FDR FORENSIC DATA RECOVERY INC.

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

Analysis of AMS Elections 2010

Voting System

CaseID: 82104

Report Prepared by:

Dean Krenz

Senior Associate, Digital Forensics and eDiscovery Services

FDR Forensic Data Recovery Inc.

FDR FORENSIC DATA RECOVERY INC.

Table of Contents

FDR FORENSIC DATA RECOVERY INC.

Background

FDR Forensic Data Recovery Inc. was retained by the Alma Mater Society of UBC Vancouver (AMS) to provide forensic preservation and analysis of the AMS Elections 2010 online voting system.

Summary of Findings

After having forensically preserved the subject voting system server data, subsequent digital forensic analysis revealed a major security vulnerability within the Elections 2010 voting system (a web-based student voting application and database), and it appears that this vulnerability was exploited during the Elections 2010 vote.

Additional details regarding these findings can be found in the *Impact Assessment* section of this report.

1. Analysis has revealed that on January 29, 2010 between 12:44:33 PM and 16:00:00 PM, 731 votes[1] were submitted from a single IP address (the "IP Address").

2. Two anomalies were found in the database that provide evidence the system was exploited:

    a. Of the 731 votes cast during this time period from this IP address (one vote per student number), 18 votes contain ineligible student numbers. As ineligible student numbers cannot normally cast votes successfully through the normal process, the fact that 18 votes were cast using ineligible student numbers is an indication of fraudulent activity.

    b. Of the 731 votes cast during this time period from this IP address, two hidden fields on the Board of Governors vote section received votes, although there are no candidates associated with the two hidden form fields. This evidence suggests that votes were received and processed through a different channel than the normal voting process.

[1] For the purposes of this document, a vote is defined as one student's ballot selections in the 2010 election, which included each of the individual elections and referenda conducted using the Elections 2010 voting system.

3. The available evidence suggests that only the notable IP address was used to exploit the voting system, as it was the only IP Address used to generate a multitude of votes by bypassing the normal vote process.

4. The available evidence confirms that a vote submitted through the exploit would not delete or modify a vote that was previously submitted by a student with the same student number. No submitted / cast votes made by students via the normal vote process were deleted, overwritten, or modified as a result of the exploit. If a vote submitted via the exploit used the same student number as a student that had already submitted a vote, the exploit vote was rejected, leaving the original student vote intact.

5. The available evidence confirms that a vote submitted through the exploit could overwrite a student vote in the situation where a vote submitted by the exploit used the same student number as a student that previously saved but did not submit their vote. In other words, a saved vote could be overwritten if one of the fraudulent votes happened to have the same student number as a saved vote. There is no available evidence to suggest that the student numbers used in the exploit were harvested for the direct purpose of overwriting existing saved votes. There is available evidence that 15 saved votes were overwritten as a result of the exploit. The 15 overwritten votes occurred at random intervals during the timeframe of the exploit.

6. The origin of the student numbers used in the exploit has not been determined. However, there are lists of student numbers readily available to the public on various UBC websites.

FDR has performed no analysis on the candidate choices and selections of the notable 731 votes.

Further, FDR has undertaken no analysis on the attributes of the notable IP address.

Vote Submission Process

The following section provides an overview of the online voting process using the AMS Elections 2010 voting system.

Authentication and Authorization

Students enter the voting system via the main AMS home page. Students must then authenticate themselves to the voting site through the UBC Campus-Wide Login (CWL) security portal. The CWL security portal provides two important functions:

- Authentication – this is the process of confirming the visitor's identity. When a visitor accesses an application secured by CWL, the visitor must enter their username and password so that CWL can verify their identity.

- Authorization – Once the visitor has been authenticated, they must be authorized to access the voting application.

Through normal process, students that fail either the authentication or authorization checks are not able to proceed to the vote selection page.

