ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ИНСТИТУТ РАДИОТЕХНИКИ,
ЭЛЕКТРОНИКИ И АВТОМАТИКИ (ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ)»

Курсовая работа

на тему:

«Защитные механизмы ОС»

Выполнил студент:
Группы ИТВ – 6–07
Саидов Рустам

Москва.2010 г.

Идентификация и аутентификация

Для начала рассмотрим проблему контроля доступа в систему. Наиболее распространенным способом контроля доступа является процедура регистрации. Обычно каждый пользователь в системе имеет уникальный идентификатор. Идентификаторы пользователей применяются с той же целью, что и идентификаторы любых других объектов, файлов, процессов. *Идентификация* заключается в сообщении пользователем своего идентификатора. Для того чтобы установить, что пользователь именно тот, за кого себя выдает, то есть что именно ему принадлежит введенный идентификатор, в информационных системах предусмотрена процедура *аутентификации* (authentication, опознавание, в переводе с латинского означает "установление подлинности"), задача которой - предотвращение доступа к системе нежелательных лиц.

Обычно *аутентификация* базируется на одном или более из трех пунктов:

- то, чем пользователь владеет (ключ или магнитная карта);
- то, что пользователь знает (пароль);
- атрибуты пользователя (отпечатки пальцев, подпись, голос).

Пароли, уязвимость паролей

Наиболее простой подход к *аутентификации* - применение пользовательского пароля.

Когда пользователь идентифицирует себя при помощи уникального идентификатора или имени, у него запрашивается пароль. Если пароль, сообщенный пользователем, совпадает с паролем, хранящимся в системе, система предполагает, что пользователь легитимен. Пароли часто используются для защиты объектов в компьютерной системе в отсутствие более сложных схем защиты.

Недостатки паролей связаны с тем, что трудно сохранить баланс между удобством пароля для пользователя и его надежностью. Пароли могут быть угаданы, случайно показаны или нелегально переданы авторизованным пользователем неавторизованному.

Есть два общих способа угадать пароль. Один связан со сбором информации о пользователе. Люди обычно используют в качестве паролей очевидную информацию (скажем, имена животных или номерные знаки автомобилей). Для иллюстрации важности разумной политики назначения идентификаторов и паролей можно привести данные исследований, проведенных в AT&T, показывающие, что из 500 попыток несанкционированного доступа около 300 составляют попытки угадывания паролей или беспарольного входа по пользовательским именам guest, demo и т. д.

Другой способ - попытаться перебрать все наиболее вероятные комбинации букв, чисел и знаков пунктуации (атака по словарю). Например, четыре десятичные цифры дают только 10 000 вариантов, более длинные пароли, введенные с учетом регистра символов и пунктуации, не столь уязвимы, но тем не менее таким способом удается разгадать до 25% паролей. Чтобы заставить пользователя выбрать трудно угадываемый пароль, во многих системах внедрена реактивная проверка паролей, которая при помощи собственной программы-взломщика паролей может оценить качество пароля, введенного пользователем.

Несмотря на все это, пароли распространены, поскольку они удобны и легко реализуемы.

Шифрование пароля

Для хранения секретного списка паролей на диске во многих ОС используется криптография. Система задействует одностороннюю функцию, которую просто вычислить, но для которой чрезвычайно трудно (разработчики надеются, что невозможно) подобрать обратную функцию.

Например, в ряде версий Unix в качестве односторонней функции используется модифицированный вариант алгоритма DES. Введенный пароль длиной до 8 знаков преобразуется в 56-битовое значение, которое служит входным параметром для процедуры crypt(), основанной на этом алгоритме.

Результат шифрования зависит не только от введенного пароля, но и от случайной последовательности битов, называемой привязкой (переменная salt). Это сделано для того, чтобы решить проблему совпадающих паролей. Очевидно, что саму привязку после шифрования необходимо сохранять, иначе процесс не удастся повторить. Модифицированный алгоритм DES выполняется, имея входное значение в виде 64-битового блока нулей, с использованием пароля в качестве ключа, а на каждой следующей итерации входным параметром служит результат предыдущей итерации. Всего процедура повторяется 25 раз. Полученное 64-битовое значение преобразуется в 11 символов и хранится рядом с открытой переменной salt.

В ОС Windows NT преобразование исходного пароля также осуществляется многократным применением алгоритма DES и алгоритма MD4.

