3. Rao M., Dudek G., Whitesides S. Randomized algorithms for minimum distance localization// Internat. J. Robotics Research. 2007. Vol. 26. P. 917–934.

4. Дао Зуй Нам. Сравнительный анализ алгоритмов локализации мобильного робота, использующего карту// 66-я науч.-техн. конф. профессорско-преподавательского состава СПбГЭТУ «ЛЭТИ» 2013: тез. докл., СПб., 1–8 февр. 2013. СПб.: Изд-во СПбГЭТУ "ЛЭТИ", 2013. С. 112–115.

5. Скворцов А. В. Построение объединения, пересечения и разности произвольных многоугольников в среднем за линейное время с помощью триангуляции // Вычислительные методы и программирование. 2002. Т. 3. С. 116–123.

6. Seidel R. A simple and fast incremental randomized algorithm for computing trapezoidal decompositions and for triangulating polygons// Computational Geometry. Theory Application. 1991. Vol. 1(1). P. 51–54.

7. Qi M., Cao T.-T., Tan T.-S. Computing 2D Constrained Delaunay Triangulation Using Graphics Hardware // Technical Report # TRB3/11. 2011. March / National University of Singapore. Singapore, 2011.

8. Боресков А. В., Харламов А. А. Основы работы с технологией CUDA. М.: ДМК-Пресс, 2010.

Dao Duy Nam, S. A. Ivanovskiy
Saint-Petersburg state electrotechnical university «LETI»

EXPERIMENTAL ANALYSIS OF ALGORITHMS FOR LOCALIZING A MOBILE ROBOT

We consider three approximation algorithms for the robot localization problem. One of them is based on a simple triangulation of a polygon representing a map. On the basis of their program implementation conducted experimental studies of these algorithms. The numerical results and their interpretation.

Robotics, robot localization, computational geometry, algorithm complexity, approximation algorithm, polygon triangulation

УДК 681.3.06 (075.8)

Е. С. Федотов, Е. С. Новикова
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Система журналирования системных параметров локального компьютера для выявления внутреннего нарушителя

Представлены результаты исследования систем, регистрирующих действия пользователей, определены системные параметры компьютера, позволяющие описать поведение пользователя, приведен разработанный авторами компонент сбора и подготовки исходных данных для системы визуального анализа поведения пользователя.

Журналирование действия пользователей, поведение пользователя, обнаружение аномалий

Задача обнаружения внутреннего нарушителя в настоящее время является актуальной из-за увеличения объемов конфиденциальной информации и персональных данных пользователей, обрабатываемых информационными системами (ИС). Под *внутренним нарушителем* понимается легальный пользователь ИС, имеющий доступ к конфиденциальным информационным ресурсам системы и использующий данные ресурсы не по назначению специально или по неосторожности [1], [2]. Существует достаточно большое число программных решений, предназначенных для анализа и контроля за состоянием локальной ИС (компьютера), мониторинга и определения различных внутренних нарушений, выявления вирусов и другого вредоносного программного обеспечения (ПО), а также ведения логов действий (локального) пользователя. В большинстве случа-

ев для обнаружения внутреннего нарушителя используются методы интеллектуального анализа данных (data mining) [3]. В настоящей статье предлагается использовать методики визуального анализа данных для обнаружения отклонений в поведении пользователей и выяснения причин выявленных аномалий. Благодаря использованию способности человека быстро выявлять шаблоны и отклонения в графических данных визуальный анализ может значительно повысить эффективность работы специалиста по информационной безопасности.

В данной статье представлены первые результаты разработки системы визуального анализа для обнаружения внутреннего нарушителя. В ней обсуждаются необходимые исходные данные, позволяющие описать поведение пользователя ИС, и приводится разработанный программный модуль сбора исходных данных. Данный модуль представляет собой программный продукт, который позволяет регистрировать нагрузку центрального процессора (ЦПУ), список выполняемых процессов и активность пользователя.

Обзор систем сбора данных о действиях пользователя. Признаками внутреннего нарушителя могут быть большая загрузка ЦПУ при низкой активности пользователя, запуск программ или процессов, не характерных для заданного пользователя. Под активностью пользователя подразумеваются все действия пользователя, например чтение файла, набор текста или нажатие кнопки мыши. Следует отметить, что эти признаки не всегда свидетельствуют о нарушении политик безопасности. Однако проектируемая система визуального анализа должна позволить изучить подобные аномалии и, как следствие, может быть использована как система поддержки принятия решения, является ли данный случай нарушением информационной безопасности или нет. Кроме того, разрабатываемое ПО позволит более точно задавать пороги и условия срабатывания систем обнаружения вторжений и тем самым снизить число ложноположительных срабатываний.

