International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:3, No:11, 2009

Security Analysis on the Online Office and Proposal of the Evaluation Criteria

Hyunsang Park, Kwangwoo Lee, Yunho Lee, Seungjoo Kim, Dongho Won

***Abstract*—**The online office is one of web application. We can easily use the online office through a web browser with internet connected PC. The online office has the advantage of using environment regardless of location or time. When users want to use the online office, they access the online office server and use their content. However, recently developed and launched online office has the weakness of insufficient consideration. In this paper, we analyze the security vulnerabilities of the online office. In addition, we propose the evaluation criteria to make secure online office using Common Criteria. This evaluation criteria can be used to establish trust between the online office server and the user. The online office market will be more active than before.

***Keywords*—**Online Office, Vulnerabilities, Common Criteria(CC)

I. Introduction

THE online office operates through a web browser with internet connected PC. The online office can be used without time or location constrains. Also, the online office can alleviate the inconvenience of having to save data in a separate storage.

However, the online office has the same issues of security vulnerabilities of the existing web application programs. When the online office is used, an attacker can recover temp file since it remains in the hard disk of PC. Also, the contents of office files can be leaked when the packet is not encrypted. The seriousness of the issue increases even further if the leaked office file contains confidential work information or privacy information.

The rest of the paper is organized as follows. Section 2 reviews related works, Section 3 analyzes vulnerability online office. Section 4 presents the Common Criteria. Finally, In Section 5, we present our conclusions.

II. Related Works

The online office is one of the web application programs that are receiving much attention. Four companies such as Google[1], Hannsoft[2], Zoho[3] and Microsoft[4] are leading the online office market through their products such as Google Docs by Google, Thinkfree by Hannsoft, Zoho office by Zoho and Microsoft Office Live by Microsoft.

H. Park, K. Lee, Y. Lee, S. Kim and D. Won are with Information Security Group, Sungkyunkwan University, 300 Cheoncheon-dong, Jangan-gu, Suwon-si, Gyeonggi-do, 440-746, Republic of Korea ({hspark, , kwlee, leeyh, skim,dhwon}@security.re.kr)

Corresponding author: Dongho Won.

A. Functional Characteristics

The online office can be classified according to the functions they provide, whether or not they support large size files and which browser they support. The following shows the characteristics of the functions provided by each online office. (see Table 1)

TABLE I FUNCTIONAL CHARACTERISTICS

Function	Google Docs	Thinkfree	Zoho Office	MS Office Live
Word processor	O	O	O	Desktop Office integration
Spreadsheet	O	O	O	Desktop Office integration
Presentation	O	O	O	Desktop Office integration
Open API	X	O	O	X
Collaboration	O	O	O	O
Large Size File	X	O	X	X
Web Storage	O	O	O	O
Browser Support	IE*,FF*	IE, FF, Safari	IF, FF	IE
Development Platform	Ajax	Ajax/Java	Ajax	Ajax/Win 32

*IE: Internet Explorer, FF:Firefox

The online office company is still in progress to process large size file and support various office files. Among them, Thinkfree online office is supporting the most diverse formats of files and processing of large size file of over 10Mb. (see Table 2)

III. Vulnerability Analysis

The online offices are being developed without sufficiently considering the countermeasures for the security vulnerabilities of the existing web application programs.

The security vulnerabilities of web application programs are being presented every year by The Open Web Application Security Project (OWASP) group. The modeling for the web application programs should be done upon considering the possible vulnerabilities even from the design level [5].

TABLE II SUPPORTING FILES

Classification	Google Docs	Thinkfree	Zoho Office	MS Office Live
Word Processor	Max. (500Kb) txt, rtf, odt, sxw, doc	Large size file support doc, dot, docx, xml, htm, html,	Unknown html, doc, sxw odt, rtf, jpg,	Large size file support Dependent on MS Office

		rtf, txt	gif, png ,txt	
Spreadsheet	Max. (1Mb)	Large size file support	Unknown	Large size file support
	csv, xls, ods	xls, xlsx, xlt, txt, csv, xml, htm, html	xls, scx, ods,csv, tsv	Dependent on MS Office
Presentation	Local (10Mb), Web (2Mb), E-mail (500Kb)	Large size file support	Max. (10Mb)	Large size file support
	ppt, pps	ppt, pptx, pps, ppsx, pot, potx	ppt, pps, odp, sxi	Dependent on MS Office

A. Vulnerabilities Analysis

The analysis was conducted based on "Top 10 Web application vulnerabilities for 2007" presented by OWASP to discover the issues of the online office.(see Table 3) As the result, the vulnerabilities confirmed in the online office included "Information Leakage and Improper Error Handling", "Insecure Cryptographic Storage" and "Insecure Communications".

