Визитка

*СЕРГЕЙ СЛЕПКОВ, ведущий инженер отдела технического консалтинга, ООО «С-Терра СиЭсПи»*

# Аутентификация в системах VDI

Инфраструктура виртуальных рабочих столов (Virtual Desktop Infrastructure, VDI) сегодня является мощным инструментом для снижения эксплуатационных расходов и экономии на лицензиях для необходимого программного обеспечения

Системы VDI позволяют пользователям получить доступ к своим рабочим машинам с необходимым набором программ из любой точки мира, повышая мобильность бизнеса и одновременно снижая расходы на ИТ-инфраструктуру. Современные системы удаленного доступа к VDI поддерживают широкий спектр пользовательских устройств и операционных систем: как мобильных телефонов и планшетов, так и стационарных терминалов и тонких клиентов. И контроль доступа с такого большого количества возможных устройств становится серьезной задачей для специалистов ИБ.

Несмотря на то что инфраструктура VDI заметно увеличивает производительность работы сотрудников компании, она также требует применения надежных средств аутентификации и авторизации пользователей, которые получают удаленный доступ к ресурсам компании. Несанкционированный доступ – одна из основных угроз информационной безопасности в системах VDI. В наши дни все чаще в СМИ появляется информация о взломах аккаунтов как популярных пользовательских сервисов, так и корпоративных ресурсов: фишинг, вирусы, кей-логгеры. Взлом аккаунта пользователя VDI с доступом к сети компании представляет еще большую угрозу, финансовые риски которой нельзя недооценивать.

Для нейтрализации этих угроз корпоративные заказчики все чаще выбирают строгую двухфакторную аутентификацию с использованием персональных токенов и смарт-карт. И хотя технологиям аутентификации по токенам и смарт-картам уже не один десяток лет, широко внедряться они начинают только в последнее время, с появлением унифицированных систем управления доступом к различным системам (в том числе и СКУД). Использование одноразовых паролей (One Time Password, OTP) в системах VDI менее эффективно и затруднено из-за широкого спектра различных пользовательских устройств и рабочих станций, хотя такая функциональность тоже есть у лидеров рынка. Внедрение токенов, смарт-карт и персональных X.509 сертификатов позволяет максимально защитить периметр от несанкционированного доступа и усилить контроль подключенных пользователей, хотя и требует дополнительных ресурсов на управление и менеджмент ключевых носителей и PKI-инфраструктуры.

Удаленный доступ пользователей к критичной информации в российских реалиях накладывает дополнительные требования по защите передаваемых данных, например, необходимо применять VPN с криптографической защитой с использованием ГОСТ алгоритмов и стандартов. И это добавляет определенные неудобства в использовании и сложности в управлении: смарт-карта для СКУД, токен/смарт-карта для доступа к VDI и логина в домен (RSA), токен для хранения ключей для VPN и ЭП (ГОСТ). Довольно-таки серьезный набор брелоков у пользователя, и за всеми надо следить, управлять, регулярно обновлять.

У одного из наших заказчиков была такая задача, и решение ее оказалось довольно интересным. Сегодня смарт-карты и токены имеют flash-память размера, достаточного для записи туда нескольких ключей от разных систем. Это позволяет разместить персональный RSA-сертификат для логина в домен (в том числе и посредством VDI) и персональный ГОСТ-сертификат для удаленного доступа и электронной подписи документов и сообщений на одном USB-токене или смарт-карте с доступом к СКУД – на выбор пользователя. Современные системы управления доступом и ключевыми носителями тоже не стоят на месте и дают возможность привязать к одной учетной записи пользователя несколько ключей для различных нужд, имеют удобное и наглядное отображение и управление всем набором из единой консоли. И, что особо приятно, среди лидеров в этой области есть и российские разработчики.

Использование строгой двухфакторной аутентификации предотвращает угрозы проникновения злоумышленника в корпоративную сеть через двери систем VDI, однако не спасает от попадания различных троянов и вирусов внутри самой терминальной сессии. Естественно, антивирусы и средства контроля вторжений и аномальной активности сегодня являются обязательными компонентами на клиентских рабочих местах, однако и они не всегда обеспечивают должный уровень защиты. Наиболее безопасным решением

может быть использование замкнутой программной среды на клиентской стороне. Такой вариант особенно актуален, когда затруднен контроль над составом и содержанием удаленных рабочих станций – например, многочисленные информационные киоски, терминалы обслуживания клиентов или мобильные пункты продаж.