Хранятся только кодированные пароли. В процессе *аутентификации* представленный пользователем пароль кодируется и сравнивается с хранящимися на диске. Таким образом, файл паролей нет необходимости держать в секрете.

При удаленном доступе к ОС нежелательна передача пароля по сети в открытом виде. Одним из типовых решений является использование криптографических протоколов. В качестве примера можно рассмотреть протокол опознавания с подтверждением установления связи путем вызова - CHAP (Challenge Handshake Authentication Protocol).

Опознавание достигается за счет проверки того, что у пользователя, осуществляющего доступ к серверу, имеется секретный пароль, который уже известен серверу.

Пользователь инициирует диалог, передавая серверу свой идентификатор. В ответ сервер посылает пользователю запрос (вызов), состоящий из идентифицирующего кода, случайного числа и имени узла сервера или имени пользователя. При этом пользовательское оборудование в результате запроса пароля пользователя отвечает следующим ответом, зашифрованным с помощью алгоритма одностороннего хеширования, наиболее распространенным видом которого является MD5. После получения ответа сервер при помощи той же функции с теми же аргументами шифрует собственную версию пароля пользователя. В случае совпадения результатов вход в систему разрешается. Существенно, что незашифрованный пароль при этом по каналу связи не посылается.

В микротелефонных трубках используется аналогичный метод.

В системах, работающих с большим количеством пользователей, когда хранение всех паролей затруднительно, применяются для опознавания сертификаты, выданные доверенной стороной (см., например, [Столлингс, 2001]).

Авторизация. Разграничение доступа к объектам ОС

После успешной регистрации система должна осуществлять авторизацию (authorization) - предоставление субъекту прав на доступ к объекту. Средства авторизации контролируют доступ легальных пользователей к ресурсам системы, предоставляя каждому из них именно те права, которые были определены администратором, а также осуществляют контроль возможности выполнения пользователем различных системных функций. Система контроля базируется на общей модели, называемой *матрицей доступа*. Рассмотрим ее более подробно.

Как уже говорилось в предыдущей лекции, компьютерная система может быть смоделирована как набор субъектов (процессы, пользователи) и объектов. Под объектами мы понимаем как ресурсы оборудования (процессор, сегменты памяти, принтер, диски и ленты), так и программные ресурсы (файлы, программы, семафоры), то есть все то, доступ к чему контролируется. Каждый объект имеет уникальное имя, отличающее его от других объектов в системе, и каждый из них может быть доступен через хорошо определенные и значимые операции.

Операции зависят от объектов. Например, процессор может только выполнять команды, сегменты памяти могут быть записаны и прочитаны, считыватель магнитных карт может только читать, а файлы данных могут быть записаны, прочитаны, переименованы и т. д.

Желательно добиться того, чтобы процесс осуществлял авторизованный доступ только к тем ресурсам, которые ему нужны для выполнения его задачи. Это требование минимума привилегий, уже упомянутое в предыдущей лекции, полезно с точки зрения ограничения количества повреждений, которые процесс может нанести системе. Например, когда процесс P вызывает процедуру A, ей должен быть разрешен доступ только к переменным и формальным параметрам, переданным ей, она не должна иметь возможность влиять на другие переменные процесса. Аналогично компилятор не должен оказывать влияния на произвольные файлы, а только на их хорошо определенное подмножество (исходные файлы, листинги и др.), имеющее отношение к компиляции. С другой стороны, компилятор может иметь личные файлы, используемые для оптимизационных целей, к которым процесс P не имеет доступа.

Различают *дискреционный* (избирательный) способ управления доступом
и *полномочный* (мандатный).

При ***дискреционном доступе***, подробно рассмотренном ниже, определенные операции над конкретным ресурсом запрещаются или разрешаются субъектам или группам субъектов. С концептуальной точки зрения текущее состояние прав доступа при дискреционном управлении описывается матрицей, в строках которой перечислены субъекты, в столбцах - объекты, а в ячейках - операции, которые субъект может выполнить над объектом.

Полномочный подход заключается в том, что все объекты могут иметь уровни секретности, а все субъекты делятся на группы, образующие иерархию в соответствии с уровнем допуска к информации. Иногда это называют моделью многоуровневой безопасности, которая должна обеспечивать выполнение следующих правил.