TABLE III TOP 10 WEB APPLICATION VULNERABILITIES FOR 2007

Vulnerabilities	Contents
Cross Site Scripting (XSS)	XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.
Injection Flaws	Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.
Malicious File Execution	Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise. Malicious file execution attacks affect PHP, XML and any framework which accepts filenames or files from users.
Insecure Direct Object Reference	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.
Cross Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker. CSRF can be as powerful as the web application that it attacks.
Information Leakage and Improper Error Handling	Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Attackers use this weakness to steal sensitive data or conduct more serious attacks.
Broken Authentication and Session Management	Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other users' identities.
Insecure Cryptographic Storage	Web applications rarely use cryptographic functions properly to protect data and credentials. Attackers use weakly protected data to conduct identity theft and other crimes, such as credit card fraud.
Insecure Communication	Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications.
Failure to Restrict URL Access	Frequently, an application only protects sensitive functionality by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.

B. Attack Scenario

The following attack scenario is set to examine and review the vulnerabilities that occur when using the online office. The attacker processes sending an e-mail attached backdoor program.

Through the backdoor program installed in the user PC, the attacker checks to see if there is remaining residual information for the office file the user worked in the temp folder. And the office file is recovered upon downloading the office file to the attacker PC if residual information remains. Also, the attacker attempts forgery of each data by sniffing the transmission information when the user PC is using the online office.

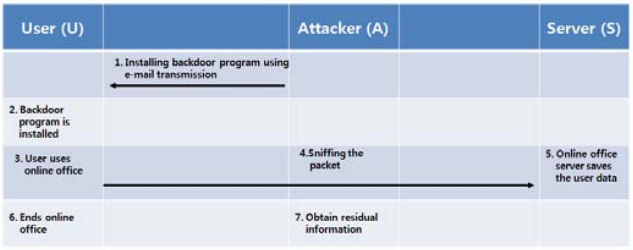

Fig. 1 Attack Scenario

C. Test Environment and Results

To verify the information leaked from various online office products, this test checks to see if the document contents leak through packet by checking if there is residual information in the temp folder and the packet when the online office is being used. As for the tools for packet analysis, WireShark[6] was used through which real-time packet analysis is possible and the analysis was conducted by sniffing.

It was found in Google Docs that there was no information leak in the temp folder. However, it was found that sensitive personal information was being leaked through the above packet when the online office was used in PC, as shown in (Fig.2)

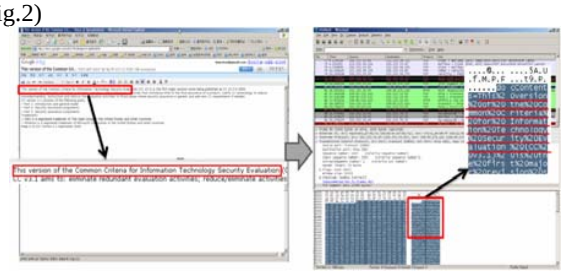

Fig. 2 Packet Data that Leaked While Using Google Docs

In Thinkfree, the packet data leaked while using PC was confirmed, and, as shown in (Fig. 3), it was found that temp file was created in the temp folder while opening office file through a web browser.

Fig. 3 Temp File Created While Opening Thinkfree Office File

Upon changing the extension from .tmp to .ppt, the office file can be opened by MS Office 2007, as shown in (Fig. 4).

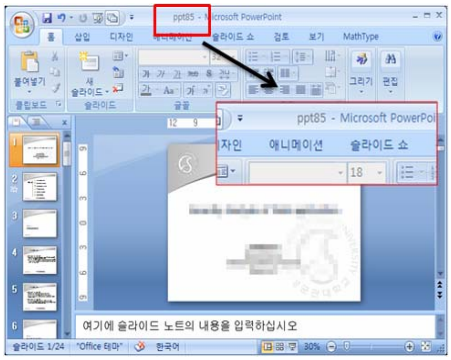

Fig. 4 Recoverable Temp File After Ending Thinkfree Office

In Thinkfree, along with the issue of remaining temp file, it was found that the data packet of the office file edited in web platform leaked as was the case in Google Docs, as shown in (Fig. 5).

