An Analysis of the Green Dam Youth Escort Software

Frankie Li, Hilton Chan, Kam-Pui Chow, Pierre Lai

Chapter 4

AN ANALYSIS OF THE GREEN DAM YOUTH ESCORT SOFTWARE

Frankie Li, Hilton Chan, Kam-Pui Chow and Pierre Lai

Abstract According to official Chinese media sources, the Green Dam Youth Escort (GDYE) software is intended to protect young citizens from viewing unhealthy information on the Internet. However, critics maintain that GDYE has serious security vulnerabilities that allow hackers to take control of computers installed with GDYE. Critics also claim that the software is designed to collect user data and keystrokes for transmission to remote servers for unknown purposes. GDYE was originally mandated to be pre-installed on every computer sold in the People's Republic of China. However, the plan was suddenly shelved in the face of intense international media attention. This paper evaluates the GDYE software's advertised functions and additional non-advertised capabilities. As the software may have spyware and malware functionality, the evaluation monitored the software behavior in a specialized controlled environment. The analysis was performed from a forensics perspective to collect digital evidence and traces in order to prove or disprove that GDYE captures and disseminates private information.

Keywords: Green Dam Youth Escort, analysis, forensic perspective

1. Introduction

Green Dam Youth Escort (GDYE) is an Internet filtering software developed in the People's Republic of China. According to a June 20, 2009 article in *CaiJing Magazine*, GDYE is designed to filter unhealthy information, control surfing time and restrict Internet gaming by Chinese children and youth. With the help of GDYE, parents may view web access logs and screen snapshots.

Under a directive from the Chinese Ministry of Industry and Information Technology (MIIT), GDYE had to be pre-installed on the hard disk and be stored in the recovery partition and on the recovery CD

of every personal computer sold in Mainland China on or after July 1, 2009. However, on June 30, 2009, just one day before the deadline, MIIT announced that the mandatory installation of GDYE was postponed to an undetermined date for unspecified reasons.

Starting on July 1, 2009, GDYE was available for download free-of-charge, and was installed on computers in schools, Internet cafes and public locations [8]. According to the China Daily News [4], an MIIT official indicated that the government would definitely carry out its "directive" regarding GDYE, and it was just a matter of time. On August 13, 2009, the Head of MIIT disclosed to the media that GDYE was undergoing a bug fixing process and the plan would be implemented after considering comments from the public. He also disclosed that the option of using a better software system had not been rejected outright.

Since its initial introduction to the public, GDYE has received mixed reactions, both positive and negative, from various entities. One of GDYE's principal goals was to control the access of unhealthy information by Chinese children. However, many individuals are concerned that the government-backed software was created with a hidden agenda to control the flow of information and to restrict the Chinese people from accessing "inappropriate" information on the Internet.

In the light of GDYE's development history and strong government support, it is likely that the software or another similar system will be forced on the public in the near future. However, the questions concerning the leakage of personal information, governmental surveillance and hidden filtering have not been answered. This paper attempts to verify if the software provides special censorship and spying functions that may be used to monitor an individual's online activities.

2. Background

Under an MIIT directive, Zhengzhou Jinhui Computer System Engineering Company (Jinhui) and Beijing Dazheng Human Language Technology Academy (Dazheng) were selected to develop Internet filtering software for MIIT. Project managers from these two companies were subsequently tasked with developing GDYE.

The official websites of Jinhui [7] and Dazheng [5] indicate that the two companies are linked to the Chinese Academy of Sciences, the largest government-funded science and technology research center in China. Jinhui identifies itself as an expert in the area of identifying and filtering pornographic images from the Internet and states that it developed a system that can filter unhealthy images or collect "evidence" from cel-

lular networks. As such, Jinhui was responsible for providing technical expertise related to the image filtering function of GDYE.

Dazheng is a spin-off of the Institute of Acoustics of the Chinese Academy of Sciences. The company website discloses that it invented the notion of a "hierarchical network of concepts" that supports the translation and filtering of Chinese-language messages from computer networks and the Internet. Dazheng is believed to have been responsible for designing and implementing the text filtering function of the GDYE software.

