Благодаря свойствам предложенного метода появляется возможность создания новых технологий защиты информации.

В докладе рассматривается один из вариантов реализации данного метода на основе функций с переменной длиной образа и некоторые возможные его применения.

Одним из таких применений, является технология для реализации безопасных телекоммуникационных связей между абонентами по открытым каналам (например, Интернет), которая обеспечивает контроль целостности передаваемой информации, идентификацию отправителя и аутентификацию сообщений.

УЯЗВИМОСТИ MICROSOFT INTERNET EXPLORER

А.Л. ГАРЦУЕВ, И.Н. ОБЕРНИХИН, А.В. БОРЗЕНКОВ

Благодаря своей популярности Microsoft Internet Explorer привлекает к себе внимание многочисленных хакеров, а также профессионалов по компьютерной безопасности.

Существует несколько типов уязвимостей, касающихся браузера Internet Explorer.

1. Уязвимости, приводящие к нестабильной работе браузера или его "зависанию".

2. Межсайтовый скриптинг (cros-site scripting). Злонамеренный сайт в интернете может узнать содержимое ваших "cookie"-файлов. Полученная информация может быть использована для выяснения таких личных данных пользователя, как адрес его электронной почты или, например, точных сведений о покупках, совершенных им на каком-либо сайте. Эти уязвимости также позволяют читать и выполнять локальные файлы на системе клиента, то есть те файлы, которые уже находятся (предустановлены) на копьютере.

Существует универсальная уязвимость, связанная с методом showHelp(). Последний патч от Microsoft (6 февраля 2003 г.), который должен был справиться с этой проблемой, все варианты использования не покрывает. Возможности: чтение cookie, чтение произвольных файлов, запуск файлов.

3. Выполнение произвольного кода, загруженного с сервера.

Используя уязвимость с showhelp(), можно запускать программы с параметрами. К примеру вставить в качестве запускаемой программы "mshta.exe" (для работы с активными web-страницами) и передать ей параметр — ссылку на активную html-страницу (name.hta). Эта страница в свою очередь может содержать код vbscript, который имеет права на чтение/запись/запуск любых файлов.

Литература

1. Абашин В.В., Бокун Н.В., Борзенков А.В. Анализ угроз информационной безопасности и путей защиты от них// Известия Белорусской инженерной академии, 2002. Т. 1(13)/2, С. 159–161.

ИСПЫТАНИЯ ПРОГРАММНЫХ ПРОДУКТОВ НА ОТСУТСТВИЕ НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ

Е.В. ШИПЕРКО, Л.И. КИРИЛЛОВА

Введение

В последние годы в Республике Беларусь значительно активизировалась работа по созданию системы сертификации в области защиты информации. Это можно объяснить тем, что происходящие в стране процессы существенно затронули организацию системы защиты информации во всех ее сферах – разработки, производства, реализации, эксплуатации средств защиты, подготовки соответствующих кадров. Исследование средств защиты информации (СЗИ), поступающих на рынок Республики Беларусь, затрагивает ряд актуальных проблем. Рынок СЗИ сегодня представлен продукцией, как зарубежных производителей, так и отечественных. Эта продукция должна быть сертифицированной. В докладе рассматриваются общие вопросы сертификации СЗИ и вопросы сертификации программных средств.

Состояние системы сертификации СЗИ

В Республике Беларусь действует Национальная система сертификации, созданная республиканским органом по стандартизации, метрологии и сертификации, и могут действовать созданные другими юридическими лицами системы сертификации продукции по показателям, по которым законодательством Республики Беларусь проведение обязательной сертификации не предусмотрено.

В Национальной системе сертификации проводится как обязательная, так и добровольная сертификация, могут быть созданы системы сертификации по видам продукции и по отдельным требованиям.

Система сертификации продукции имеют свои знаки соответствия.

Система сертификации и знаки соответствия подлежат регистрации в порядке, установленном республиканским органом по стандартизации, метрологии и сертификации.

Участниками обязательной сертификации являются республиканский орган по стандартизации, метрологии и сертификации, органы по сертификации, аккредитованные испытательные лаборатории, изготовители (продавцы) продукции.

