomplish GOAL B.1.1
```

〔그림 2〕 랜덤 공백 키보드 기법의 사용자 작업 서술



〔그림 3〕 랜덤 공백 키보드 기법의 공격자 작업 서술

튼을 누르는 USER_SGOAL C.(d) 조작 이후에 수행되어야 한다. 따라서 〔그림 3〕의 오른쪽 박스처럼, 사용자의 특정 작업 후에 이루어지는 공격자의 작업이 의사코드 서술에 포함된다.

4.1.2 랜덤 공백 키보드 기법의 CPM 집합 서술

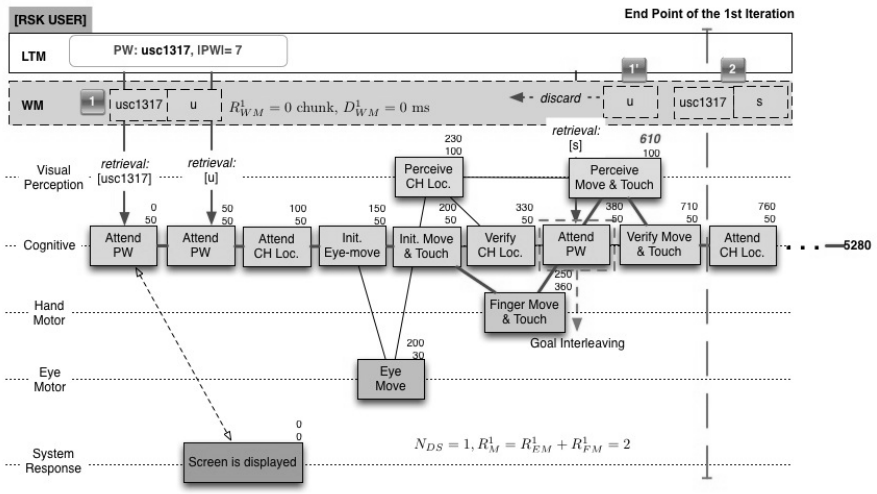
의사코드로 서술된 랜덤 공백 키보드 기법의 사용자와 공격자 작업에 포함된 방법들을 CPM 조작들로 표현한다. 방법별로 표현된 CPM 조작들을 의사코드의 실행 순서에 따라 연결하여 CPM-GOMS 모델의 스케줄 차트로 표현한다. 스케줄 차트에서 최악의 시간을 주요 경로로 선택한다. 의사코드를 방법별 CPM 집합으로 서술하기 전, 두 서술 사이의 맵핑을 위해 조작별로 CPM 집합으로 표현하는 단계를 가지며 해당 단계와 방법별 CPM 집합 표현에 대한 그림은 본 논문에서 생략한다.

4.2 분석

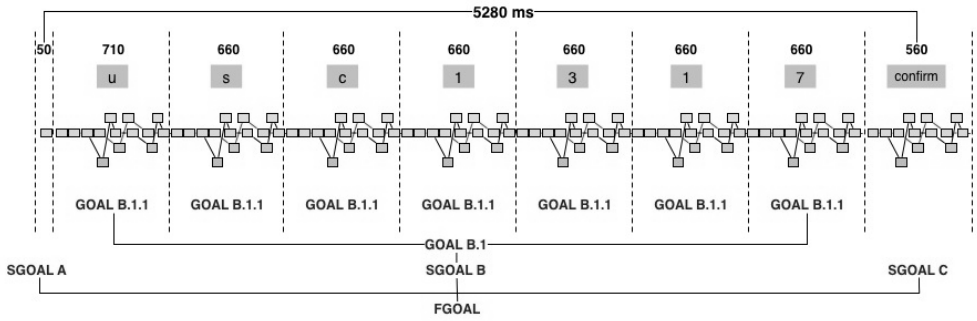
STM-GOMS 모델의 의사코드 및 CPM 집합으로 서술된 사용자와 공격자의 작업을 토대로 사용자와 공격자의 스케줄 차트를 작성하여 사용성을 분석하고 사용자와 공격자의 작업 스케줄 차트 동기화를 통해 안전성을 분석하는 단계이다. 사용자와 공격자의 작업은 반복적인 동작을 포함하므로 작업에 포함된 반복적인 동작과 서로 다른 방법들을 통해 전체 작업을 완성된 스케줄 차트로 표현한다.

