БЕЗОПАСНОСТЬ ВЕБ-ТЕХНОЛОГИЙ

М. **Смирнов**, itech

Веб-технологии стали неотъемлемой частью нашей жизни и работы, их использование уже принесло грандиозное расширение наших возможностей и сулит еще большее в будущем. Это утверждение в полной мере применимо к интеграции веб-технологий и автоматических систем управления производством. Ее дивидендом в первую очередь является стандартизация передаваемых данных, кроссплатформенность — огромное достоинство, когда мы имеем дело с гетерогенной средой. Информация передается в едином формате и доступна для просмотра и обработки с помощью стандартных средств. Это делает применение веб-технологий целесообразным уже на уровне локальных объектов без доступа в глобальные вычислительные сети. Использование же последних (то есть, прежде всего, сети Интернет) дает широкие возможности дистанционного мониторинга и управления. Однако, как обычно, розы не обходятся без шипов. Например, недостатком применения Интернета является сравнительно низкая скорость передачи информации. Впрочем, этот параметр, как правило, не является критичным для достижения преследуемых целей. Гораздо большей проблемой являются различные угрозы нарушения безопасности. Для защиты от них необходимо принимать целый комплекс мер и отслеживать современные тенденции в этой области; в противном случае возможны серьезные финансовые потери, «утечка» конфиденциальной информации, парализация работы предприятия и нанесение ущерба окружающей среде.

АВТОМАТИЗАЦИЯ ПРОИЗВОДСТВА И ВЕБ-ТЕХНОЛОГИИ

К настоящему времени разработано множество способов использования всемирной сети Интернет в автоматизации. Будучи предназначенными в основном для получения оперативных данных об основных параметрах процессов, они наиболее активно применяются на уровне SCADA. Эти технологии позволяют получать информацию о состоянии объектов, порою находящихся за тысячи километров от пользователя.

Распространенным и действенным способом использования сети Интернет в системах SCADA является передача уведомлений (обычно сигналов тревоги) по электронной почте. За счет этого простого метода пользователи SCADA, имея в своем распоряжении мобильные устройства с функцией приема таких сообщений, могут практически всегда и везде оперативно получать важнейшую информацию о состоянии объектов.

Более широкий спектр сведений может передаваться с помощью отчетов в формате HTML, в которые может входить графическая информация, например диаграммы. Пользователь может просматривать эти отчеты дистанционно с помощью веб-браузера. Также распространено создание отчетов в формате XLS.

Существуют и технологии, предоставляющие возможность не только мониторинга, но и непосредственного дистанционного управления. Для этого используются системы SCADA с поддержкой управления по сети по стеку протоколов TCP/IP. При этом компьютер пользователя может быть либо «толстым клиентом» (на нем имеется и обрабатывается копия проекта управления производством, исполняемого на сервере, а по сети передаются только текущие данные о состоянии объектов и команды пользователя), либо «тонким клиентом» (без копии проекта на нем; обработка данных происходит на сервере, на компьютере же удаленного пользователя устанавливаются подключаемые модули для веб-браузера, принимается информация о проекте и происходит визуализация).

Кроме того, существует технология дистанционного управления с помощью веб-серверов в программируемых логичес-

ких контроллерах без использования систем SCADA. При этом вторичная обработка данных может осуществляться на компьютере пользователя – в целях снижения загрузки процессора ПЛК.

АСПЕКТЫ БЕЗОПАСНОСТИ

Обеспечение безопасности веб-технологий складывается из указанных ниже составляющих.

- **Конфиденциальность.** Необходимо обеспечивать передачу информации по сети без утраты конфиденциальности.
- **Санкционированный доступ.** Необходимо обеспечивать аутентификацию пользователей, блокируя для посторонних лиц доступ к важным узлам.
- **Защита от вредоносных программ и хакерских атак.** Необходимо защищать компьютерные системы от хакерских атак, вирусов и других вредоносных программ.

КОНФИДЕНЦИАЛЬНОСТЬ

Передача данных по сети Интернет обладает огромными преимуществами, обусловленными ее протяженностью и доступностью. Однако в связи с этими же характеристиками при использовании Интернета остро встает проблема обеспечения конфиденциальности. Для безопасной передачи данных по публичных каналам используется метод организации виртуальных частных сетей VPN (англ. virtual private network). При его применении за счет шифрования внутри публичной сети создаются частные каналы, недоступные для посторонних лиц.

