Content Quotation Security

The Lix Security Model is a state of the art digital rights management platform which protects any copyrighted content made available through Lix from being tampered with, or extracted and illegally distributed.

This level of content security is achieved through a combination of cryptography and user-behaviour monitoring. Additional information about the Lix Security Model (LSM) and how the Lix Platform protects the digital content rights of our publishing partners can be found in our white paper, Content Delivery Security.

This white paper presents a methodology which builds on the foundation of the Lix Security Model. Our methodology protects all digital content available on the Lix Platform from unauthorised distribution, whilst our technology continues to allow paragraph-sized quotations to be exported from the platform.

Student expectations when quoting published content

When working with physical books, students often use markers to highlight relevant or interesting paragraphs of text. Often these extracts are copied and incorporated into assignments to support specific claims or add weight to an argument.

When using digital books, students expect to be able to copy the text directly from the book and paste it into their text editor, as they would do when citing an article on Wikipedia or a journal article in PDF format.

In addition to supporting paragraph sized copying, we enable students to accurately cite these abstracts in a variety of different styles, including APA, MLA and Harvard.

At Lix, the needs of students are paramount to the technology we develop, and offering the facility to copy and paste extracts from books is essential. However, such a feature cannot compromise the security of our publishing partners' digital content. Any copy feature needs to protect publishers from the activities of malicious users seeking to create illegal pirated copies of digital books.

Content security engineers at Lix have designed a set of algorithms that ensure the copy feature can't be used maliciously, whilst still providing the flexibility students need to help them in their day-to-day work.

Content Quotation Security Algorithm

The basis of the Content Quotation Security (CQS) algorithm is a number of parameters that specify how much text a student is allowed to copy. If a student tries to copy a piece of text that exceeds any of these parameters, the copy function is prevented. The parameters are as follows:

- The total character count of copied text within a book cannot exceed 5% of the total character count of that book.
- The total character count of copied text within a chapter cannot exceed 10% of the total character count of that chapter.
- The total length of any copied content cannot exceed 200 words. If the highlighted text to be copied exceeds 200 words, only the first 200 words will be copied.
- The total length of consecutive copies cannot exceed 600 words. If four 200-word highlights are placed one after the other, the fourth highlight cannot be copied.
- A spacing of at least 50 words must exist between the consecutive highlights in order to cancel the above-mentioned 600-word limitations.

When a student copies a piece of text, this is registered as a user-behaviour action. This means we can guarantee that any one student cannot break the above-mentioned parameters. The user-behaviour is also an input in the Lix Security Model system to facilitate fraud detection.

The Lix Security Model and CQS

Within the LSM, we already monitor for suspicious scrolling activities that indicate systematic scrolling which could be performed by automatic screenshot tools. With the addition of the CQS algorithm, we are able to carry out cross-user fraud detection by monitoring for users that might co-ordinate copying in order to break the 50-word spacing rule.

This behavioural activity information, in addition to activity about inter-student connections, allows us to detect fraud with a high degree of certainty. If any fraudulent activity is detected, a Content Security Engineer at Lix is immediately notified and performs a security review to determine if an attempt at malicious usage has occurred.

Conclusion

By pairing the existing Lix Security Model with our Content Quotation Security algorithm, we are able to provide a state-of-the-art digital rights management solution to our publishing partners, whilst ensuring students have the flexibility they need in their day-to-day work.