4.2.1 랜덤 공백 키보드 기법의 사용성 분석

랜덤 공백 키보드 기법(RSK)의 사용성 분석을 위해, 사용자의 패스워드를 "usc1317"로 가정한다. 사용자가 패스워드 첫 번째 문자를 입력하는 과정을 첫 번째 반복으로 두고 〔그림 4〕와 같이 스케줄 차트로 표현할 수 있다. 이를 바탕으로 첫 번째 문자 입력을 위한 실행 시간, 메모리 복잡도, 인터페이스 복잡도를 예측한다. 사용자의 LTM 복잡도는 패스워드 길이와 같으며, 사용자는 패스워드를 기억해내는 것 이외에 WM을 사용할 필요가 없으므로 WM 복잡도를 나타내는 값은 모두 0 값을 가진다. 처음 디스플레이된 랜덤 공백 키보드가 패스워드 전체 입력 동안 변하지 않



〔그림 4〕 패스워드 첫 문자 'u' 입력에 대한 사용자 작업 스케줄 차트



〔그림 5〕 랜덤 공백 키보드 기법의 사용자 전체 작업 스케줄 차트

으므로 $N_{DS}=1$이 된다. 또한 첫 번째 문자 입력을 위해 한 번의 눈 움직임과 한 번의 손가락 움직임을 요구하므로 $R_M=2$가 된다. 일부 반복 작업에 대한 스케줄 차트를 이용하여 전체 스케줄 차트를 작성 가능하지만, 가독성을 높이기 위해 방법 별 스케줄 차트의 축약본을 이용하여 〔그림 5〕와 같이 표현한다. 목표들을 표시하고, 목표 달성을 위한 시간을 방법별 시간을 이용하여 예측하였다. 예측 결과 사용자가 랜덤 공백 키보드 기법을 이용하여 패스워드를 입력하는 시간은 총 5.3초(5,280밀리초)가 소요된다. 〔표 5〕는 랜덤 공백 키보드 기법의 사용성 분석 결과를 보여준다.

〔표 5〕 사용성 분석 결과

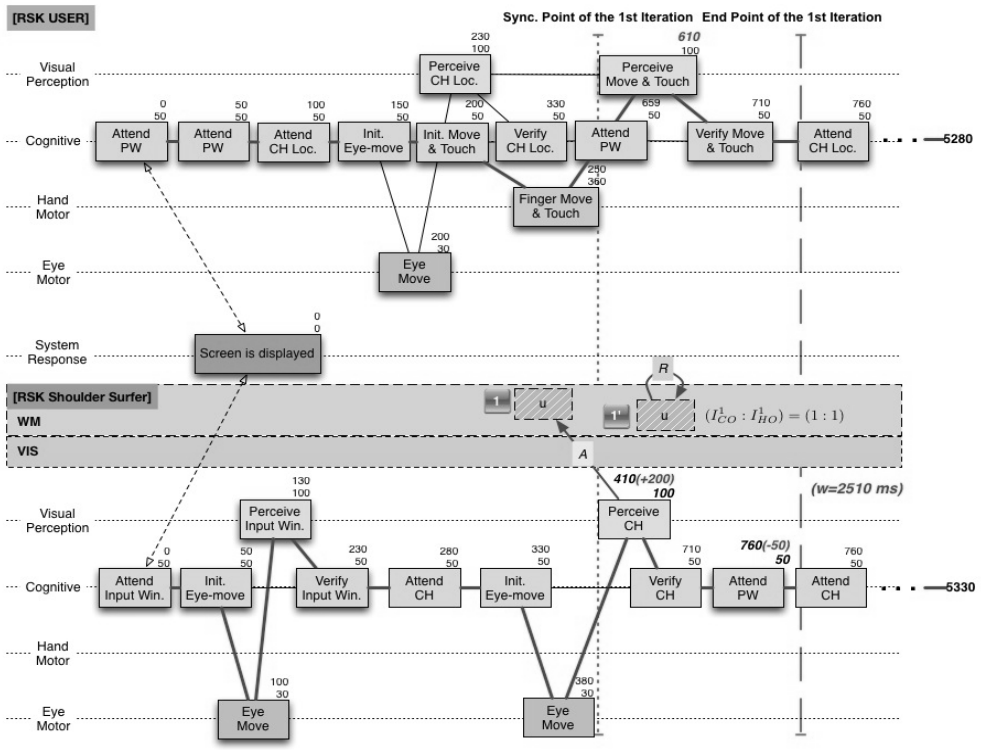
T_U (밀리초)	C_{MEM}	C_{IF}
5,280	〔7: 0(0)〕	〔1,16〕

4.2.2 랜덤 공백 키보드 기법의 안전성 분석

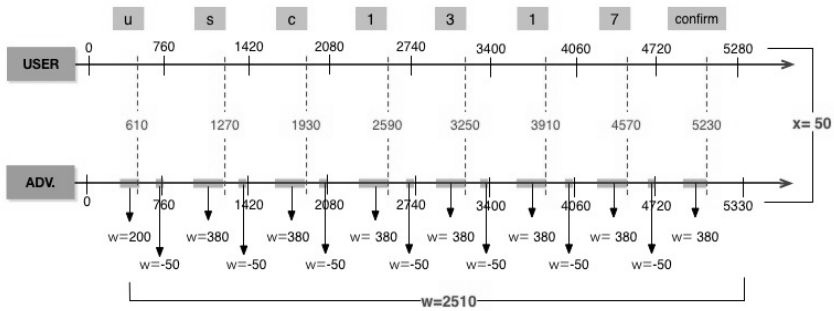
공격자의 관찰 작업은 반드시 사용자의 특정 작업 이후에 이루어지는 것이므로 사용자의 작업 스케줄 차트와의 동기화 및 비교를 통해 분석해야만 한다. 〔그림 6〕은 랜덤 공백 키보드 기법 사용 시작과 함께 패스워드 첫 문자 'u'를 입력하기까지의 사용자 작업과 공격자 작업 스케줄 차트를 비교 분석한 것이다. 