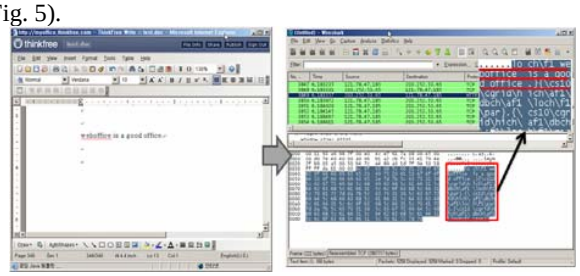

Fig. 5 Packet Data that Leaked While Using Thinkfree

In Zoho office, the packet data leaked for the office file while editing or saving the file, as shown in (Fig. 6).

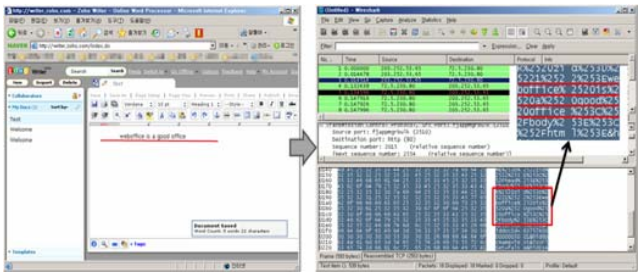

Fig. 6 Packet Data that Leaked While Using Zoho office

The summary of the information of major online office that leak based on the test results is as shown below. (see Table 4)

TABLE IV LEAKED INFORMATION

Leaked Information	Google Docs	Think free	Zoho Office	MS Office Live
Document contents leak through sniffing tool	O	O	O	X
Office file leak through temp file	X	O	X	X

IV. PROPOSAL OF EVALUATION CRITERIA

Nowadays, when we use the online office, security solution is not installed. Although the secure login using SSL is applied in the login process to use the online office, a problem occurs of being able to identify the document contents during the data transmission and storage after the login. Therefore, to improve the security vulnerabilities of the online office, evaluation criteria will be derived in this section using the common criteria v3.1 according to ISO/IEC 15408 and common methodology v3.1 to allow sufficient considerations on security[7,8,9]. The operating environment and security functions of the online office are defined. The threats against the online office are analyzed. Also, we choose additional potential threats from the vulnerability analyze site and vulnerability database. In addition, the security objectives needed to eliminate the threats are proposed, and the evaluation criteria is presented by itemizing the proposed security objectives.

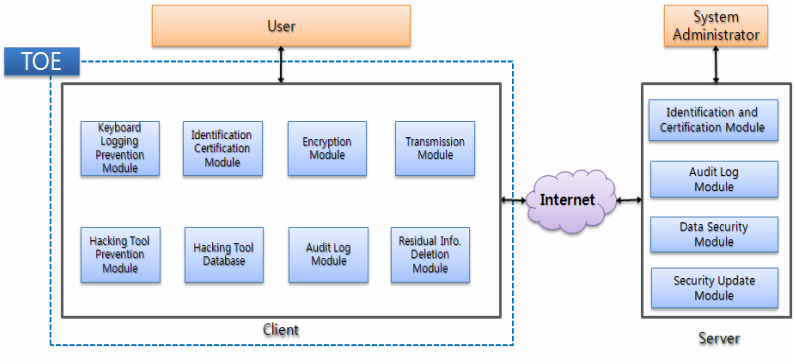

Fig. 7 Target of Evaluation (TOE)

A. Assets

The information has to be protected by TOE. Therefore, the assets that need to be protected in the online office are classified into inputted information, transmitted information and saved information. There are three kinds of assets to be protected.

- Input Information: it is the information inputted by users to connect to the online office through a web browser, which includes the login ID and password.
- Transmit Information: it is the information transmitted between the user and the online office server, and includes the login ID and password and the contents of the office files created by users through a web browser.
- Save Information: it refers to the information sent to the temp folder or on the memory when the user uses the online office and the office files of the user saved in the server.

B. Threat Agents

The threat agents of the online office are classified into five types.