До недавнего времени испытания СЗИ в Республике Беларусь проводились специалистами Государственного центра безопасности информации (ГЦБИ) в добровольном порядке, в связи с

отсутствием нормативно-методической базы. ГЦБИ аккредитован Госстандартом Республики Беларусь в качестве органа по сертификации средств и продукции по требованиям безопасности информации (аттестат аккредитации № BY/112 01.1.0.0062 от 15 октября 2000г.). Во взаимодействии с Госстандартом Республики Беларусь ГЦБИ проводит работы по созданию и аккредитации лабораторий, способных проводить сертификационные испытания СЗИ и продукции по требованиям безопасности информации.

Одной из таких лабораторий является лаборатория сертификационных испытаний, организованная на базе УП "Научно-исследовательский институт технической защиты информации". В настоящее время готовится доаккредитация этой лаборатории по следующим направлениям:

сертификационные испытания аппаратно-программных СЗИ от несанкционированного доступа (НСД);

сертификационные испытания на отсутствие компьютерных вирусов и вредоносных программ;

сертификационные испытания программного обеспечения (ПО) СЗИ на отсутствие недекларированных возможностей (НДВ).

В Республике Беларусь сертификационные испытания такого характера не проводились и должного внимания проблема недокументированных возможностей ПО не получила.

Белорусский рынок СЗИ представлен продукцией различных производителей. Многие поставщики СЗИ имеют экспертные заключения на свою продукцию. В основном это СЗИ, поставляемые российскими производителями. Испытания таких СЗИ имеют свои особенности.

В ходе сертификационных испытаний выявляется соответствие/несоответствие /программно-аппаратных СЗИ нормативных актов, конкретных стандартов или других нормативных документов по стандартизации, на территории Республики Беларусь.

Сертификационные испытания аппаратно-программных СЗИ проводятся на специализированных стендах, отвечающих требованиям нормативных документов и стандартов, согласно специальным методикам, утвержденным соответствующими органами.

Результаты испытаний фиксируются экспертами в протоколах, которые являются основанием для принятия сертификационной комиссией решения о присвоении сертифицируемым СЗИ знака соответствия.

Для большинства информационных систем аппаратное обеспечение, системное и прикладное ПО, коммуникационное оборудование и эксплуатационные средства должны быть сконфигурированы воедино и протестированы во время сертификации. Результатом сертификации должна является выдача документа, который устанавливает, соответствует ли система требованиям безопасности, описывает все известные уязвимые места и сообщает все эти сведения лицу или органу, уполномоченному принимать решение об утверждении.

Что дает сертификация СЗИ?

Определенная гарантия качества СЗИ (подтвержденная сертификатом) со стороны государства с точки зрения выполняемых функций по защите. Возможность аттестации информационной системы, в которой используются сертифицированные средства защиты.

Гарантия отсутствия программных закладок, заложенных производителем с целью НСД к защищаемым системам.

Маркетинговый ход, призванный увеличить привлекательность программного продукта и поднять престиж компании-заявителя, а также повысить доверие потребителя к сертифицируемому продукту.

В дальнейшем, говоря об испытаниях ПО на отсутствие НДВ, не будем останавливаться на особенностях механизма сертификации, а более полно опишем методы, используемые при испытаниях ПО СЗИ, поскольку, кроме того, что часто испытывается как законченное изделие, в ряде случаев является составной частью всех комплексов аппаратно-программной защиты информации.

Испытания ПО СЗИ на отсутствие НДВ

Что такое недокументированные (недекларированные) возможности?

Недекларированные возможности - это программа (подпрограмма) или логически законченный набор команд, преднамеренно разработанные и внедренные в ПО с целью реализации функций, выполнение которых потенциально возможно в процессе эксплуатации; в то же время не описано в достаточном для тестирования объеме ни в одном из документов из состава программной документации на ПО (описание программы или пояснительная записка, описание применения программы, исходный текст программы).

Реализацией НДВ, в частности, являются программные закладки.

Программные закладки – преднамеренно внесенные в ПО функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций ПО, приводящих к нарушению конфиденциальности, доступности или целостности обрабатываемой информации.

Сертификация на отсутствие НДВ (программных закладок) ориентирована на специализированное ПО, предназначенное для защиты информации ограниченного доступа.

На сегодняшний день объем специализированного ПО, достаточно велик. Вопрос защиты информации актуален для организаций любой формы собственности. Потенциальными потребителями специализированного ПО являются как государственные, так и коммерческие структуры.