- Простое свойство секретности. Субъект может читать информацию только из объекта, уровень секретности которого не выше уровня секретности субъекта. Генерал читает документы лейтенанта, но не наоборот.
- *-свойство. Субъект может записывать информацию в объекты только своего уровня или более высоких уровней секретности. Генерал не может случайно разгласить нижним чинам секретную информацию.

Некоторые авторы утверждают [Таненбаум, 2002], что последнее требование называют *-свойством, потому что в оригинальном докладе не смогли придумать для него подходящего названия. В итоге во все последующие документы и монографии оно вошло как *-свойство.

Отметим, что данная модель разработана для хранения секретов, но не гарантирует целостности данных. Например, здесь лейтенант имеет право писать в файлы генерала. Более подробно о реализации подобных формальных моделей рассказано в [Столлингс, 2002], [Таненбаум, 2002].

Большинство операционных систем реализуют именно *дискреционное управление доступом*. Главное его достоинство - гибкость, основные недостатки - рассредоточенность управления и сложность централизованного контроля.

Домены безопасности

Чтобы рассмотреть схему *дискреционного доступа* более детально, введем концепцию *домена безопасности* (protection domain). Каждый домен определяет набор объектов и типов операций, которые могут производиться над каждым объектом. Возможность выполнять операции над объектом есть права доступа, каждое из которых есть упорядоченная пара <object-name, rights-set>. Домен, таким образом, есть набор прав доступа. Например, если домен D имеет права доступа<file F, {read, write}>, это означает, что процесс, выполняемый в домене D, может читать или писать в файл F, но не может выполнять других операций над этим объектом. Пример доменов можно увидеть на рис.16.1.

Объект / Домен	F1	F2	F3	Printer
D1	read			
D2				print
D3		read	execute	
D4	read write		read write	

Рис. 16.1. Специфицирование прав доступа к ресурсам

Связь конкретных субъектов, функционирующих в операционных системах, может быть организована следующим образом.

- Каждый пользователь может быть доменом. В этом случае набор объектов, к которым может быть организован доступ, зависит от *идентификации*пользователя.
- Каждый процесс может быть доменом. В этом случае набор доступных объектов определяется *идентификацией* процесса.
- Каждая процедура может быть доменом. В этом случае набор доступных объектов соответствует локальным переменным, определенным внутри процедуры. Заметим, что когда процедура выполнена, происходит смена домена.

Рассмотрим стандартную двухрежимную модель выполнения ОС. Когда процесс выполняется в режиме системы (kernel mode), он может выполнять привилегированные инструкции и иметь полный контроль над компьютерной системой. С другой стороны, если процесс выполняется в пользовательском режиме, он может вызывать только непривилегированные инструкции. Следовательно, он может выполняться только внутри предопределенного пространства памяти. Наличие этих двух режимов позволяет защитить ОС (kernel domain) от пользовательских процессов (выполняющихся в user domain). В мультипрограммных системах двух доменов недостаточно, так как появляется необходимость защиты пользователей друг от друга. Поэтому требуется более тщательно разработанная схема.

В ОС Unix домен связан с пользователем. Каждый пользователь обычно работает со своим набором объектов.

Матрица доступа

Модель безопасности, специфицированная в предыдущем разделе (см. рис. 16.1), имеет вид матрицы, которая называется ***матрицей доступа***. Какова может быть эффективная реализация *матрицы доступа*? В общем случае она будет разреженной, то есть большинство ее клеток будут пустыми. Хотя существуют структуры данных для представления разреженной матрицы, они не слишком полезны для приложений, использующих возможности защиты. Поэтому на практике *матрица доступа* применяется редко. Эту матрицу можно разложить по столбцам, в результате чего получаются **списки прав доступа** (access control list - ACL). В результате разложения по строкам получаются *мандаты* возможностей (capability list или capability tickets).

Список прав доступа. Access control list

Каждая колонка в матрице может быть реализована как список доступа для одного объекта. Очевидно, что пустые клетки могут не учитываться. В результате для каждого объекта имеем список упорядоченных пар <domain, rights-set>, который определяет все домены с непустыми наборами прав для данного объекта.

