https://doi.org/10.5392/JKCA.2019.19.12.313

오프라인 대리사용자 및 해커로부터 특정 컴퓨터 보호를 위한 실시간 대응방안

Real-time Responses Scheme to Protect a Computer from Offline Surrogate Users and Hackers

송태기, 조인준
배재대학교 사이버보안학과

Tae-Gi Song(taegi827@gmail.com), In-June Jo(injune@pcu.ac.kr)

요약

현재 발생하고 있는 많은 해킹 피해 사례들의 요인들 중 하나는 사회 공학적 공격이다. 이러한 공격을 수행하는 주체는 악의적인 배신자 혹은 무지한 내부자인 경우가 많다. 이에 대한 해법으로 조직 내 직원의 보안 교육과 같은 관리적 보안의 강화를 들고 있다. 그럼에도 불구하고 현업에서는 불가피하게 컴퓨터를 공유하는 상황들이 빈번하게 일어나고 있다. 이런 경우 컴퓨터의 소유자는 공유를 받는 특정 대리인이 언제 접근했고 어떤 행위를 하는지에 대한 실시간 추적 및 대응이 어려운 점이 있다. 본 논문에서는 해킹된 인증수단 혹은 공유를 받은 인증수단을 통해 대리인이 오프라인으로 컴퓨터에 접근했을 때 컴퓨터의 소유자가 스마트폰을 통해 대리인들이 언제 컴퓨터에 접근하는 지를 실시간으로 추적하는 방안을 제안한다. 또한 비정상 접근 시에 스마트폰을 통해 PC의 중요 파일을 암호화 및 백업함으로써 중요 정보 유출에 대응하는 방안을 제안한다.

■ 중심어 : | 사회 공학적 공격 | 스마트폰 | 암호화 | 추적 | 대응 |

Abstract

One of the causes of many damage cases that occur today by hacking attack is social engineering attack. The attacker is usually a malicious traitor or an ignorant insider. As a solution, we are strengthening security training for all employees in the organization. Nevertheless, there are frequent situations in which computers are shared. In this case, the person in charge of the computer has difficulty in tracking and responding when a specific representative accessed and what a specific representative did. In this paper, we propose the method that the person in charge of the computer tracks in real time through the smartphone when a representative access the computer, when a representative access offline using hacked or shared authentication. Also, we propose a method to prevent the leakage of important information by encrypting and backing up important files of the PC through the smartphone in case of abnormal access.

■ keyword : | Social Engineering Attack | SmartPhone | Encryption | Tracking | Response |

* 본 논문은 2019학년도 배재대학교 교내학술연구비 지원에 의하여 수행된 것임

접수일자 : 2019년 09월 24일
심사완료일 : 2019년 10월 17일
수정일자 : 2019년 10월 17일
교신저자 : 조인준, e-mail : injune@pcu.ac.kr

I. 서론

사회 공학적 공격은 컴퓨터 시스템에서 기술적 수단이 아닌 신뢰를 바탕으로 사람들을 속여 정상적인 보안 절차를 깨트리는 공격이다[1]. 이러한 공격을 통한 피해 사례로 한국수력원자력과 인터파크 해킹사건 그리고 비트코인과 같은 가상화폐 보유자의 개인정보를 노린 해킹사건이 있다[2]. 사회 공학적 해킹 공격은 기술적 문제와 더불어 인적 문제까지 해결해야하기 때문에 어려움을 겪고 있는 실정이다[3]. 이러한 문제를 해결하기 위해 범국가적으로 조직 내 보안 교육의 강화를 실시하고 있지만 그 피해는 지속되고 있다[4]. 사회 공학적 공격은 보통 조직의 내부자들에 의해 수행되고 있다. 이러한 내부자들은 악의적인 배신자와 보안에 무지한 내부자로 분류할 수 있다[5]. 악의적인 배신자에 의한 피해의 원인 중 하나는 개인에게 할당된 PC를 여러 사람들이 공유하는데 있다. 보안에 무지한 내부자는 외부 해커들의 사회 공학적 공격에 쉽게 노출되고 자신도 모르는 사이에 공격이 수행되어 피해를 입는다. 조직 내에서 업무처리를 위해 개인 소유 PC를 불가피하게 공유해야 하는 상황들이 발생한다. 이 때 PC소유자는 무지한 내부자와 배신자의 접근으로부터 악의적인 해킹 공격의 피해를 막아야 하지만 비정상적인 행위를 감지하고 대응하기 어려운 것이 현실이다.

