HARBOR LABS

SOFTWARE & NETWORKING EXPERTS

Evaluation of the MarkMonitor AntiPiracy System

March 3rd 2014

Executive Summary

In July 2011, certain copyright owning entities, including the MPAA and the RIAA and their member companies entered into a Memorandum of Understanding (MOU) with the five leading U.S. internet service providers to create the Copyright Alert System (CAS) as a way to reduce copyright infringement. Under the rules of the CAS, those member content owners retained MarkMonitor to identify instances of alleged copyright infringement and pass notices on to ISPs in the form of copyright notices. To do this work MarkMonitor users their automated AntiPiracy system and tracks file sharing within peer-to-peer networks, detects apparent cases of copyright infringement and notifies ISPs of those alleged infringements. Pursuant to the MOU and at the request of the Center for Copyright Information (CCI), Harbor Labs conducted an independent review of the MarkMonitor AntiPiracy system and its use by the content owner members of the CAS. A prior independent review of the same automated anti-piracy system was conducted by the firm of Stroz Friedburg.

Neither the public nor CAS member content owners have any tolerance for false positives that lead to incorrect notices generated by MarkMonitor for the content owners. Therefore, we analyzed the MarkMonitor AntiPiracy system to evaluate if this system is likely to generate incorrect notices now or in the future. Our review focused on design, operational policies, and quality assurance policies. For sources, we used the provided technical documentation as well as interviews with technical staff. We did not review source code or conduct our own tests of the mechanism. We did, however, have access to test results conducted previously by Stroz Friedberg as part of their independent review conducted in the fall of 2012 prior to the launch of the CAS.

We conclude, based on our review, that the MarkMonitor AntiPiracy system is designed to ensure that there are no false positives under reasonable and realistic assumptions. Moreover, the system produces thorough case data for alleged infringement tracking. CCI has informed us that, to date, there are no known instances of this system generating incorrect notices, increasing confidence that the design of the system is sound.

However, even a system that is correctly designed can be implemented incorrectly or inappropriately used. While MarkMonitor does employ a quality assurance process that involves a significant amount of testing to increase confidence that the implementation matches the design, we believe that the system would benefit from additional testing and that the existing structure leaves open the potential for preventable failures.

Additionally, we recommend that certain elements of operational security be enhanced. In particular, while the evidence collection by the MarkMonitor AntiPiracy system is thorough, we believe that this collected evidence and other potentially sensitive data is not adequately controlled. While MarkMonitor does protect the data from outside parties, its protection against inside threats (e.g., potential rogue employees) is minimal in terms of both policy and technical enforcement.

Accordingly, we recommend the following:

- MarkMonitor should extend its testing to be more thorough. For example, in addition to their unit-tests, they should consider automated end-to-end tests with that actively attempt to cause a failure. Such tests are necessary to actively demonstrate that failures will be caught and handled correctly. Ideally, MarkMonitor should have their testing policy and implementation reviewed by outside experts in software reliability.
- MarkMonitor verifies that content is infringing by having a human review all newly identified content. However, given that this step underlies the entire correctness of the system, MarkMonitor should use two analysts to reduce the risks of accidental misidentification.
- MarkMonitor should be able to trace every step of the case-building and notification process in both a tamper-resistant and tamper-evident fashion. While tamper-resistance provides protections against data alteration, tamper-evident mechanisms, which reveal unauthorized changes, provide assurance that data has not been altered.
- MarkMonitor should implement additional internal security policies to protect collected data and any derivative metadata. These policies need to address issues such as which employees can access data, how long data will be retained, how data will be destroyed, and how data is adequately protected from theft. MarkMonitor needs to ensure that employees are properly trained in these policies and that policies are appropriately monitored, adequately enforced, and regularly updated.

In conclusion, the MarkMonitor AntiPiracy system has been designed with accuracy in mind, and our review suggests that it is and has been functioning within the established parameters. The continued successful operation of the system, as well as assurance of data security and customer privacy, will depend to a large extent on the implementation of these recommendations.

It is our belief that stable operation has been reached for the MarkMonitor AntiPiracy system, and that the achievement of more defensible and correct handling of security and report generation is straightforward.