피싱공격 차단을 위한 PSMS 설계 및 구현

유재형* · 이동휘* · 양재수** · 박상민*** · 김귀남*

요 약

최근의 공격은 URL과 사이트를 속이는 형태와 지능화된 악성코드를 침투하는 기술적 은닉기법을 이용한 공격이 사용되고 있다. 그러나 상대적으로 피싱보안 기술들은 아직 피싱 수법들을 따라가지 못하는 경우가 많다. 이에 본 연구에서는 웹 환경의 급변화함에 따른 개방된 정보교류 강화를 위해 웹서버와 클라이언트 간 네트워크 단에 프락시서버를 설치하여 유해사이트 분석 및 피싱URL을 화이트도메인리스트와 비교하여 필터링하고 안정된 웹 기반의 정보교류를 할 수 있도록 설계하여 최소한의 규제와 능동적인 제어를 통해 피싱차단 할 수 있는 설계 및 구조를 제시하고 이를 검증하고자 한다.

PSMS Design and Implementation for a Phishing Attack Intercept

Jae Hyung Yoo* · Dong Hwi Lee* · Jae Su Yang** · Sang Min Park*** · Kuinam J. Kim*

ABSTRACT

Recently, Phising attack uses trick of URL and sites, and technical concealment method which infiltrates sophisticated malicious code. However, sometimes Phising security technology cannot cover all of Phising methods.

Consequently, this research proposes inspection to solve this problem. First, we can install Proxy server for a strong open information exchange of web environment between web servers and clients. Therefore, it compares and analyzes harmful site and Phising URL with White domain list, and filters them. Finally, designs for stable web based information so that we can block Phising with least regulation and active control. So the purpose of this paper is introducing this design system and structure, and inspect them.

Key words : Web2.0, White Domain, Malicious Code, Phising

* 경기대학교 정보보호학과
** 경기도 정보화보좌관
*** 인천대학교 산업경영학과

1. 서 론

최근 피싱 공격은 사람들의 URL과 사이트를 속이는 형태와 지능화된 악성코드를 침투하는 기술적 은닉 기법을 이용한 피싱 공격이 발견되고 있다. 특히 시스템 변조를 통한 피싱은 안티피싱 워킹그룹(Anti-Phishing Working Group, APWG)에도 알려진 바가 없는 신종 피싱 유형으로 이 같은 사용자의 PC 환경을 공략하는 피싱 기법들이 계속하여 등장하고 있다. 시시각각 변화하고 있는 피싱의 트렌드에 주목하고 이들 패턴을 파악, 방어할 수 있는 보안시스템의 개발이 요구된다. 진화되고 있는 피셔들을 막아내기 위해서는 안티피싱 워킹그룹(APWG) 등 세계적인 차원의 피싱 보안 공조체 와의 협력을 통해 새로운 피싱 정보를 발빠르게 공유하는 것이 필요하다. 또 보안 솔루션을 기본으로 보안시스템을 프로세스화하고 매뉴얼화하여 체계적으로 접근하여 보안 프로세스를 지속적으로 진화시켜 나가야 할 것이다.

이에 본 연구에서는 웹 환경의 급변화함에 따른 개방된 정보교류 강화를 위해 웹서버와 클라이언트 간 네트워크 단에 프락시서버를 설치하여 유해사이트 분석 및 피싱URL을 화이트도메인리스트와 비교하여 필터링하고 안정된 웹 기반의 정보교류를 할 수 있도록 설계한다. 이같이 피싱차단시스템을 설계하기 위해서는 안전하고 원활히 웹 서비스될 수 있도록 최소한의 규제와 능동적인 제어를 통해 피싱차단 할 수 있는 설계 및 구조를 제시하고 이를 검증하고자 한다[1, 2].