본 논문에서는 내부자의 실수나 배신에 의한 사회 공학적 공격을 스마트폰을 통해 추적하고 대응하는 방안을 제안한다. 제안방안을 요약하면, 첫째, 조직 내 PC 소유자는 자신의 PC에 자신 이외의 접근을 스마트폰을 통해 추적할 수 있다. 즉, 자신의 PC로의 비정상 접근을 추적해 PC 소유자가 즉시 위험에 대한 사실을 인지할 수 있게 하였다. 둘째, PC소유자는 비정상 접근 사실을 인지하고 PC 소유자의 중요 파일을 스마트폰에서의 명령을 통해 즉시 암호화할 수 있다. 이를 통해 PC 소유자는 사회 공학적 공격에 대한 위험을 즉각 인지하고 원격지에서 중요 파일의 유출을 막기 위한 대응을 할 수 있게 하였다. 이와 같은 일련의 과정을 통해 PC 소유자는 내부자의 접근부터 중요 정보 유출 전까지, 즉 골든타임 내에 사회 공학적 공격을 방어하기 위한 방안을 제안하였다.

II. 제안 방안

사회 공학적 공격으로 인한 피해는 지속되고 있다. 이러한 피해의 원인 중 하나는 조직 내 업무 PC의 관리의 문제이다. 조직 내 사회 공학적 공격을 막기 위해서는 직원들의 보안 교육을 강화해 업무 PC의 관리를 철저히 해야 한다. 하지만 실제 조직에서는 이러한 보안 강화를 위한 교육과 지침들이 업무 처리를 불편하게 만들고 있고 불가피하게 업무 PC를 공유하는 일이 빈번히 일어나고 있다. 이로 인해 PC소유자 이외의 공유를 받은 대리인들의 업무 PC에 대한 무분별한 접근이 가능해지고, 사회 공학적 공격에 대한 위험도 증가하게 된다. 업무처리를 위해 불가피하게 PC 소유자의 PC를 공유할 경우 PC소유자는 악의적인 대리인들의 접근 시점에 대해 알 수가 없다. 이는 PC소유자도 모르는 사이에 업무 PC로부터 중요 정보가 유출될 수 있는 문제를 야기한다. 이와 더불어 PC소유자가 접근 사실을 인지하였더라도 원격에서 중요 정보의 유출을 막기 위한 즉각적인 대응도 어렵다.

본 논문에서는 보안 교육만으로 해결할 수 없는 사회 공학적 공격 문제에 대해 좀 더 효과적인 방안을 제안하였다. 즉, 공유 PC에 대한 사회 공학적 공격을 막기 위해 추적과 대응의 관점에서 PC소유자의 스마트폰을 이용한 능동적 대응방안을 제안하였다. 이를 요약하면, 첫째, 제안 시스템은 스마트폰을 통한 공유 PC 추적 기능을 제공하였다. 추적 기능은 대리인들의 공유 PC 접근 사실에 대해 PC 소유자가 인지할 수 있게 하였다. 이는 예상치 못한 비정상 접근으로 소유자도 모르는 사이에 이루어지는 공격 문제를 해결할 수 있다. 둘째, PC 소유자가 자신의 PC에 비정상 접근을 인지했을 때 대응 기능을 제공하였다. 즉, PC소유자의 스마트폰을 통해 비정상 접근을 인지하고 스마트폰을 통해 공유 PC의 중요 정보를 암호화해 유출 공격에 즉각 대응할 수 있게 하였다. 이는 원격지의 PC 소유자가 자신의 PC에 대한 비정상 접근에 즉각 대응할 수 없는 문제를 해결하였다.