3. Related Work

An analysis of GDYE was released on June 11, 2009 by researchers from the University of Michigan, and an update was published seven days later. The report [10] included the following key findings:

- GDYE contains serious security vulnerabilities due to programming errors that potentially enable websites visited by the user to exploit these problems and seize control of the computer, steal private data, send spam or incorporate the computer in a botnet.
- The GDYE blacklist update process potentially allows the developers, or any third-party impersonating them, to execute malicious code during the filter update.
- The blacklists are taken from CyberSitter and GDYE contains code libraries from OpenCV, an open source image recognition system.

On June 13, 2009, a GDYE update (Version 3.17) was released that supposedly addressed the original web filtering security vulnerability, disabled the blacklists that were copied from CyberSitter, and brought the software into compliance with the OpenCV license. However, a new filtering vulnerability was found. On June 18, 2009, researchers with the Professional Information Security Association (PISA) of Hong Kong demonstrated the re-engineered results of certain binaries of GDYE [11]. Their key findings were:

- The existence of false positive and false negative errors for the URL filtering and pornographic image filtering functions of GDYE.
- GDYE forces certain running processes to close, including Internet Explorer and Microsoft Word and Notepad, when politically-sensitive text (e.g., "June 4 Massacre") is entered.
- Screen snapshots are saved every three minutes by default and the saved information may disclose sensitive information (e.g., details

of online banking sessions, decrypted messages and private communications) to the GDYE administrator.

Faris, Roberts and Wang of the OpenNet Initiative [6] performed a detailed evaluation of the filtering functions by analyzing surfing activities involving Internet Explorer under different versions of GDYE. The goal of the evaluation was "to investigate, expose and analyze Internet filtering and surveillance practices in a credible and non-partisan fashion." Their key findings were:

- GDYE places intrusive controls and actively monitors individual computer behavior by installing components deep in the kernel.
- GDYE provides more functionality than is necessary to protect children online and it subjects users to security risks. GDYE could be used to monitor personal communications and Internet browsing behavior by logging it on the local machine.
- The GDYE implementation for individual computers represents a shift in the filtering strategy to distribute control mechanisms in client-side software in order to offload the burden of sorting through content to individual machines on a network.
- The possibility of personal information leaks could be high (however, the OpenNet Initiative evaluation did not confirm that personal information was being gathered in a central location).

A report by unknown Mainland Chinese researchers [2] indicates that twelve folders and 110 files are created or added to the file system during GDYE installation. After the system is rebooted, four processes and one driver are started and loaded. The process `XNet2.exe` attempts to contact two IP addresses, `211.161.1.134` and `203.171.236.231`, for unknown reasons. Furthermore, the file `XNet2_lang.ini` contains the words "AOption0_1117 = (Upon discovery of harmful information, report automatically to Jinhui Corporation)." This implies that GDYE is capable of sending private information for unknown purposes. GDYE monitors a number of instant messaging applications (e.g., `wow.exe`, `yahoomessenger.exe`, `wangwang.exe` and `qq.exe`) by creating handles using `inject.dll` for Internet Explorer with the clear purpose of collecting private user information. The report further reveals that GDYE monitors TCP and UDP ports to prevent proxy connections if the FreeGate proxy is used.

Another report [1] discovered that all installation paths of GDYE are contained in the setup file `xstrings.s2g`. After the system is rebooted, it loads `mgtaki.sys` (driver) and starts the execution of services

such as `MPSvcC.exe`, `Xnet2.exe` and `XDaemon.exe`. The `XNet2.exe` and `gn.exe` processes are protected to prevent the live deletion of the files. The `kwpwf.dll` file contains the MD5 hash of the admin password, and the magic password `7895123` was found to allow administrative login. The report also noted that the files `cximage.dll`, `CImage.dll`, `xcore.dll`, `Xcv.dll` and `XFImage.xml` are from OpenCV; and the files `HncEng.exe`, `HncEngPS.dll`, `SentenceObj.dll` and `FalunWord.llb` are from Dazheng. Some applications were found to be monitored upon checking the strings information in `injlib.exe`. Finally, when a user surfs the Internet, all content is filtered by WinSock 2 SPI.

Several critics have argued that by applying the blacklist and text filtering functions, GDYE can: (i) filter unwanted political information, including text and images; (ii) act as a tool for the "cyberpolice" to obtain digital evidence of crimes for possible prosecution; and (iii) collect private information from the users, including (but not limited to) web surfing activities and keystrokes, and secretly send the information to certain IP addresses for unknown reasons.