Различают симметричное и асимметричное шифрование. В первом из этих вариантов для шифрования и расшифровки информации используется один и тот же ключ. Достоинствами этой схемы по сравнению с асимметричной криптографией являются скорость и простота реализации, меньшая длина ключа при аналогичной стойкости и изученность. Главный ее недостаток – то, что единственный ключ должен каким-либо образом передаваться между получателем и отправителем информации, а его «утечка» делает информацию доступной для посторонних. Кроме того, недостатком является сложность управления ключами в большой сети (где требуется огромное их количество для осуществления различных операций).

При асимметричном же шифровании применяются два ключа, один из которых является открытым, а другой – закрытым (секретным). Получатель информации создает эти ключи и передает открытый отправителю, при этом его «утечка» не несет угрозы. Закрытый ключ не передается по ненадежным каналам. Отправитель шифрует информацию с помощью открытого ключа, после чего она может быть расшифрована только с использованием закрытого, и передает ее получателю. Тем не менее при применении этой схемы в чистом виде ничто не может помешать злоумышленнику отправить получателю с помощью открытого ключа какую-либо свою информацию в неблаговидных целях. Для решения этой проблемы используются цифровые сертификаты, заверяемые уполномоченными на это органами.

Для приведения к балансу преимуществ и недостатков этих способов шифрования применяются гибридные схемы. В них большие объемы данных шифруются симметричной криптографией с помощью сеансового ключа, а для его передачи используется асимметричная криптография.

Основной дилеммой в отношении безопасности, появляющейся при подключении систем SCADA к Интернету, является выбор между, с одной стороны, использованием стандартных продуктов (например, операционных систем семейства Windows), унифицированных технологий (таких как OLE / Active X и OPC-серверы) и общих методов защиты, с другой – применением уникальных решений. Первый подход, все более распространяющийся, является выражением прогрессивной тенденции интеграции, облегчая взаимодействие и наращивание систем. Однако он также повышает их «прозрачность» для злоумышленников и вероятность «взлома»; например, при получении злоумышленниками сведений о какой-либо уязвимости в одной из ОС семейства Windows у них появляется возможность использовать ее в своих интересах в любых компьютерных системах, в которых применяется эта ОС (причем «работа» в этом направлении в отношении ОС Windows и других распространенных продуктов постоянно и интенсивно ведется широкими кругами злоумышленников). По этой причине уникальные «закрытые» решения могут быть предпочтительнее в отношении безопасности (хотя сама по себе уникальность этого еще не гарантирует, – требуется высокий уровень разработки). Таким образом, необходимо найти верный баланс между «закрытостью» и «открытостью». Для повышения защиты, например, могут применяться специальные методы шифрования, такие как сетевые протоколы собственной разработки. Используемые же стандартные решения должны проверяться и своевременно обновляться для устранения уязвимостей в них, которые становятся известными.

САНКЦИОНИРОВАННЫЙ ДОСТУП

Однако все усилия по обеспечению конфиденциальной передачи данных окажутся бессмысленными, если злоумышленник получит непосредственный доступ к важным узлам. При использовании традиционного способа аутентификации с помощью пользовательского идентификатора («логина») и пароля необходимо применять надежные методы защиты этих данных от посторонних и обеспечивать правильное обращение с ними персонала. В целом такой способ

Безопасность веб-технологий

аутентификации приходится признать не совсем надежным: используемые идентификаторы и пароли могут быть довольно легко подобраны, перехвачены или получены какими-либо другими способами; значительную роль играет человеческий фактор; кроме того, пользователя трудно уличить в неправомерных действиях, так как он может сослаться на то, что его пароль был украден и т. п. В настоящее время существует ряд других, более надежных, способов аутентификации: например, с использованием цифровых сертификатов и аппаратных средств

для их применения – смарт-карт и токенов (специальных USB-устройств), а также с помощью криптокалькуляторов и различных биометрических решений. В последних может использоваться аутентификация по отпечаткам пальцев, радужной оболочке или сетчатке глаза, лицу, форме кисти руки, голосу, почерку, ДНК. Наиболее надежным из вышеописанных вариантов в настоящее время считается использование цифровых сертификатов с помощью специальных аппаратных средств. Зачастую различные способы аутентификации применяются совместно, что повышает безопасность.

Рассмотрим подробнее схему контроля над доступом к защищаемым ресурсам (данным и функциям) в АСУ ТП. Так как здесь необходима конкретизация, в качестве примера системы, способной обеспечить безопасность АСУ ТП со сложной структурой, большим количеством узлов, пользователей, а также методов получения данных и работы с ними, приведем решение, которое реализовано в программно-инструментальном комплексе InfinitySuite от компании ЭлеСи. Этот SCADA-пакет работает с ОС семейства Windows, и его система обеспечения безопасности интегрируется со службой каталогов MS Active Directory, при контроле над доступом используются учетные записи пользователей Windows, аутентификация проводится по протоколам Kerberos и NTLM.

