http://dx.doi.org/10.5392/JKCA.2012.12.05.032

개인정보 입력 감지를 이용한 사회공학적 공격 대응방안

Countermeasure against Social Technologic Attack using Privacy Input-Detection

박기홍*, 이준환**, 조한진**
포스코 경영연구소 GIH기획실*, 극동대학교 스마트모바일학과**

Ki-Hong Park(foodwest@hanmail.net)*, Jun-Hwan Lee(hijuneh@hotmail.com)**,
Han-Jin Cho(hanjincho@hotmail.com)**

요약

온라인을 통해 서비스를 제공받기 위해서는 회원가입이 필요하고, 이렇게 회원가입을 통해 수집된 개인정보는 해킹으로 인한 개인정보의 유출로 이어진다. 특히, 유출된 개인정보에 의해 사용자가 지속적으로 공격 받고 피해를 입어 심각한 사회문제가 되고 있다. 이러한 사회공학적 공격 방법은 사람의 심리를 기반으로 하기 때문에, 대부분의 경우 피해를 입기 쉽다. 이러한 공격을 막기 위해 블랙리스트를 이용하여 피싱 사이트를 차단하는 방법이 있다. 하지만 이러한 방법은 짧은 생명 주기로, 새로 생성되는 피싱 사이트에 대해서는 대처 할 수가 없다는 문제를 가지고 있다. 본 논문에서는 사용자의 개인정보 유출 사고를 최소화 하는 두 가지 방안을 제시하였다. 블랙리스트와 화이트리스트 비교를 통해 사이트 신뢰를 표시하여 사용자에게 사이트의 진위여부를 판단할 수 있도록 하고, 새로 생성된 사이트에 대해서는 개인정보 입력 감지를 통하여 개인정보 유출을 사전에 차단을 하여, 사용자의 개인정보 유출 사고를 최소화 하는 방안을 제시하였다.

■ 중심어 : | 개인정보 | 입력감지 | 사회공학적 공격 | 피싱 |

Abstract

When you want to be given the on-line service, their homepage requires sign-up with detail personal information. This collected private information lead to mass data spill by hacking. Especially, this makes terrible social problems that the users who sign up their site are persistingly attacked and damaged by hackers using this information. As methods of the social technologic attacks are simple but based upon human psychology, it is easy that people become a victim in the majority of cases. There is a strategy blocking fishing sites by using the black list for defending these attacks. This tactic, however, has some problems that it isn't possible to handle new fishing sites having a short life-cycle. In this paper, we suggest two solutions to minimize data spill. One marks existing sites with the sign of a reliability measured by a comparison between black list and the white list; therefore, the user check the authenticity about the homepage. The other shut off previously the leaking of private information by sensing a entry of personal information into new sites.

■ keyword : | Privacy | Input-Detection | social technologic Attack | Phishing |

접수번호 : #120312-003
접수일자 : 2012년 03월 12일
심사완료일 : 2012년 03월 23일
교신저자 : 조한진, e-mail : hanjincho@hotmail.com

I. 서 론

누구나 인터넷을 사용할 정도로 보편화가 되어 쉽게 인터넷을 접할 수 있게 되었다. 기존에는 인터넷을 사용하려면 공간적 제약이 있어 이용의 불편함이 있었지만, 기기의 발전과 통신 기술의 발전으로 공간적 제한이 사라지면서 언제 어디서든 필요시 인터넷에 바로 접속이 가능해졌다.

공공기관, 기업, 은행을 직접 찾아가지 않아도 인터넷을 통해 다양한 서비스를 이용할 수 있어, 사용자의 편의를 극대화 시키고 비용을 절감하는 등 인터넷은 우리 실 생활에 많은 변화 가져다주고 있다. 이처럼 인터넷은 사용자에게 많은 편의를 가져다주었지만 무분별하게 개인정보를 수집하면서 불법적인 개인정보 수집 및 유출 사고가 끊임없이 나타나고 있으며, 이를 이용한 악의적인 범죄가 갈수록 증가하고 있다.

