Regular paper | Journal of the KIECS. pp. 1059-1064, vol. 13, no. 5, Oct. 31 2018, t. 91, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2018.13.5.1059

전자 메일첨부 편집파일의 안전한 저장과 관리를 위한 분실 방지 시스템 WatchDog 개발

홍준후* · 최철재**

Development of Loss Prevention System WatchDog for Safe Saving and Management of Edited E-mail Attachment

Jun-Hu Hong* · Chul-Jae Choi**

요 약

많은 사용자가 편집한 파일을 분실하여 큰 고통을 받고 있다. 매우 심각한 시간과 비용의 손실이다. 이런 문제는 전자 메일첨부 파일을 '받은메일함'에서 편집하고 곧바로 '저장하기'로 컴퓨터를 종료하기 때문에 발생한다. 임시 폴더에 '저장하기' 한 것을 안전한 하드디스크에 저장했다고 착각하기 때문에 발생한다. 본 논문은 전자 메일첨부 파일의 안전한 저장과 폴더 관리를 위한 분실 방지 시스템 WatchDog을 제안한다. 제안한 시스템은 첨부 파일의 '열기(O)'와 '저장하기'할 때 경고창 팝업을 동작한다. 또한, 안전한 복사 및 이동을 위한 편리한 폴더 관리방안을 프로그램 예시를 통해 실증적으로 보인다.

ABSTRACT

Many users feel a great pain owing to losing edited files. It is very serious loss in time and money. This problem occurs because email attachments are edited in 'Inbox' and the compute immediately shuts down with 'Save'. This is caused by the illusion that the 'save' in a temporary folder is saved to a secure hard disk. Our thesis proposes a loss-prevention system WatchDog for safe storage and folder management of the e-mail attachments. The proposed system operates a warning window pop-up when we 'Open(O)' and 'Save' the attachment. In addition, convenient folder management plans for safe copying and movement are shown through example programs.

키워드

E-mail, Attachment File, Temporary Folder, Folder Management, Loss Prevention System
전자 메일, 첨부 파일, 임시 폴더, 폴더 관리, 분실 방지 시스템

Ⅰ. 서 론

전자 메일로 수신한 첨부 파일을 열고 발신자의 요구에 신속하게 답신할 목적으로 서둘러서 편집 작업을 하는 경우, 무심코 '저장하기' 클릭만으로 작업을 마치고 전원을 끄면 낭패를 당한다. 방금 전에 편집한 파일이 시스템이 임의로 지정한 임시 폴더에 저장되기 때문이다. 다행히 컴퓨터 전원을 끄지 않은 상태라면 '불러오기'의 '최근문서' 메뉴에서 찾을 수 도 있겠지만, 전원을 껐다면 찾지 못하고 포기한 채 다시 작

* 경동대학교 정보보안학과(bsitc.thomas@gmail.com)
** 교신저자 : 경동대학교 정보보안학과
· 접 수 일 : 2018. 06. 20
· 수정완료일 : 2018. 08. 17
· 게재확정일 : 2018. 10. 15
· Received : Jun. 20, 2018, Revised : Aug. 17, 2018, Accepted : Oct. 15, 2018
· Corresponding Author : Chul-Jae Choi
Dept. of Cyber Security for information, Kyungdong University.
Email : cj-choi@kduniv.ac.kr

업을 하는 방법 외에는 달리 대안이 없었다.

사용자가 전자 메일의 첨부 파일을 열고, 특정 폴더 를 설정하고 '다른 이름으로 저장하기(A)'를 하지 않는 경우, 시스템이 임의로 생성한 임시 폴더에 자동 저장되기 때문에 발생하는 심각한 문제이다. 황급히 편집한 파일을 찾기 위해 임시 폴더를 추적해보지만 임시 폴더의 경로추적이 용이하지 않기 때문에 포기하는 경우가 대부분이다. 사용자들은 이런 참담한 현상을 보통 '파일을 날려버렸다'라고 표현한다.