Ярким примером терминального решения с замкнутой программной средой является «ПОСТ» от российской компании «С-Терра СиЭсПи», основанный на технологии среды построения доверенного сеанса (СПДС). Специальный загрузочный USB-носитель содержит в себе эталонный образ операционной системы с преднастроенным терминальным клиентом – RDesktop, Citrix Receiver или VMware View Client. Во время загрузки с такого USB-носителя происходит контроль целостности загружаемой операционной среды, автоматически поднимается VPN-соединение с шифрованием по ГОСТ-алгоритмам и открывается терминальная сессия. При таком подходе у пользователя отсутствует возможность запустить какое-либо приложение, исчезает угроза появления вредоносного ПО и проникновения его в корпоративную инфраструктуру. Специальный загрузочный USB-носитель хранит в себе ключи и ГОСТ-сертификат, что позволяет обеспечить строгую двухфакторную аутентификацию пользователя.

Широкое применение это решение получило при использовании многопользовательского режима в составе терминальной станции или тонкого клиента, когда устройства СПДС «ПОСТ» являются несъемными загрузочными носителями и обеспечивают проверку целостности, контроль запускаемой программной среды и шифрование передаваемых данных. Благодаря наличию функции проброса в терминальную сессию подключаемых USB-токенов и смарт-карт у сотрудников появляется возможность доступа к инфраструктуре с помощью своего единого персонального токена из любого места и в любое время: с ноутбука из дома по VPN через Интернет, с терминальной станции в пункте продаж, со своего рабочего места в офисе.

Производители токенов тоже не стоят на месте и предлагают заказчикам все более широкий спектр различных форм-факторов и исполнений, в отличие от традиционного USB-формата – MicroUSB, Secure MicroSD, Bluetooth. Особенно интересны Bluetooth-токены, позволяющие аутентифицироваться, не доставая свой токен из кармана. Это дает возможность использовать мобильные устройства и планшеты пользователей, расширяя границы доступа к единой системе виртуализации рабочих столов и приложений.

## Наиболее безопасное решение — использование замкнутой программной среды на удаленной рабочей станции

• • •

В наше время популярность различных идентификационных токенов и смарт-карт растет не только в сфере ИБ и доступа к ИТ-сервисам. Во многих странах идут разработки и внедрение универсальных ID-карт как замены традиционному паспорту. В некоторых странах такие карты уже пережили не одно поколение и содержат не только персональную информацию о человеке, но сочетают в себе банковскую карту, проездной билет на автобус/метро, хранят истории болезней и посещений медучреждений. В Китае, например, последнее поколение ID-карт позволяет записать на смарт-карту абсолютно любую информацию при наличии специального авторизированного устройства. И уже сейчас на вашу личную ID-карту можно записать ваш ключ для доступа к СКУД на работе. И это только начало.

Не за горами то время, когда унификация идентификационных карт и токенов будет повсеместна, и для аутентификации в любом сервисе вам понадобится лишь приложить карту к считывателю. Или чип, вживленный под кожу. Как в фантастических фильмах. ADV

Применение технологии среды построения доверенного сеанса (СПДС) дает, в сравнении с традиционными технологиями защиты удаленных и мобильных клиентов, целый ряд преимуществ:

- Обеспечивается целостность программной среды терминала удаленного доступа. При всякой инициализации доверенного сеанса производится загрузка эталонного образца СФ. Никакие данные по результатам работы пользователя в течение предыдущих сеансов в СФ не вносятся. Таким образом, можно отказаться от применения средств защиты от вирусов, опасного ПО и закладок. Это обстоятельство позволяет не только сэкономить средства на антивирусном программном обеспечении, но и существенно облегчить процесс эксплуатации мобильных терминалов, поскольку нет необходимости контролировать их конфигурацию, следить за составом программного обеспечения.
- Обеспечивается изоляция вычислительного процесса клиента удаленного доступа в ходе доверенного сеанса: модуль загрузки среды функционирования исключает взаимодействие с «грязной «периферией» и загрузку недоверенного программного обеспечения.
- Строгая аутентификация пользователя при доступе к доверенному сеансу работает по традиционной двухфакторной схеме: пользователь аутентифицируется перед загрузкой СФ при помощи стойкого установленного администратором безопасности пароля (число попыток ввода пароля ограничено), доступ в корпоративную сеть и к серверным ресурсам осуществляется при помощи цифрового сертификата X.509, хранящегося на защищенном носителе. При необходимости, эти средства аутентификации могут быть усилены средствами аутентификации в составе целевых приложений.
- Сетевая среда доверенного сеанса полностью изолирована от посторонних воздействий: трафик шифрован на основе криптоалгоритма ГОСТ 28147, обеспечивается целостность передаваемых данных и целостность потока пакетов. Поскольку в защищенную сеть может войти только владелец секретного ключа – контроль доступа в защищенный сегмент сети приобретает криптографическую стойкость, недоступную для некриптографических методов контроля сетевого доступа.