사이버 범죄의 형태도 기존에는 공공기관이나 기업을 타깃으로 하였지만, 점차 개인을 타깃으로 하는 범죄가 증가하고 있다. 공공기관이나 기업을 공격하기 위해서는 많은 위험성이 필요 했지만 개인을 타깃으로 하는 공격은 이러한 위험성이 없고 사회공학적 공격을 이용하여 개인정보 및 금융정보를 쉽게 획득 할 수가 있어 사회공학적 공격을 통한 사용자의 피해 건수와 피해 금액은 갈수록 증가 하고 있다.

사회공학적 공격 방법인 피싱(Pishing)은 개인정보(Private Data)와 낚시(Fishing)의 합성어로, 불특정 다수에게 전화, 이메일, 메신저, SNS, 컴퓨터 시스템의 해킹을 통해 해커 의도대로 유도함으로써 각종 금전과 개인 정보를 취득하는 등 사회공학적 공격과 혼합하여 공격하는 금융사기 수법이다[1].

피싱의 지속되는 피해를 막기 위해 언론이나 매체를 통하여 예방 활동을 하고 있지만, 다양한 방법을 통해 공격이 이루어지고 방법 또한 교묘하기 때문에 피싱으로 피해를 보는 사용자가 지속적으로 발생하고 있다. 이러한 피싱 피해자를 줄이기 위해 많은 기업들이 안티 피싱 제품을 만들어 사용자에게 제공 하고 있지만, 대부분의 피싱 사이트가 짧은 시간동안만 노출 되었다가 없어지기 때문에 사이트를 차단한다고 해도 예방 효과가 짧고 새로 생성되는 피싱 사이트에 대해서는 신속하게 대처를 할 수 없다는 문제점을 가지고 있다. 이에 본 논문은 웹 환경에서 피싱 사이트로부터 안전하게 개인정보를 보호하기 위해 블랙리스트와 화이트리스트를 통하여 기존에 만들어진 피싱 사이트를 조기에 차단하고 블랙리스트에 검출 되지 않는 신규 피싱 사이트에 대해서는 개인정보 입력을 감지를 통하여 개인정보 유출 피해를 사전에 차단하고자 한다.

논문의 구성은 1장에서 논문의 배경 및 목적에 대해서 간략히 설명하고, 2장에서 사회공학적 공격의 유형과 방법에 대해서 살펴보고, 알려진 피싱 기법에 대하여 분석하였다. 3장은 개인정보 입력감지를 이용한 피싱 사이트 대응 방안을 제안하고 본 시스템의 구성과 설계에 대해 설명한다. 4장에서는 제안 기법에 대한 세부 구성 사항과 실험을 통한 검출 결과를 제시한다. 마지막으로 5장에서 본 연구의 결론과 향후 연구를 제시하였다.

II. 관련연구

1. 사회공학적 공격

사회공학적 공격 기법이란, 고도의 기술이 접목된 해킹기술과는 전혀 무관한 것으로, 기술적인 방법을 이용하는 것이 아니라, 인간의 심리적인 면을 이용하여 개인정보 또는 신용정보와 같은 중요한 정보를 획득하거나, 타인 스스로가 악의적인 결과를 발생하는 행위를 하도록 유도하는 것을 말한다[2].

사회공학적 공격은 사람의 심리를 공격해 어느 공격보다 예방과 차단하기가 어렵다. 노출이 된 개인정보를 이용하여 지인을 사칭하거나, 사고, 돈 환급 및 미납, 이벤트 당첨 등 여러 가지 방법을 이용하여 사용자를 속이고 공격자의 지시대로 따르도록 하여 피해를 주는 형태로 공격방법에 대한 지식이 없으면 속수무책으로 당하기 쉽다.

범죄가 갈수록 조직화 되고 교묘해져가고 있으며 기업이나 공공기관의 발신번호가 같도록 조작하거나 웹사이트의 주소 및 첫 화면을 비슷하게 위장하는 등 갈

수록 진화된 공격 방법으로 기존의 공격에 대한 지식을 가지고 있더라도 새로운 공격 방법을 통해 피해가 지속적으로 발생하고 있어 사회적으로 많은 문제가 발생되고 있다.