막대한 시간과 비용의 손실이다. 몇 시간 또는 심지어 하루 종일 작성한 논문, 연구보고서, 중요업무파일 등을 한순간에 잃어버리는 일들이 오피스업무환경에서 자주 발생하고 있다. 그런데도 지금까지 문제해결을 위한 적극적인 연구가 없었다. 너무나 오랫동안 방치상태에 있었다. 최근 윈도우 버전의 MS오피스 파일은 다운로드하면 읽기전용으로 열린다. 별도 폴더에 '다른 이름으로 저장'하도록 개선되었으나 *.HWP 파일 등은 여전히 위험가운데 노출되어 있다.

본 논문은 전자 메일첨부 파일을 열고 편집한 후 저장하기를 클릭하여 발생하는 분실위험성을 원천적으로 방지하는 방법을 제안한다. 편집파일이 임시 폴더에 저장되는 것을 경고하고, 분실위험성이 있는 파일임을 알려주며 동시에 임시 폴더의 경로를 추적하는 도구인 분실 방지 시스템 WatchDog을 제안하고 실행결과를 예시로 보인다.

II. 일반적 해결방안

2.1 다운로드 파일저장

Melanie Pinola는 브라우저에서 파일을 다운로드 할 때, 시스템의 환경에 따른 '다운로드'폴더의 위치를 아래와 같이 보이고 있다[1].

·On Windows XP, it's under
\Documents and Settings\[username]\My Documents\Downloads
·Vista and Windows 7, the path is \Users\[username]\Downloads
·For Mac, the full path is /Users/[username]/Downloads
·On Linux it's home\[username]\Downloads

2.2 전자 메일첨부 파일

Melanie Pinola는 전자 메일에서 첨부 파일을 열고 저장하면 해당 파일이 사라진 것처럼 보이는 것은 임시 폴더에 저장되기 때문이며, Outlook이 유명하다고 지적하고 있다. Office 2010에서 전자 메일첨부 압축파일을 열면 AppData> Local> Microsoft> Windows> Temporary Internet Files> Content.Outlook> 9PDH6FAT와 같은 임의생성 폴더의 위치를 확인할 수 있다.

Nalts는 Mac에서도 Outlook을 통해 열었던 임시파일을 찾기 위해 보통 15-30 분이 소요되는 번거로운 일이 몇 달에 한 번씩 반복되고 있으며, 결국 임시 폴더를 찾지 못하는 분실파일의 위험성은 여전한 실정을 지적하고 이 문제를 해결하는 방안으로 그림 1과 같이 top-secret 911 솔루션[2]을 제시했다. 이것으로 Mac 시스템 환경에서 Outlook 전자 메일첨부 파일을 임시 폴더를 찾을 수 있다고 밝히고 있다.

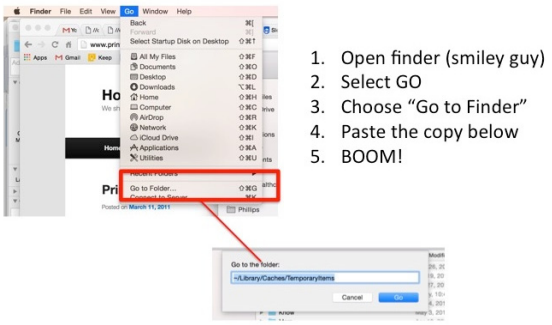

그림 1. Mac에서 분실 폴더 찾기
Fig. 1 Find for lost folder on the Mac

2.3 한컴오피스 첨부 파일

전자 메일이나 인터넷상에서 첨부된 한컴오피스 한글문서 파일을 바로 열면 화면 위쪽에 복잡한 경로가 표시된다. 아래 그림 2처럼 [C:\Documents and Setting\3302-20\Local Settings\Temporary Internet Files \ContentIE\JDVGLZ\]라는 자동지정경로 폴더에 저장된다.