Элементами списка могут быть процессы, пользователи или группы пользователей. При реализации широко применяется предоставление доступа по умолчанию для пользователей, права которых не указаны. Например, в Unix все субъекты-пользователи разделены на три группы (владелец, группа и

остальные), и для членов каждой группы контролируются операции чтения, записи и исполнения (rwx). В итоге имеем ACL - 9-битный код, который является атрибутом разнообразных объектов Unix.

Мандаты возможностей. Capability list

Как отмечалось выше, если *матрицу доступа* хранить по строкам, то есть если каждый субъект хранит список объектов и для каждого объекта - список допустимых операций, то такой способ хранения называется ***"мандаты"*** или ***"перечни возможностей"*** (capability list). Каждый пользователь обладает несколькими *мандатами* и может иметь право передавать их другим. *Мандаты* могут быть рассеяны по системе и вследствие этого представлять большую угрозу для безопасности, чем списки контроля доступа. Их хранение должно быть тщательно продумано.

Примерами систем, использующих *перечни возможностей*, являются Hydra, Cambridge CAP System [Denning, 1996].

Другие способы контроля доступа

Иногда применяется **комбинированный способ**. Например, в том же Unix на этапе открытия файла происходит анализ ACL (операция open). В случае благоприятного исхода файл заносится в список открытых процессом файлов, и при последующих операциях чтения и записи проверки прав доступа не происходит. Список открытых файлов можно рассматривать как *перечень возможностей*.

Существует также схема **lock-key**, которая является компромиссом между списками прав доступа и *перечнями возможностей*. В этой схеме каждый объект имеет список уникальных битовых шаблонов (patterns), называемых locks. Аналогично каждый домен имеет список уникальных битовых шаблонов, называемых ключами (keys). Процесс, выполняющийся в домене, может получить доступ к объекту, только если домен имеет ключ, который соответствует одному из шаблонов объекта.

Как и в случае *мандатов*, список ключей для домена должен управляться ОС. Пользователям не разрешается проверять или модифицировать списки ключей (или шаблонов) непосредственно. Более подробно данная схема изложена в [Silberschatz, 2002].

Смена домена

В большинстве ОС для определения домена применяются идентификаторы пользователей. Обычно переключение между доменами происходит, когда меняется пользователь. Но почти все системы нуждаются в дополнительных механизмах смены домена, которые используются, когда некая привилегированная возможность необходима большому количеству пользователей. Например, может понадобиться разрешить пользователям иметь доступ к сети, не заставляя их писать собственные сетевые программы. В таких случаях для процессов ОС Unix предусмотрена установка бита **set-uid**. В результате установки этого бита в сетевой программе она получает привилегии ее создателя (а не пользователя), заставляя домен меняться на время ее выполнения. Таким образом, рядовой пользователь может получить нужные привилегии для доступа к сети.

Недопустимость повторного использования объектов

Контроль *повторного использования объекта* предназначен для предотвращения попыток незаконного получения конфиденциальной информации, остатки которой могли сохраниться в некоторых объектах, ранее использовавшихся и освобожденных другим пользователем. Безопасность повторного применения должна гарантироваться для областей оперативной памяти (в частности, для буферов с образами экрана, расшифрованными паролями и т. п.), для дисковых блоков и магнитных носителей в целом. Очистка должна производиться путем записи маскирующей информации в объект при его освобождении (перераспределении). Например, для дисков на практике применяется способ двойной перезаписи освободившихся после удаления файлов блоков случайной битовой последовательностью.

Выявление вторжений. Аудит системы защиты

Даже самая лучшая система защиты рано или поздно будет взломана. Обнаружение попыток вторжения является важнейшей задачей системы защиты, поскольку ее решение позволяет минимизировать ущерб от взлома и собирать информацию о методах вторжения. Как правило, поведение взломщика отличается от поведения легального пользователя. Иногда эти различия можно выразить количественно, например подсчитывая число некорректных вводов пароля во время регистрации.

Основным инструментом выявления вторжений является запись данных *аудита*. Отдельные действия пользователей протоколируются, а полученный протокол используется для выявления вторжений.

Аудит, таким образом, заключается в регистрации специальных данных о различных типах событий, происходящих в системе и так или иначе влияющих на состояние безопасности компьютерной системы. К числу таких событий обычно причисляют следующие:

- вход или выход из системы;
- операции с файлами (открыть, закрыть, переименовать, удалить);
- обращение к удаленной системе;
- смена привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя и т. п.).

