граница времени поиска $T^{min}(V_0)$=19 мин. В левой части остальных вершин для каждого уровня указаны текущая верхняя граница значения функции цели $R(V_s)$, в правой части – нижняя граница общего времени $T(V_s)$. Жирными линиями выделен путь поиска оптимального решения на множестве $V_д$ допустимых вариантов. Результаты обоснования задач ИБ ОТС состоят в распределении ресурса средств ИБ: на 1-ом уровне решается задача №1; на 2-ом – №3; на 3-ем – №2; на 4-ом – №5 и на 5-ом – №4.

Результаты проведенных расчетов задач ИБ ОТС показали, что оптимальное значение целевой функции составляет $R^*(V_д) = 10$ при $T^*(V_д) = 22$ мин, не превышающем Тз=23 мин.

Предложенный метод обеспечивает решение задачи обоснования задач ИБ для различной типа и структурной сложности ОТС на основе оптимального распределения временного ресурса средств ИБ на иерархических уровнях системы.

Литература:

1. *Мистров Л.Е.* Метод выбора и распределения ресурсов в обеспечивающих организационно-технических системах // Автоматизация и современные технологии. – 2006. – №11. – С. 24-29.

2. *Денисов А.А., Колесников Д.Н.* Теория больших систем. – Л.: Энергоиздат, 1982. – 287 с.

DOI: 10.25728/iccss.2022.83.42.028

Саломатин А.А.

Анализ характеристик аппаратного обеспечения для задач информационной безопасности

Аннотация: В работе авторами проводится исследование характеристик аппаратного обеспечения для решения задач информационной безопасности. Выделяют наиболее значимые задачи, среди которых основное внимание в работе уделено задачам аутентификации и идентификации пользователей. Рассматриваются статические и динамические характеристики основных аппаратных

платформ, применимых в данных задачах. Описанные особенности характеристик и процесса их вычисления позволяют выбирать конкретные характеристики аппаратного обеспечения для обеспечения более высокого уровня информационной безопасности в задачах.

Ключевые слова: кибербезопасность, информационная безопасность, аппаратное обеспечение, аутентификация, идентификация, цифровой след

В настоящее время растущей становится проблема кибербезопасности сетей и критически важных элементов инфраструктуры. Необходима поддержка высокого уровня информационной безопасности, при котором информация обладает достаточной степенью конфиденциальности, целостности и доступности на различных уровнях использования.

Эффективными становятся средства защиты, позволяющие детектировать атаки на системы ещё на ранних этапах [1, 2]. Однако, разработка таких мер является сложной комплексной задачей, поскольку предметная область должна учитывать большой объём данных, связанных с пользовательским программным и аппаратным обеспечением.

Задачи аутентификации и идентификации пользователей сетей выступают в центре внимания исследователей. Современные подходы к решению представленных задач постоянно обновляются, поскольку совместно с разработкой методов аутентификации создаются способы обхода защиты, что может привести к серьёзным негативным последствиям для системы и её пользователей [3, 4].

Исследование данного направления показало, что перспективным является проведение аутентификации пользователя на основе его уникального многокритериального цифрового следа [5]. Цифровой след содержит данные о различных статических и поведенческих характеристиках профиля субъекта доступа. Например, данные браузера, операционной системы и аппаратного обеспечения, данные, связанные с запросами, и т.д.

Более жёсткую связь пользователя с устройствами и более слабую подверженность успешным кибератакам даёт цифровой след на основе характеристик аппаратного обеспечения.

В [6] для формирования цифрового следа рассматриваются характеристики статического и динамического характера ПО компьютера, полученные с помощью Диспетчера устройств, «Информации системы» и AIDA64 Engineer v. 6.33.5700.

Характеристики первого типа являются неизменными для устройства. Их число большое и зависит от конкретных используемых аппаратных платформ. Вычисляют названия подключенных устройств и составляющих компонент, определяются текущие аудиовходы и аудиовыходы, вычисляют показатели работы батареи, характеристики монитора, материнской платы, батареи, оперативной памяти и др.

Характеристики второго типа связаны с изучением работы компонент системы по истечению определённого временного промежутка. Проводятся тесты различных типов: чтение из памяти, запись в память, копирование в память, CPU Queen, CPU PhotoWorxx, CPU ZLib, CPU AES, FPU Julia, FPU Mandel и др.

В результате исследования определян оптимальный набор тестов, позволяющих наиболее успешно проводить аутентификацию пользователя.

Похожие исследования были проведены также в [7], где для определения динамических характеристик каждого устройства проведены тесты 4 типов с помощью собственных написанных программ. Результаты эксперимента показывают, что вычисленные результаты тестов могут помочь в формировании цифрового следа с высокой уникальностью и стабильностью при его формировании и использовании.