The reviews and reports described above describe the functionality and technical aspects of GDYE. Some of the unconfirmed findings are important, especially the suggestion that GDYE can hide itself in the kernel to open a secret channel that sends private information to certain IP addresses. In view of these and other hidden functions, we treated GDYE as spyware or malware and analyzed it in a controlled environment.

Our work focused on the technical aspects of GDYE and on validating its functionality and behavior while ignoring the political and social rhetoric. In particular, we used digital forensic and reverse engineering tools to scientifically test the hypotheses that (i) using GDYE can result in the loss of private information; and (ii) GDYE is designed to collect private information from users and provide the collected information to centralized servers for unknown purposes.

4. GDYE Analysis

Our objective was to study GDYE's censorship and spying functions. After June 9, 2009, several updates of the GDYE Version 3.17 software were released within a short period of time, supposedly to address the problems pointed out by critics. Due to the presence of multiple GDYE Version 3.17 packages, it is possible that the results presented here may not be reproducible in other packages.

This section describes our analysis of the installation and behavior of GDYE. Installation analysis involved the identification of all the changes

Table 1. MD5 and SHA-1 values for the two GDYE versions.

Version	Function	Hash Value
3.17_000	MD5	d31aa54dcc339ecdee300c35107f2555
3.17_000	SHA-1	4aaa6cec69b4dfd952eda3512a0b45c1f34a0f7c
3.17_001	MD5	548c2d2cf32d50a47c69faa8a7640258
3.17_001	SHA-1	ee93d0ead4982b53d489b4766d6f96e7618fcd6e

made to the system during the installation of an official copy of GDYE in the testing environment. Behavioral analysis involved the study of the dynamic behavior of GDYE with emphasis on its supposed censorship and spying functions.

4.1 Installation Analysis

This section describes our GDYE installation procedures and the results of the installation analysis.

GDYE Software Versions GDYE Version 3.17 was the first one analyzed by the public. As mentioned above, a number of problems were reported [10]. Version 3.17 was then removed from the official website and was no longer available for public download. For our evaluation, we obtained the original GDYE Version 3.17 (v. 3.17_000) from a PISA member in Hong Kong. We also evaluated an updated version of GDYE (v. 3.17_001), which we downloaded from the official web site on June 19, 2009.

Upon checking the MAC times and file sizes under file properties, we discovered that v. 3.17_000 with a size of 10,355,637 bytes was modified and accessed on Tuesday, June 9, 2009 at 11:55:10 am. On the other hand, v. 3.17_001 with a size of 10,200,230 bytes was modified and accessed on Saturday, June 13, 2009 at 8:02:38 am. Following standard digital forensic procedures, we calculated the MD5 and SHA-1 hash values for the two GDYE versions (Table 1) and saved them for future reference.

Analysis Environment We set up a specialized, controlled malware analysis environment to test the installation and monitor the behavior of GDYE. The laboratory environment, shown in Figure 1, used the malicious Windows executable (MWC2008) [3]. The Linux version Ubuntu 2.6.28-11-server was used in the Safegate.

The iptables configuration was set to allow DNS to pass through to the Safegate. For Bind9, the query logging functionality was added

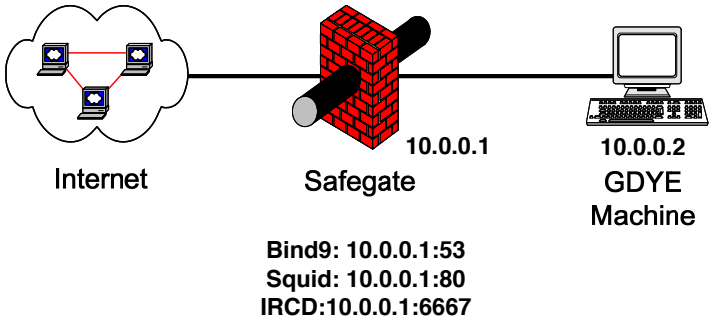

Figure 1. GDYE analysis environment.

to the `named.conf` configuration file. Windows XP SP2 was installed on the GDYE machine without additional patches. Several monitoring and analytical tools, including Autoruns, RegShot and Wireshark, were installed.

Changes During Installation Upon using the RegShot and Autoruns tools, we discovered that the installation process added and modified some Windows registry entries and added files to the %WinDir% folder for XP at C:\Windows and to the %WinSysDir% folder for XP at C:\Windows\system32. By removing some of the prefdata files (i.e., temporary performance-related files created by the Windows system during installation), temporary files and some other unimportant files (e.g., screen files and temporary logs), we found that v. 3.17_000 added 119 files to the system while v. 3.17_001 added 84 files.