Если фиксировать все события, объем регистрационной информации, скорее всего, будет расти слишком быстро, а ее эффективный анализ станет невозможным. Следует предусматривать наличие средств выборочного протоколирования как в отношении пользователей, когда слежение осуществляется только за подозрительными личностями, так и в отношении событий. Слежка важна в первую очередь как профилактическое средство. Можно надеяться, что многие воздержатся от нарушений безопасности, зная, что их действия фиксируются.

Помимо протоколирования, можно периодически **сканировать** систему на наличие слабых мест в системе безопасности. Такое сканирование может проверить разнообразные аспекты системы:

- короткие или легкие пароли;
- неавторизованные set-uid программы, если система поддерживает этот механизм;
- неавторизованные программы в системных директориях;
- долго выполняющиеся программы;
- нелогичная защита как пользовательских, так и системных директорий и файлов. Примером нелогичной защиты может быть файл, который запрещено читать его автору, но в который разрешено записывать информацию постороннему пользователю;
- потенциально опасные списки поиска файлов, которые могут привести к запуску "троянского коня";
- изменения в системных программах, обнаруженные при помощи контрольных сумм.

Любая проблема, обнаруженная сканером безопасности, может быть как ликвидирована автоматически, так и передана для решения менеджеру системы.

Анализ некоторых популярных ОС с точки зрения их защищенности

Итак, ОС должна способствовать реализации мер безопасности или непосредственно поддерживать их. Примерами подобных решений в рамках аппаратуры и операционной системы могут быть:

- разделение команд по уровням привилегированности;
- сегментация адресного пространства процессов и организация защиты сегментов;
- защита различных процессов от взаимного влияния за счет выделения каждому своего виртуального пространства;
- особая защита ядра ОС;
- контроль *повторного использования объекта*;
- наличие средств управления доступом;
- структурированность системы, явное выделение надежной вычислительной базы (совокупности защищенных компонентов), обеспечение компактности этой базы;
- следование принципу минимизации привилегий - каждому компоненту дается ровно столько привилегий, сколько необходимо для выполнения им своих функций.

Большое значение имеет структура файловой системы. Например, в ОС с дискреционным контролем доступа каждый файл должен храниться вместе с дискреционным списком прав доступа к нему, а, например, при копировании файла все атрибуты, в том числе и ACL, должны быть автоматически скопированы вместе с телом файла.

В принципе, меры безопасности не обязательно должны быть заранее встроены в ОС - достаточно принципиальной возможности дополнительной установки защитных продуктов. Так, сугубо ненадежная система MS-DOS может быть усовершенствована за счет средств проверки паролей доступа к компьютеру и/или жесткому диску, за счет борьбы с вирусами путем отслеживания попыток записи в загрузочный сектор CMOS-средствами и т. п. Тем не менее, по-настоящему надежная система должна изначально проектироваться с акцентом на механизмы безопасности.

Windows Vista

Введение

В данной курсовой работе сконцентрировано описание всех основных нововведений в системе безопасности ОС Windows Vista Дело в том, что работ посвященных именно безопасности Windows Vista на русском языке я не встречал, а то, что мы узнаем из новостей, составляет неполную картину о защищенности данной ОС. В данной курсовой работе я попытался собрать, по возможности, все сведения о нововведениях в системе безопасности Windows Vista, пользуясь, в основном, официальными материалами англоязычного сайта Microsoft, поэтому данная статья выражает только совокупность официальных сведений о технологиях безопасности новой ОС. Надеюсь, что эта курсовая работа поможет сформировать определенную картину о защищенности Windows Vista.

Windows Vista – это первая клиентская операционная система от Microsoft, в которой контроль за безопасностью осуществляется на всех этапах разработки (технология Microsoft's Security Development Lifecycle). Это означает, что во главу угла ставится именно безопасность новой ОС. Согласно технологии SDL, к разработчикам ПО с самого начала приставляется консультант по безопасности, который контролирует все этапы разработки на предмет отсутствия уязвимостей. Кроме того, Microsoft собирается сертифицировать Windows Vista по стандарту ISO «Общие Критерии» с целью получения сертификатов EAL4 и Single Level OS Protection Profile.