1. 제안 시스템 구성

제안 시스템의 기본구성은 [그림 1]과 같다. 주요 구성요소는 사용자 스마트폰, 사용자 단말(PC), 중계 웹서버로 이루어진다. 사용자 스마트폰은 추적요청 및 대응요청 기능을 중계 웹서버를 통해 원격의 사용자 단말을 제어하는 역할을 한다. 사용자 단말은 추적요청과 대응요청에 대해 중계 웹서버를 통해 요청에 응답하는 역할을 한다. 중계 웹서버는 사용자 스마트폰과 사용자 단말 사이에 오가는 요청과 응답을 중계해주는 역할을 한다. 또한 대응 모듈로 인해 발생할 수 있는 중요 데이터에 대한 백업 기능을 수행해 중요 데이터 저장소에 사용자 단말로부터 수신한 중요 데이터를 저장하는 역할을 한다. 세 가지 구성요소는 사용자 계정에 의해 동기화 된다. 사용자 계정은 사용자 단말과 사용자 스마트폰에서 생성 및 관리하고 중계 웹서버가 사용자 계정을 인증하는 역할을 한다.

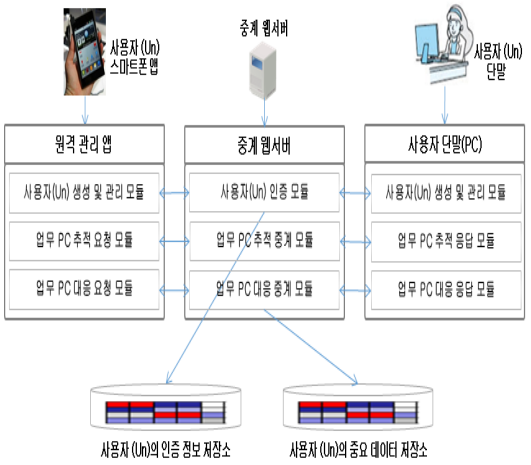

그림 1. 제안 시스템 구성도

[그림 1]의 제안 시스템 구성도의 추적과 대응 모듈에 대해 설명하면 다음과 같다. 첫째, 추적 모듈은 사용자가 원격지에 있는 사용자 단말 상태를 스마트폰을 통해 확인할 수 있는 기능들을 제공한다. 이를 위해 추적 모듈은 로그인 알림 기능, 프로세스 모니터링 기능, GPS 추적 기능, 캠 사진 찍기 기능을 가지고 있다. 로그인 알림 기능은 사용자가 원격의 사용자 단말이 로그인되면 스마트폰의 알림을 통해 확인할 수 있게 하고, 스마트폰을 통해 로그인 상태를 상시 체크할 수 있게 한다. 프로세스 모니터링 기능은 사용자가 스마트폰을 통해 원격지 사용자 단말의 현재 프로세스 모니터링을 할 수 있게 한다. GPS 추적 기능은 노트북을 포함해 GPS 장비가 부착된 사용자 단말의 도난 시 추적을 위한 기능으로 스마트폰을 통해 사용자 단말의 GPS 정보를 확인할 수 있게 한다. 캠 사진 찍기 기능은 사용자가 스마트폰을 통해 사용자 단말의 현재 대리사용자를 확인하기 위한 기능이다. 사용자 단말에 부착된 캠을 통해 찍은 사진을 스마트폰에서 확인할 수 있게 한다. 둘째, 대응 모듈은 사용자가 추적 모듈을 통한 정보를 확인 후 비정상 접근을 감지하였을 때 공격의 피해를 막기 위한 기능을 제공한다. 이를 위해 대응 모듈은 암호화 기능, 백업 기능을 가지고 있다. 암호화 기능은 사용자 단말로의 비정상 접근을 감지하였을 때 사용자 스마트폰을 통해 암호화 명령을 수행해 사용자 단말의 중요 데이터를 암호화할 수 있게 한다. 백업 기능은 암호화 기능이 수행된 후 즉시 중계 웹서버로 암호화된 데이터가 전송되며 암호화된 중요 데이터가 공격자에 의해 삭제될 위험에 대응할 수 있게 한다.

2. 제안 시스템 상세 설계

제안시스템에서 핵심이 되는 업무 PC 추적과 업무 PC 대응 두 가지 모듈을 수행하기 위해 설계한 내용을 설명한다. 업무 PC 추적 모듈에는 로그인 알림 기능, 프로세스 모니터링 기능, GPS 추적 기능, 캠 사진 찍기 기능이 있고, 업무 PC 대응 모듈에는 암호화 기능, 백업 기능이 있다.