1) https://lifehacker.com/5815144/how-to-find-a-file-you-just-saved-thats-now-missing
2) http://willvideoforfood.com/2016/05/31/how-to-find-the-missing-file-you-opened-via-outlook-on-a-mac/

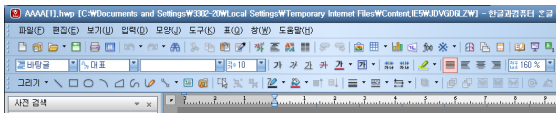

그림 2. 첨부 파일 열기의 자동경로지정
Fig. 2 Automatic path with opening attachment

그러나 복잡한 자동지정경로를 입력하더라도 그 폴더에 접근할 수가 없다. 다른 방법으로 열기에서 최근 문서 목록을 검색하지만 마찬가지다. 사용자 설정방법으로 '환경설정', '임시 폴더에 저장할 때 안내문 띄우기'를 체크하면 된다. 그러면 메일이나 인터넷에서 바로 '열기(O)'한 한글문서를 '다른 이름으로 저장(A)'이 아닌 '저장하기'를 클릭하면 아래 그림 3처럼 "임시 폴더에 저장하면 삭제될 수 있으므로 다른 위치에 저장하는 것이 좋습니다."라는 경고창이 팝업된다[3].

그림 3. 임시 폴더에 대한 경고 창
Fig. 3 Warning dialog of temporary folder

2.4 그 밖의 선행연구

전자 메일에 관한 그 밖의 선행연구들로는 송수신 파일의 흔적을 추적하는 메모리 덤프를 이용한 정보의 취득방법론[1]에 관한 연구와 웹메일 HTML파일의 임시 저장 삭제를 관찰하여 복구기술로 일부내용을 추측한 연구[2]가 있다. 전자 메일통제방안[3-4], 메일탐지[5], 체계적인 이메일 파일관리[6-7] 등이 있으나, 전자 메일에서 수신한 보안문서[8]나 첨부 파일의 분실위험성을 사전에 경고하여 원천적으로 안전한 전자 메일관리 방안의 제안에 관한 연구는 없는 실정이다.

III. 프로그램을 이용한 위험 최소화

3.1 WatchDog

본 논문에서 제안하는 WatchDog은 탐지견을 뜻하며 위험경로 감지 및 첨부 파일을 추적한다. C# 언어로 구현하였고, 다운로드 및 파일이동을 동시에 감지하여 위험성이 있는 임의경로가 지정되면 알림 메시지 팝업창을 띄우도록 하였다.

WatchDog은 첨부 파일, 인터넷 다운로드파일, 파일복사 등 전반을 감지한다. 전자 메일 클라이언트에서 첨부 파일을 다운로드 한 뒤 열기를 클릭하고 문서를 수정 편집 할 경우 위험성이 있는 경로를 감지하도록 설계되어 있다. 만일, 문서 내의 저장버튼과 사용자의 키보드를 인식하면 동일하게 경고창을 팝업한다. 아울러 WatchDog내에서 위험성이 있는 파일경로가 확인 될 경우 프로그램 내에서 클릭 한번으로 파일이동이 가능하도록 설계하였다.

3.2 임시 폴더 진입감지

본 논문에서 제안하여 개발한 WatchDog 툴은 전자 메일 클라이언트에서 첨부 파일을 다운로드하여 '열기(O)를 하여 임시 폴더 경로가 지정되면 이를 감지하여 그림 4와 같은 경고 창을 팝업한다.

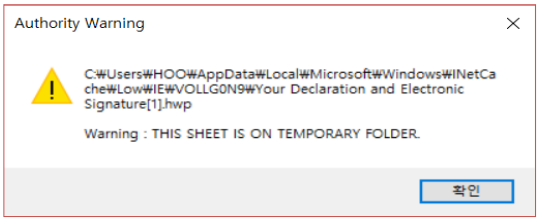

그림 4. 임시 폴더 경로 감지
Fig. 4 Authority warning for the temporary folder

첨부 파일을 열어서 문서 편집 작업을 마친 다음 서식창의 '저장하기' 버튼을 클릭하거나 메뉴방식 파일(F)에서 '저장하기(S)을 시도하면 임시 폴더에 저장되는 이상 경로를 감지함과 동시에 이때에도 사용자에게 그림 4와 같은 경고 메시지를 팝업한다. 또한 이상 경로 및 임시 저장 폴더로 저장을 시도할 경우에도 키보드와 문서 내의 저장 버튼을 감지하여 동일한 메시지가 출력한다. 단, USB를 이용하여 WatchDog을 실행하려면 '관리자 권한으로 실행(A)에서 구동해야하는 제한 조건은 있다.

