Storage Covert Channels in fehlerkorrigierenden Block-Codes

Fehlerkorrigierende Block-Codes sind redundante Daten, die während einer Datenübertragung oder -speicherung dazu genutzt werden, um die Wiederherstellbarkeit der Daten zu gewährleisten. Eine erneute Übertragung ist dann beispielsweise nicht mehr notwendig.

Diese redundanten Daten können allerdings zum Verstecken und Übertragen geheimer Nachrichten missbraucht werden. Sogenannte Covert Channel sind Methoden der Übertragung, die eigentlich nicht zum Übertragen von Daten gedacht waren. Damit verletzen sie typischerweise Sicherheitsrichtlinien der Computersysteme, was dazu führt, dass geheime Daten auf Sicherheitsebenen mit sehr eingeschränkten Schreib- und Leserechten auf einmal von deutlich weniger sicheren Prozessen gelesen werden können.

Es wurde im Rahmen dieser Arbeit gezeigt, dass ein Covert Channel in fehlerkorrigierenden Block-Codes nicht nur theoretisch möglich ist, sondern ebenfalls bezüglich Robustheit, Bandbreite und Detektierbarkeit analysiert. Die Bandbreite hängt dabei sehr stark vom gewählten fehlerkorrigierenden Block-Code ab. Hier gibt es u.a. die Möglichkeit Hamming-Codes, wie in dieser Arbeit verwendet, BCH-Codes oder RSH-Codes zu nutzen. Tatsächlich ist die Implementierung eines Covert Channels in der Theorie auf allen gängigen fehlerkorrigierenden Block-Codes möglich.

Die Robustheit des Covert Channels sinkt mit schlechter werdender Übertragungsqualität bei der Datenübertragung. Ein wichtiger Faktor ist hier, dass natürlicherweise die Wiederherstellbarkeit aller Daten sinkt, je mehr Fehler auftreten – was wiederum bei geringerer Übertragungsqualität der Fall ist. Ebenfalls einen Einfluss hat die Reduktion und Manipulation der redundanten Daten, die normalerweise zur Widerherstellung der Übertragungsdaten genutzt werden. Im Zuge dessen reduziert eine höhere genutzte Bandbreite auch die Robustheit, da mehr redundante Daten für den Covert Channel und damit nicht mehr für die Datenwiederherstellung genutzt werden.

Die Detektierbarkeit des Covert Channels konnte mittels eines Naiven Bayes-Klassifikator bestätigt werden. Der Naive Bayes-Klassifikator wägt dabei für erhaltene Daten anhand ihrer vorhandenen Fehler ab, ob diese Daten eine geheime Nachricht enthalten oder nicht. Dabei wurden mehr als drei von vier Nachrichten immer richtig klassifiziert. Bei höherer Übertragungsqualität lag die Zahl der richtig klassifizierten Nachrichten sogar nochmal darüber.

Für den Covert Channel hat die Analyse der Robustheit und Detektierbarkeit aufgezeigt, dass es ein Optimum zur Geheimhaltung des Covert Channels ohne zu große Robustheitseinbüßen gibt. Es ist jedoch anzunehmen, dass ein gut angelegter und an Covert Channel in fehlerkorrigierenden Block-Codes speziell angepasster Klassifikator auch im optimalen Arbeitsbereich des Covert Channels eine hohe Detektierbarkeit aufzeigt.