2. 관련 연구

피싱(Phishing)은 개인정보(PrivateData)와 낚시(Fishing)의 합성어로 개인정보를 낚시하듯 낚아챈다는 말에서 유래되었다. 최근에는 DNS 하이재킹 기술을 이용하여 사용자를 위장 웹사이트로 유인한 후 개인 정보를 절도하는 피싱의 방법이 진화하고 있다. 하이재킹은 패킷이 목적지까지 전달되지 못하고 중간에 정보를 가로채어 다른 곳으로 이동시키는 행위를 뜻한다. 파밍은 DNS(Domain Name Server)하이재킹을 통해 DNS 정보를 변조하여 사용자들이 피싱 사이트로 접속하도록 유도하여 사기 사이트로 이동하는 형태로 발전하고 있다. 변화된 피싱 공격방식으로 스피어 피싱(SpearPhishing)을 들 수 있는데, 소규모 집단을 대상으로 공격을 시도 지적 재산이나 민감한 기업 정보를 유출하는 것을 의미한다. 이외에도 사회공학기법을 이용한 피싱 사기수법은 무수히 많다. 이러한 피싱과 사회공학적기법은 점차 다른 기술들과 융합하여 진화하고 있다[4, 5].

1.1 URL Address Spoofing

대부분 URL Address Spoofing 기법은 Microsoft의 Internet Explorer의 취약점을 이용 한 것이 가장 많다. 예를 들면 아래와 같은 IE의 %01, %00 처리를 못해서 발생하는 취약점으로 인해 Windows 상태창에서 클릭 시 피싱 사이트 URL이 보이지 않게 할 수 있는 공격이 가능하다[6].

1.2 URL Redirection

URL를 조작하는 피싱공격 방법중 URL Redirection를 활용하는 방법도 많이 사용된다. URL Redirection 기법중에서도 구글 검색엔진의 Redriection 기능을 이용하여 Long URL 형태로 공격하는 형태가 일반적이다[7].

1.3 Bad 도메인 Name

유사 URL를 이용하여 사용자가 혼동하도록 하는 방법. 정상적인 http://www.mybank.com/ 대신에 http://www.mybank.com.ch처럼 유사형태의 도메인을 악용하는 방법

1.4 Friendly Login URL's

일반적인 피싱기법으로 인증한 정보처럼 위장하여 URL를 조작하는 방법

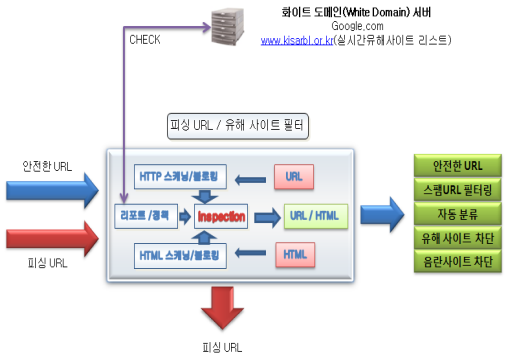
1.5 Hidden Frames

프레임(Frame)은 Hidding 공격에 가장 많이 사용되는 방법이다. 한 개의 프레임은 정상적인 URL 정보가 포함되어 있고. 다른 한개의 프레임은 숨겨진 Phishing 페이지를 참조하도록하고있다. 숨겨진 프레임내에는 Phishing 콘텐츠로 링크되어 있다. 이러한 공격(AJAX를 이용한 스크립 캡쳐, 키로깅)을 통해 세션 ID 또는 민감한 정보가 노출될 수 있다[3].