프로그램을 시작하면 그림 5의 탐색기와 유사한 화면이 보인다. 여기서 ①시작을 클릭하면 녹색 타임라

3) http://myperfectfreedom.tistory.com/266

인 게이지가 증가하면서 프로그램이 동작한다. 웹에서 다운로드 할 때는 임시 폴더의 경로 로그가 ②Log데이터에 기록된다. 그리고 이상 경로에서 직접 파일이동도 가능하도록 설계하였다.

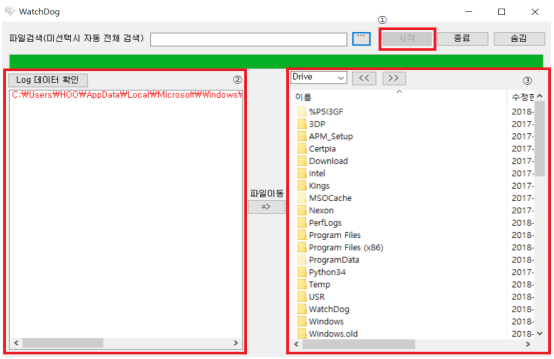

그림 5. 임시 저장 경로 감지 도구
Fig. 5 Temporary storage path sensing tool

3.3 탐지 경고창 프로그램

파일처리 방법[9-10] 가운데 첨부 파일을 클라이언트에서 다운로드 하는 경우 실행되는 파일 확장자를 식별하는 프로그램 코드는 그림 4와 같다.

```
foreach (FileSystemWatcher w2 in watchers2)
{
    if (w2 == null) continue;
    w2.Filter = "*.zip";
    w2.IncludeSubdirectories = true;
    w2.EnableRaisingEvents = true;
    w2.Changed += Fsw_Changed;
    Thread.Sleep(100);
    w2.Deleted += Fsw_Deleted;
    w2.Renamed += Fsw_Renamed;
  }
```

그림 6. 확장자 검색 조건
Fig. 6 Searching for file extension

foreach문을 이용하여 OS에 설치된 드라이브에 다운로드 된 파일을 FileSystemWatcher로 감지한다. 모든 파일의 확장자는 for문을 이용해 다운로드되는 순간 감지하며 필터링한다. 그림 7은 필터링 파일이 임시 폴더와 같은 임시 저장장치로 다운로드 되는 위험성이 있으면 이를 감지하는 코드이다.

```
Invoke(new MethodInvoker(delegate ()
{
        String Search = "tmp";
        String Search2 = "$";
        String Search3 = "Cookies";
        String Search4 = "Content.IE";
        String Search5 = "AppData";
```

그림 7. 임시 저장 경로의 확장자 감지
Fig. 7 Detect extensions of temporary storage path

임시 저장 폴더 및 이상 경로로 첨부 파일의 이동이 감지되면 이벤트가 발생하며 문서를 저장할 때와 같은 동일한 경고창이 활성화 된다. 이벤트 활성화 코드는 그림 8과 같다. 이로써 사용자는 자신이 어떠한 작업 상태인가를 알게 된다.

```
if (cnt == 0) {
    if (0==total_cnt) {
        this.CopyListBox.Items.Add(e.FullPath);

MessageBox.Show(System.IO.Path.GetFullPath(e.FullPath)
        "Authority Warning", MessageBoxButtons.OK,
        MessageBoxIcon.Warning);
        FileWrite(e.FullPath,e.ChangeType.ToString());
        cnt++;
        total_cnt2++;
    }
}
```

