PcVue Secure

PcVue Secure. Защита SCADA-системы PcVue с использованием технологий на базе KasperskyOS

kaspersky BRING ON THE FUTURE

KasperskyOS®

Задача

Обеспечение информационной безопасности АСУТП – чрезвычайно важная задача, актуальность которой все время растет. С одной стороны, появляются новые требования регулирующих органов, например, Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ. С другой стороны, АСУТП становятся все более сложными и глубоко интегрированными в самые разные сферы повседневной жизни. При всех неоспоримых преимуществах, использование парадигмы Industry 4.0 означает, что поверхность атаки на АСУТП-системы становится очень велика.

Ситуация усугубляется тем, что многие существующие АСУТП несут наследие тех времен, когда об информационной безопасности мало кто думал. Как следствие, такие системы слабо защищены, а повышение их безопасности требует существенных инвестиций, вплоть до полной переработки таких решений. Но даже эти меры не позволяют получить 100% гарантию безопасности, поскольку среда функционирования компонентов АСУТП также является недостаточно защищенной. В наиболее распространенных операционных системах постоянно обнаруживаются критические уязвимости.

Решение

«Лаборатория Касперского» уже более 20 лет работает в сфере защиты информации и предлагает эффективные технологии и решения по защите АСУТП.

Использование операционной системы KasperskyOS и связанных с ней технологий позволяет решить важные вопросы по защите SCADA-систем, которые являются ключевым элементом АСУТП.

«Лаборатория Касперского» совместно с компанией ARC Informatique работает над решением PcVue Secure – защищенной SCADA на базе продуктов PcVue и KasperskyOS.

PcVue Solutions - масштабируемая программная платформа, обеспечивающая полный контроль технологических процессов предприятия и поддерживающая широкий спектр оборудования различных производителей. Главным компонентом платформы является SCADA-пакет PcVue.

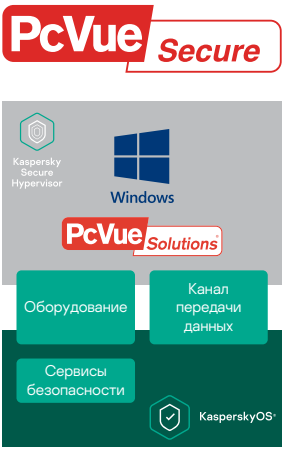
PcVue – это полнофункциональная SCADA, работающая под управлением Windows и предназначенная для создания систем сбора данных, диспетчерского управления и мониторинга решений различного масштаба: от автономных станций оператора до распределенных систем управления с клиент-серверной архитектурой, в которых задействовано большое количество рабочих станций и серверов, с поддержкой возможности удаленного доступа, включая доступ с использованием мобильных клиентов.

В настоящее время под управлением PcVue Solutions работают тысячи объектов по всему миру. Список отраслей, использующих платформу, включает АСУЗ (BMS), энергетику, водоснабжение, транспорт, инфраструктуру, нефть и газ, производство и др.

Операционная система KasperskyOS и гипервизор Kaspersky Secure Hypervisor позволяют существенно повысить безопасность SCADA-решения, причем данный подход может быть реализован без модификаций или с минимальными модификациями последнего.

Результат

Описание подхода



«Лаборатория Касперского» разработала защищенную операционную систему KasperskyOS, которая предоставляет высокий уровень гарантий безопасного функционирования программных компонентов, работающих под ее управлением. Отличительной особенностью данной ОС является ее подсистема безопасности Kaspersky Security System (KSS), которая позволяет задавать чрезвычайно гибкие политики безопасности, контролирующие взаимодействия между программными компонентами внутри KasperskyOS. Данные политики основываются на различных моделях безопасности, причем можно использовать несколько таких моделей одновременно.

