Content Delivery Security

Protecting all digital content hosted on and distributed via the Lix platform from tampering is crucial to our core business and that of our publishing partners.

The Lix Security Model (LSM), consists of several layers of protection against digital theft and uses technologies such as cryptography, content-streaming and user-behavioural fraud detection algorithms to deliver a state-of-the-art digital rights management solution. Third party experts at different publishers, aggregators such as Gardners and CoreSource have verified and approved our security methodology.

This white paper gives a brief introduction to each of the different security layers and outlines the process from initial content retrieval to end-user delivery.

Initial content retrieval and storage

When our publishing partners wish to offer digital content via the Lix platform, they first deliver the raw content to us by uploading a book over an encrypted FTP or HTTP connection. This ensures that the content cannot be intercepted by any adversaries whilst in flight.

Once retrieved by Lix, the content is stored and automatically processed on machines which can only be accessed by our software engineers who have security certificates installed on their machines.

End-user content delivery

In order to facilitate content streaming and more granular security, each book is broken up into multiple smaller parts during the initial content retrieval process. When a user wishes to read a book, only a few of its constituent parts are requested and made accessible at any one time, preventing the entire book from being copied or printed.

Furthermore, each of the parts are encrypted with a unique key per user-book-session as they are delivered to the reader device. This prevents an adversarial user from utilizing network inspection to intercept and automatically combine each of the smaller parts.

User behaviour monitoring

Any action that a user performs on the Lix platform - from scrolling through a book, to highlighting, copying and taking notes - is seamlessly recorded and monitored, making a wealth of user-behaviour data available on the LSM for real-time analytics.

While a user-book-session is in progress, we detect any malicious patterns in activity - such as systematic paging and copying of content - which automatically flags the user for inspection by our security team.

When the user is operating in offline mode, all activities are securely stored and sent to us. When the same user later connects to the Lix platform, the analysis is performed and automatic fraud detection occurs.

Our unique user-behaviour algorithms monitor and analyse simultaneous sessions, allowing the Lix platform to detect usage from different devices at the same time, which is likely to indicate account-sharing.

Conclusion

The Lix Security Model provides end-to-end digital rights management for all content hosted on the platform, ensuring seamless piracy protection for all our partners and end-users.

Furthermore, our real-time user-behaviour fraud detection technology automatically notifies Lix security engineers of any malicious activity, enabling swift action against adversaries trying to infringe upon our partners' copyright.