2.1 업무 PC 추적 모듈의 로그인 알림

본 절에서는 업무 PC에 대리인이 로그인하였을 때 소유자가 스마트폰을 통해 로그인 알림을 확인할 수 있도록 하는 절차에 대하여 설명한다. 본 절에서 설명하는 로그인은 사용자 단말에 설치된 OS인 Windows 시스템에 로그인 하는 것을 말한다.

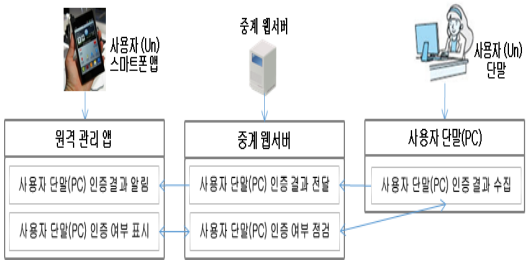

그림 2. 업무 PC 추적 모듈의 로그인 알림 기능

Step 1) 업무 PC의 소유자는 대리인에게 업무 PC 즉 사용자 단말의 인증정보(Windows 패스워드)를 공유해 대리인이 사용자 단말에 접근 가능하게 한다.

Step 2) 대리인은 소유자의 업무와 관련해 대리 처리를 위해 소유자의 사용자 단말에 로그인을 한다.

Step 3) 사용자 단말에 설치된 제안시스템이 사용자 단말에 로그인한 결과를 중계 웹서버로 전달하고, 중계 웹서버는 전달받은 결과를 원격 관리 앱으로 전달한다.

Step 4) 소유자의 스마트폰에 설치된 원격 관리 앱에서 전달받은 결과를 알림을 통해 알려준다.

Step 5) 소유자가 스마트폰의 원격 관리 앱을 통해 사용자 단말의 상태를 확인하려 할 때, 소유자는 원격 관리 앱에서부터 현재 상태를 조회한다.

Step 6) 중계 웹서버는 원격 관리 앱으로부터의 조회 요청을 받고, 사용자 단말의 로그인 상태를 조회한다.

Step 7) 중계 웹서버는 조회한 결과를 원격 관리 앱으로 전달하고 소유자는 사용자 단말의 현재 로그인 상태를 확인할 수 있게 된다.

2.2 업무 PC 추적 모듈의 프로세스 모니터링

본 절에서는 업무 PC에 로그인한 대리인이 현재 어떤 작업을 수행중인지 확인하기 위해 소유자의 스마트폰에 설치된 원격 관리 앱을 통해 사용자 단말의 현재 프로세스 목록을 확인할 수 있도록 하는 절차에 대하여 설명한다.

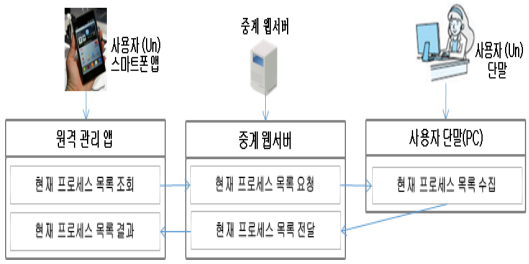

그림 3. 업무 PC 추적 모듈의 프로세스 모니터링

Step 1) 소유자는 사용자 단말을 사용 중인 대리인이 현재 어떤 작업을 수행하고 있는지 확인하기 위해 원격 관리 앱을 통해 현재 프로세스 목록 조회 기능을 수행한다.

Step 2) 중계 웹서버는 원격 관리 앱으로부터 조회 요청을 수신하고 사용자 단말에 조회를 요청한다.

Step 3) 요청을 받은 사용자 단말은 현재 프로세스 목록을 수집해 중계 웹서버로 전달한다.

Step 4) 중계 웹서버는 전달받은 결과를 원격 관리 앱으로 송신하고 소유자는 원격 관리 앱을 통해 수신한 프로세스 목록을 확인할 수 있다.