2. 사회공학적 공격 유형

2.1 전화를 이용한 방법

공신력이 있는 기관을 사칭하여 공격하면 대부분의 피해자는 그의 말을 쉽게 믿어 버리는 경우가 많기 때문에 금융기관 및 공공기관을 사칭하여 피해자의 예금을 보호나 돈 환급, 납치협박 등의 이유로 피해자를 ATM 기기 앞으로 유인하여 공격자의 대포통장으로 돈을 이체하게 하여 피해자의 예금을 편취 하는 방법이다[3].

2.2 이메일을 이용한 방법

공격자는 현재 이슈가 되고 있는 일들이나 이벤트를 가장하여 이메일을 무작위로 피해자에게 발송하고 피해자는 공격자의 이메일에 속아 개인정보를 적어 답장을 보내거나 공격자가 넣어둔 링크를 통해 공격자가 만들어 놓은 피싱 사이트로 이동하여 피해자의 개인정보를 편취 한다[4].

2.3 메신저 이용한 방법

피해자의 개인정보를 이용해 메신저에 접속을 하고 등록되어 있는 친구 목록을 이용하여 마치 피해자인 듯 신분을 사칭해 대화를 하고 경조사나 사고를 이유로 돈을 이체시키도록 하는 방법이다[5].

2.4 SNS을 이용한 방법

공격자가 SNS(Social Networking Service) 계정으로 로그인해 피싱 사이트로 연결하는 단축 URL을 올리면, 피드를 통해 링크가 자동으로 배포되고 수 분내에 수백 혹은 수천 명의 계정으로 피싱 링크가 전달되어 개인정보를 편취 한다[6].

2.5 사이트를 이용한 방법

금융기관 및 공공기관의 홈페이지를 가장한 피싱 사이트를 개설하고 전화를 이용하여 피해자의 예금 통장이 사기 사건에 연루 되었다는 등 여러 가지 방법을 이용하여 접근한 뒤 피해자를 피싱 사이트로 유인 하여 피해자가 개인 정보를 입력 하도록 유도 하는 방법이다[7].

2.6 카드론을 이용한 방법

카드론은 전화나 인터넷을 이용하여 사용자의 개인정보(카드번호, CVC, 비밀번호, 계좌번호, 공인인증서, 보안카드 등)을 이용하여 카드론을 신청하면 피해자의 계좌에 대출한 돈이 정상적으로 입금 되고 공격자는“돈을 잘못 입금 했다”는 등의 말로 피해자를 속이고 미리 만들어둔 대포통장으로 피해자의 돈을 이체하게 하여 피해자의 돈을 편취해 가는 방법이다[8].

3. 개인정보 공격 유형

3.1 피싱

피싱은 1996년 AOL 메신저를 사용하는 해커들이 일반 사용자에게 조작된 전자우편을 보내는 해킹기법에서 유래되었다[9]. 피싱은 불특정 사용자에게 공공기관 및 신분을 사칭하여 피해자에게 주민등록번호, 카드번호, 계좌번호, 비밀번호 등 개인정보를 입력하도록 하여 개인정보 및 금융정보를 획득하고 금전적으로 피해를 주는 방법이다[10].

대부분의 사용자가 접속한 페이지의 형태만 확인하고 이용한다는 것을 악용하는 것으로 사이트의 소스를 그대로 가져와 사이트를 생성하고 사용자를 속이는 방법이다.

변조된 사이트 주소는 정상 도메인 주소에서 몇 글자를 추가ㆍ삭제하는 등 부분적으로 변경하는 방법으로 사이트를 위조한다. 이렇게 위조된 도메인은 정상적인 도메인과 비슷하기 때문에 사용자가 유심히 보지 않는 이상 찾아내가 무척 어렵다.

3.2 파밍

파밍(Pharming)은 피싱 공격이 사용자에 의해 쉽게 탐지되는 것을 극복하기 위한 기법이다. 피싱은 사용자의 웹 사이트 사용 허점을 이용해 개인정보를 획득하는

반면 파밍은 피싱이 가지고 있는 사용 허점과 기술적인 공격을 더해 사용자의 개인 정보를 유출 시키는 기법이다[1].