An analysis of the Windows registry revealed that both GDYE versions added and modified the same registry keys and values, which allow the automatic loading of the driver (`mgtaki.sys`) and services (`MPSvcC.exe` and `Hnceng.exe`). GDYE also modified the registry key with a filter called `dbfilter.dll` (HKLM\System\CCS\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries). This registry key is frequently used by spyware and malware of WinSock hijackers, which is referred to as the Layered Service Provider (LSP) [9]. It is well known that if LSP is not registered properly or if the LSP is buggy, the WinSock catalog in the registry could be corrupted and the computer would no longer be able to access a network. This could be the reason why some GDYE users claim that they lose their Internet connections after unloading the software.

Upon checking the setup file `xstrings.s2g` in the C:\Windows folder with a text editor, we found all the installation paths used by GDYE, which was consistent with the findings in [1]. When we analyzed the bi-

Table 2. Modified files.

Name	Version	Modified Time	Created Time	Size
adwapp.dat	3.17_000	4/27/09 6:26:08 am	4/27/09 6:26:08 am	223,572
adwapp.dat	3.17_001	6/10/09 1:33:26 am	6/10/09 1:33:26 am	223,674
dbfilter.dll	3.17_000	5/22/09 12:47:38 am	5/22/09 12:47:38 am	57,344
dbfilter.dll	3.17_001	6/9/09 8:57:06 pm	6/9/09 8:57:06 pm	57,344
FalunWord.lib	3.17_000	5/12/09 3:36:14 am	5/12/09 3:36:14 am	5,564,613
FalunWord.lib	3.17_001	6/12/09 7:18:36 am	6/12/09 7:18:36 am	5,564,271
HncStdRun.ini	3.17_000	7/19/09 10:43:05 am	7/19/09 10:43:05 am	22
HncStdRun.ini	3.17_001	8/2/09 7:18:36 am	8/2/09 7:18:36 am	22
Surfgd.dll	3.17_000	4/24/09 2:59:36 am	4/24/09 2:59:36 am	126,976
Surfgd.dll	3.17_001	6/13/09 6:26:32 am	6/13/09 6:26:32 am	131,072
XNet2.exe	3.17_000	5/22/09 5:01:48 am	5/22/09 5:01:48 am	667,648
XNet2.exe	3.17_001	6/13/09 7:02:28 am	6/13/09 7:02:28 am	667,648
xnet2_lang.ini	3.17_000	7/19/09 11:00:17 am	7/19/09 11:00:17 am	7,748
xnet2_lang.ini	3.17_001	8/2/09 7:18:34 am	8/2/09 7:18:34 am	6,842

naries using IDA Pro, we discovered that `XDaemon.exe` and `gn.exe` were not started by the operating system, but by the main process `Xnet2.exe`.

GDYE Version Comparison As mentioned above, a new version of GDYE (v. 3.17_001) was released soon after the first version (v. 3.17_000). The main problems addressed in the new release include the web filtering security vulnerability, the blacklists copied from the CyberSitter program, and the OpenCV license violation. The HashMyFiles tool was used to identify the files that were updated and removed between the two versions. Our analysis revealed that seven files were modified (Table 2) and 35 data files were removed.

Upon checking the modification times of the files, we discovered that the majority of the changes were made between June 9, 2009 and June 13, 2009. The timing of these changes is a strong indicator that the software was modified in response to the public criticism after GDYE's initial release.

To verify the assumption that the removed files were copied from CyberSitter, we conducted an analysis of the data files after applying decoding scripts. We discovered that all the data files that were eliminated in the new version – except for `xwordh.dat`, `xwordl.dat` and `xwordm.dat` – were associated with CyberSitter [10].

4.2 Behavioral Analysis

This section describes our GDYE behavioral analysis procedures and the results of the analysis.

Figure 2. Configuration page.

Filtering GDYE provides three types of filtering functionality: (i) website filtering based on URLs; (ii) image filtering; and (iii) text filtering. It filters most of the popular pornographic and obscene websites (e.g., www.playboy.com, www.sex.com and www.angelteen.com). However, the software administrator can access the configuration page (Figure 2) and add URLs to the whitelist and override the blacklisted URLs. In most cases, the web browser does not display HTML status codes and messages to indicate that a blacklisted URL has been blocked.