2.3 업무 PC 추적 모듈의 GPS 추적

본 절에서는 GPS가 부착된 사용자 단말에 해당하는 경우로 도난 발생 시에 스마트폰을 통해 사용자 단말의 위치를 확인할 수 있도록 하는 절차에 대하여 설명한다.

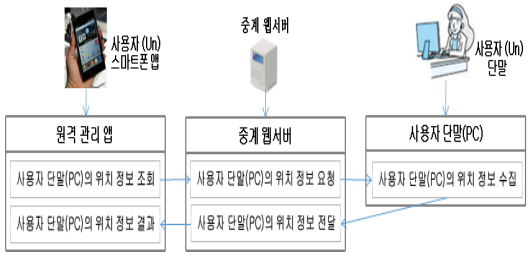

그림 4. 업무 PC 추적 모듈의 GPS 추적

Step 1) 사용자 단말의 소유자는 단말 도난 발생 시 자신의 스마트폰의 원격 관리 앱을 통해 사용자 단말의

위치 정보를 조회 한다.

Step 2) 중계 웹서버는 위치정보 조회 요청을 사용자 단말에 전달한다.

Step 3) 사용자 단말은 자신의 위치정보를 수집해 중계 웹서버로 결과를 응답한다.

Step 4) 원격 관리 앱은 중계 웹서버로부터 위치정보 조회 결과를 수신하고 사용자 단말의 소유자는 결과를 확인해 사용자 단말의 위치를 확인할 수 있다.

2.4 업무 PC 추적 모듈의 캠 사진 찍기

본 절에서는 캠이 부착된 사용자 단말에 해당하는 경우로 소유자가 현재 자신의 사용자 단말을 사용하고 있는 대리인을 원격 관리 앱을 통해 확인할 수 있도록 하는 절차에 대하여 설명한다. 캠 사진을 통해 현재 사용자 단말을 사용하고 있는 대리인이 올바른 대리인인지를 판단할 수 있고 비정상 접근 시 공격자의 얼굴을 판단할 수 있다.

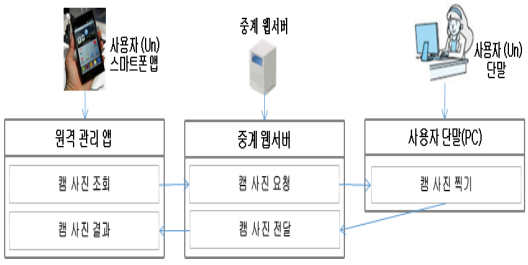

그림 5. 업무 PC 추적 모듈의 캠 사진 찍기

Step 1) 사용자 단말의 소유자는 현재 사용자 단말을 사용하고 있는 대리인을 확인하기 위해 스마트폰의 원격 관리 앱을 통해 사용자 단말에 부착된 캠 사진을 찍고 결과를 조회 한다.

Step 2) 중계 웹서버는 캠 사진 조회 요청을 사용자 단말에 전달한다.

Step 3) 사용자 단말은 캠 사진을 찍고 중계 웹서버로 결과를 응답한다.

Step 4) 원격 관리 앱은 중계 웹서버로부터 캠 사진 결과를 수신하고 사용자 단말의 소유자는 결과를 확인해 현재 사용자 단말을 사용하고 있는 대리인을 확인할 수 있다.

2.5 업무 PC 대응 모듈의 암호화

본 절에서는 사용자 단말의 소유자가 사용자 단말로의 비정상 접근을 감지했을 경우, 소유자가 사용자 단말의 중요 파일을 자신의 스마트폰의 원격 관리 앱을 통해 즉시 암호화할 수 있도록 하는 절차에 대하여 설명한다[7]. 파일을 암호화 하는데 사용되는 키는 제안 시스템에서 사용하는 계정의 암호를 통해 만들어 낸다.

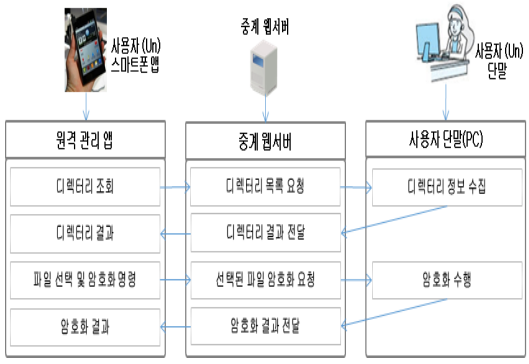

그림 6. 업무 PC 대응 모듈의 암호화

Step 1) 비정상 접근을 감지한 사용자 단말의 소유자는 중요 데이터를 암호화하기 위해 원격 관리 앱을 통해 사용자 단말의 디렉터리 조회를 실시한다.