파밍은 합법적으로 소유하고 있던 사용자의 도메인을 탈취하거나 도메인 네임 시스템 또는 프락시 서버의 주소를 변조하여 사용자들로 하여금 진짜 사이트로 오인하여 접속하도록 유인한 뒤 개인정보를 훔치는 방법으로 사용자가 주의 깊게 이용을 한다 해도 사용자 스스로 감지 해내는 것은 어렵다[11].

III. 개인정보 감지를 이용한 대응 방안

기존 기법은 URL주소를 비교하거나 IP주소를 비교하여 사용자가 비정상적인 사이트에 접속하였는지 확인하거나 HTML소스 및 데이터 송수신하는 사이에 검증 값을 추가하는 방식 등을 이용하여 피싱 사이트의 여부를 확인한다. 하지만 이러한 방법은 새로 생성되는 피싱 사이트나 사회공학적 공격 방법에 대해 신속히 대응할 수 없다는 문제점이 있다. 이에 본시스템은 기존에 URL주소 비교 나 HTML 소스를 통해서 피싱사이트에 대해 확을 작업을 거친뒤 신뢰하지 않은 사이트에 대해서는 키 로그를 통해 입력 값을 추출하고 추출한 값을 통해 개인정보 입력이 감지되면 이를 사용자에게 경고하여 사용자의 입력을 중지시키고 검색을 통해 신뢰 있는 사이트로 이동하여 사용자의 피해를 차단한다. 사이트 신뢰성을 구별하기 위해서는 소스검사를 통해 전송하는 과정에서 개인정보를 암호화를 하는지 암호화를 하지 않은 상태에서 개인정보를 전송(Plain text)하는 것을 확인을 하거나 화이티리스트 블랙리스트를 이용하여 등록되어 있는 피싱 사이트와 공공기관 및 금융기관 등 신뢰 있는 사이트에 대해 미리 등록하여 표시를 하는 방법으로 사이트를 구별하여 표시한다

이에 본 논문에서는 사용자가 신뢰 있는 사이트를 통해 개인정보를 입력할 수 있도록 실시간 입력을 감지하는 기법을 제안하고자 한다.

1. 시스템 순서도

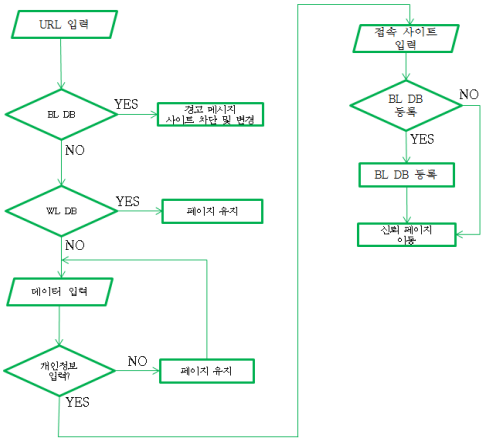

그림 1. 시스템 순서도

본 논문에서 제시하는 시스템 순서도는 다음과 같다. 웹 브라우저에 URL을 입력하면 웹페이지는 IP 주소를 추출하여 블랙리스트를 검색하고, 일치하면 경고 메시지를 사용자에게 알리고 금융감독원(서민금융 119서비스) 사이트로 이동하여 범죄 동향 정보를 사용자가 알 수 있도록 하여 추가적인 피해를 방지한다.

블랙리스트와 일치하는 값이 없으면 다음으로 화이트리스트와 비교하여 IP 주소가 일치하는지 확인하고 일치하면 사이트의 신뢰를 사용자에게 알려 사용자가 안심하고 사이트를 이용할 수 있도록 유도한다.

화이트리스트 · 블랙리스트에도 나오지 않은 사이트에 대해서는 사용자의 입력을 감시하고 입력 값이 패턴과 일치하면 경고 메시지를 사용자에게 알려 주고 검색을 통해 안전한 사이트로 이동을 한다.

