УДК 004.056.53

ПРОГРАММНЫЙ КОМПЛЕКС АБОНЕНТСКИЙ ОБЛАЧНЫЙ ТЕРМИНАЛ

В.О. Писковский
Московский государственный университет им М.В. Ломоносова, Факультет вычислительной математики и кибернетики
Россия, 119991, ГСП-1 Москва, Ленинские горы, МГУ имени М.В. Ломоносова, д.1, стр. 52, 2-й учебный корпус, факультет ВМК
E-mail: vpiskovski@lvk.cs.msu.ru

А.А. Грушо
Федеральный исследовательский центр «Информатика и управление» Российской академии наук
Россия, 119333, Москва, ул. Вавилова, д. 44, кор. 2
E-mail: grusho@yandex.ru

Ключевые слова: задачи управления и оптимизации работой пользовательских рабочих мест, встроенные средства защиты, стеганография, цифровой водяной знак, технология виртуализации, влияние сетевых характеристик

Аннотация: Практическая деятельность предприятий обычно требует предоставления возможности одновременной работы с внутренними, распределенными информационными ресурсами и доступом в сеть Интернет. Необходимость решения этой задачи обуславливает использование соответствующих организационно-технических методов защиты информации, в основе которых лежит идея изоляции доменов. В докладе представлен исследование применения программного комплекса «Абонентский облачный терминал» (АОТ) для решения этой задачи путём использования технологий виртуализации на рабочих станциях пользователей.

1. Введение

Программное средство общего назначения с встроенными средствами защиты (программный комплекс) «Абонентский облачный терминал» (АОТ) решает задачу путём совмещения на одной аппаратной единице, персональном компьютере, произвольного количества разнородных, изолированных, не зависимых друг от друга рабочих мест. Каждое рабочее место работает под управлением своей операционной системы, в своём программном и сетевом окружении, включая возможность полной изоляции от сети.

АОТ реализует защиту критичных данных и приложений пользователя от несанкционированного доступа. Криптографическое преобразование данных предотвращает несанкционированный доступ к информации даже в случае утраты или кражи систем хранения данных.

Удаленное рабочее место администратора АОТ включает в себя:

- подсистемы: удалённого администрирования, мониторинга работы АОТ и действий пользователей, информационного обеспечения и поддержки;
- интеграцию с системами доступа с функцией электронной подписи, предотвращения вторжений, антивирусной защиты, доверенной загрузки.

АОТ также является составной частью принципиального подхода к обеспечению информационной безопасности при использовании частных облачных вычислительных сред с развитой инфраструктурой средств защиты информации, см. рис. 1. В этом случае, абоненты частных облачных инфраструктур используют функции информационной безопасности как услугу, интегрируемую с АОТ на уровне гипервизора.