GDYE is designed to filter pornographic images. We observed false positive and false negative errors, but no meaningful statistics were obtained with respect to filtering performance. Nevertheless, we discovered that GDYE tends to filter pornographic images that contain light flesh tones rather than dark flesh tones. The software administrator may turn off the image filter function in the configuration page.

GDYE also filtered politically-sensitive phrases such as "June 4 Massacre," "Falun Gong," "Master Li Hongzhi" and "Evil Jiang." When these phrases or others are typed into Microsoft Word or Notepad, GDYE kills the process, which forces the application to crash, causing unsaved work to be lost. We discovered that the time taken for the applications to crash is relatively unpredictable. In some cases, the application does not close immediately after the politically-sensitive phrases are typed, but may close at some point in the future. Note also that the

software administrator is unable to access, modify or delete the blacklisted terms.

GDYE also force-closed Internet games such as Warcraft at various stages of game initialization. The software administrator may use the configuration page to restrict Internet connections during specific time periods.

Version Update The software administrator may use the configuration page to manually start the GDYE update process. The DNS query logs indicate that the official GDYE website was accessed during the update process. Wireshark logs showed that the files `kwdata.dat` and `winet.dll` were downloaded.

After performing the download, the update process starts automatically and asks for permission to reboot the system. We discovered that the system did not modify or create new keys/values in the Windows registry. Also, several files were modified or removed when updating GDYE v. 3.17_000 to GDYE v. 3.17_001.

Uninstallation An uninstallation option is not provided under the Windows control panel. However, the software administrator may use the configuration page to "unload" the software. Most of the files and folders are removed during uninstallation, except for the driver file `mgtaki.sys` and two folders at C:\Windows\snap and C:\Windows\log. The Internet can be accessed in a normal manner after uninstallation, which indicates that the WinSock SPI registry was handled properly by the uninstallation process.

Spyware and Malware Behavior Additional testing of the malware and logging functionality was performed using Wireshark, FileMon, Regmon and TCPView. The following results were obtained:

- **Snapshots:** GDYE creates screen snapshots in JPEG format every three minutes by default. The snapshot files are saved in the folder C:\Windows\snap. Interestingly, no files are displayed when viewing this folder using Windows Explorer, but issuing a `dir` command under the command prompt will display all the JPEG files. However, if the files are copied to another folder under the command prompt, Windows Explorer can display them without difficulty. All the JPEG files are removed when GDYE is uninstalled.

- **Logging:** Log files are stored in plain text format in the folder C:\Windows\log. As with the snapshots folder, no information is

Figure 3. Standard image displayed when something is filtered.

displayed by Windows Explorer, but the command prompt can be used to copy and display the log files. Also, the files can be viewed using Windows Explorer when they are copied to another folder. However, the log files are removed when GDYE is uninstalled.

- **Pop-Ups:** GDYE does not generate unwanted pop-ups. In some cases, however, GDYE displays the standard image shown in Figure 3 when text is filtered.

- **URL and Text Filtering:** GDYE performs its filtering functions through a WinSock SPI using the `dbfilter.dll` file. It does not display filtered information, but instead displays a normal HTTP message code (402) or performs a TCP reset to the accessing server without sending a message to the browser client. Thus, the user is not notified when an accessed URL has been filtered by GDYE.

- **Connections to External IP Addresses:** Wireshark was used to monitor TCP packets for four 24-hour periods. No Internet activities were seen, except for time synchronization UDP packets sent to the NIST time servers. Also, no obvious Internet transmissions were discovered during the test periods. However, two suspicious IP addresses, `211.161.1.134` and `203.171.236.231`, were found when decoding `XNet2.exe` with IDA Pro. Program messages reading "Preparing to registerK" were found a few bytes after the

IP address `211.161.1.134`, and the message "Report successful" was found two jump blocks after the IP address `203.171.236.231`. Additional tests were performed to check if any actions triggered these two sections of codes, but no network activity related to these IP addresses was discerned in the Wireshark captures.

- **Keystroke Logging:** Upon monitoring the FileMon logs and comparing the changes at different time periods using RegShot, no key logging files were discovered and no files appeared to have been created.
- **Software Uninstallation:** An uninstall option is not provided in the control panel or under the program menu. However, GDYE can be uninstalled from the configuration page by the software administrator. As mentioned above, some folders and files remain in the file system after uninstallation. In addition, one driver was left in the file system.
- **Killing Processes:** Similar to normal malware, the key processes `XNet2.exe`, `XDaemon.exe` and `gn.exe` are protected by handles pointed to each other. When one process is killed, one of the other processes starts up and spawns the killed process as a sub-process.
- **File Modification:** No files were modified in a stealthy manner during our tests.