В другой работе [8] для вычисления статических характеристик пользователя авторы используют JavaScript и HTML5 API. В качестве вычисляемых характеристик выступают некоторые показатели монитора, батерии, подключенные устройства в виде камеры и микрофона и др. Также в работе вычисляются браузерные отпечатки, которые хоть и не являются характеристикам аппаратного обеспечения, но могут составлять будущий цифровой след.

Стоит отметить, что класс устройств может быть расширен и дополнен другими мобильными устройствами, для которых возможно выделить классы данных аппаратного обеспечения, на основе которых проводится аутентификация. В отмеченных группах

данных присутствуют как статические, так и динамические показатели.

- Датчики (магнитометр, показатели ориентации, показатели света, вектор ротации, показатели температуры, CAP_PROX, RPC, показатели цветодатчика, линейное ускорение и др.).
- Центральный процессор (SoC модель, архитектура ядра, технологический процесс, наборы инструкций, число ядер, частотные характеристики, поддержка стандартов хеширования, шифрования).
- Отображение (разрешение экрана, технология, размер экрана, диагональ экрана, плотность пикселей, производитель, рендерер, версия графического процессора).
- Сеть (сетевой оператор, состояние передачи данных, активность данных, Wi-Fi, тип сети и др.).

Выбор количества и типа данных для любой аппаратной платформы зависит от конкретной ситуации и цели. Универсальная методика пока не разработана. Использование большего числа статических, нежели динамических, параметров позволяет избежать лишних временных задержек при решении задач информационной безопасности. В свою очередь, использование динамических характеристик отдельно или совместно со статическими характеристиками позволяет точнее проводить аутентификацию в связи с анализом большего объёма данных как из-за их динамики, так и из-за их количества и уникальности определения для пользователей.

Исследование выполнено при финансовой поддержке гранта Президента Российской Федерации для государственной поддержки молодых российских ученых – кандидатов наук МК-3172.2021.1.6

Литература:

1. *Хозяинова Т.В,, Шечева И.А., Кобзев Д.А., Бенгарт З.С., Кутлубаева Е.Г.* Организация процесса мониторинга уязвимостей программного обеспечения и оборудования АСУТП // Наука и технологии трубопроводного транспорта нефти и нефтепродуктов. – 2019. – № 9. – С. 458-466.

2. *Avizienis A., Laprie J.-C., Randell B.* Fundamental concepts of dependability // Research Report. – 2001. – Vol. 1145. – P. 1-6.

3. *Бабаев Д.И., Полетыкин А.Г., Промыслов В.Г., Тимофеев*

М.Ю. Управление архитектурой кибербезопасности АСУТП атомных электростанций // Проблемы управления. – 2018. – № 3. – С. 47-55.

4. *Cherdantseva Y., Burnap P., Blyth A., Elden P., Jones K., Soulsby H., Stoddart K.* A review of cyber security risk assessment methods for SCADA systems // Computers & security. – 2016. – Vol. 56. – P. 1-27.

5. Струков А.В., Ветлугин К.А. О методах количественного анализа кибербезопасности технических систем на основе логико-вероятностного подхода // Интернет-журнал «Науковедение». – 2017. – Том 9. №4. – URL: http://naukovedenie.ru/PDF/01TVN417.pdf (дата обращения 15.10.2022).

6. *Salomatin A.A., Iskhakov A.Yu., Meshcheryakov R.V.* Formation of a Digital Footprint Based on the Characteristics of Computer Hardware to Identity APCS Users / Proceedings International Russian Automation Conference (RusAutoCon). – Sochi, Russia: IEEE, 2021. – P. 314-320.

7. *Dong S., Farha F., Cui S., Ning H., Ma J.* CPG-FS: A CPU perfomance graph based device fingerprint scheme for devices identification and authentication / Proc. of the 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing. – IEEE, 2019. – P. 266-270.

8. *Takasu K., Saito T., Yamada T., Ishikawa T.* A survey of hardware features in modern browsers: 2015 Edition / Proc. of the 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. – IEEE, 2015. – P. 520-524.

DOI: 10.25728/iccss.2022.72.91.029

Сомов С.К.

Показатели надежности распределенной системы с невосстанавливаемыми узлами

Аннотация: В работе выполнен анализ показателей надежности функционирования распределенных систем обработки данных, использующих оперативный резерв из нескольких копий массивов данных для повышения надежности обработки в узлах запросов к системе. Рассматривается ситуация, при которой система не восстанавливает оперативный резерв в случае его