Сертификационные испытания ПО на отсутствие НДВ не относится пока к числу мероприятий, регулируемых Белорусским государством в интересах информационной безопасности, но с утверждением в системе сертификации Республики Беларусь проекта руководящего документа *"Защита от*

несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей" они будут нести обязательный характер.

Сертификационные испытания на отсутствие НДВ предполагают глубокое исследование ПО и связаны с анализом, как исполняемого кода, так и исходного с целью установления факта отсутствия (либо наличия) в некотором программном решении функциональных возможностей, не документированных разработчиком.

Методы испытаний основаны на общих принципах анализа программ с учетом аспектов, связанных с информационной безопасностью. Теоретические и практические работы в данной области известны давно.

При проведении сертификационных испытаний, используются классические методы, применяемые в мировой практике сертификации качества ПО.

В основе проверок лежит возможность четко соотнести исходный и исполняемый код ПО, выявить и устранить избыточность представленного на испытания исходного кода (которая присуща многим проектам, особенно большим по объему и разработанным разными программистами), однозначно определить действия ПО в процессе начальной инсталляции и деинсталляции по отношению к системным областям операционной системы ЭВМ, получить ряд других характеристик ПО.

Метод установления факта наличия или отсутствия в программах недекларированных элементов основан на оценке модели воздействия закладного элемента программы.

Оцениваемая модель предусматривает наличие в программных модулях такого элемента, который до наступления определенного события (выполнения определенного условия) является неактивным (не получает управления), и активизируется (получает управление) после выполнения некоторого условия (события).

Действия, выполняемые активизированным недекларируемым элементом, не предусмотренным функциональным назначением программы, могут быть:

разрушительными, ведущими к нарушению требуемого алгоритма функционирования ПО средств защиты информационных ресурсов;

замедляющими ход вычислительного процесса в информационных системах без нарушения алгоритма функционирования проверяемого ПО;

отвлекающими пользователя (мерцание экрана, пятно на экране и др.) без нарушения нормального хода вычислительного процесса и логики функционирования ПО и др.

Метод установления факта структурно-логического соответствия реальных и декларируемых функциональных возможностей ПО основан на оценке устойчивости функционирования, работоспособности, полноты реализации, логической корректности программ.

Данный метод позволяет без исполнения программы в машинных кодах на ПЭВМ проводить символическое тестирование корректности обработки данных:

анализируются функции программ, записанных в символическом (на языке программирования) виде, связывающих наборы входных переменных программы и выходных переменных, и участвующих в исполнении программы по определенному маршруту;

области определения входных и выходных данных для конкретных маршрутов разбиваются на соответствующие им подобласти;

разрабатываются тесты таким образом, что каждому тесту ставится в соответствие определенный набор входных и выходных переменных с конкретными границами подобластей и указанием реализуемого маршрута;

устанавливается соответствие между областями определения наборов данных (входных и выходных) и маршрутами их обработки в программе.

Обработка программой данных считается корректной, если не обнаружено несоответствия маршрутов и данных.

Результаты испытаний могут быть использованы разработчиком для проведения углубленного анализа своего продукта, планирования и реализации корректирующих воздействий по отношению к ПО в части усовершенствования процессов его разработки и сопровождения.

Несмотря на то, что разработчика ПО, которое позиционируется как средство защиты конфиденциальной информации, никто не заставляет проводить сертификацию на отсутствие НДВ (она добровольна) тем не менее, такую сертификацию стоит проводить.

Предпосылки повышения актуальности испытаний на отсутствие НДВ

Во-первых, существенно вырос уровень возможностей разнообразных СЗИ, что сделало дорогостоящими и малоперспективными мероприятия по взлому систем защиты "в лоб", без знания их принципов построения и функционирования.

Во-вторых, неизмеримо возросла значимость и ценность защищаемой информации разной степени конфиденциальности.

В-третьих, потребитель информации в целом вник в суть проблемы и стал опасаться попыток НСД к своей информации не только со стороны так называемых хакеров, но и со стороны разработчиков ПО, фискальных органов и т.п.

Итак, мы имеем две стороны одной медали:

для получения НСД к информации злоумышленнику гораздо проще воспользоваться заранее подготовленными закладками в ПО;

потребитель хочет иметь гарантии того, что таким способом к его информации доступа нет.