그림 8. 사용자 경고 알람
Fig. 8 User warning alarm

3.4 사용자 편의 추가 기능

사용자 편의를 위해 기록된 로그의 경로에서 파일의 직접이동이 가능한 기능을 제공한다. 파일이동 버튼을 클릭하여 활성화시키면 간단히 해결된다. 그림 9는 파일이동 버튼을 클릭하면 동작하는 코드이다. try문을 이용해 버튼 클릭 시 무조건 동작을 하도록 설계하였으며 공백을 없애는 변수와 결과를 나타내는 변수를 지정했다. 또한 사용자가 시각적으로 확인 가능하도록 불필요한 문자열을 판별하는 변수를 적용했다. 좌측경로 리스트에서 옮기고자 하는 파일을 선택한 후 해당 파일을 옮길 드라이브를 선택할 수 있다. 그림 10은 실행후의 화면 상태이다.

```
private void button4_Click(object sender, EventArgs e)
 {
  try
  {
    int index = CopyListBox.SelectedIndex;
    String temp = (String)CopyListBox.Items[index];
    temp = temp.Trim();
    String Rsearch = "";
    string[] result = temp.Split(new char[] { '\\' });
    for (int i = 0; i < result.Length; i++)
    {
       if(i == result.Length-1) {
       Rsearch = result[i];
       }
    }
   FileInfo fileinfo = new FileInfo(temp);
   progressBar1.Value = 10;
   fileinfo.MoveTo(@""+ webBrowser1.Url.ToString()
   .Substring(8) + "" + "\\" + Rsearch);
   MessageBox.Show("file move complete!");
  }
```

그림 9. 파일이동 버튼 활성화
Fig. 9 File move button on

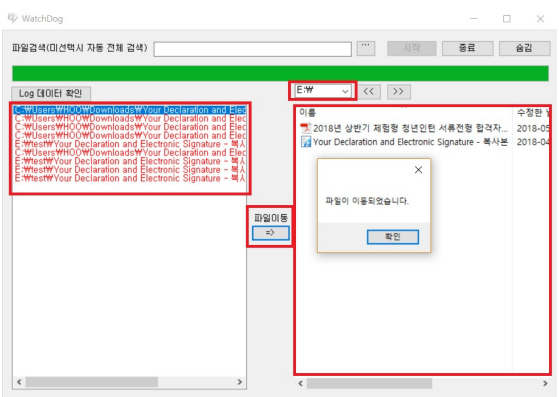

그림 10. 파일이동 완료
Fig. 10 Moved file

드라이브 선택 후 파일이동 버튼을 클릭함과 동시에 해당 코드가 동작하며 문제없이 이동 될 경우 그림 9.와 같이 알림 메시지 팝업창을 활성화시킨다. 또한 OS내 BackGround에서 동작이 가능하도록 숨김 기능과, 숨김 상태에서 응용프로그램을 재 활성화 하는 기능을 실행하도록 구현했다.

활성창의 우측 위에 위치한 숨김 버튼을 클릭하면 버튼클릭 이벤트가 발생하며 현재 폼을 최소화 하는 WindowState 코드가 동작한다. 이와 동시에 숨김 버튼이 비활성화 되며 윈도우에 있던 프로그램은 최소화 되어 윈도우 바 내에 숨김 프로그램 표시 공간 안에 WatchDog 아이콘이 그림 11처럼 생성된다.

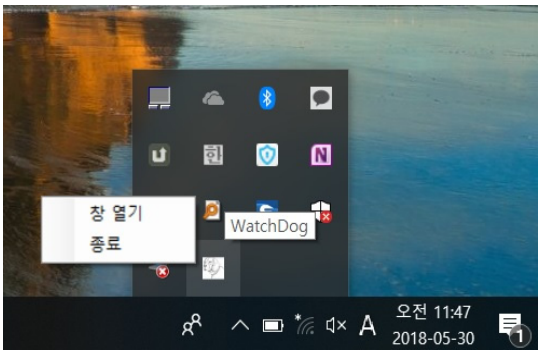

그림 11. 프로그램 숨김 기능 활성화
Fig. 11 Program hiding function activation

프로그램 숨김 기능이 활성화 된 후, 사용자가 기능을 해제하고 싶다면 윈도우 바 우측 하단에 위치한 숨김 파일 표시 창에서 WatchDog을 찾은 뒤 마우스 우측 클릭에서 <창 열기>를 클릭하면 원래 크기로 복귀한다. notifyIcon1을 이용해 창열기 버튼을 클릭할 경우 false 값이 동작해 숨겨진 아이콘 표시 창에서 비활성화 되어 사라진다.