Аппаратная защита Windows Vista

Технология NX (No Execute)

Вредоносное ПО может завладеть пользовательской машиной с использованием переполнения буфера или путем исполнения кода в областях памяти, предназначенной для хранения данных. SDL и другие аналогичные инструменты способны предотвратить возможность переполнения буфера еще на стадии проектирования или программирования, однако существует еще один путь борьбы с переполнением – использование технологий NX (No Execute) на аппаратном уровне. NX позволяет программному обеспечению помечать сегменты памяти, в которых будут хранится только данные, и процессор не позволит приложениям и службам исполнять произвольный код в этих сегментах.

Множество современных процессоров поддерживают ту или иную форму NX, и Microsoft, в свою очередь, начиная с Windows XP SP2, включила поддержку процессоров с NX-технологией посредством инструмента Data Execution Prevention. Windows Vista обеспечивает дополнительную поддержку NX, позволяя производителям ПО встраивать защиту NX в свои программные продукты. Независимые продавцы ПО могут помечать свои продукты как NX-совместимые, что позволит повысить безопасность при загрузке программы. Данный подход позволяет значительно увеличить количество программных продуктов, поддерживающих защиту NX. Особенно это актуально для 32-битных платформ, поскольку в них стандартная политика совместимости для NX сконфигурирована только для защиты компонентов ОС. На 64-битных версиях Windows защита NX – стандарт.

Случайное расположение адресного пространства (Address Space Layout Randomization (ASLR))- это еще один вид защиты в ОС Windows Vista, который затрудняет использование системных функций вредоносным ПО. Каждый раз, когда компьютер перезагружается, ASLR в случайном порядке назначает 1 из 256 возможных вариантов адреса для расположения ключевых системных DLL и EXE файлов. Это осложняет эксплоиту задачу поиска нужных файлов, а, следовательно, противодействует выполнению его функций. ASLR лучше использовать в связке с Data Execution Prevention, потому что в некоторых случаях компонент Data Execution Prevention можно обойти путем построения эксплоита, который сам по себе не выполняется (он вызывает системные функции для атаки).

Windows Vista также содержит в себе ряд улучшений по сравнению с Windows XP SP2, связанный с определением переполнения «кучи» (области памяти, выделяемой программе для динамически размещаемых структур данных). При вмешательстве в буфер «кучи» к ОС поступает сигнал, и она, в свою очередь, может немедленно завершить скомпрометированную программу, тем самым сократив ущерб от вмешательства. Эта технология используется для защиты компонентов ОС, включая встроенные системные службы, хотя может использоваться и сторонними производителями ПО через специальный одиночный API-вызов.

Защита ядра для x64. 64-битные версии Windows Vista поддерживают технологию защиты ядра (иногда используется термин PatchGuard), которая запрещает неавторизованному ПО изменять ядро Windows.

Для того чтобы разобраться в сути данной технологии, необходимо понять, что означает термин kernel patching (изменение ядра).

Kernel patching – это техника, использующая внутренние системные вызовы, а также различные неподдерживаемые ОС механизмы, с целью изменения или замены кода, а, возможно, и критических структур данных ядра Windows на другой «неизвестный» код или данные, которые могут быть и вредоносными. Под понятием «неизвестный» имеется в виду код, не авторизованный Microsoft как часть ядра Windows.

Производители ПО иногда патчат ядро для своих целей, изменяя адрес функции-обработчика системного вызова (указатель функции) в таблице системных вызовов (system service table, SST), которая представляет собой массив из указателей функций, находящихся в памяти. Такая процедура изменения адреса называется хуком (hook). Когда выполняется любой системный вызов (например, NtCreateProcess), диспетчер системных вызовов по номеру вызова восстанавливает адрес функции-обработчика данного системного вызова. Соответственно, если поменять адрес функции-обработчика, на адрес начала «неизвестного» кода, диспетчер системных вызовов перейдет по этому

адресу, и «неизвестный» код будет исполнен. Именно по этой причине модификация ядра запрещена в 64-битных версиях Windows Vista. Конкретнее запрещена модификация следующих компонентов ядра:

- Таблицы системных вызовов (system service tables, SST)

- Таблица прерываний (interrupt descriptor table (IDT))

- Таблица глобальных дескрипторов (global descriptor table (GDT))

- Изменение любой части ядра (работает только на AMD64-системах)

При попытке изменения вышеописанных частей ядра операционная система генерирует bug check и завершает свою работу. Соответственно, для своей корректной работы приложения и драйверы не должны изменять структуру данных частей ядра. Со временем, список защищаемых компонентов ядра может быть увеличен.