Система обеспечения безопасности пакета InfinitySuite функционирует как на уровне серверов, так и на уровне клиентов.

Защищаемые ресурсы на уровне сервера ввода-вывода InfinityServer:

- подключение к серверу оперативных данных;
- оперативные данные о состоянии технологического процесса. Имеющие доступ лица делятся на две категории: с правами на чтение и на изменение значений. Право на изменение может выдаваться по каждому сигналу в отдельности;
- администрирование сервера оперативных данных и подсистемы резервирования. Контролируются запуск и останов сервера, права доступа к агенту резервирования и подключение к нему, резервные переходы;
- конфигурирование сервера оперативных данных. Контролируются права доступа к конфигурации сервера, ее чтение и изменение.

Разветвленная система защиты в пакете InfinitySuite реализована и на уровне клиентских приложений. Она позволяет распределять права доступа не только по отдельным приложениям, но и по наборам функций в рамках одного приложения, а также ограничивать доступ к сторонним приложениям и функциям ОС, что зачастую является необходимым. Общий для всех клиентских приложений аспект защиты – право пользователя на их запуск. Также защищаются следующие функции отдельных компонентов пакета InfinitySuite:

- в среде разработки и исполнения графических мнемосхем InfinityHMI: просмотр мнемосхем, переход в режим разработки, видимость слоев мнемосхемы, запуск редактора VBA, закрытие программы;
- в программе для отображения истории изменения технологических параметров InfinityTrends: просмотр дерева технологических параметров, администрирование программы;
- в программе для отображения сообщений о событиях и авариях InfinityAlarms: квитирование сообщений, администрирование программы.

И, разумеется, защищается сама настройка параметров в InfinityClientSecurity – системе управления доступом пользователей к ресурсам. С помощью нее также возможно определять права доступа по интервалам времени. Такая разветвленная схема контроля позволяет минимизировать вероятность нарушения безопасности АСУ ТП.

ЗАЩИТА ОТ ВРЕДОНОСНЫХ ПРОГРАММ И ХАКЕРСКИХ АТАК

Важным аспектом обеспечения безопасности веб-технологий является также защита от вредоносных программ. Под таковыми подразумевается программное обеспечение (ПО), предназначенное для несанкционированного получения, копирования, уничтожения, модифицирования информации или блокирования доступа к ней, а также для нарушения работы компьютера или компьютерной сети. Зачастую все вредоносные программы называют «вирусами», но специалисты используют это название для обозначения только одной из разновидностей вредоносного ПО. Впрочем, единой, принятой всеми классификации сейчас не существует. Однако важно знать типы вредоносных программ, их действие, пути распространения и способы защиты от них. При этом следует учитывать, что зачастую одна вредоносная программа сочетает в

себе свойства различных типов.

Существуют вредоносные программы, способные к саморепликации (размножению) на зараженном компьютере. Собственно, это и является содержанием понятия «вирус» в узком смысле. Такой возможностью обладают многие образцы вредоносного ПО, но не все. Программы, способные к самостоятельному распространению через компьютерные сети, называются «сетевыми червями». Они могут передаваться по электронной почте, сетям обмена данными между мобильными устройствами, P2P, IRC и другим сетям. Большинство «червей» распространяются в виде файлов, но существуют и такие, которые передаются как сетевые пакеты и проникают непосредственно в память компьютера. Вредоносные программы, маскирующиеся под полезное ПО (зачастую с выполнением его полезных функций) для совершения несанкционированных действий, обычно называются «троянскими программами» или просто «троянами». Различные средства для сокрытия посторонней активности (имитации нормального состояния системы) как таковые принято называть «руткитами» (rootkit). Программы, предоставляющие возможность несанкционированного дистанционного управления компьютером, именуются «backdoor-программами» (англ. «задняя дверь»). Вредоносное ПО может получать несанкционированный доступ к ресурсам за счет использования ошибок в операционных системах и прикладных программах (или даже специально созданных разработчиками возможностей), подбора паролей (по словарям наиболее распространенных или простым перебором), извлечения паролей и другой важной информации из сетевого трафика. Шпионские программы (spyware), попадая на компьютер и инсталлируясь на нем, могут собирать различную информацию – вплоть до снимков экрана, паролей, параметров сетевых подключений, сведений о посещенных веб-сайтах, используемом ПО и нажатиях клавиш. Кроме того, существуют вспомогательные вредоносные программы, предназначенные для загрузки и установки себе подобных, информирования злоумышленника и т. д.