3. 피싱차단시스템 설계 및 구현

3.1 피싱필터링 설계

설계 하고자 하는 피싱차단시스템은 화이트도메인 서버를 통해 웹 URL차단 리스트정책을 운영하며, 클라이언트간의 네트워크 단에서 프락시 서버를 통해 피싱URL과 유해사이트를 스캐닝을 하여 분석 및 파싱 하게 되며, 이곳에서 피싱과 유해리스트로 판명되면 프럭시 서버에서 블러킹하여 세션을 끊게 된다. 프럭시 서버를 통해 피싱과 파밍, IFRAME 등의 악성 URL들을 검색하여 목록화하고, 필터링을 통해 각각의 URL에서 포착된 결과를 화이트도메인과 비교하여 필터링 한다. 이때 시작 페이지로부터 파생되는 모든 URL을 분석하며, 노출되지 않은 각종 숨겨진 URL을 포함하여 추출한다. 저장된 정보는 리스트는 화이트 도메인 서버에 보내지고 이는 다시 화이트도메인 리스트와 유해차단사이트 프럭시 서버와 비교하여 갱신하게된다. 프럭시 서버에서 파악된 악성 URL이 포함된 웹사이트는 보안 취약 요소를 분석하고 이를 보완함으로써 이미 알려진 공격들을 사전에 차단한다.



(그림 1) 피싱필터링 시스템 구성도

3.2 피싱차단시스템 설계

PSMS(Phishing Security Management System)은 안전한 웹서비스를 위해 기존방식인 서버기반이 아닌 네트워크 기반의 프락시 서버를 통해 능동적인 피싱차단을 제공된다. PSMS은 네트워크기반에 포괄적인 URL필터링, HTTP 분석 및 모니터링 되어 안전하게 보안관리 할 수 있다. 네트워크 기반 필터링은 개별 사용자나 그룹의 정보 전송에 대한 액세스를 통제함으로써 PSMS과 유기적인 연동으로 능동적인 피싱차단 관리가 이루어진다.

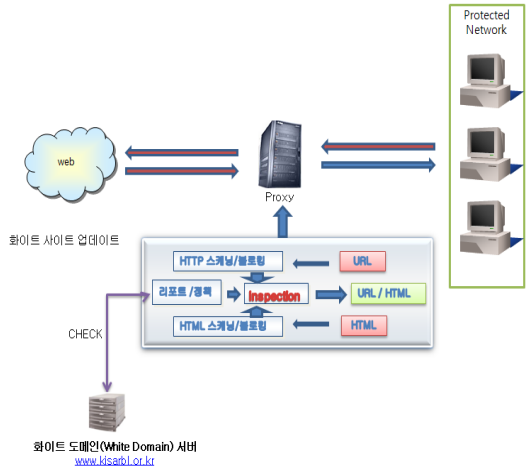
HTTP 분석 필터링을 통해 분석을 통한 메시지가 통보되며 실시간 모니터링과 PSMS과의 화이트웹사이트 정책서버와 유기적인 보안정책 공유로 안정하지 못한 URL 및 피싱사이트를 사전에 예방하여 안전한 정보교류관리 되며, 필터링과 모니터링을 통해 분석되어진다. 피싱공격 과 유해사이트가 확인되면 즉각적으로 그에 맞는 대응을 취함으로써 피해를 최소화 하며, 전체적인 URL 필터링을 통한 분석뿐만 아니라 HTTP까지 조사해 서버와 클라이언트 간 안정적인 정보교류를 할 수 있도록 한다.

PSMS는 능동형 보안 기능은 기존의 임계치나 패턴을 이용한 방법보다 발전된 네트워크의 분석

및 필터링을 통해 피싱사이트 발생 시 이를 즉각적으로 차단하는 방법이다. 실제 서비스 네트워크에서 효과적으로 동작하기 위해서는 공격 발생 시 얼마나 이를 빨리 감지하고 차단하느냐가 중요하며, (그림 2)은 능동형 보안 기능이 어떻게 피싱사이트을 차단하는지 볼 수 있다. 먼저 웹서버 앞단에 프락시서버를 설치하여 클라이언트에서 유입되는 피싱URL과 웹페이지들을 분석하고 링크URL을 검색하여 실시간 정보를 수집하고, 해당 정보를 분석 하여 실시간 화이트도메인 리스트와 비교하며 피싱URL과 유해사이트 차단뿐만 아니라 주기적인 최신 화이트도메인서버 정책을 받아 적용 할 수 있다.

