December 13, 2017

Automatic context-based alerts for content sharing

Matthew Sharifi

Jakob Foerster

Automatic context-based alerts for content sharing

ABSTRACT

This disclosure describes techniques for automatic detection of unintentional sharing of content. A user attempt to share content, e.g., from a clipboard via a paste operation, is detected. With user permission, the clipboard contents and the context in which the content is being shared are analyzed to determine suitability of the content to the context. An alert is provided to the user upon detection that sharing the content is likely unintentional.

KEYWORDS

- Clipboard
- Paste operation
- Operating system
- Messaging application
- User intent
- User context

BACKGROUND

Users often utilize copy-paste functionality on computing devices, e.g., mobile phones, tablets, computers, etc. Cut or copy functionality enables a user to select text from one application. The selected text is copied into a clipboard, and is inserted into a destination application when the user performs a paste operation.

One common destination for copied text is messaging apps that are used to share content with others. Users can accidentally paste text in a messaging app that is unsuitable or irrelevant to the conversation, e.g., when the clipboard includes such content. For example, the text can be private or sensitive, e.g., content from other messaging conversations, hyperlinks to personal

photos, passwords, etc. When such text (or other clipboard content) is sent to other parties in the messaging conversation, it leads to other parties potentially accessing such information.

DESCRIPTION

This disclosure describes techniques to automatically detect unintended content that is inserted into a messaging conversation (or other destinations) via a paste operation. The techniques are implemented upon specific user permission to access and analyze clipboard contents and/or content within a destination application. The techniques employ trained machine learning models and can be implemented within a messaging application, other software applications, or an operating system.

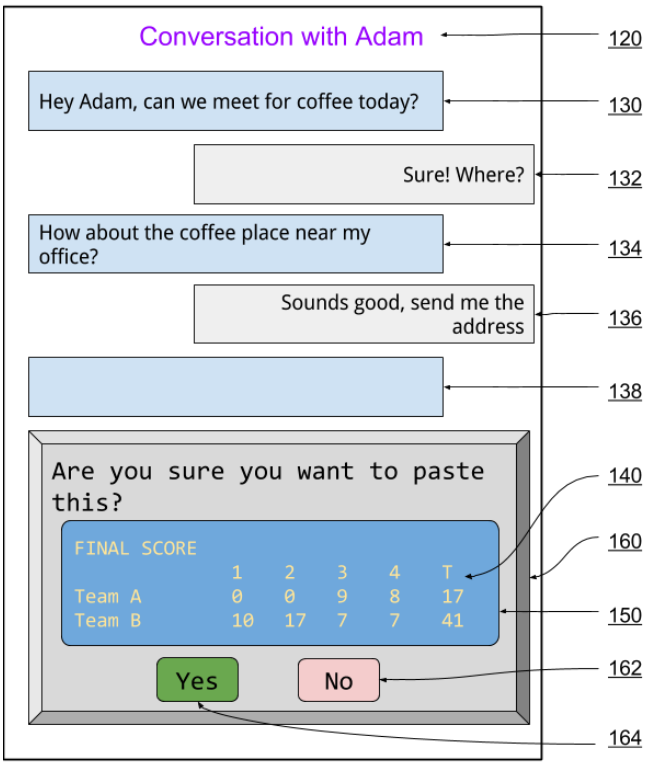

Fig. 1: Automatic alerts when sharing content

Fig. 1 is an example user interface that illustrates automatic detection of paste within a messaging application, in an example conversation (120) conducted using a messaging

application. After an exchange of messages (130, 132, 134, and 136), the user attempts to paste into the send box (138).

When the user provides permission for implementation of the described techniques, the clipboard contents and the conversation context are analyzed locally on the device using the trained machine learning model. Analysis of contents of the clipboard is performed to determine the type of the content and whether the copied content could be private. For example, when the clipboard content is a web address (e.g., a uniform resource locator (URL), the URL is analyzed to classify the underlying URL type, e.g., a photo album, a public news website, etc. In some instances, e.g., when there is a simple mapping from domain name to URL type, the URL need not be processed with a classifier. The model is trained using labeled examples from a variety of prior content (including potentially private content and other content) obtained with permission for use as training data.

Prior to an action being taken on pasted text, the current screen context and/or conversation context is also analyzed to determine whether the pasted content matches the context in which the text is being pasted. For example, if the context is a conversation with a work colleague, the model can determine that it is unlikely that a user would send a password or share a link to a private photo album.

The model is a binary classifier that predicts the likelihood of the paste content being relevant to the current conversation context. With user permission, the features or classification results from the copy model and the current conversation text are provided as inputs to the classifier. Other factors can be utilized for determination of whether a paste operation is unintentional, e.g., that the pasted content is unlikely. For example, a recent selection of a text

area by the user, without a corresponding copy action can be indicative of an unexpected paste. The context information of the paste event can be utilized to determine the intended paste target.

If the pasted content is deemed suited for the messaging conversation, the content is inserted into text box (138) and is available for sending in the messaging conversation. If the pasted content is determined to be an unintentional paste, a message or warning is provided in the user interface.

In the example illustrated in Fig. 1, it is determined based on analysis of the pasted content (140) that it is the score from a football game. Further, based on analysis of the messaging conversation (messages 130-136), it is determined that the conversation is about a location ("coffee place near my office"). When the user attempts to paste content, e.g., the box score from a football game (150), the warning (160) is provided to the user, along with options to continue (164) or cancel (162) the paste operation. When the content type is inferred, the warning can include the determined content type (e.g., URL, password, etc.)

When the described techniques are implemented in an operating system, the operating system can suggest a different field based on the paste action. For example, if a password is being pasted into a username field, the password field is recognized as a more suitable field and presented to the user as a suggested paste location.

Further to the descriptions above, a user may be provided with controls allowing the user to make an election as to both if and when systems, programs or features described herein may enable collection of user information (e.g., information about a user's social network, social actions or activities, profession, a user's preferences, or a user's current location), and if the user is sent content or communications from a server. In addition, certain data may be treated in one or more ways before it is stored or used, so that personally identifiable information is removed.

For example, a user's identity may be treated so that no personally identifiable information can be determined for the user, or a user's geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a user cannot be determined. Thus, the user may have control over what information is collected about the user, how that information is used, and what information is provided to the user.

CONCLUSION

This disclosure describes techniques for automatic detection of unintentional sharing of content. A user attempt to share content, e.g., from a clipboard via a paste operation, is detected. With user permission, the clipboard contents and the context in which the content is being shared are analyzed to determine suitability of the content to the context. An alert is provided to the user upon detection that sharing the content is likely unintentional.