Наличие у производителя или поставщика ПО сертификата, подтверждающего отсутствие в продукции программных закладок, позволяет учитывать последнее обстоятельство вместе с тем, к сертифицированной продукции существенно повышается доверие старых заказчиков, крупных корпоративных потребителей. В нынешних условиях это очень важно.

Технологическая операция по динамическому анализу ПО предусматривает его тестирование. Причем, такое тестирование является углубленным, учитывающим не только функциональные возможности исследуемого ПО, но и его технологические и структурные особенности.

Полезность для разработчика для разработчика такого исследования, выполненного независимой организацией, очевидна.

Кроме того, результаты тестирования могут быть использованы разработчиком при сопровождении своего продукта, а также разработке новых версий или новых программных продуктов.

Следующий важный момент – процесс испытаний на отсутствие НДВ объективно предполагает тесный постоянный контакт испытателя и разработчика, что зачастую позволяет разработчику оперативно улучшать функциональные и потребительские свойства ПО непосредственно в процессе испытаний.

При этом в интересах разработчика испытания могут быть выполнены на его производственной базе.

О потребительских или маркетинговых преимуществах можно сказать следующее:

Государственный документ – сертификат – с определенной степенью вероятности, зависящей от уровня проведенного контроля, подтверждает тот факт, что в проверенном ПО нет явных программных конструкций, использование которых предполагает возможность НСД, нарушения целостности защищаемой информации.

По результатам проведенных испытаний ПО приобретает четкий идентификационный признак – зафиксированные контрольные суммы исходных и исполняемых файлов, позволяющий осуществлять мероприятия по контролю целостности сертифицированного ПО на этапах эго разработки, тиражирования и эксплуатации.

Тот факт, что за доставку к потребителю именно сертифицированного ПО отвечает не только его разработчик, но и проводившая испытания сертификационная лаборатория, которой нормативными документами вменены соответствующие контрольные функции, также имеет немаловажное значение для маркетинга.

Кроме того, рассматриваемый вид испытаний подтверждается соответствующим актом установки именно сертифицированного ПО на объектах конечных пользователей.

Наличие сертификата на отсутствие НДВ является неоспоримым преимуществом для программных решений, претендующих и дальше позиционироваться на государственном рынке СЗИ, поскольку процедура подтверждения и пролонгации действия сертификата, основана на анализе соответствия сертифицированных свойств вновь представляемого на сертификацию продукта по отношению к аналогичным свойствам сертифицированного эталона.

Таким образом, еще раз можно подчеркнуть то, что, используя сертифицированное на отсутствие НДВ в ПО заказчик получает средства, которые с определенной степенью вероятности делают две простые вещи:

корректно и гарантированно выполняют функции по защите его информации;

не имеют встроенных механизмов, позволяющих нанести этой информации вред.

ПРОФИЛЬ ЗАЩИТЫ ДЛЯ ОПЕРАЦИОННОЙ СИСТЕМЫ СЕРВЕРА ДЕМИЛИТАРИЗОВАННОЙ ЗОНЫ

А.И. МАТУК, С.Л. ПУГАЧ, Г.Д. ТОМИНА

1. Роль и место "Критериев оценки безопасности информационных технологий" в сфере защиты информационных технологий.

"Критерии оценки безопасности информационных технологий" ("Критерии") регламентируют все стадии разработки и квалификационного анализа продуктов и систем ИТ, отвечающих требованиям информационной безопасности. "Критерии" устанавливают метрики информационной безопасности и являются основой для создания и развития глобальной системы сертификации безопасности продуктов и систем ИТ. Согласно "Критериям" [1], безопасность ИТ может быть достигнута посредством применения предложенной в них технологии разработки и общей схемы сертификации продуктов и систем ИТ.

"Критерии" позволяют использовать множество независимых частных показателей безопасности и ранжировать требования безопасности по частично упорядоченному набору шкал. Отказ от единой шкалы ранжирования требований безопасности позволяет достичь адекватности реализации средств защиты объекта оценки (ОО) принятой политике безопасности организации, что свидетельствует о преобладании "качества" обеспечения защиты над "количеством" и позволяет потребителю не только приспособить требования к своим нуждам, но и оптимизировать выбор средств защиты по критерию качество/стоимость.

"Критерии" определяют множество типовых требований, которые в совокупности с механизмом Профилей защиты позволяют пользователям создавать частные наборы требований, отвечающие их нуждам. Разработчики могут использовать Профиль защиты как основу для создания спецификаций