〔그림 6〕에서 보는 바와 같이 사용자가 가상 키보드에서 문자를 손가락을 이용하여 터치 한 후, 공격자는 해당 터치 입력을 관찰하여 공격을 시도한다. 즉, 공격자는 두 번째 〔Eye Move〕 조작을 사용자의 〔Finger Touch〕 이후에 수행하므로 공격자의 두 번째 〔Eye Move〕 조작의 시작 시간은 610밀리초이며, 동기화 시점에 있는 〔Perceive CH〕 조작의 원래 시작 시간은 410밀리초로 200밀리초의 대기 시간(w)을 포함하게 된다.

〔그림 7〕은 전체 작업 비교를 시간에 따른 그래프로 표현한 것이다. 사용자와 공격자의 시간 축에 표시된 시간은 하나의 세부목표를 수행한 결과 시간을 의미하며, 사용자와 공격자 축을 연결하는 점선과 그 시간은 사용자와 공격자의 조작이 동기화되는 시점이다. 공격자의 시간 축에서 세부적으로 나뉜 부분은 공격을 위한 순수 작업 시간과 사용자 입력을 위해 대기해야 하는 시간을 구분한다. 〔그림 7〕과 같이 랜덤 공백 키보드 기법을 공격하는 공격자의 총 대기시간은 $w=2{,}510$밀리초이며, 사용자의 작업이 마치는 시간과 공격자의 작업이 마치는 시간에서 $x=50$밀리초 정도가 차이가 나지만 공격자의 대기시간을 여분의 시간으로 가져 공격의 정확성을 높이는데 활용 가능하므로 공격이 가능하다고 볼 수 있다. 즉, 공격자의 실제 공격 실행 시간 T_A는 $T_A = T_U - w + x = 5280 - 2510 + 50 = 2{,}820$밀리초가 된다. 사용자의 전체 실행 시간인 $T_U=5{,}840$밀리초 보다 T_A가 적으므로 공격 가능성이 존재한다.

〔그림 6〕에서 공격자가 지각해야 하는 정보는 사용자가 입력하는 첫 번째 문자 'u'이며, 대기시간이 존재하므로 공격자는 입력 문자를 관찰할 시간이 충분한 것으로 볼 수 있으며 관찰을 통해 지각하게 되는 정보는 지각해야 하는 정보와 일치한다. 즉, 첫 번째 문자 입력 관찰 과정을 제외한 나머지 반복에서도 대기시간을 가지며 지각해야 하는 정보와 지각할 수 있는 정보 모두 문자 하나이므로 랜덤 공백 키보드 기법의 숄더 서핑 공격자가 가지는 지각 정보 비율은 100%이다. 결론적으로, $T_U \geq T_A$이며, $I_P=100\%$이므로 랜덤 공백 키보드 기법은 숄더 서핑 공격에 안전하지 않다.