Злоумышленников, которые, обладая соответствующей квалификацией, совершают какие-либо злонамеренные действия в сфере информационных технологий, в настоящее время принято называть «хакерами» (сейчас такое словоупотребление является практически общепринятым, хотя изначально этим словом назывались просто специалисты-энтузиасты, а компьютерные злоумышленники именовались «крэкерами»). Вредоносные программы, по сути, являются инструментами, служащими хакерам для осуществления их неблаговидных целей. Основными направлениям «работы» этих злоумышленников являются хищение информации, получение контроля над компьютерными системами и вывод их из нормального состояния. Помимо описанного выше вредоносного ПО, можно упомянуть еще ряд угроз, исходящих от хакеров.

Существует немало методов, с помощью которых они могут перехватывать и изменять сетевой трафик, выдавать себя за легитимного пользователя или задействовать свои команды (осуществлять так называемые «инъекции») в недостаточно защищенных системах. Большую опасность представляют злоумышленники, действующие изнутри атакуемой компании.

Использование хакерами человеческого фактора известно как «социальная инженерия»; например, злоумышленник может каким-либо образом подтолкнуть сотрудника атакуемой компании зайти со своего рабочего компьютера на веб-узел, с которого распространяется вредоносное ПО, или выведать у него пароль.

Хакерами могут осуществляться атаки типа DoS (англ. denial of service – «отказ в обслуживании») или DDoS (англ. distributed denial of service – «распределенная атака типа “отказ в обслуживании”»), для этого ими может применяться специальное вредоносное ПО, действующее извне компьютера жертвы. В ходе такой атаки хакер создает ситуацию, в которой компьютерная система жертвы не может нормально функционировать. Например, злоумышленник может задействовать все вычислительные ресурсы на стороне жертвы, посылая по сети огромное количество бесполезных данных, в результате чего легитимные пользователи не смогут получить доступ к этим ресурсам. Атака производится с одного компьютера (DoS) или группы компьютеров (DDoS), которую обычно составляют машины, зараженные распространяющимся по сети вредоносным ПО. Такие зараженные группы компьютеров называются «ботнетами» (англ. botnet) и могут применяться злоумышленниками не только для DDoS-атак, но и в некоторых других целях.

Для защиты от вредоносных программ и хакерских атак необходимо использовать надежное программное обеспечение и своевременно обновлять его, применять сетевые экраны (брандмауэры), действенные и также своевременно обновляемые антивирусные средства. Кроме того, требуется соблюдать некоторые меры предосторожности (например, не открывать полученные из ненадежных источников файлы и не заходить на непроверенные веб-узлы).

Итак, угрозы велики, но есть и достаточно эффективные средства защиты от них. К настоящему времени уже сформировались как определенные традиции в среде хакеров, так и каноны противодействия исходящим от них угрозам. С другой стороны, имеет место постоянная конкуренция: хакеры стремятся обойти средства защиты, а разработчики таких средств – сделать это невозможным. К сожалению, иногда злоумышленники достигают успеха. Положительной стороной такой борьбы можно считать то, что в процессе нее происходит общее развитие технологий. Быть всегда на шаг впереди злоумышленников – вот задача того, кто хочет защитить информационные системы. К необходимым мерам относится использование проверенных программных продуктов и аппаратных средств, своевременное обновление программ для устранения уязвимостей в них, применение надежных методов шифрования и аутентификации, эффективного и своевременно обновляемого антивирусного программного обеспечения, контроль над трафиком с помощью сетевых экранов.

Одной из альтернатив является выбор между программными и аппаратными средствами обеспечения безопасности. Как правило, программные средства более выгодны по цене, однако с помощью аппаратных может достигаться более высокая надежность.

При дистанционном управлении метод «толстого клиента» предпочтителен в отношении безопасности по сравнению с использованием «тонкого клиента», так как в последнем варианте через сеть передается больше важных данных.

Не меньшую роль, чем технические средства защиты, играет осведомленность сотрудников о принципах обеспечения безопасности и соблюдение ими этих принципов, а также распределение полномочий. Следует распределять ключевые функции, такие как администрирование систем, между разными сотрудниками, – это уменьшает возможный ущерб как в случае захвата посторонними злоумышленниками полномочий кого-либо из них, так и в том случае, если сам сотрудник (или бывший сотрудник) по какой-либо причине идет против интересов компании.

Грамотные, комплексные, последовательные и своевременные меры для обеспечения безопасности веб-технологий позволяют минимизировать вероятность ее нарушения. Ими ни в коем случае и ни в какой степени нельзя пренебрегать, особенно в сфере АСУ ТП, инциденты в которой могут не только причинить прямой ущерб предприятию и ухудшить его репутацию, но и привести к негативным социальным и экологическим последствиям.