В ходе работы анализировались системы, регистрирующие действия пользователей, и оценивалась возможность получения с их помощью требуемых исходных данных (загрузка ЦПУ, активность пользователей, список запущенных процессов). Результаты исследования показали, что множество существующих программных решений можно разделить на две группы: 1) логгеры активности пользователя, фиксирующие действия пользователей и предназначенные в большей степени для контроля действий сотрудников компании; 2) мониторы, позволяющие получить нагрузку ЦПУ и список задач. В таблице приведены результаты программных решений, ведущих учет действий пользователя. Под сомнительностью ПО понимается вероятность наличия у него недекларируемых возможностей, нарушающих информационную безопасность системы.

Проектирование модуля сбора данных. Анализ существующего ПО, отслеживающего действия пользователя, показал, что большинство из них регистрирует не все требуемые для анализа данные, а некоторые продукты не ведут журнал событий. В результате возникла необходимость проектирования и разработки собственного модуля сбора исходных данных для системы визуального анализа поведения пользователей ИС.

Архитектура модуля сбора исходных данных достаточно проста и включает в себя следующие компоненты:

1) класс pro, в котором происходит запуск кода (основа программы);

2) класс thr, создающий поток для выполнения программы;

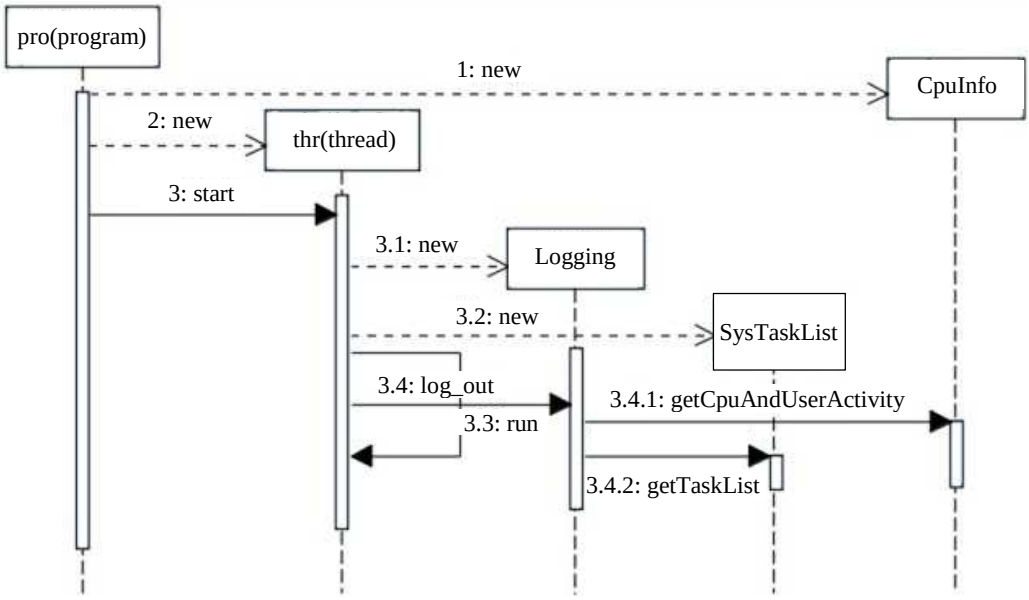
3) класс CpuInfo, получающий нагрузку CPU и активность пользователя;

4) класс SysTaskList, получающий список выполняемых задач;

5) класс журналирования данных Logging, который отвечает за создание папок для записи данных, а также за создание файлов-журналов, последующую запись и дозапись данных. На рисунке представлена UML-диаграмма зависимостей классов модуля. В настоящий момент программа фиксирует следующие параметры ИС: активность пользователя (в процентах), загрузку ЦПУ (в процентах) и список запущенных сервисов и процессов (в виде строки, в которой задачи перечислены через запятую). Регистрация данных происходит через заданный пользователем интервал времени (по умолчанию он равен 15 с). Логи программы записываются в формате JSON[1]. JSON – текстовый формат обмена данными, основанный на языке программирования JavaScript и обычно используемый именно в связке с этим языком. Поскольку

[1] Формат обмена данными JSON. http://www.json.org/.