이를 이용해 대응을 판단하는데 만약 피싱사이트 위험도가 높다고 판단되면 차단하게 된다. PSMS의 장점은 별도의 룰 설정 없이도 피싱사이트 발생 시 이를 신속하게 차단할 수 있다.

PSMS는 네트워크 설정 변경 없이 끊임없이 네트워크 환경을 자동으로 확인하고 화이트도메인 정책서버 와 유기적인 연동으로 다양한 피싱공격에 대해 신속히 차단가능하며, 웹서버의 최소한의 규제와 필터링을 통해 안정된 서비스를 제공할 수 있다.



(그림 2) 피싱차단시스템 구성도

3.3 피싱차단시스템 아키텍처 구현

피싱차단시스템 아키텍처 구성은 안정된 정보교류를 위해 웹서버 앞단에 프럭시서버를 설치하여 클라이언트간의 안정된 공유와 개방을 위한 피싱URL과 웹페이지들을 분석하고 링크URL을 검색하여 화이트도메인 리스트와 비교하여 피싱URL과 유해사이트 필터링을 통해 능동적으로 제어 할 수있도록 아키텍처를 구성한다.

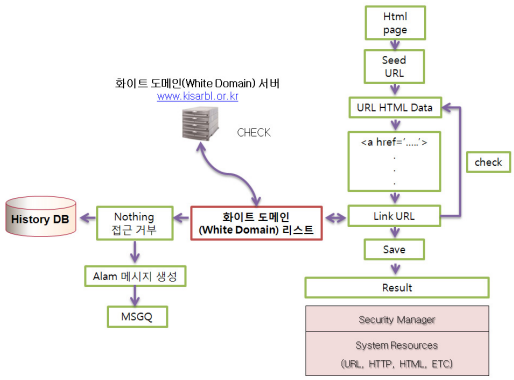
먼저 화이트도메인 서버 리포트의 업데이트에 따라 본 논문의 피싱차단시스템의 성능이 좌우 된다고 해도 과언은 아닐것이다. 화이트도메인 서버 리포트 업데이트 설계는 현재 운영중인 웹사이트를 화이트도메인 서버에 등록 한다. 국내에 대표적인 사이트(http://www.kisarbl.or.kr)의 DNS ZONE 리스트 파일(kisabl.or.kr IN TXT “v = spf1 ip4:61.251.112.142-all”을 받아 피싱차단리스트에 update하고 이 리스트를 다음과 같이 웹 페이지 파싱을 통해 필터링을 거치게 된다.

피싱URL과 웹페이지들을 분석하고 링크URL을 검색하여 화이트도메인 리스트와 비교하여 피싱URL과 유해사이트 파싱 필터링은 다음과 같은 단계를 거쳐 구현 한다.

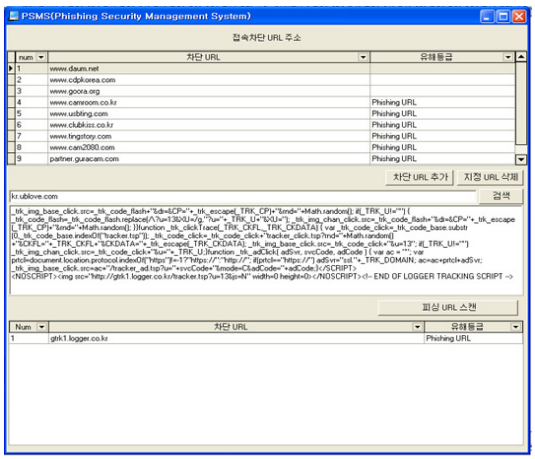
구현은 델파이 7.0을 통해 구현 하게 되며, 설계 절차는 다음과 같다. 화이트도메인 서버에서 지정한 피싱url 데이터를 입력하게 되면 관련 url을 조회하게 되며, 화이트도메인 리스트는 언제든 조회, 삭제, 입력, 수정이 가능하게 설계된다. 화이트도메인 리스트를 통해 입력받은 html리스트를 파싱을 거쳐 숨겨 져있는 url를 검색하여 피싱url은 스캔을 통해 차단 url에 입력되어 있는 데이터를 조회 차단 결과 리스트를 통해 보여주게 된다.