2. 키 로그 패턴

2.1 주민등록 검증

주민등록 번호와 검증 숫자를 각각 곱하는데 곱한 값이 두 자리가 나온 수에 대해서는 각각의 자리를 서로 더해 한자리 수로 만들고 모두 곱한 값의 수를 모두 더하면 A라는 값이 나오는데 A를 11로 나누면 나머지 값 C가 나오고 마지막으로 11에서 C를 빼면 최종 D값이 나온다. 최종 D값과 주민등록 마지막 값과 비교해서 일

치하면 올바른 주민등록 번호이다.

2.2 카드번호 검증

카드번호는 홀수 번째는 2를 곱하고 짝수 번째는 1을 곱한다. 만약 숫자가 두 자리가 되면 각각 자리의 수를 서로 더해 한자리의 수로 만들고 곱해서 나온 값을 모두 더해주면 A라는 값이 나오는데 A를 10으로 나눈 나머지 값이 0이 나온다면 올바른 카드번호이다.

2.3 계좌번호 검증

계좌번호는 10자리에서 부터 14자리까지 다양하게 구성되어 있다. 각 금융기관 마다 계좌번호 자리수가 다르고 검증 방법 또한 다르기 때문에 일정한 패턴이 없어 DB에 계좌번호를 등록을 하고 비교하는 방식을 이용하여 검증한다. 계좌번호 10자리 이상을 입력하면 10자리를 DB와 비교하여 값이 일치하면 경고 창을 통해 사용자에게 알려 준다.

3. 코드

[그림 2]는 사이트 신뢰등급을 표시하는 코드이다.

```
Query = "Select * From DBList where BM_IP like '%"
        + IpAddress + "%'"
        FieldName[0] = "BM_NAME"
        FieldName[1] = "BM_URL"
        FieldName[2] = "BM_IP"
        FieldName[3] = "BM_ACCESS"
        BlacklistDB.SearchDB(Query, FieldCount, FieldName);
        FieldData = BlacklistDB.FieldData;
        RecordCount = BlacklistDB.RecordCount;
        BlacklistDB.SearchDB(Query, FieldCount, FieldName);
        FieldData = BlacklistDB.FieldData;
        RecordCount = BlacklistDB.RecordCount;
        for (int i = 0; i < RecordCount; i++)
        {
            J_Name = string.Format("{0}", FieldData[i, 0]);
            J_URL = string.Format("{0}", FieldData[i, 1]);
            J_IP = string.Format("{0}", FieldData[i, 2]);
            for (int i = 0; i < RecordCount; i++)
Query = "Select * From DBList where BM_IP like '%"
        + IpAddress + "%'"
```

```
FieldName[0] = "BM_NAME"
FieldName[1] = "BM_URL"
FieldName[2] = "BM_IP"
FieldName[3] = "BM_ACCESS"
BlacklistDB.SearchDB(Query, FieldCount, FieldName);
FieldData = BlacklistDB.FieldData;
RecordCount = BlacklistDB.RecordCount;
BlacklistDB.SearchDB(Query, FieldCount, FieldName);
FieldData = BlacklistDB.FieldData;
RecordCount = BlacklistDB.RecordCount;
for (int i = 0; i < RecordCount; i++)
{
    J_Name = string.Format("{0}", FieldData[i, 0]);
    J_URL = string.Format("{0}", FieldData[i, 1]);
    J_IP = string.Format("{0}", FieldData[i, 2]);

for (int i = 0; i < RecordCount; i++)
{
    J_Name = string.Format("{0}", FieldData[i, 0]);
    J_URL = string.Format("{0}", FieldData[i, 1]);
    J_IP = string.Format("{0}", FieldData[i, 2]);
    J_ACCESS = string.Format("{0}", FieldData[i, 3]);
    InAccess = J_ACCESS;
}
if ((InAccess == "차단"))
{
    site.Text = "위험"
    site.BackColor = Color.Red;
    axWebBrowser1.Navigate("s119.fss.or.kr");
MessageBox.Show("안전한 사이트가 아닙니다.
차단되어 있습니다.");
}
                    중략..
if (InAccess == "허용")
{
    site.Text = "신뢰"
    site.BackColor = Color.Blue;
    InAccess = ""
}
                    중략..
```