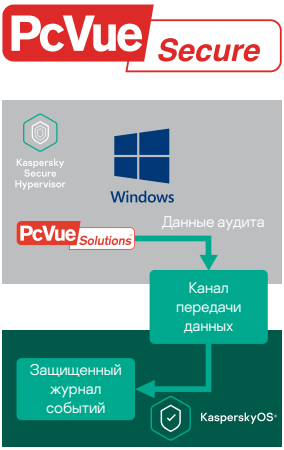
Для KasperskyOS также разработана подсистема виртуализации Kaspersky Secure Hypervisor (KSH). Это гипервизор второго типа (наряду с гипервизором в контексте KasperskyOS могут полноценно работать и другие программные компоненты), реализованный с использованием аппаратных средств Intel VT-x, VT-d. Kaspersky Secure Hypervisor поддерживает различные гостевые операционные системы, включая Windows (XP, 7, 8, 10) и наиболее популярные дистрибутивы на базе ядра Linux.

В решении PcVue Secure, SCADA запускается из гостевой операционной системы Windows 10, работающей на виртуальной машине на базе KSH, который предоставляет контролируемый канал взаимодействия между программными компонентами гостевой операционной системы и KasperskyOS.

KSH контролирует все аспекты работы виртуальной машины, в том числе позволяет предоставлять/ограничивать доступ к периферийному оборудованию, а само оборудование виртуальной машины может предоставляться из KasperskyOS как есть либо эмулироваться. В последнем случае появляется возможность средствами KSH и KasperskyOS наделять оборудование новыми свойствами прозрачно для гостевой операционной системы. Например, для сетевого адаптера можно добавить функцию шифрования трафика, а для клавиатуры – функцию перехвата/замены ввода.

Такая схема позволяет реализовывать различные сценарии защиты SCADA-решения, некоторые из которых описаны ниже.

Защищенный журнал событий



Надежное сохранение данных журнала событий является важной задачей информационной безопасности. Подмена журнала событий служит важным звеном большого количества компьютерных атак.

Однако обеспечить надежное сохранение журнала событий при работе в операционной системе общего назначения очень сложно – например, из-за того, что для журнала событий требуется достаточно специфическая политика безопасности, обладающая следующими свойствами:

- Есть возможность добавлять новые записи в журнал событий.
- Нет возможности модифицировать записи после добавления.
- Нет возможности удалять записи, за исключением пользователя, обладающего специальными привилегиями.
- Возможность просмотра записей зависит от привилегий пользователя.

При использовании KasperskyOS эта задача легко решается.

SCADA реализует механизм, позволяющий осуществлять захват логов и передачу их приложению для работы с событиями на стороне KasperskyOS.

Средствами KSS задается требуемая политика безопасности при работе с данными.

Поскольку сведения о событиях сохраняются в контексте доверенной среды, гостевая операционная система не имеет к ним доступа, и после того, как данные получены, их модификация невозможна. Все дальнейшие операции с данными журнала событий проводятся с использованием KasperskyOS в соответствии с заданными для решения политиками безопасности.

Дополнительно «Лаборатория Касперского» предлагает технологию надежного сохранения данных аудита Secure Audit, реализованную с использованием технологии блокчейн, которая позволяет гарантировать целостность данных даже в том случае, если к ним был получен несанкционированный доступ. При использовании Secure Audit есть возможность достоверно определить, имела место подмена данных или нет.

Усиленная аутентификация

Стандартные механизмы аутентификации, предлагаемые операционной системой Windows, являются достаточно слабыми. К примеру, в случае использования парольной защиты существует набор стандартных проблем: сложный пароль трудно запомнить, а простой пароль легко скомпрометировать. С другой стороны, есть большое количество механизмов аутентификации, не поддерживаемых Windows.

Использование гипервизора позволяет реализовать надежный механизм аутентификации пользователей, независимый от Windows.

Kaspersky Secure Hypervisor дает возможность управлять доступом виртуальной машины к периферии – в частности, реализовать сценарий блокировки виртуальной машины, когда от нее отключаются устройства пользовательского ввода/вывода.