Eligibility

Once a valid student is authenticated and authorized, the student number provided by CWL is passed back to the AMS voting system, which stores the student number for future use. The voting system also checks that the student number exists within the list of eligible student numbers (defined as the list of student numbers within the 'eligible' or 'international' tables in the elections database). If ineligible, the student is not able to proceed to the voting selection page and is returned to the CWL login page.

Vote Selection and Submission

If the student is found to be eligible to vote, the student can submit only one vote. The system checks to see if the student has already submitted a vote, and if so returns the student to the CWL login page.

Eligible students who have not yet submitted a vote are then presented with the vote selection / ballot page. At this point, the student can click on the various check boxes and drop-down selections of candidates and questions on the electronic ballot, and then either save or submit their vote.

Submitted votes are cast and cannot be revised by the student at a later date. Once submitted, the student is presented with page of poll questions, and then returned to the CWL logon page. Once the vote is submitted, the system will prohibit the student from going back to the vote selection page. However, the system does allow students to save a vote without submitting it, and return to the saved vote at a later date to finalize their selections and submit their final vote selections at that time.

Vulnerability

By reconstructing and simulating the Elections 2010 system within the FDR lab, we were able to reproduce the security vulnerability. We are able to demonstrate that an eligible student could exploit the voting system and submit an unlimited number of votes on behalf of any other student number, including ineligible student numbers.

Several vulnerabilities were found on the vote selection and processing page.

a) The vote selection page uses a hidden HTML element to store the student number that is received by the CWL login process. Because the HTML element is a 'hidden' field, the student number is not displayed on the vote selection page as rendered by a web browser. However, `student number` is a form field element of the page and displayed in plain text within the source HTML file, therefore exposing the field and the student number value to potential data integrity issues.

b) At the point of submission, the system does not verify, authenticate, or determine eligibility of the student number used on the vote against the actual user submitting the vote.

Exploit

The source HTML code from the vote selection page can be used to exploit the student number vulnerability. The exploiter can easily create a cloned version of the vote selection page, and because the student number is in a form field, the exploiter can change the value of the student number within the cloned version. The exploiter could then submit a fraudulent page of vote selections to the AMS server, and the vote selections would be committed to the vote total database. The exploiter could submit an unlimited number of votes by simply inserting different student numbers into the cloned page and submitting the page to the AMS server. This process can be easily automated, resulting in fraudulent votes being submitted on a very frequent basis (approximately 1 per second).

Impact Assessment

On January 29, 2010 between 12:44:33 PM and 16:00:00 PM, 731 votes were submitted from one IP address.

1. This volume of votes equates to an average of approximately one vote every 16 seconds for the time period, although the actual vote submissions are not timed consistently. In many cases, votes were submitted 6 to 10 seconds apart.

2. Two anomalies were found in the database that provide evidence that the system had been exploited:

    a. Of the 731 votes (one vote per student number), 18 votes contain ineligible student numbers, which suggests fraudulent activity, because an ineligible student can not normally submit a vote through the vote process and security provisions. 18 student numbers were found in the submitted votes table, but these student numbers are not found in the eligible or international student number tables.

    b. The database contains another data integrity anomaly that is not possible through the normal voting process. Of the 731 votes cast during this time period from this IP address, two hidden fields on the Board of Governors vote section received votes, although there are no candidates associated with the two hidden form fields. This evidence suggests that votes were received and processed through a different channel than the normal voting process.

    Within the University Board of Governors ballot section of the voting page there are four hidden fields that are not displayed – board1, board2, board4, and board8. There are no candidates associated with these fields, and these fields would not be displayed when viewed by a web browser. Although the fields exist on the form and in the database, they were not used during the elections 2010 process. However, within the database, there are 58 votes where board2 has been selected and 75 votes where board8 has been selected. All of the board2 and board8 selections in the entire database were submitted from the same notable IP address. The existence of data content in these two database fields indicates that form data (ultimately vote selections) has been altered and submitted outside of the normal vote submission process.

3. The available evidence suggests that only the notable IP address was used to exploit the voting system, as it was the only IP Address used to generate a multitude of votes and bypassed the normal vote process.