그림 2. 사이트 신뢰등급 표시

다음 [그림 3]은 주민등록 검출을 위한 코드이다.

```
void Jumin(int Num, int Count)
    {
JuminHap = JuMinSum[0] + JuMinSum[1] + JuMinSum[2] +
 JuMinSum[3] + JuMinSum[4] + JuMinSum[5] + JuMinSum[6]+
  JuMinSum[7] + JuMinSum[8] + JuMinSum[9] + JuMinSum[10] +
 JuMinSum[11];
        JuminResult = 11 - (JuminHap % 11);
        if (JuminResult == 10)
        {
            JuminResult = 0;
        }
if ((((Juminar[6] == 3) | (Juminar[6] == 4)) | ((Juminar[6] == 1) |
  (Juminar[6] == 2))) & (((Juminar[2]== 0) | (Juminar[2] == 1)) &
  ((Juminar[4] == 0) | (Juminar[4] == 1))))
        {
        if (Juminar[12] == JuminResult)
         {
         MessageBox.Show("주민번호입력");
                        중략..
```

그림 3. 주민등록번호 검출

Ⅳ. 대응 시스템 구현 및 결과

1. 제안 기법

피싱 사이트는 도메인 주소를 속이거나 사이트를 똑같이 만들어 속이는 방법으로 공격한다. 블랙리스트를 이용한 사이트 차단은 도메인 주소 변경을 통해 공격이 가능하고 공격이 가능하기 때문에 블랙리스트로는 한계가 있고 사이트를 변경하는 방법으로 이러한 공격을 막기 위해서는 기존 방법에서 좀 더 다른 방법이 필요하다.

개인정보는 사용자가 변경하거나 폐기하기 전까지 하나의 고유 값을 가지고 있다. 이러한 개인정보의 고유 값을 이용하여 입력을 감지하고 피싱 사이트의 여부를 판단하는 방법으로 피싱 사이트를 차단할 수 있다.

2. 제안 기법 시나리오

웹 브라우저는 사이트에 대한 신뢰등급을 표시하는데 위험, 신뢰, 보통으로 구분하여 나타내 준다. 위험은 사용자가 블랙리스트에 추가하거나 기존에 등록된 피싱 사이트로서 접근을 시도하면 빨간색으로 표시해 나타내준다.

신뢰는 화이트리스트에 등록되어 있는 금융기관이나 공공기관 등 신뢰 있는 사이트에 접근을 하면 파란색을 표시한다. 보통은 화이트리스트 · 블랙리스트에 등록되지 않은 사이트로서 [그림 4]처럼 노란색을 표시해 나타내 준다.

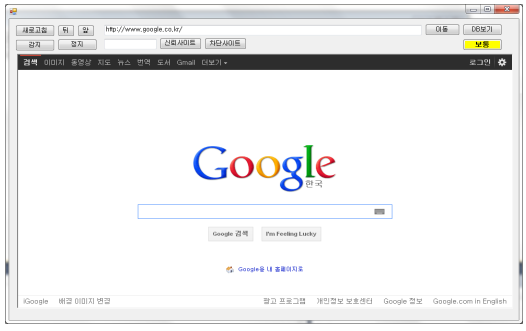

그림 4. 브라우저 상태

[그림 5]처럼 블랙리스트를 통해 피싱 사이트를 차단하고 금융감독원(서민금융 119서비스)로 이동을 하여 사기나 피싱의 피해 사례를 참고하여 또 다른 사기나 피싱에 대해 대비를 할 수 있도록 한다.