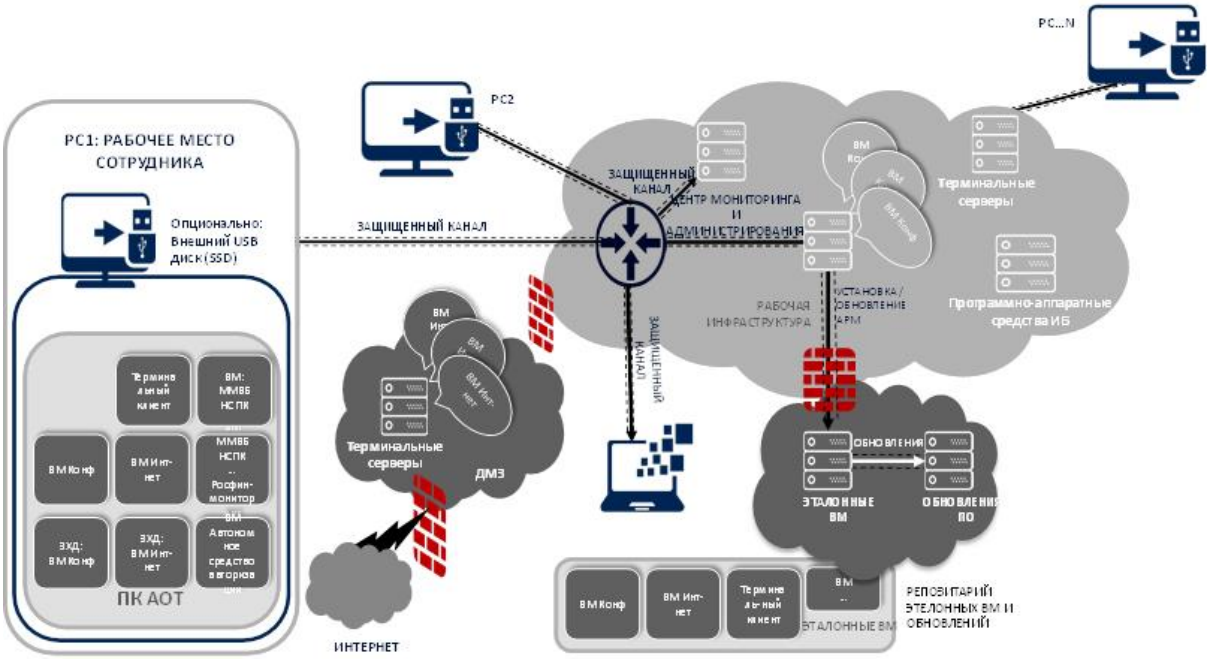

Рис. 1.Принципиальная схема использования Программного комплекса Абонентский облачный терминал в корпоративной сети предприятия.

2. Применение ПК АОТ для стандартизации и защиты рабочих мест сотрудников

2.1. Централизованная вычислительная структура предприятия

Рабочая инфраструктура централизованной [облачной] вычислительной структуры (ЦВС)[1] предприятия может содержать репозитарий контейнеров с виртуальными машинами (ВМ), реализующими рабочие места сотрудников и прошедшими принятую на предприятии процедуру внедрения в постоянную эксплуатацию.

Репозитарий эталонных ВМ и обновлений содержит эталонные ВМ, серверы с обновлениями программного обеспечения. Задачи, решаемые этим компонентом ЦВС: формирование проверенных, согласованных, безопасных эталонных рабочих мест в виде контейнеров с типовыми ВМ. Образы ВМ копируются на локальные диски АОТ, см. Рис. 1.

Однако одним из существенных недостатков такого решения является то, что для размещения на персональном компьютере образа виртуальной машины с установленной на ней полноценной ОС, например, MS Windows 10, необходимо скопировать и передать по сети около 40 Гб, что выливается в длительную процедуру обновления и приводит к коллапсу¿ локальной сети. Чтобы избежать такой ситуации, предлагается запускать ВМ в режиме расширенного фильтра записи. В этом режиме можно настроить образ ВМ так, чтобы он оставался доступным только для чтения, а все изменения, внесенные пользователем, сохранялись локально на специальном слое

файловой системы. Решение поставленной задачи должно снизить время загрузки образа ВМ и нагрузку на сеть.

2.2. ВМ в режиме расширенного фильтра записи

Целью исследования является зависимость времени запуска виртуальной машины (ВМ) в режиме расширенного фильтра записи на АОТ от способа хранения и протокола доступа к данным виртуального диска.

Обозначения и постановка задачи – найти зависимость времени запуска $S_{VM}(t) = f_s(t; w, \tau_0, N_c, T_{OS}, C_S, P_a)$ и скорость чтения данных виртуального диска $Rx_{VM}(t) = f_{Rx}(t; w, \tau_0, N_c, T_{OS}, C_S, P_a)$, где: $S_{VM}(t)$ время регистрации запуска ВМ (сек), w – пропускная способность сети (Мбит/сек), τ_o – задержка отправления пакетов в сети (мсек), T_{os} – тип операционной системы, C_S – критерий регистрации старта ВМ на рабочем месте, Pa – сетевой протокол доступа к данным виртуального диска

Критерий регистрации старта ВМ – загрузка сетевого интерфейса ВМ и графической оболочки. Применяемые протоколы доступа: SMB3, NFSv4, NBD.