Название ПО	Тип ПО	Возможности ПО	Платное/ бесплатное ПО	Недостатки
TimeHunter 2.8[2]	Логгер	Программа для учета времени проводимого за компьютером: документы, программы, Интернет, игры и т.д. Выдает отчеты о работе одного человека или целой группы	Условно-бесплатная (29.95$)	Сомнительность ПО
ZABBIX[3]	Сетевой монитор	Свободная система мониторинга и отслеживания статусов разнообразных сервисов компьютерной сети, серверов и сетевого оборудования. Отсутствует журнал событий	Бесплатная	Не подходит тип ПО
ActiveKeyLogger[4]	Логгер	Программа-шпион, записывает в лог-файл все действия пользователя за компьютером	Платная (29.99...49.99 $)	Сомнительность ПО, платное ПО
StaffCop[5]	Логгер	Программа для слежения за пользователями компьютеров в локальной сети и терминальных серверов. Обеспечивает удаленный контроль действий сотрудников, анализ эффективности труда и защиту информации от утечек	Платная (990 р.)	Платное ПО
RealSpyMonitor[6]	Логгер	Программа-шпион, записывает в лог-файл все действия пользователя за компьютером	–	Сомнительность ПО



графический интерфейс пользователя разрабатывается с помощью графических библиотек, написанных на JavaScript, то использование данного формата позволит в дальнейшем упростить работу над модулем визуализации полученных данных, сократив время разработки ПО и количество кода. Логи программы имеют следующий вид: {“dateTime”: “2013/11/22 00:43:31”, ”cpu”: “36,7%”, “userActivity”: “27.8%”, “taskList”: {“System”, “System”, ”smss.exe”, “csrss.exe”, “wininit.exe”}}. При реализации модуля по сбору си-

[2] Система учета действий пользователя ПК TimeHunter 2.8. www.softarchive.ru/item /18181.html.

[3] Сетевой монитор ZABBIX. www.zabbix.com.

[4] Система учета действий пользователя ПК ActiveKeyLogger. http://active-keylogger-home.en.softonic.com.

[5] Система учета действий пользователя ПК StaffCop . http://www.staffcop.ru/.

[6] Система учета действий пользователя ПК RealSpyMonitor. www.winline.ru/soft/312/real_spy_monitor.

стемных данных была использована библиотека SIGAR[7]. SIGAR– это кроссплатформенный интерфейс, позволяющий работать с системным API, благодаря которому были получены нагрузка CPU и активность пользователя.

Таким образом**,** в настоящей статье представлены результаты проектирования модуля сбора исходных данных для системы визуального анализа поведения пользователя ИС. Был проведен анализ существующих решений, регистрирующих действия пользователя, и показана необходимость разработки собственного модуля сбора данных.

Дальнейшие исследования связаны с разработкой модели визуализации данных, описывающих поведения пользователя ИС. Полученные результаты будут использованы для изучения и формирования «подчерка» пользователя, что позволит улучшить механизмы обнаружения атак на информационные системы. Кроме того, может быть предусмотрена возможность реализации автоматизированных механизмов реакции ПО на действия внутреннего нарушителя, что позволит защитить информацию и используемые программно-аппаратные средства.

СПИСОК ЛИТЕРАТУРЫ

1. Зима В. М., Молдовян А. А., Молдовян Н. А. Безопасность глобальных сетевых технологий. СПб.: БХВ-Петербург, 2000.

2. Миронова В. Г., Шелупанов А. А. Модель нарушителя безопасности конфиденциальной информации // Информатика и системы управления. 2012. № 1 (31). С. 28–35.

3. Schultz E. E. A framework for understanding and predicting insider attacks // Computers & Security. 2002. Vol. 21. P. 526–531.

E. S. Fedotov, E. S. Novikova
Saint-Petersburg state electrotechnical university «LETI»

THE LOGGING SYSTEM OF PERSONAL COMPUTER SYSTEM PARAMETERS FOR INSIDER ACTIVITY DETECTION

This paper presents the results of user activity logging systems. It describes computer system parameters that can be used for insider activity detection and presents the component registering defined system parameters for the visual analytics system designed to assess the user behavior.

User activity logging, user behavior, anomaly detection

УДК 004.94

Аль-Шами Мохаммед Хуссейн Ахмед
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Архитектура базы данных сеанса проектирования для схемотехнических САПР

Рассматриваются вопросы организации web-ориентированной базы данных сеанса проектирования (БДСП) для схемотехнических САПР. Обсуждается возможность коллективного использования БДСП в сети Интернет. Анализируется содержимое БДСП и состав управляющего web-приложения.

Схемотехническая САПР, архитектура базы данных сеанса проектирования, серверное web-приложение БДСП

Развитие и массовое применение глобальных сетевых технологий в различных областях способствовали внедрению интернет-среды в инфраструктуру современных промышленных предприятий, разрабатывающих и производящих радиоэлектронную аппаратуру. С другой стороны, су-

[7] Библиотека SIGAR. http://www.hyperic.com/products/sigar.