- An attacker
- An authorized user
- A privileged user
- An administrator
- A system owner or developer

The attacker is the existence that seeks to obtain the information of the users without being certified and has the ability to perform the method tested in the above ‘ . *VULNERABILITY ANALYSIS-C.Test Environment and Results’*.

This attacker has the ability to obtain the input information of the user or transmitted information by using sniffing tool or hacking tools.

C. Vulnerabilities and Attack Methods

The vulnerabilities of the online office are classified into the following two based on the basis tested in the above ‘ . *VULNERABILITY ANALYSIS-C.Test Environment and Results’*.

- Obtain the personal information of users from the packet by sniffing the packet transmitted in plaintext
- Obtain or damage input information or saved information using hacking tools

D. Operating Environments

The online office is composed of a web browser and server that provide the online office. The online office can be used as the user that tries to use the online office connects to the online office server through the identification and authentication through a web browser with internet connection. According to the requests of the web browser of the user, the online office server provides the online office and performs the role of saving the data the user created for edit. For a safe system operation, the user and online office server provide the security functions such as access control, user identification and authentication, secure communication, keyboard input security, hacking prevention, etc.

E. Security Problem Definition

1) Threats

The threats are derived through the threat against the assets and attack methods. It describes of the possibility of damaging the assets through threats. To derive threats based on the test analyzed in the above ‘ . *VULNERABILITY ANALYSIS-C.Test Environment and Results’*.

There are ‘key logging, ‘damaging saved information’, ‘damaging transmitted information’, ‘sniffing’ and ‘residual information.’

Through the five kinds of threats, additional threats can be derived such as ‘defective codes’, ‘impersonation’, ‘continuous authentication attempt’ and ‘replay attack’, and the threats such as 'bypass access' is derived through 'impersonation' threat. Also, the threat called 'unreliable management' can be derived through the open vulnerability sites for the threats in addition to the ones analyzed through the test. (see Table 5)

TABLE V VULNERABILITIES AND VULNERABILITIES INFORMATION LIST

Classification	Content

Vulnerabilities Analysis Sites	CERTCC-KR(http://www.certcc.or.kr) CERTCC(http://www.cert.org) BUGTRAQ(http://www.securityfocus.com) PacketStormSecurity(http://www.packetstormsecurity.org) MITRE(http://cve.mirte.org) SANS ICS(http//ics.sans.org) CIAC(http://www.ciac.org/ciac) BLACKHAT(htt://www.blackhat.com) MCAFEE Threat Center(http://www.mcafee.com/us/threat_center)
Vulnerabilities Analysis Information Sites	Zdnet(http://ww.zdnet.com) Security New Portal(http://www.securitynewportal.com)
Threats & Vulnerabilities Database	JISEC Threats Database JISEC Vulnerability Database

The threats that can be applied to the online office are described in the following. (see Table 6)

TABLE VI THREATS

Threat	Explanation
T. Key Logging	Unauthorized users can obtain authentication information by sniffing the keyboard input of the users using backdoor program.
T. Saved Information Damage	Authorized users or unauthorized users can obtain the residual data remaining in the temp file by using the file control function of backdoor program.
T. Transmitted Information Damage	Unauthorized users can damage the data information of users by changing the transmitted data by being in the middle of the web browser and online office server.
T. Sniffing	Unauthorized users can obtain information through the packet not encrypted in the communication between the web browser and online office server by using sniffing tools.
T. Residual Information	Unauthorized users can obtain deleted information by recovering the deleted temp files.
T. Defective Codes	Problems can occur for the online office users of leaking transmitted data or allowing other users to view the data from the section that is not encrypted among the personal information sections at the mistake of the developer.
T. Impersonation	Unauthorized users can impersonation themselves as legitimate users by using the personal information of the users obtained by using key logging tool and sniffing tool.
T. Continuous Authentication Attempt	Unauthorized users can succeed in the authentication as certified users through the complete enumeration survey that continuously attempts authentication to the online office server.
T. Replay attack	Unauthorized users can access the online office server by using the authentication data of certified users.
T. Bypass Access	Unauthorized users can steal the document data of users by approaching it by bypassing the security function of the online office server.
T. Unreliable Management	When the security function of the online office is revised or deleted, it might not operate or errors might occur.
T. Distributed Installation	The security function of the online office can become damaged when the online office is distributed, installed or updated by uncertified users through the unjust approach to the online office server.