Step 2) 중계 웹서버는 디렉터리 목록 조회 요청을 사용자 단말에 전달한다.

Step 3) 사용자 단말은 현재 디렉터리 목록을 조회해 중계 웹서버로 결과를 응답한다.

Step 4) 소유자는 원격 관리 앱을 통해 사용자 단말의 현재 디렉터리를 목록들을 확인하고, 즉시 암호화할 중요 파일들을 선택해 암호화하도록 명령한다.

Step 5) 사용자 단말은 암호화 명령을 수행하기 전 사용자로부터 제안 시스템 계정의 암호를 입력받아 올바른 사용자인지 여부를 확인하고 올바른 사용자이면 계정 암호를 암호화 키 값을 생성하는데 사용한다.

Step 6) 중계 웹서버는 암호화 명령을 전달받고 사용자 단말로 선택된 파일에 대한 정보를 전달한다.

Step 7) 사용자 단말은 요청받은 암호화를 수행하고 결과를 응답해 최종적으로 소유자는 스마트폰에서 암호화 수행 결과를 확인할 수 있다.

2.6 업무 PC 대응 모듈의 백업

본 절에서는 사용자 단말의 소유자가 비정상 접근을 감지하고 암호화를 수행한 후, 암호화된 파일이 삭제되는 위험을 방지하기 위해 백업할 수 있도록 하는 절차에 대하여 설명한다.

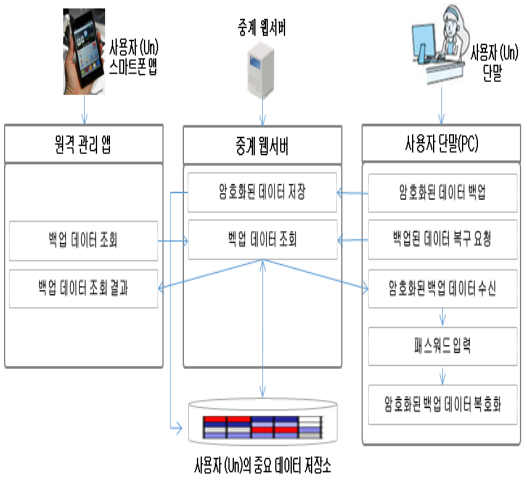

그림 7. 업무 PC 대응 모듈의 백업

Step 1) 앞선 2.5에서 설명한 암호화 과정이 수행된 후 사용자 단말의 암호화된 파일은 중계 웹서버로 자동으로 송신된다.

Step 2) 중계 웹서버는 수신한 파일을 사용자의 중요 데이터 저장소에 안전하게 저장한다.

Step 3) 사용자 단말의 소유자는 스마트폰의 원격 관리 앱을 통해 파일이 안전하게 백업되었는지 조회한다.

Step 4) 중계 웹서버는 백업 파일을 조회해 스마트폰으로 결과를 송신하고 소유자는 스마트폰을 통해 백업된 데이터들을 확인할 수 있다.

Step 5) 사용자 단말의 소유자는 사용자 단말로 복귀해 백업된 데이터를 복구한다.

Step 6) 중계 웹서버는 사용자의 중요 데이터 저장소에서 백업된 데이터를 가져와 사용자 단말의 복구 요청에 응답한다.

Step 7) 사용자 단말은 암호화된 백업 데이터를 수신하고 소유자는 비밀번호를 입력해 백업 데이터를 안전하게 복호화 할 수 있다.