〔그림 6〕 패스워드 첫 문자 'u' 입력에 대한 사용자 작업과 공격자 작업 비교 및 동기화



〔그림 7〕 전체 사용자 작업과 공격자 작업 비교 시간 그래프

V. 실험을 통한 분석 결과 검증

STM-GOMS 모델의 분석 결과를 검증하기 위해, 실제로 랜덤 공백 키보드 기법을 구현하여 사용자 실험과 공격 실험을 시도하였다.

5.1 랜덤 공백 키보드 기법 구현

사용자 실험과 공격 실험을 위해, 랜덤 공백 키보드 기법을 삼성 갤럭시 S2에서 실행 가능하도록 안드로이드 플랫폼을 이용하여 구현하였다. 공백 대신 특수 문자(별 문자)를 사용하였다.

5.2 랜덤 공백 키보드 기법 사용자 실험 및 공격 실험

랜덤 공백 키보드 기법의 실험을 위해, 평균 나이가 26.9세인 컴퓨터 공학 전공의 스마트 기기에 능숙(평균 휴대폰 사용 기간: 10.5년, 평균 스마트폰 사용 기

간: 2년)한 대학생 및 대학원 생 15명(남: 10명, 여: 5명)이 참여하였다. 모두 실험에 자발적으로 참여하였으며, 모두 손가락 터치를 이용한 가상키보드 사용에 능숙한 사용자로 구성하였다. 또한 모두 왼손으로 스마트폰을 잡고 오른손을 이용하여 패스워드를 입력하였으며, 세로 버전에서 실험하였다.

5.2.1 사용자 실험

피실험자는 영문과 숫자를 혼합한 패스워드 7자리를 임의로 설정하여 10번의 입력을 시도하도록 하였다. 〔표 6〕과 같이 실험 결과 패스워드에 대한 입력 시간 평균(ET_U)은 4.9초(4,853밀리초)로 평가되었다.

〔표 6〕 사용자 실험 결과

(단위: 밀리초)

최소	최대	평균	표준편차
3,006	8,763	4,853	1,546

5.2.2 공격 실험

공격 실험을 위해, 15명의 피실험자들은 5개의 팀으로 나누어 공격을 진행하였으며, 트레이닝을 통해 최대한 사용자 입력 평균 시간인 4.9초에 가깝게 입력하는 실험 조교 5명이 임의의 7자리 패스워드를 입력하였다. 15명의 피실험자들은 5명의 실험 조교가 입력하는 패스워드를 차례로 관찰하였다. 모든 피실험자는 5개의 패스워드를 정확히 알아내어 100%로 공격에 성공(P: 공격 성공률)하였다.

5.3 분석 및 실험결과 비교

STM-GOMS 모델로 분석한 사용성과 안전성, 사용자 실험을 통한 사용성과 안전성(공격 성공 여부 측정)을 분석한 결과를 정리하면 〔표 7〕과 같다. 실제 실험에서의 사용성과 STM-GOMS 모델에서의 사용성은 427밀리초 밖에 차이가 나지 않으며, 모델을 통한 안전성 분석 결과 숄더 서핑 공격이 성공 가능함을 보였듯이, 실제 공격 실험의 결과인 100%의 공격 성공률(P)이 이를 뒷받침해준다.

〔표 7〕 랜덤 공백 키보드 기법 분석 및 실험 결과

	사용성	안전성
실제 실험	$ET_U = 4,853ms$	$P = 100\%$
STM-GOMS 모델	$T_U = 5,280ms$	$T_A = 2,820ms$
		$I_P = 100\%$

VI. 결론 및 향후 계획

본 논문에서는 모바일 스마트 기기 환경을 위한 인증 인터페이스 안전성 및 사용성 분석 모델인 STM-GOMS 모델을 제안하였다. STM-GOMS 모델은 HCI 인지 모델을 활용하여 인증 기법의 사용성과 동시에 숄더 서핑 공격에 대한 안전성 분석을 제공한다. 랜덤 공백 키보드 기법을 예로 들어 STM-GOMS 모델을 설명하였으며, 실제 구현과 실험을 통해 모델 분석 결과를 검증하였다. 랜덤 공백 키보드 기법 이외에 STM-GOMS 모델을 통한 다른 인증 기법의 안전성 및 사용성에 대한 분석 결과가 존재하며, 사용자 및 공격 실험을 통해 해당 분석 결과가 유효함을 검증하였다〔8〕〔11〕〔12〕〔13〕.