Доступ к виртуальной машине может быть предоставлен лишь в случае, если проведена успешная аутентификация пользователя средствами KasperskyOS.

Данный подход имеет ряд преимуществ:

- Использование KasperskyOS гарантирует, что процедура аутентификации не может быть скомпрометирована.
- Есть возможность реализации различных механизмов аутентификации, независимо от гостевой ОС.
- Информация о пользователе появляется в KasperskyOS, что позволяет использовать эти данные в соответствующих политиках безопасности, например, для реализации ролевой модели доступа.

Безопасный удаленный доступ

Возможность удаленного доступа к информационным системам дает множество преимуществ, но в то же время – и для SCADA-систем это особенно актуально – представляет сложную проблему с точки зрения информационной безопасности. Использование KasperskyOS позволяет ее эффективно решить и реализовать безопасный удаленный доступ к SCADA.

Основной проблемой удаленного доступа с точки зрения информационной безопасности является организация защищенного канала связи, гарантирующего конфиденциальность, целостность и аутентичность данных.

Использование криптографических стеков популярных операционных систем позволяет получить лишь ограниченные гарантии. Но даже если рабочая станция SCADA хорошо защищена, обеспечить безопасность удаленных клиентов намного сложнее, поскольку они работают в условиях повышенной возможности компрометации.

Программные компоненты KasperskyOS функционируют в защищенном окружении и под постоянным контролем, что дает намного более высокие, по сравнению с другими ОС, гарантии безопасности. В сценарии удаленного доступа средствами KasperskyOS независимо от гостевой ОС реализуется защищенный канал информационного обмена с возможностью использования различных криптографических алгоритмов, например, симметричных схем шифрования.

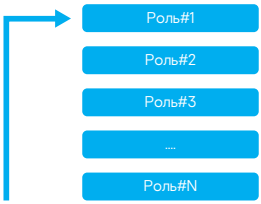
Средствами KSH производится эмуляция сетевого адаптера для виртуальной машины, при этом трафик перехватывается в KSH и зашифровывается с использованием криптографического стека KasperskyOS.

SCADA PcVue версии 12 предоставляет веб-интерфейс для удаленного доступа (WebVue).

Трафик WebVue с рабочей станции SCADA защищается средствами KasperskyOS и перенаправляется на удаленную рабочую станцию, также работающую под управлением KasperskyOS с установленным приложением Web Browser. Поскольку удаленная рабочая станция управляется KasperskyOS, для нее также можно обеспечить высокие гарантии безопасности.

Таким образом, требования целостности, конфиденциальности и аутентичности выполняются на всем пути передачи данных между рабочей станцией SCADA и рабочей станцией удаленного доступа.

Ролевое разграничение доступа



При аутентификации пользователя средствами KasperskyOS появляется возможность реализации сценариев, основанных на ролевой модели доступа.

В KasperskyOS идентификатор роли может быть использован в качестве параметра в политиках безопасности, реализуемых Kaspersky Security System. Возможность подмены идентификатора при этом исключается.

Рассмотрим возможные варианты ролей и соответствующих полномочий, применимых к SCADA-системе PcVue. Данный список является неполным и служит для иллюстрации подхода. В реальных проектах он может быть модифицирован или расширен.

Роль №1 – «Наблюдатель». Позволяет получить доступ к гостевой ОС для просмотра ее экрана, без возможности совершения каких-либо действий (доступен вывод на дисплей, но недоступны устройства ввода).

Используя канал информационного обмена между гостевой ОС и KasperskyOS, последняя может уведомить гостевую ОС о входе пользователя в систему, после чего гостевая ОС может отобразить информацию, предназначенную для данного пользователя.