По результатам экспериментов протокол NBD в среднем показал наилучшие результаты. Время регистрации запуска ВМ при его использовании в большинстве случаев оказывается наименьшим, что объясняется тем, что в протоколе NBD реализованы эффективные механизмы кэширования данных, которые позволяют уменьшить количество запросов и увеличить скорость доступа к данным. Протокол SMB показал хорошие результаты при условии небольшой сетевой задержки. При увеличении задержки измеренное в случае использования протоколов NFS и NBD, время регистрации запуска ВМ больше, что объясняется отмеченной в литературе чувствительностью протокола SMB чувствительностью к сетевым задержкам. Также производительность в тестах скорости чтения в случае SMB оказалась очень низкой. NFS в среднем показал результаты лучше, чем протокол SMB. Время регистрации запуска ВМ при низкой задержке гораздо больше, чем у NBD и SMB. При увеличении задержки время регистрации запуска ВМ с использованием NBD становится меньше, чем при использовании SMB.

Оптимальным выбором для работы с ВМ в режиме расширенного фильтра записи является протокол NBD. Благодаря реализованным оптимизирующим механизмам протокол эффективен при разных значениях скорости и задержек в сети. В случае низкой задержки в сети лучше выбирать протокол SMB, так как он позволит сократить время регистрации запуска ВМ.

3. Применение ПК АОТ для идентификации рабочего места по фотоснимку экрана компьютера

3.1. Актуальность и постановка задачи

Одной из актуальных проблем является охрана конфиденциальной информации [8-10]. Массовое распространение мобильных телефонов, оснащенных средствами фото и видео фиксации, привело к возникновению нерегистрируемого способа утечки информации путем фотографирования конфиденциальной информации (документов), выводимой на монитор рабочего места сотрудника. Такой способ позволяет быстро отправить большие порции снимков другому человеку или сохранять на мобильном устройстве, тем самым легко выносить информацию. В этом случае, идентификация автоматизированного рабочего места (АРМ), оснащенного программным комплексом АОТ помогла бы, если не устранить канал утечки, то хотя бы установить источник.

Предварительные исследования по методу идентификации докладывались на международной конференции MoNeTec-2020 [4]. Одним из наиболее эффективных решений представляется идентификация АРМ посредством интеграции цифрового водяного знака (ЦВЗ) в изображение, проецируемое на экран компьютера [5–7].

Постановка задачи. Рассмотрим задачу стеганографического сокрытия информации. Обозначим множество контейнеров, скрываемых сообщений и ключей *Z, D* и *K* соответственно. Процедура встраивания и извлечения сообщения определяется следующим образом:

$$F_* = Z \otimes D \otimes K \to Z, \overline{z} = F_*(z, d, k), z \in Z, k \in K, d \in D, \|z - \overline{z}\| \to \min$$
$$F_{**} = Z \otimes K \to D, \overline{d} = F_{**}(\overline{z}, k), k \in K, \overline{d} \in D, \left\|d - \overline{d}\right\| \to \min,$$

где $z, \overline{z}$ – исходный и заполненный контейнеры, а $d, \overline{d}$ – исходное и восстановленное сообщения.

3.2. Свойства решения задачи

Надежность. Предложенный алгоритм получился достаточно надежным. Исследовались разные уровни освещенности при фотографировании экрана, с разным разрешением (до 2000 пикселей по горизонтали), под разными углами отклонения от вертикали (до 40%), на разные модели телефонов. Помимо этого, изображение подвергалось обработки разными фильтрами, включая сжатия (до 60%). К примеру, для текстовых документов и схем можно использовать быстрый пороговый фильтр, который закрашивает все пиксели черным цветом, яркость которых превосходит определенный порог (до 57%), а другие оставляет белыми.

Для текстовых документов в данной работе не рассматривался способ оцифровки документа, когда определяются именно буквенные последовательности, так как при таком переносе информации все графические особенности экрана стираются и в выходном файле сохраняются только коды символов.

Прозрачность. Выяснилось, что можно пожертвовать прозрачностью водяного знака в пользу надежности. Предложенный метод можно считать достаточно прозрачным, так как ЦВЗ в документах практически незаметен, и информация в них не искажается.