2) Organization Policies

The regulations for performing the security objectives are needed for organizations. Therefore, implementation of the security objectives should be mandated through the security organizations policy. The security policies that need to be applied and operated in the online office environment are as shown in the following. (see Table 8)

TABLE VIII ORGANIZATION POLICIES

Organization Policy	Explanation
P. Audit	To trace the responsibility of security related actions, TOE needs to be accurately recorded and safely maintained of the security related events and it should be able to appropriately review the audit data.
P. Secure Management	Authorized administrator should be able to manage TOE in secure methods, and maintain TSF data in up-to-date condition.
P. Recovery	TOE should be recovered in safe condition when it needs to be recovered.
P. Password	The password algorithm and module used in TOE should be the ones approved by the Director of the National Intelligence Service.

3) Assumptions

The threats analyzed above are the threats that can direct damage online office, and the threats against the operating environment are solved through the assumptions. The environment that needs to be safely operated through the assumptions is shown in the following. (see Table 7)

TABLE VII OPERATING ASSUMPTIONS

Assumption	Explanation
A. Security Maintenance	When the internal network environment changes from the network composition change, host and service rise and fall, and the same level of security as before is maintained by reflecting the changed environment and security policy immediately to TOE operation policy.
A. Reliable Administrator	The authorized administrator of TOE should have no ill intent and appropriately trained for TOE administrative functions and accurately perform the responsibilities according to the administrator guidelines.
A. Dynamic Management	TOE is managed to allow appropriately handle the changes in the protection target assets that dynamically change.
A. Safe Installation / Operation	TOE is based on the basic operating system that is installed and operated in safe ways.
A. Operating System Strengthen	The reliability and safety of the operating system should be guaranteed by performing the strengthen work for the vulnerabilities of operating system.

F. Security Objectives

The security objectives through which each threat can be solved need to be presented. Therefore, the security objectives in response to the threats are identified and described. Also, show the rationales of at least one security objective for each threat by analyzing the corresponding relation between each threat and security objective.
The corresponding relation between threats and security objectives are shown in the following. (see Table 11)

G.Security Functions

The online office has the following security functions.

・Identification and Authentication
Through the administrator that manages the server and a web browser, the online office server identifies and certifies the users connecting to the online office. The online office users are identified and certified through the member information of the online office server.

・Audit
The online office server saves the audit log of the connection by the certified users and inspects for normal

connections. It identifies if the online office users make certified connections and saves the audit information of the online office server. Also, it leaves the audit information on the failed events when the connect fails.

・Management
The online office server securely saves and manages the information to the database. When using the online office through a web browser, the users perform updates by checking to see if the program of the online office server has been updated. The communication between the online office server and users through a web browser provides reliable timestamp for time synchronization.

・Secure Communication
The online office server performs safe secure communication through encryption when communicating with the web browser of users.

・Keyboard Input Security
Encryption is performed for safe data transmission between the online office server and the web browser of users and securely manages the key for encryption.

・Hacking Prevention
It provides the hacking prevention function of detecting and removing the hacking tools such as key logging or backdoor program in the user PC during the connection to the online office server through the web browser of the users.

TABLE IX THREAT AND SECURITY OBJECTIVES

Threat	Security Objective
T. Key Logging	Need for the function to prevent hacking tool used in key logging (hacking tool prevention)
T. Saved Information Damage	Need for the function to prevent hacking tool used in remote system file control (hacking tool prevention) Need for the function to protect saved information (saved information protection) Need for the function to protect the key used in encryption/decoding of saved information (key protection)
T. Transmitted Information Damage	Need for the function to protect transmitted information (transmitted information protection) Need for the function to protect the key used in encryption/decoding of transmitted information (key protection)
T. Sniffing	Need for the function to protect transmitted information (transmitted information protection)
T. Residual Information	Need for the function to completely remove the residual information left by online office in operating environment to prevent reuse (residual information protection)
T. Defective Codes	Need for the function to conduct faultiness test to see if there are defective codes in the online office (defective code test)
T. Impersonation	Need for safe identification and authentication function (identification and authentication)
T. Continuous Authentication Attempt	Need for safe identification and authentication function (identification and authentication)
T. Replay attack	Need for the function to prevent the access to the online office by reusing the authentication data of the authorized user (identification and authentication)
T. Bypass Access	Need for the function to protect the self function from the attempts for bypass access (self function protection)
T. Unreliable Management	Need for the function to safely install/operate/management the online office (management)
T. Distributed Installation	Need for the function to safely install/operate/management the online office (management)