Роль №2 – «Локальный оператор SCADA». Позволяет оператору получить доступ к Web browser – локальному приложению KasperskyOS, работающему совместно с гипервизором. Оно предварительно сконфигурировано таким образом, чтобы обеспечить выделенный контролируемый канал связи с компонентом WebVue SCADA PcVue. Выделенный контролируемый канал реализуется с использованием эмулируемого сетевого устройства для виртуальной машины, в контексте которой работает SCADA PcVue. Таким образом, для SCADA взаимодействие полностью прозрачно, но поверхность атаки на SCADA при этом невелика. Пользователь лишен возможности эскалации привилегий с использованием уязвимостей гостевой ОС, поскольку он не взаимодействует с ней напрямую.

При этом веб-интерфейс, предоставляемый SCADA, практически не налагает ограничений на функциональность решения, что позволяет полноценно использовать доступные пользователю возможности PcVue.

Роль №3 – «Администратор». Предоставляет максимальные полномочия для пользователя. При аутентификации с полномочиями администратора пользователь получает полный доступ к интерфейсу гостевой операционной системы, включая ввод данных с помощью клавиатуры и мыши. Дополнительно, в зависимости от настроек решения, применяемых на уровне KasperskyOS, может быть предоставлен либо ограничен доступ пользователя к периферийным устройствам, таким как флеш-накопители, приводы компакт-дисков и др.

Пользователь с правами администратора может конфигурировать гостевую ОС, модифицировать проект SCADA, и фактически его полномочия соответствуют полномочиям обычного оператора рабочей станции SCADA, если решение запущено без гипервизора.

Перечень приведенных выше ролей не является исчерпывающим. В зависимости от сценариев использования могут вводится новые роли с различными полномочиями.

Следует отметить, что перечисленные выше сценарии защиты требуют минимальных модификаций как самой SCADA, так и гостевой ОС. Однако если компоненты, работающие в контексте создаваемой средствами KSH виртуальной машины, «знают» о KasperskyOS и могут использовать сервисы, предоставляемые на ее стороне, появляется широкий набор дополнительных возможностей для SCADA-системы как с точки зрения функциональности, так и с точки зрения безопасности.

О «Лаборатории Касперского»

«Лаборатория Касперского» – международная компания, работающая в сфере информационной безопасности с 1997 года. Глубокие экспертные знания и многолетний опыт компании лежат в основе защитных решений и сервисов нового поколения, обеспечивающих безопасность бизнеса, критически важной инфраструктуры, государственных органов и рядовых пользователей. Обширное портфолио «Лаборатории Касперского» включает в себя передовые продукты для защиты конечных устройств, а также ряд специализированных решений и сервисов для борьбы со сложными и постоянно эволюционирующими киберугрозами. Технологии «Лаборатории Касперского» защищают более 400 миллионов пользователей и 270 тысяч корпоративных клиентов во всем мире.

Об ARC Informatique

ARC Informatique (Франция), разработчик программных продуктов PcVue Solutions, работает на рынке промышленного программного обеспечения уже более 35 лет. Компания имеет головной офис в Париже и 15 офисов по всему миру: в США, Европе, Азии и Латинской Америке, а также свою партнерскую сеть. Каждая дочерняя компания занимается продажами и технической поддержкой, а также участвует в разработке программных продуктов. Компания сертифицирована по ISO 9001 и ISO 14001.

PcVue Solutions, набор программных и аппаратных решений, предоставляет гибкое решение и необходимые инструменты для сбора данных, диспетчерского контроля, управления сетью, аварийными сигналами и базой данных.

ARC INFORMATIQUE известна на рынке программ промышленной автоматизации, такими продуктами, как: PcVue™, ContextVue™, PlantVue™ и решениями для удаленного доступа - WebVue™, SnapVue™, TouchVue™.

Более 75 000 лицензий установлено и работает по всему миру под управлением PcVue Solutions в разных областях.

KasperskyOS®

Подробнее на os.kaspersky.ru

www.kaspersky.ru

© АО «Лаборатория Касперского», 2019. Все права защищены. Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.