Безопасность. Под безопасностью понимается невозможность сохранения водяного знака после применения атак, которые могут нарушить целостность знака, а воссоздание и наложение данного знака на новые изображения. В предложенном протоколе используется односторонняя функция, которая не дает возможности получить корректные данные, если у инициатора нет идентификаторов пользователя и записи о его взаимодействии с системой.

Невысокая сложность. В рассматриваемой области водяной знак вносится в каждый кадр, следовательно, алгоритм должен достаточно быстро встраивать ЦВЗ в изображение. Желательной скоростью обновления кадров в секунду является не менее 24 кадров в секунду. Если скорость будет ниже, глаз уже не сможет сглаживать картинку и видеоряд станет не пригодным для просмотра. Таким образом, при проведении тестов обработка одного кадра производилась не дольше 41 мсек. Такая скорость работы алгоритма вполне подходит для беспроблемной работы с видео.

4. Заключение

Применение программного комплекса «Абонентский облачный терминал» позволяет оптимизировать капитальные и операционные затраты на оснащение и безопасное функционирование рабочих мест предприятия, включая регистрацию действий работы пользователей, аудит рабочих мест, идентификацию каналов

распространения документов ограниченного пользования по фотоснимкам экранов компьютера.

Список литературы

1. Грушо А.А., Николаев А.В., Писковский В.О., Сенчило В.В., Тимонина Е.Е. Подход к обеспечению информационной безопасности при использовании частных облачных вычислительных сред. Абонентский облачный терминал. MoNeTec2020, 2020.
2. Server Message Block (SMB) Protocol Versions 2 and 3, Microsoft, 2020, URL: https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-smb2/165606ad47-5ee0-437a-817e-70c366052962. Дата обращения: 2.11.2022.
3. The NBD protocol description, URL: github.com/NetworkBlockDevice/nbd. Дата обращения: 25.02.2023
4. RFC 7530, Internet Engineering Task Force (IETF), URL: www.rfc-editor.org/rfc/rfc7530.html. Дата обращения: 2.10.2022.
5. An Overview of NFSv4, Storage Networking Industry Association, 2012, URL: https://www.snia.org/sites/default/files/SNIA_An_Overview_of_NFSv4-3_0.pdf. Дата обращения: 26.10.2022.
6. Diskspd, Microsoft, URL: github.com/microsoft/diskspd. Дата обращения: 25.02.2023.
7. Minho Lee, Young Ik Eom Efficient Data Cluster Management Scheme for Qcow2-based Virtual Disk in Home Cloud Server // IEEE International Conference on Consumer Electronics (ICCE), 2018.
8. Grusho A.A., Nikolaev A.V., Piskovsky V.O., Sentchilo V.V., Timonina E.E. Edge point cloud terminal as an approach to secure the use of an enterprise private cloud // 3rd International Scientific and Technology Conference «Modern Network Technologies–2020 (MoNeTeC)». IEEE, 2020. P. 45-48.
9. Adelsbach A., Katzenbeisser S., Veith H. Watermarking schemes provably secure against copy and ambiguity attacks // DRM ’03: Proceedings of the 3rd ACM Workshop on Digital Rights Management. Washington, DC, USA, 2003. P. 111-119.
10. Bloom J.A., Polyzois C., Watermarking to track motion picture theft // Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers. Vol. 1. CA, USA: Pacific Grove, 2004. P. 363-367.
11. Grusho A.A., Piskovsky V.O., Semenikhin D.A., Sudarikov I.V., Timonina E.E. The research of a method to identify a workplace via a monitor snapshot // 3rd International Scientific and Technology Conference «Modern Network Technologies–2020 (MoNeTeC)». IEEE, 2020. P. 49-54.
12. Писковский В.О., Семенихин Д.А., Грушо А.А., Забежайло М.И., Метод идентификации рабочего места по фотоснимку экрана компьютера // Вестник Московского университета. Сер. 15. Вычислительная математика и кибернетика. 2023. № 3. С. 56-57.