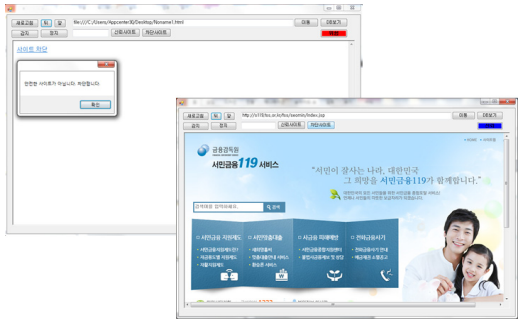

그림 5. 브라우저 차단

신뢰등급이 신뢰인 사이트에서는 키 로그가 작동을 안 하지만 신뢰등급이 보통이면 [그림 6]처럼 키 로그를 이용해 입력을 감지하고 입력된 키를 가지고 개인정보 패턴을 검출한다. 키 로그는 숫자만을 입력 받고 그 외에 입력에 대해서는 입력을 받지 않는다.

키 로그 감지에서 주민등록번호는 회원가입이나 비밀번호를 찾을 때 사용하기 때문에 신뢰등급이 보통인 사이트에도 주민등록번호 사용이 가능해야 한다. 그래서 브라우저의 소스 검사를 통해서 불필요한 개인정보 요구사항이 없으면 키 로그를 작동 하지 않는다.

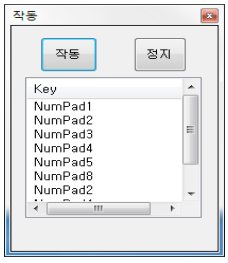

그림 6. 키 로그

2011년 09월 01일 개인정보보호법을 제정으로 회원가입할 때 주민등록번호 대처 수단과 개인정보 수집 동의가 사용자의 선택으로 변경되면서 개인정보의 오남용이 줄어들겠지만 아직 법이 확립이 안 되어 있어 동의하지 않으면 회원가입이 안되거나 서비스 이용의 제한이 있는 등 아직 많은 문제점이 남아 있다. 피싱 사이트는 개인정보 입력을 중점으로 하기 있기 때문에 이를 역 이용 하여 [그림 7]처럼 개인정보 입력 시 이를 감지하여 피싱 사이트를 차단한다.

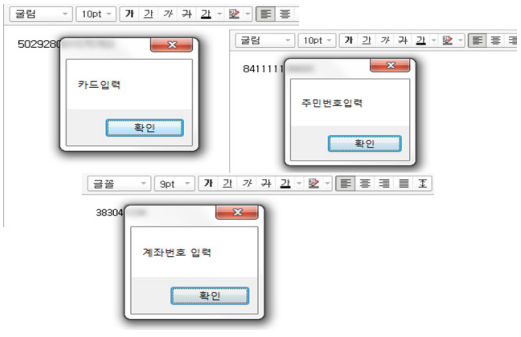

그림 7. 개인정보 감지

HTML 소스 분석을 통해 전송을 암호화 하는지 판단하여 사용자에게 알리고 또 등록한 조건의 값과 일치하면 [그림 8]처럼 각각의 감지 경고 창을 통해 사용자에게 알리며 이러한 소스 분석을 통해 개인정보 입력만으로 부족했던 부분을 채울 수 있다

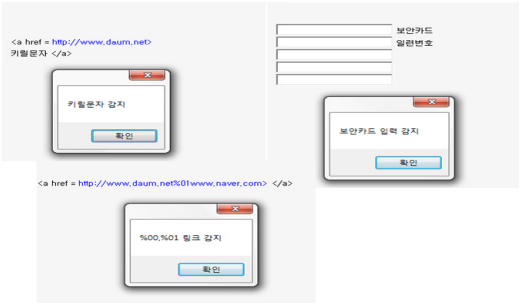

그림 8. HTML 소스 감지

V. 결론

인터넷을 통해 다양한 활동이 가능해 지면서 인터넷 이용자는 급격히 늘어났지만, 무분별한 개인정보 수집과 기업의 개인 정보 유출로 인해 누구든 범죄의 표적이 될 수 있다.

이처럼 갈수록 교묘해지는 사회공학적 공격으로 피해가 갈수록 커져 가고 있으며 이러한 피해를 통해 한 가정이 파탄이 나는 등 사회적으로 많은 문제가 되고 있다.

범죄가 점점 조직화 되고 공격 기법이 다양해지기 때문에 이를 조기에 발견하여 차단을 하더라도 도메인 주소 변경을 통해 지속적으로 공격하기 때문에 블랙리스트만 이용하여 차단하는 방법은 한계가 있다.