(그림 3)은 연동되는 흐름을 보여주는데. 먼저 실행 인자로 시작 지점이 될 seed URL 리스트를 받아 실행 인자들을 이용해 URL리스트 필터링을 하고 HTTP GET 명령을 통해 해당 URL의 HTML 데이터를 파싱해서 <a href = ‘…’>에 있는 link URL

들을 추출 후 화이트도메인 리스트와 비교하여 저장 또는 차단되며 이 과정을 반복하게 된다. 다음과 같은 아키텍처를 기본으로 UI를 구현 (그림 4)와 같이 구현되며, 피싱URL 차단시스템이 운영 관리 되어 지게 된다.



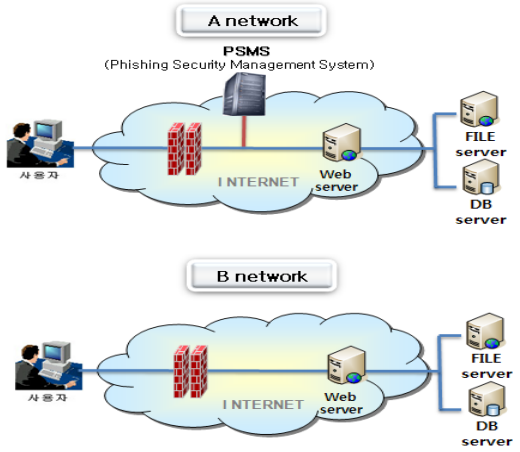
(그림 3) 피싱차단시스템 아키텍쳐 프레임워크



(그림 4) 피싱차단시스템(PSMS) UI

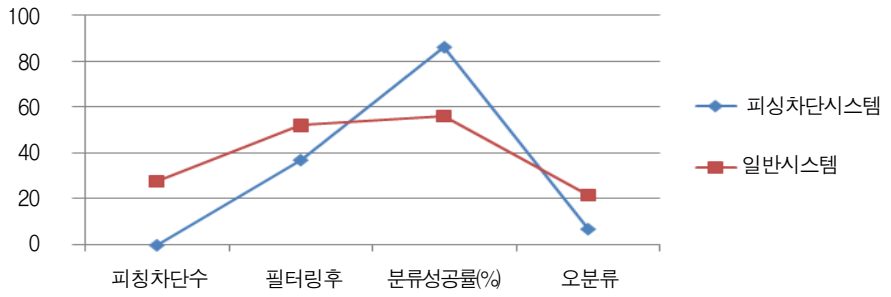
4. 분석 및 성능 평가

본 장에서는 구현한 피싱차단시스템PSMS(Phishing Security Management System)을 적용 시스템에 대한 성능분석을 한다. 실험 환경은 피싱차단시스템 테스트를 위해 같은 네트워크 기반에 피싱차단시스템을 장착한 미들급 서버 1대(CPU 3G, HDD 160G, RAM 1G)를 구동을 하였다. A 네트워크에서는 피싱차단시스템(PSMS)을 적용하였고, B 네트워크에서는 기본적인 네트워크 구조에 방어벽만을 추가하여 구성하였다. 이와 같이 구성된 이유는 네트워크 기반에서 화이트사이트URL과 피싱URL을 무작위로 다량의 트래픽을 적용 하였을 경우 파싱된URL과 탐색시간을 측정하고자 한다.