또한 WindowState 변수가 동작하여 본래의 크기로 복귀한다. 최소화 상태에서 사용자가 바로 종료하기를 원한다면 마우스 우측 클릭 버튼으로 종료를 클릭 하면 된다. 최소화 상태에서 추가 기능이 동작하지 않고 곧바로 프로그램 종료와 동시에 BackGround 동기화가 비활성화 되어 프로그램을 완벽하게 종료한다.

Ⅳ. 결 론

전자 메일첨부 파일을 성급히 다운로드하여 지정한 폴더에 지정하지 않은 채 문서작성을 끝마치는 실수로 파일을 분실하는 경우가 허다하다. 하드디스크나 안전한 폴더에 저장하지 않아 발생한 허탈한 경험들이다. 본 연구는 전자 메일첨부 편집문서의 분실을 최

소화하기 위한 파일분실 방지 시스템 WatchDog을 제안하고 구현했다. 파일의 분실위험을 알리는 경고창과 파일 이동 및 다운로드의 모니터링 기능을 부가하여 안정적인 폴더 관리방안을 개발하였다. 추후 사용자 경험을 피드백정보로 활용하여 시스템의 개선요구를 반영하는 연구가 필요하다.

Reference

[1] S. Kim, "Extract method of large attachments in e-mail forensics," Master's Thesis, *Korea University,* 2015.

[2] S. Park, "A Study on the Analysis and classification of the HTML files in the unallocated area of the Storage," Master's Thesis, *Korea University*, 2008.

[3] Y. Kim and J. Seo, "Indirection Model and Application of Electronic Mail Control System Considering High Availability," *The J. of the Korea Institute of Maritime Information & Communication Sciences*, vol. 9 no. 2, 2005, pp. 348-354.

[4] S. Lee and M. Hwang, "Implementation of Web-based Performance Monitoring System for E-Mail Server," *J. of the Korea Institute Of Information and Communication Engineering*, vol. 15, no. 9, 2013, pp. 2105-2112.

[5] S. Hong, G. Sin, and M. Han, "A Classification Model for Attack Mail Detection based on the Authorship Analysis," *Korean Society for Internet Information Transactions on Internet and Information Systems*, vol. 18. no. 6, 2017, pp. 35-47.

[6] J. Jang, D. Kim, and C. Choi, "Study on Hybrid Type Cloud System," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 11, no. 6, 2016, pp. 611-618.

[7] W. Ryu, "Delayed Block Replication Scheme of Hadoop Distributed File System for Flexible Management of Distributed Nodes," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 12, no. 2, 2017, pp. 367-374.

[8] C. Choi, Y. Lee, and T. Lee, "Improvement Method of ELIS Local Laws and Regulations Format for Personal Information Protection," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 11, no. 11, 2017, pp. 1017-1024.

[9] J. Jang, D. Kim, and C. Choi, "Study on Hybrid Type Cloud System," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 11, no. 6, 2016, pp. 611-618.

[10] S. Kim, Y. Kim and W. Kim, "The Design of Method for Efficient Processing of Small Files in the Distributed System based on Hadoop Framework," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 10, no. 10, 2015, pp. 1115-1122.

저자 소개

홍준후(Jun-Hu Hong)

2018년 경동대학교 정보보안학과 4학년 재학 중
2015년 SK네트웍스서비스(주) 근무
2016년 한일네트웍스 DSC사업부 근무
2016년 BSITC(주) 필리핀 마닐라 본사 파견근무
※ 관심분야 : 모바일보안, 웹서버보안

최철재(Chul-Jae Choi)

1983년 광운대학교 전자계산학과 졸업(이학사)
1987년 한양대학교 산업대학원 전자계산학전공 졸업(공학석사)
2000년 강원대학교 컴퓨터과학과 졸업(이학박사)
1988년~현재 경동대학교 정보보안학과 교수
2015년~2016년 경동대학교 평생교육원장
※ 관심분야 : 데이터처리, 영상처리, 웹보안