Динамическое шифрование не предполагает загрузку расшифрованной сборки в память. Расшифровка частей сборки осуществляется по мере необходимости. Такой подход делает дамп малоинформативным, однако несет в себе достаточно большую сложность реализации и высокие накладные расходы ресурсов, вследствие чего его эффективное применение целесообразно для ограниченного количества критичных к защите от дизассемблирования участков программы. Данный тип защиты также несет в себе дополнительные уязвимости, вследствие чего основанные на нем алгоритмы следует использовать в совокупности с дополнительными средствами защиты, которые сами по себе достаточно сложны для реализации и не будут рассмотрены в рамках данной работы.

Предлагаемый подход основан на подходах с использованием шифрования. Преимущественно в его основе лежит статическое шифрование как компромиссный вариант (незначительные накладные расходы производительности, простота реализации и интеграции, приемлемый уровень защиты). Однако подход не несет в себе ограничений на тип шифрования и может быть легко адаптирован для использования динамического шифрования.

Платформа Mono 2.10.6 (как и ее более ранние версии), распространяемая с открытым исходным кодом, содержит богатые возможности встраивания в сторонние приложения, что позволяет тесно интегрировать ее с разрабатываемой .NET-программой, требующей защиты от декомпиляции. Непосредственно для обеспечения защиты код Mono должен быть подвергнут модификации, позволяющей платформе работать с зашифрованными сборками прозрачно для нее самой . Преимущество данного подхода также состоит в том, что при полном сохранении совместимости с Microsoft .NET (готовые .NET-сборки подвергаются постобработке) виртуальная машина, используемая в Mono, может быть достаточно сильно модифицирована, что создает дополнительную сложность при анализе кода злоумышленником. Данная возможность реализована в рамках предлагаемого подхода в совокупности с рядом методов по защите памяти от дампинга, нацеленных на снижение информативности получаемого дампа. Программное решение, реализующее предлагаемый подход, представляет собой модифицированную платформу Mono, а также программу-шифратор, выполняющую шифрацию .NET-сборок и их дополнительную модификацию, нацеленную на обеспечение контроля целостности в рамках предотвращения инъекций кода.

Выводы

Предложенный подход позволяет повысить эффективность защиты .NET-приложений от инъекций кода и обратной инженерии. Эффективность подхода подтверждена по результатам независимого аудита безопасности.

Тем не менее, как и любой другой подход в сфере информационной безопасности, предложенное решение не обеспечивает 100-процентной защиты, однако сильно усложняет процесс обратной инженерии и может быть рекомендовано для использования в проектах со средней стоимостью разработки.

С. Д. Кулик, Д. А. Никонец, К. И. Ткаченко, И. А. Лукьянов, Н. Е. Гунько

УСТРОЙСТВО ОПРЕДЕЛЕНИЯ РУКОПИСНЫХ ДОКУМЕНТОВ, ПРИНАДЛЕЖАЩИХ ОДНОМУ ИСПОЛНИТЕЛЮ

Практика убедительно показывает, что преступник практически всегда оставляет следы, например свой почерк. Существует средство ввода рукописного документа и перевода его в

электронный вид — цифровая координатная ручка PC Notes Taker, позволяющая получать как обычный бумажный документ с подписью руководителя, так и его электронную копию. Важным источником данных для криминалистических экспертиз и решения идентификационных задач является биометрическая информация. Биометрические системы, использующие рукописный текст, применяются не только для идентификации личности по почерку, но и для определения психологических характеристик.

Методика [1] позволяет установить исполнителя кратких рукописных текстов. Разработаны методики для установления пола и возраста исполнителя кратких рукописных текстов и создается новая методика для определения психологических характеристик личности по почерку. Принцип действия разработанных ранее методик одинаков: эксперту-криминалисту необходимо выявить признаки, найти сумму их весов, сравнить с заранее известным порогом и принять решение. В каждой методике приведены свои наборы весов, признаков и порогов.

Опираясь на опыт разработки устройств [2, 3, 4], для решения задач в области криминалистики совместно исследователями НИЯУ МИФИ и МГППУ было разработано новое устройство (рис. 1) для определения рукописных документов, принадлежащих исполнителю текста на русском языке.

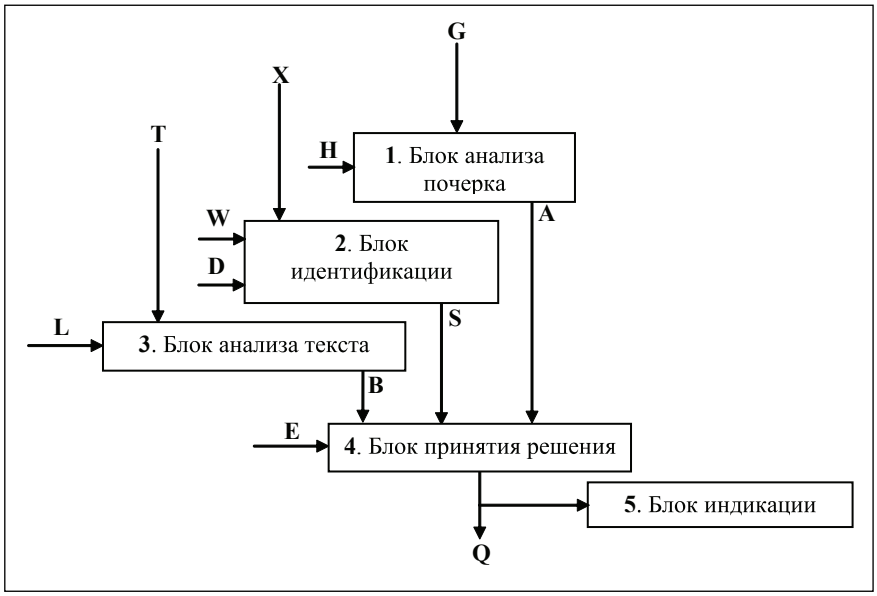

Рис. 1. Схема устройства

Предлагаемое устройство в виде полезной модели содержит: блок принятия решения, блок индикации, W — *вход весов*, D — *вход порога для идентификации*, X — *вход признаков*, E — *вход эксперта*, блок анализа почерка, блок идентификации, блок анализа текста, G — *вход параметров почерка*, H — *вход порога для анализа почерка*, T — *вход параметров текста*, L — *вход порога для анализа текста*, A — выход блока анализа почерка, S — выход блока идентификации, B — выход блока анализа текста, Q — выход блока принятия решения является выходом устройства. Более подробное описание работы данного устройства представлено в [5].