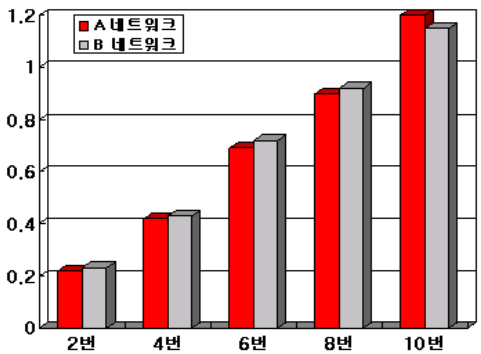
(그림 5) PSMS과 일반시스템 비교

피싱차단시스템 성능 평가를 위해 총 80개 URL 중 30개의 일반URL과 50개의 피싱, 유해 사이트를 가지고 순서구분 없이 무작위로 피싱URL들과 일반사이트들을 석었다. 피싱URL탐색 시간 측정을 위해 똑같은 방식으로 10번의 A와 B네트워크에 똑같은 방법으로 반복테스트를 시행하여 짝수번 시행결과 시간을 측정하였다. 화이트사이트정책서버에서 추출한 1248개의 URL정보를 가지고 출현한 URL들의 리스트를 사전을 구축했다. 본 논문에서 제안한 피싱차단시스템은 피싱차단수 43개 URL과 분류일 된거에 비해 피싱차단 시스템을



(그림 6) 피싱URL 필터링 성능 비교

	2번	4번	6번	8번	10번
A 네트워크	0,22 초	0,42 초	0,69 초	0,90 초	1,2 초
B 네트워크	0,23 초	0,43 초	0,72 초	0,92 초	1,15 초



(그림 7) 피싱URL 탐색시간 비교

가동하였을 경우 43개의 피싱URL과 정상적인 URL 37개로 필터링 되었으며, 7개의 피싱 URL이 오분류 되어 일반 시스템과 비교하여 월등한 성능을 보였다. 피싱URL 필터링 결과는 <표 1>과 (그림 6) 같은 성능 분석 결과가 나왔다. 위 실험 결과, 피싱시스템이 없음에도 방어벽을 통한 일반 시스템의 경우 피싱차단수가 28개가 필터링 된것을 볼 수있었다. 성공률은 56%라는 저조한 성능을 보였으며, 논문에서 제시한 파싱차단 시스템은 43개를 필터링하여 분류성공률에 대해서 86% 높은 성공률을 보였다.

실험에서 나타난 오분류된 URL의 대부분은 HTML형식의 URL이며, 이러한 URL을 분류하기에는 소스를 파싱 과정에서 발생하였다. (그림 6)은 피싱URL 필터링한 결과를 일반 시스템과의 비교 결과는 확연한 성능의 차이를 보였다.

〈표 1〉 피싱URL 필터링 결과

	피싱차단 시스템	일반 시스템
피싱차단수	43	28
필터링후	37	52
분류성공	86%(43/50)	56%(28/50)
오 분 류	7	22

다음은 피싱URL탐색 시간 측정을 위해 똑같은 방식으로 10번의 A와 B네트워크에 똑같은 방법으

로 반복테스트를 시행하여 짝수번 시행결과 시간을 측정한결과이다. A네트워크와 B네트워크의 탐색시간의 큰 차이는 없었다. 근소한 차이를 보이고 있지만 2번~8번까지는 A네트워크의 짧은 측정시간이 나왔으며, 10번째에서는 B네트워크의 시간이 더 짧은 것을 볼 수 있다. 전체적으로 피싱 URL 탐색시간 A네트워크가 2%~4% 정도의 탐색 시간 단축을 얻을 수 있었다.

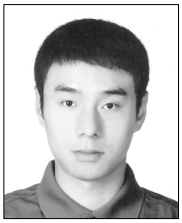
본 논문에서 제안한 방법인 피싱차단시스템의 성분 분석 결과 피싱필터링 성능면에서는 30%높게 나왔으며, 탐색시간측정에서는 평균 3%정도의 높게 나와 A네트워크가 피싱차단에 있어 성능이 좀더 효과적임을 알수있다. 하지만, 탐색시간은 더많은 연구를 통해 보강하여야 하며, 탐색 오류 부분은 차후 오차범위를 최대한 낮추어야 할 것으로 판단된다.