Ⅲ. 기존 방안과 비교 및 검토

이 장에서는 본 논문에서 제안한 원격 관리 앱을 이용한 사회 공학적 공격의 실시간 추적 및 대응 방안을 기존의 자신의 PC를 원격 관리하기 위한 방안들과 비교하여 제안 방안의 차별성을 설명하였다. 제안 방안의 비교에 있어서 전제는 개인의 PC를 보안상 목적으로 안전하게 관리하기 위해 원격 관리 앱을 사용할 경우이며, 기존의 개인 PC를 원격으로 관리하기 위한 상용 원격 관리 앱을 비교 대상으로 하였다[8].

상기에서 제시한 기존의 원격 관리 앱과 본 논문에서 제안한 원격 관리 시스템의 상대적인 비교결과를 [표 1]에 정리하였다. [표 1]에서 본 바와 같이 본 논문에서 제안한 스마트폰 앱에 기반한 원격 관리 시스템이 여러 비교요소들에서 우수성을 보이고 있다. 이는 기존의 원격 관리 앱과 제안 시스템의 근본적인 목적의 차이 때문이라고 볼 수 있다. 기존 원격 관리 앱은 자신의 PC를 원격에서 단순히 관리하기 위한 목적을 가진다. 따라서 PC에 해킹 공격을 당한 사실을 인지하고 대응하기 어렵다. 하지만 제안 시스템은 사회 공학적 공격에 대응 하는데 목표를 두고 있어 [표 1]의 내용과 같이 기존 유사한 시스템보다 보안 요소들의 우수한 결과가 나타난다.

[표 1]에 따른 원격 관리 앱을 이용한 제안 시스템은 기존 원격 관리 제품과 비교해 해킹 공격을 추적하고 대응하는데 목적을 두고 있다. 또한 제안 시스템은 원격 관리 앱을 통해 관리하는 대상 PC의 사용자를 기존 원격 관리 앱에서 본인으로 제한하는 것과 달리 대리인의 사용까지 고려하였다. 이는 기존 원격 관리 앱과 달리 실제 업무 처리를 위해 빈번히 일어나는 업무 PC의 공유로 인한 사회 공학적 공격의 피해에 대응할 수 있

게 한다. 제안 시스템은 기존 원격 관리 앱과 마찬가지로 해당 시스템을 이용하기 위한 별도의 계정을 필요로 한다. 이는 해당 시스템 계정을 통해 원격 관리 앱과 관리 대상 PC를 연결하고 대응 모듈 이용 시 계정과 패스워드를 기반으로 데이터에 대한 소유권을 부과하기 위함이다.

앞서 설명한 기존 시스템과 제안 시스템을 사용하는 배경 차이에 의해 제안 시스템은 기능과 효과에서 기존 시스템과 확연한 차이를 가진다. 첫째, 제안 시스템은 원격 관리 대상이 되는 PC의 자원뿐만 아니라 PC의 위치정보와 사진정보가 추적의 범위 내에 있다. 이는 기존 시스템이 단순 관리 목적인 것과 비교해 관리 대상 PC의 위치 추적과 해커의 얼굴을 추적하기 위한 목적으로 보안 목적을 갖고 있다. 둘째, 기존의 단순 관리 목적의 시스템은 관리 대상 PC가 사회 공학적 공격을 받을 때 원격에서의 대응이 불가능하다. 하지만 제안 시스템은 비정상 접근에 대해 감지했을 때 암호화와 백업을 통해 즉각 대응이 가능하다. 마지막으로 이러한 요소들을 통해 제안 시스템은 관리 대상 PC가 사회 공학적 해킹 공격을 당했을 때 대응 기능 자체가 없는 기존 원격 관리 제품에 비해 그 피해 수준이 기존 시스템에 비해 현저히 떨어진다고 할 수 있다. 본 논문에서 제안한 시스템이 이러한 우수성을 보인 요인은 기존 시스템이 개인의 단순 관리에 목적을 둔 것에 비해 제 3자의 공격 위험을 추적하고 대응하는데 목적을 두었기 때문이다.