По заявлениям Microsoft, систему защиты ядра отключить нельзя. Защита ядра автоматически отключается лишь в случае работы в системе отладчика ядра. Ядро может изменяться и официальными патчами от Microsoft.

Программная защита

Подписывание драйверов для x64. Для того чтобы пользователи могли видеть поставщиков драйверов и других программных продуктов, начиная с Windows 2000, в ОС присутствует механизм проверки цифровой подписи драйверов. Хотя раньше и была возможность запретить установку неподписанных драйверов, в конфигурации по умолчанию пользователь лишь предупреждался о том, что собирается устанавливать неподписанный драйвер. Системные администраторы, однако, могли заблокировать установку неподписанных драйверов посредством Групповой политики (Group Policy), но, поскольку, количество нужных неподписанных драйверов было достаточно велико, администраторы не пользовались этой возможностью. Вредоносное программное обеспечение обычно устанавливается скрытно от пользователя, и, поскольку никаких проверок изменения ядра до появления Windows Vista не было, вредоносное ПО успешно устанавливалось (имеется в виду, что установка производилась от имени пользователя с административными привилегиями).

При установке Windows Vista на 64-битные системы их безопасность на уровне ядра значительно возрастает в случае, если все драйверы режима ядра (kernel mode) имеют цифровую подпись. Цифровая подпись обеспечивает подлинность и целостность кода. Поврежденный модуль ядра не загрузится. Любой драйвер, не имеющей соответствующей цифровой подписи не получит доступа к ядру и не загрузится.

Хотя подписанный драйвер и не является гарантией безопасности, все равно он помогает определить и предотвратить множество злонамеренных атак, в тоже время позволяя Microsoft помочь разработчикам улучшить общее качество драйверов и сократить число сбоев по вине последних.

Обязательное подписывание драйверов также помогает повысить надежность Windows Vista, потому что большинство сбоев ОС – уязвимости в драйверах режима ядра. Принуждая авторов этих драйверов идентифицировать себя, Microsoft облегчает себе задачу определения причин сбоя ОС и позволяет работать с производителями с целью разрешения возникших проблем. На основе вышеизложенного, можно сделать такой вывод: неподписанные драйверы на Windows Vista установить не удастся.

WindowsServiceHardening

Системные службы это фоновые процессы, которые загружаются для поддержки ключевых функций ОС. Они всегда были целью злонамеренных атак, потому что обычно загружаются с самыми высокими привилегиями в системе, то есть под учетной записью LocalSystem. Атаки, направленные на системные службы могут вызвать серьезные проблемы, поскольку позволяют исполнять

произвольный код с административными полномочиями на машинах пользователей (черви Slammer, Blaster и Sasser атаковали именно системные службы).

Чтобы каким-то образом ослабить данную угрозу, Windows Vista предлагает концепцию «ограниченных служб» (restricted services), которые загружаются с минимальными привилегиями, и влияние их на компьютер и сеть ограничено. Данный подход позволяет существенно сократить число служб, способных нанести серьезный вред пользовательской машине.

Персональный межсетевой экран в Windows Vista тесно связан с компонентом Windows Service Hardening, который позволяет усилить защиту как входящего, так и исходящего трафика в процессе межсетевого взаимодействия. Необходимо добавить, что службы могут быть однозначно идентифицированы, что позволяет вести списки контроля доступа для каждой службы, разрешая, например, службам записывать только в определенные места файловой системы, реестра или других системных ресурсов.

Кроме того, применение данного подхода позволяет предотвратить изменение важных настроек файловой системы или реестра скомпрометированной службой.

Встроенные службы Windows имеют собственные профили, которые определяют необходимые права для каждой службы, правила доступа к системным ресурсам и сетевые порты, которые службам разрешено использовать. Если служба попытается отправить или получить данные с сетевого порта, который ей не разрешен для использования, межсетевой экран заблокирует эту попытку. Например, службе удаленного вызова процедур (Remote Procedure Call service) запрещено перемещать системные файлы, модифицировать реестр, вмешиваться в конфигурации других служб в системе (например, ей нельзя изменять конфигурацию и сигнатуры вирусов антивирусного ПО).