5. 결 론

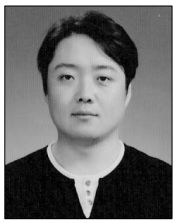
본 논문에서는 피싱을 정의하고, 대응 기술을 정리 보완하여 보다 안전한 웹 서비스를 할 수 있는 대응 방안을 제시하였다. 신뢰된 목록을 통해 기존의 속임수에 대한 방어 기술을 보완하였고 이를 토대로 사용자에게 안정적인 피싱 대응 방안을 마련한 것에 그 의의가 있다. 이에 대해 본 연구는 안전한 웹 기반에서 정보교류를 할 수 있도록 PSMS (Phishing Security Management System) 메커니즘을 네트워크 기반으로 제안함으로써 피싱사이트와 불법유해 사이트 접근 차단을 통해 불필요한 트래픽의 감소, 외부 또는 내부 사용자에 의한 악의적 공격 확산 방지, 웹 취약점 보완 및 유해사이트 와 피싱 차단이 가능함으로 보여주었다. 이러한 결과는 제안된 피싱차단시스템은 네트워크 기반으로 네트워크를 지나는 HTTP/URL을 분석하므로 웹 서버의 종류와 관계없이 보호가 가능하여 별도의 네트워크 상황 변경 없이 웹 서버와 클라이언트 간 효율성과 신뢰성, 가용성을 보장하고 이용 가능성을 향상시킬 수 있음을 보여주고 있다. 향후 본격적으로 본 논문에서 기술된 내용을 보강하여 보다 안전한 웹 환경에 대비한 다양한 기술 및 네트워크 장비에 대한 연동성을 세밀하게 검토하여 발전시키고자 한다.

참 고 문 헌

[1] Anti-PhishingWorkGroup. http://www.antiphishing.org, 2006.
[2] “Gartner Survey Shows Frequent Data Security Lapses and Increased Cyber Attacks Damage Consumer Trust in Online, 2006.
[3] “FightingSpam, PhishingandEmailFraud”, http://www.cs.ucr.edu/~schhabra/thesis.pdf, 2005.
[4] Phishing 對應方式에 관한 硏究 , 성균관정보대학원, 車炯賑, 2006.
[5] 이동휘, 최경호, 이동춘, 김귀남, 박상민, “사회공학기법을 이용한 피싱 공격 분석 및 대응기술”, 정보・보안논문지 제6권 제4호, 2006.
[6] 민동욱, “URL 스푸핑을 이용한 피싱 공격의 방어에 관한 연구,” 고려대 정보보호대학원 2006.
[7] 차형진, “Phishing 대응 방식에 관한 연구”, 성균관대 정보통신대학원 2006.



유 재 형
2006년 인천대학교 컴퓨터 공학과 (공학사)
2007년 현재 경기대학교 정보보호학과 석사과정



이 동 휘

2001년 경기대학교 전자계산학과 (이학사)
2003년 경기대학교 정보보호기술 공학과 (공학석사)
2006년 경기대학교 정보보호학과 (이학박사)
현재 경기대학교 정보보호학과 Post-Doc

양 재 수

1981년 한국항공대학교 통신공학과 (공학사)
1985년 건국대학교 전자공학과 (공학석사)
1993년 미국 NJIT 전기및컴퓨터공학 (공학박사)
1982년~2006년 KT중앙지사장
현재 경기도 정보화보좌관

박 상 민

1970년 한양대학교 (공학사)
1983년 한양대학교 (공학석사)
1990년 한양대학교 (공학박사)
2002년~현재 동북아전자물류연구센터 소장
현재 인천대학교 산업경영학과 교수

김 귀 남

미국 캔자스대학 (학사)
미국 콜로라도주립대학 (석사)
미국 콜로라도주립대학 (박사)
현재 경기대학교 정보보호학과 교수