향후, STM-GOMS 모델에서 분석 가능한 공격을 숄더 서핑 공격에서 레코딩 공격과 악성 코드를 이용한 스파이웨어 공격으로 확대할 예정이다.

참 고 문 헌

〔1〕 S.K. Card, T.P. Moran and A. Newell, "The keystroke-level model for user performance time with interactive systems," *Communications of the ACM, vol. 23, no. 7,* pp. 396-410, July 1980.

〔2〕 S.K. Card, T.P. Moran and A. Newell, "The psychology of human-compute interaction," *Lawrence Erlbaum Publishers,* 1983.

〔3〕 N. Cowan, "The Magical Mystery Four: How is Working Memory Capacity Limited, and Why?" *Psychological Science, vol. 19, no. 1*, pp. 51-57, Feb. 2010.

〔4〕 A. De Luca, K. Hertzschuch and H. Hussmann, "ColorPIN-Securing PIN Entry through Indirect Input," In Proc. of *CHI'10,* pp. 1103-1106, Apr. 2011.

〔5〕 P.M. Fitts, "The information capacity of the human motor system in controlling

the amplitude of movement," *Journal of Experimental Psychology, vol. 7,* pp. 381-391, June 1954.
〔6〕 W.D. Gray, B.E. John and M.E. Atwood, "The Precis of Project Ernestine or an overview of a validation of GOMS," In Proc. of *CCS'92,* pp. 307-312, May 1992.
〔7〕 D.E. Kieras, "Towards a practical GOMS model methodology for user interface design," In M. Tauber and D. Ackermann, *The handbook of human computer interaction,* pp. 135-158, 1988.
〔8〕 T. Kwon, S. Na and S. Shin, "Covert Attentional Shoulder Surfing: Human Adversaries Are More Powerful Than Expected," *Submitted* (2012).
〔9〕 A.H. Lashkari, S. Farmand, O.B. Zakaria and R. Saleh, "Shoulder Surfing attack in graphical password authentication," *IJCSIS, vol. 6, no. 2,* pp. 145-154, Nov. 2009.
〔10〕 V. Roth, K. Richter and R. Freidinger, "A Pin-Entry Method Resilient Against Shoulder Surfing," In Proc. of *CCS'04,* pp. 236-245, Oct. 2004.
〔11〕 S. Shin, S. Na, T. Kwon, and H. Moon, "Modeling and Analysis of Regular PIN Entry Method and Its Improvements," In Proc. of *CNSI'12, ASTL, 8,* pp. 835-840, July 2012.
〔12〕 나사랑, 신수연, 권태경, "STM-GOMS 모델을 이용한 스마트 환경에서의 일반 PIN 입력 기법에 대한 사용성 및 안전성 분석," *한국정보보호학회 하계학술대회(CISC S'12)*, pp. 85-90, 2012 6월.
〔13〕 신수연, 나사랑, 권태경, "STM-GOMS 모델을 이용한 스마트 기기에서의 ColorPIN 기법에 대한 사용성 및 안전성 분석," *한국정보보호학회 하계학술대회(CISC S'12)*, pp. 357-362, 2012 6월.

〈著者紹介〉

신 수 연 (Sooyeon Shin) 학생회원
2004년 2월: 세종대학교 컴퓨터공학과 학사
2006년 2월: 세종대학교 컴퓨터공학과 석사
2012년 8월: 세종대학교 컴퓨터공학과 박사
2012년 9월 ~ 현재: 세종대학교 컴퓨터공학과 Post Doc.
〈관심분야〉 프라이버시 보호기술, 익명성 기술, RFID, 센서 네트워크 보안, HCI 보안 등

권 태 경 (Taekyoung Kwon) 종신회원
1992년 2월: 연세대학교 컴퓨터과학과 학사
1995년 2월: 연세대학교 컴퓨터과학과 석사
1999년 8월: 연세대학교 컴퓨터과학과 박사
1999년 ~ 2000년: U.C. Berkely Post-Doc.
2001년 ~ 현재: 세종대학교 컴퓨터공학과 부교수, 정보보호학회 이사 및 편집위원
〈관심분야〉 암호프로토콜, 네트워크 프로토콜, 센서네트워크 보안, 프라이버시 보호, HCI 보안 등