4. The available evidence confirms that a vote submitted through the exploit would not delete or modify a vote that was previously submitted by a student with the same student number. No submitted / cast votes made by students via the normal vote process were deleted, overwritten, or modified as a result of the exploit. If a vote submitted via the exploit used the same student number as a student that had already submitted a vote, the exploit vote was rejected, leaving the original student vote intact.

5. The available evidence confirms that a vote submitted through the exploit could overwrite a student vote in the situation where a vote submitted by the exploit used the same student number as a student that previously saved but did not submit their vote. In other words, a saved vote could be overwritten if one of the fraudulent votes happened to have the same student number as a saved vote. There is no available evidence to suggest that the student numbers used in the exploit were harvested for the direct purpose of overwriting existing saved votes. There is available evidence that 15 saved votes were overwritten as a result of the exploit. The 15 overwritten votes occurred at random intervals during the timeframe of the exploit.

   The analysis of overwritten votes was based on a comparison between a backup of the database performed on January 28 at approximately 11:00pm (Jan 28), and the final vote database taken at the end of the voting period on January 29 at approximately 4:15pm (Final). No other database backups were performed between January 28 and January 29.

   Note: It is possible that a new vote, saved by a student between January 28 11:00pm and January 29 4:00pm, may have been overwritten during the exploit. It is not possible to determine, from the available data, the number of votes actually affected in this scenario.

   <u>Totals:</u>
   As at Jan 28 there were a total of 510 saved votes.
   As at Final there were a total of 562 saved votes.

   <u>Jan 28 Saved, Final Submitted:</u>

There were 77 votes that were saved as of Jan 28, but were subsequently cast / submitted by Final. 15 of the 77 were from the set of notable 731 votes. 62 votes were not part of the exploit. 15 student numbers had their saved votes overwritten by the exploit.

Jan 28 no vote, Final Saved (net new):
There were 129 net new saved votes as of Final that did not exist at Jan 28. In other words, 129 students signed on and saved a vote between Jan 28 and Final.

Jan 28 Saved, Final Saved:
There were 433 votes that were saved Jan 28 and were still in saved status at Final. 5 of the 433 were modified between Jan 28 and Final, and remained in saved status at Final.

6. The confirmed origin of the student numbers used in the exploit has not been determined. However there are lists of student numbers readily available to the public on various UBC websites. For example, 649 of the 731 (89%) student numbers used in the exploit can be found in the following course grade document:

   http://econ.arts.ubc.ca/lemche/academic_f09/webfiles_f09/test%20grades.pdf

   This document was located by performing a Google search using "UBC" and several of the 731 notable student numbers as search terms.

Recommendations

The scope of our analysis and resulting recommendations is limited to the technical details regarding application security and processing by the AMS voting system.

A. Hidden form fields should not be used for user identification attributes.

B. Additional security controls should be incorporated into to the voting system to ensure that authenticated users cannot submit votes on behalf of other students.

C. Additional data integrity controls should be incorporated into the voting site as a means to catch and log irregularities, and provide immediately alerts to elections staff. Logging should include additional user identification information that would support investigation and follow-up.

D. No backup versions of the elections database were located on the server, and no scheduled backup process was found. A scheduled daily backup process must be implemented and the backup must include the elections database files.

E. Authentication by the CWL site appears to occur only once at the point of initial login. The CWL application security is not responsible for monitoring http and https domain requests, therefore the web application and the server are vulnerable to a number of different security attacks. Overall security of the server and web application must be reviewed and hardened where necessary.

F. The Elections 2010 server also contains a sub-site named Electionstest. There are several potential security vulnerabilities related to the Electionstest site, specifically the phpMyAdmin administration system, which provides complete database control and could be exploited.

G. Upon review of various audit and security logs, there is evidence to suggest that the voting system is the subject of security attacks from time to time. In order to provide effective countermeasures, the overall security of the server should be reviewed and hardened where necessary.

H. System vulnerabilities should be corrected and tested before the voting system is used again.