TABLE X SECURITY OBJECTIVES

Security Objective	Explanation
O. Hacking Tool Prevention	Prevent the data of authorized user from leaking to the attacker by preventing the operation of backdoor program that approaches the evaluation area of the online office.
O. Transmitted Information Protection	The transmitted information of the communication between web browser and online office server should be protected from unauthorized exposure and change for the evaluation area of the online office.
O. Saved Information Protection	The saved information saved in the user PC should be protected from the exposure, change and deletion for the evaluation area of the online office.
O. Identification and Authentication	The functions within the evaluation area of the online office need to identify and authenticate the users and respond to the continuous authentication failures.
O. Key Protection	The encryption/decryption keys to protect the personal information and document data of users need to be safely protected.
O. Self Function Protection	The online office evaluation area needs to protect itself from the change, deactivation and bypass attempt of the security function for the online office evaluation area from the first implementation.
O. Audit	The online office evaluation area needs to record and maintain the security related events to allow the accountability of the security related actions and provide the measure through which recorded data can be reviewed.
O. Management	The online office needs to be distributed and installed in safe methods, and the online office evaluation area needs to provide in safe ways the management measures to efficiently manage the evaluation area of the online office by the authorized administrator and provide the measure through which TSF data can be maintained up-to-date.
O. Defective Code Test	Tests need to be conducted to see if there are any defective codes developed by the developer, and to see if the defective codes are having effects among the internal composite elements of the evaluation area of the online office or connected security solution is appropriately applied.
O. Residual Information Protection	The residual information that can be used in the access rights cannot be obtained from the reallocated resources during the operation of the online office.

TABLE X1 SECURITY OBJECTIVE RATIONALES

Threat	O. Hacking Tool Prevention	O. Transmitted Information Protection	O. Saved Information Protection	O. Identification and Authentication	O. Key Protection	O. Self Function Protection	O. Audit	O. Defective Code Test	O. Management	O. Residual Information Protection
A. Maintain Security	√			√						
A. Reliable Administrator				√					√	
A. Dynamic Management								√		
A. Safe Installation/Operation									√	
A. Operating System Strengthen									√	
P. Audit						√	√			
P. Secure Management	√								√	
P. Recovery									√	√
P. Password			√		√					
T. Key Logging	√									
T. Saved Information Damage	√		√		√				√	
T. Transmitted Information Damage		√			√					
T. Sniffing						√	√			
T. Residual Information			√						√	√
T. Defective Codes								√	√	
T. Impersonation				√						
T. Continuous Authentication Attempt				√			√			
T. Replay attack				√						
T. Bypass Access						√	√			
T. Unreliable Management									√	
T. Distributed Installation									√	

V. CONCLUSION

Although the online office has the advantage of offering the same work environment, it has the issue of having high possibility of leaking and exposing documents.

In this paper, the security vulnerabilities that can occur in the online office were analyzed and the according evaluation criteria were proposed. To be perceived by users, the online office tries to develop more secure and safe.

For future study, the online office model that can be applied by companies is considering. So we need to be looked into study to establish safe document management system within companies.

ACKNOWLEDGMENT

This work was supported by Defense Acquisition Program Administration and Agency for Defense Development under the contract UD070054AD.

This research was supported by the MKE(Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency) (NIPA-2009-(C1090-0902-0016))

REFERENCES

[1] Google Docs, http://docs.google.com/
[2] Thinkfree, http://www.thinkfree.com/
[3] Zoho. http://www.zoho.com/
[4] Microsoft Office Live. http://workspace.office.live.com/
[5] OWASP, http://www.owasp.org/index.php/Top_10_2007/
[6] WireShark, http://www.wireshark.org
[7] Common Criteria, Common Criteria for Information Technology Security Evaluation; part 1: Introduction and general model, Version 3.1 R1, CCMB-2006-09-001(September 2006)
[8] Common Criteria, Common Criteria for Information Technology Security Evaluation; part 2: Security functional components, Version 3.1 R2, CCMB-2007-09-002(September 2007)
[9] Common Criteria, Common Criteria for Information Technology Security Evaluation; part 3: Security assurance components, Version 3.1 R2, CCMB-2007-09-003(September 2007)