표 1. 상용 원격 관리 제품과 제안시스템 비교분석

원격관리앱 / 비교요소	상용 원격 관리 제품	제안 시스템
사용 목적	개인 관리	해킹 공격 추적 및 대응
관리 대상 PC 사용자	본인	본인, 대리인
시스템 계정	필요	필요
추적 범위	PC 자원	PC 자원, 위치정보, 사진정보
해킹 공격 대응	불가	암호화, 백업
관리대상 PC 해킹 피해 수준	고	저

Ⅳ. 결론

본 논문은 스마트폰 원격 관리 앱을 통해 현업에서 불가피하게 이루어지는 업무 PC의 공유 시 발생하는 사회 공학적 공격 위험을 줄이기 위한 방안에 관한 내용이다. 본 논문에서 제안한 시스템은 기존의 원격 관리 앱에서는 고려하지 않은 보안 위험에 대한 문제를 다루었다. 따라서 사회 공학적 해킹 공격이 발생했을 때 기존의 방식에서 대응할 수 없던 문제를 해결하였다. 물론 보안 교육 강화와 업무 PC에 대한 공유 자체를 금하여 사회 공학적 해킹 피해에 대응하는 방안도 있지만, 현재 그렇게 하고 있음에도 불구하고 사회 공학적 해킹피해가 지속적으로 발생하고 있다. 따라서 본 논문에서 제안한 시스템은 인적 요소로 발생하는 해킹 공격에 대한 문제를 원천 차단할 수 없기 때문에 피해자 입장에서 공격에 적극적으로 대응할 수 있는 유의미한 새로운 방안이라고 볼 수 있다. 하지만 제안 시스템은 해커가 사용자 단말에 접근하여 중요 정보를 탈취하기 직전까지의 골든 타임 내에서 의미가 있다. 따라서 제안 시스템은 해킹 피해에 적극적으로 대응 하는 것에서 나아가 피해가 발생한 후 공격자를 추적하기 위한 방안에 대한 연구가 필요하다.

본 논문에서 새롭게 제안한 원격 관리 시스템이 피해자의 입장에서 사회 공학적 공격에 효과적으로 대응하기 위한 방안이 될 수 있길 기대한다.

참 고 문 헌

[1] 박재혁, 이재우, “인간의 감정 상태를 이용한 사회공학 기법 연구,” 정보보호학회지, Vol.25, No.4, pp.57-62, 2015.

[2] https://jmagazine.joins.com/economist/view/318647, 2019.10.14.

[3] 허진아, 주성빈, 이정민, 박찬혁, “사회공학적 공격에 대한 산업기술 보호방안,” 사회과학연구, Vol.23, No.1, pp.279-306, 2016.

[4] 서미숙, 박대우, “PC의 개인정보보호법 대응 방안,” 정보보호학회지, Vol.22, No.8, pp.21-25, 2012.

[5] 권영준, “해킹(hacking) 사고에 대한 개인정보처리자

의 과실판단기준," 저스티스, pp.34-72, 2012.
[6] 최양서, 서동일, "사회공학적 공격방법을 통한 개인정보 유출기술 및 대응방안 분석," 정보보호학회지, Vol.16, No.1, pp.40-48, 2006.
[7] https://docs.oracle.com/javase/8/docs/api/index. html, 2019.08.16
[8] https://teamviewer.com/ko/, 2019.08.16.
[9] http://www.cstec.kr/cstec/kor/index.html, 2019. 10.15
[10] 박기홍, 이준환, 조한진, "개인정보 입력 감지를 이용한 사회공학적 공격 대응방안," 한국콘텐츠학회논문지, Vol.12, No.5, pp.32-39, 2012.
[11] https://www.boannews.com/media/view.asp?idx=49906, 2019.10.15.

저 자 소 개

송 태 기(Tae-Gee Song) 준회원

■ 2018년 2월 : 배재대학교 사이버보안학과 졸업
■ 2018년 3월 : 배재대학교 사이버보안학과 석사과정

〈관심분야〉 : 정보보호, 모바일 보안, 보안 SW개발

조 인 준(In-June Jo) 정회원

■ 1982년 2월 : 전남대학교 계산통계학과 졸업
■ 1985년 2월 : 전남대학교 전자계산학과 석사
■ 1999년 2월 : 아주대학교 컴퓨터공학과 박사
■ 1983년 ~ 1993년 : 한국전자통신연구원 선임연구원
■ 1994년 ~ 현재 : 배재대학교 사이버보안학과 교수

〈관심분야〉 : 정보보호, 컴퓨터네트워크보안, 컴퓨터시스템 조직응용