Vulnerabilities and Exploits Internet Explorer crashed when the system running GDYE was tested against two web filtering vulnerabilities. Two exploit scripts, "Green Dam 3.17 (URL) Remote Buffer Overflow Exploit (XP/SP2)" and "Green Dam Remote Change System Time Exploit," were also tested. The first exploit caused Internet Explorer on the system running GDYE v. 3.17_000 to crash and `calc.exe` to be executed. The second exploit changed the time on the system.

5. Conclusions

Our analysis of GDYE has confirmed most of the concerns about its filtering functions. Our reverse engineering studies indicate that the text filtering function, which is monitored by `injlib32.dll`, force-closes certain applications when blacklisted text is entered; as a result, data loss is unavoidable.

GDYE maintains snapshots and web surfing logs. Any user with the appropriate system permissions can access the information contained in the snapshots and web surfing logs via the command prompt. The web surfing logs are retained in the system folder even after uninstallation.

Also, an individual who knows the magic password can access these logs "legitimately" via the configuration page. While a digital forensic examiner would be delighted to access these logs during an investigation, this aspect of GDYE raises significant privacy concerns. A system running GDYE appears to be vulnerable to custom scripts that inject shell code or exploits, which could incorporate the system in a botnet. Thus, the first hypothesis is proven to be true – GDYE will lead to loss of private information.

However, our tests did not find any evidence of keystroke logging or instances of GDYE transmitting information surreptitiously over the Internet. Although two IP addresses were found in the binary `XNNet2.exe`, no obvious TCP or UDP connections were established to these addresses during our tests. The mere presence of IP addresses in a binary does not necessarily imply that a malicious act was intended. Therefore, our tests do not confirm the critics' concerns that GDYE is designed to collect private information from users and pass it on to centralized servers for unknown purposes. Thus, the second hypothesis must be rejected. Nevertheless, we cannot rule out the possibility that the software will not be modified in the future to implement the collection and forwarding of private information.

References

[1] Anonymous, A technical analysis of the Green Dam Youth Escort software (docs.google.com/View?id=afk7vnz54wt_12f8jzj9gw), 2009.

[2] Anonymous, Green Dam Youth Escort Testing Report (www.meirendaddy.com/blog/?p=404), 2009.

[3] E. Bastuz, Malware Challenge 2008: Behavioral analysis of a malicious Windows executable (www.emre.de/wiki/index.php/MWC2008), 2008.

[4] J. Cui, X. Wang and X. Cui, Plug not pulled on Green Dam, *China Daily*, Beijing, China (www.chinadaily.com.cn/china/2009-07/02/content_8344967.htm), July 2, 2009.

[5] Dazheng, About Dazheng, Beijing, China (hncit.com/about_us.html).

[6] R. Faris, H. Roberts and S. Wang, China's Green Dam: The implications of government control encroaching on the home PC, Bulletin, OpenNet Initiative, Oxford, United Kingdom (opennet.net/sites/opennet.net/files/GreenDam_bulletin.pdf), 2009.

[7] Jin Hui, About Jin Hui, Zhengzhou, China (www.zzjinhui.com/qyjj.html).

[8] Ministry of Industry and Technology, MITT announcement, Beijing, China (www.miit.gov.cn/n11293472/n11293832/n11293907/n11368223/12433840.html), June 30, 2009.

[9] H. Wei, J. Ohlund and B. Butterklee, Unraveling the mysteries of writing a WinSock 2 Layered Service Provider, *Microsoft Systems Journal* (www.microsoft.com/msj/0599/LayeredService/LayeredService.aspx), 2009.

[10] S. Wolchok, R. Yao and J. Halderman, Analysis of the Green Dam censorware system, Revision 2.41, Computer Science and Engineering Division, University of Michigan, Ann Arbor, Michigan (www.cse.umich.edu/∼halderm/pub/gd), 2009.

[11] S. Young, A. Lai, I. Mao, C. Mok, T. Tsang and F. Li, Dissection of Green Dam, presented to the Professional Internet Security Association, Hong Kong, 2009.