본 논문은 기존에 가지고 있는 피싱 탐지방법의 한계를 극복하기 위해 키 로그를 통하여 사용자의 입력 값을 감지하여 개인정보 입력시 사이트를 차단하고 사용자에게 간단한 검색을 통해 신뢰 있는 사이트로 안전하게 이동하여 사용할 수 있는 방법을 제시하였다.

본 논문이 제시한 방법을 이용하면 지속적으로 입력을 감지하기 때문에 개인정보의 유출을 미연에 방지 할 수 있고, 화이트리스트 데이터베이스 검색을 통해 신뢰된 사이트로 이동하여 개인정보를 안전하게 입력할 수 있는 효과를 가져 올 수 있다.

향후 연구로는 갈수록 정교해지고 있어 피싱 사이트가 금융기관이나 공공기관의 소스를 그대로 가져 오는

경우가 많기 때문에 일정한 패턴을 통해 서로 비교를 하여 피싱 사이트로 판별 되면 사전에 이를 차단할 수 있도록 연구할 예정이다.

참 고 문 헌

[1] 노영근, *웹 서버 IP 주소 검증을 통한 피싱 공격 대응방안,* 숭실대학교, 석사학위논문, 2009.

[2] 최양서, 서동일 “사회공학적 공격방법을 통한 개인정보 유출 기술 및 대응방안 분석,” 한국정보보호학회, Vol.16, No.1.

[3] 허영욱, *국제 전화금융사기 범죄에 관한 연구,* 창원대학원, 석사학위논문, 2008.

[4] 보안뉴스, http://goo.gl/5z62U

[5] 금융감독원, “서민의 지갑을 터는 금융사기, 이렇게 예방하세요!”, http://goo.gl/40kOr

[6] 시만텍코리아, “시만텍 인터넷 보안 위협 보고서(ISTR) 제16호, 2011.

[7] 금융감독원, http://goo.gl/Ao4mw

[8] 금융감독원, http://goo.gl/C3wxJ

[9] 김주현, 맹영재, 양대헌, 이경희, “피싱 및 파밍 방지를 위한 인지 기반의 접근 방법,” 학국정보보호학회논문지, Vol.19, No.1, 2009.

[10] 하정애, *Whois와 DNS 레코드를 이용한 RealURL 안티피싱 기법,* 고려대학교, 석사학위논문, 2008

[11] 최인수, *신종 인터넷 사기범죄에 관한 연구,* 한양대학교, 학위석사논문, 2008.

[12] 인터넷침해대응 센터, “2005년 10월 인터넷 침해사고 동향 및 분석 월보”, 한국정보보호진흥원.

[13] 민동욱, *URL 스푸핑을 이용한 피싱 공격의 방어에 관한 연구,* 고려대학교, 석사학위논문, 2006.

[14] 김혜리, *웹 환경 내 개인정보 공격에 대한 대응방안 연구: 개인정보 위협 사례 연구 중심으로,* 성신여자대학교, 석사학위논문, 2009.

저 자 소 개

박 기 홍(Ki-Hong Park) 정회원

- 2003년 : 극동대학교 정보통신학부(멀티미디어학사)
- 2012년 : 극동대학교 정보통신공학과(공학석사)
- 2012년 ~ 현재 : 포스코 경영연구소 정보서비스실

<관심분야> : 정보보호, 네트워크 보안

이 준 환(Jun-Hwan Lee) 정회원

- 1999년 : 단국대학교 전자공학과(공학석사)
- 2001년 : 단국대학교 전자공학과(공학박사)
- 2001년 ~ 현재 : 극동대학교 스마트모바일학과 교수

<관심분야> : 스마트 앱 콘텐츠, 머신비전, 생체인식

조 한 진(Han-Jin Cho) 종신회원

- 1999년 : 한남대학교 컴퓨터공학과(공학석사)
- 2002년 : 한남대학교 컴퓨터공학과(공학박사)
- 2002년 ~ 현재 : 극동대학교 스마트모바일학과 교수

<관심분야> : 정보보호 응용, 모바일 융합 보안