На предложенное устройство была подана заявка [5] в РОСПАТЕНТ на получение патента на полезную модель. По данной заявке было получено положительное решение экспертизы о выдаче истребуемого патента.

Дальнейшие исследования авторов связаны с разработкой других аналогичных устройств, а также с созданием эффективного средства эксперта-почерковеда. Активно выполняются работы в области разработки специальных генераторов и морфологического анализа. Ведутся исследования

для создания новой методики [6, 7], связанной с составлением психологического портрета личности (злоумышленника) на основе признаков почерка.

СПИСОК ЛИТЕРАТУРЫ:

1. *Кулик С. Д., Челышев М. М.* (от МИФИ), *Левицкий А. Б., Бажакин Г. А., Белоусова О. Д., Мурашова О. С., Колесова Е. Ю.* (от МВД). Методика вероятностно-статистической оценки совпадающих частных признаков почерка в прописных буквах русского алфавита: Справочное пособие. М.: ВНИИ МВД СССР, 1990. – 260 с.
2. *Кулик С. Д.* Патент на изобретение № 2208837, Российская Федерация (RU), кл. МПК[7] G 06 F 17/30. Устройство для имитационного моделирования значений функции выхода автоматизированной фактографической информационно-поисковой системы криминалистического назначения / С. Д. Кулик (Россия). Заявка № 2001129139/09; Заяв. 30.10.2001; Зарегистр. 20.07.2003; Приоритет от 30.10.2001; Опубл. 20.07.2003; Бюл. № 20. Ч. 3. С. 752–753. (РОСПАТЕНТ).
3. *Кулик С. Д.* Свидетельство на полезную модель № 23701, Российская Федерация (RU), кл. МПК[7] G 07 D 7/00. Устройство для объединения уголовных дел, определения фальшивых банкнот, ценных бумаг и документов при раскрытии преступлений в криминалистике / С. Д. Кулик (Россия). Заявка № 2001134790/20; Заяв. 26.12.2001; Зарегистр. 27.06.2002; Приоритет от 26.12.2001; Опубл. Бюл. № 18. Ч. 2. – 399 с. (РОСПАТЕНТ).
4. *Кулик С. Д., Никонец Д. А., Ткаченко К. И., Жижилев А. В.* Патент на полезную модель № 73750, Российская Федерация (RU), кл. МПК[7] G 07 D 7/00. Устройство определения фальшивых рукописных документов на русском языке / С. Д. Кулик, Д. А. Никонец, К. И. Ткаченко, А. В. Жижилев (Россия). Заявка № 2007147832/22; Заяв. 25.12.2007; Зарегистр. 27.05.2008; Приоритет от 25.12.2007. Опубл. Бюл. № 15. Ч. 3. – 860 с. (РОСПАТЕНТ).
5. *Кулик С. Д., Никонец Д. А., Ткаченко К. И., Лукьянов И. А., Гунько Н. Е.* Заявка на выдачу Патента на полезную модель, Российская Федерация (RU), кл. МПК7 G 07 D 7/00. Устройство определения рукописных документов, принадлежащих исполнителю текста на русском языке / С. Д. Кулик, Д. А. Никонец, К. И. Ткаченко, И. А. Лукьянов, Н. Е. Гунько (Россия). Заявка № 2011127077; Заяв. 04.07.2011; Приоритет от 04.07.2011. (РОСПАТЕНТ). (получено положительное решение о выдаче патента).
6. *Гунько Н. Е.* Биометрические признаки для обеспечения информационной безопасности // Безопасность информационных технологий. 2010. № 1. С. 64–65.
7. *Гунько Н. Е.* Использование признаков почерка для систем информационной безопасности // Безопасность информационных технологий. 2011. № 1. С. 87–88.

С. Н. Кяжин, В. М. Фомичев

АЛГОРИТМЫ АНАЛИЗА ПРИМИТИВНОСТИ ОРИЕНТИРОВАННЫХ ГРАФОВ

Для распознавания примитивности графа можно определить длины $a_1,\ldots,a_k$ всех простых циклов и проверить примитивность набора натуральных чисел $(a_1,\ldots,a_k)$, т. е. проверить выполнение равенства НОД$(a_1,\ldots,a_k) = 1$. Последнее можно выполнить, применив $k - 1$ раз алгоритм Евклида к набору $(a_1,\ldots,a_k)$. Можно также воспользоваться заранее составленными таблицами примитивных наборов.

Другой подход заключается в определении показателя примитивности графа с помощью возведения в степень матрицы смежности его вершин.

Для определения длин простых циклов используется известный алгоритм поиска в глубину [1]. Наиболее подходящим способом для реализации данного алгоритма является рекурсия. В этом случае все возвраты вдоль пройденного пути осуществляются автоматически.

Оценена вычислительная сложность реализации алгоритма на однопроцессорной системе. В качестве элементарной операции выбрано обращение к памяти и сравнение пары двух чисел.