Уменьшения сложности первоначального конфигурирования служб для пользователей и системных администраторов – еще одна задача компонента Windows Service Hardening. Каждая служба, которая входит в состав ОС Windows Vista, имеет сконфигурированный заранее профиль, который применяется автоматически в процессе установки Windows. Данный процесс не требует каких бы то ни было усилий со стороны пользователей или администраторов.

Контроль пользовательских учетных записей (User Account Control)

В предыдущих версиях Windows большинство пользовательских учетных записей являлось членом локальной группы «Администратор», тем самым предоставляя пользователям все системные привилегии и возможности, требуемые для установки и конфигурирования приложений, загрузки некоторых фоновых системных процессов и драйверов устройств, изменения конфигурации системы и выполнения базовых повседневных задач.

Хотя этот подход и был удобен для пользователей, он делал компьютеры в сети более уязвимыми к вредоносному ПО, которое могло использовать системные привилегии для повреждения файлов, изменения конфигурации (например, отключение межсетевого экрана), кражи или изменения конфиденциальной информации. Кроме того, применение данного подхода повышало затраты на повседневное обслуживание компьютеров, потому что пользователь мог совершить несанкционированные или случайные изменения, которые, в свою очередь, могли нарушить работу сети и затруднить управление отдельными компьютерами. Хотя существовала возможность работы учетных записей пользователей Windows в конфигурации с ограниченными правами, она сильно сокращала продуктивность работы, потому что базовые задачи, такие как изменение системного времени, присоединение к безопасной беспроводной сети или установка драйвера принтера требовали административных привилегий.

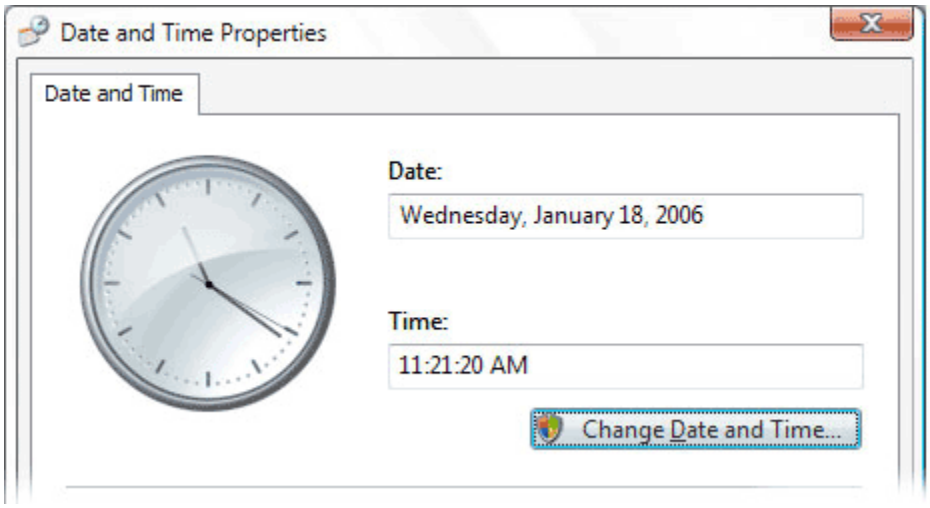
Для решения этой проблемы, Windows Vista содержит компонент User Account Control (UAC). Это новый подход, который разделяет все операции в системе на 2 категории: те, которые может выполнять пользователь со своими стандартными правами и те, которые требуют административных привилегий. Применение нового подхода сокращает плацдарм для атак на операционную систему, в то же время предоставляя обычным пользователям большинство функций, которые им требуются каждый день.

UAC обладает двумя преимуществами: во-первых, он переопределяет список стандартных возможностей пользователя, путем включения в него множества базовых функций, которые не несут риска нарушения безопасности, хотя раньше требовали административных привилегий. К этим новым функциям можно отнести:
- Изменение временной зоны
- Настройку системы управления питанием
- Добавление принтера и других устройств, при условии, что драйверы для них уже установлены в системе
- Установку новых шрифтов
- Изменение настроек экрана
- Создание и настройка VPN-соединения
- Установка WEP (Wired Equivalent privacy) для соединения с защищенной беспроводной сетью
- Просмотр календаря и системного времени
- Загрузка и установка обновлений, при условии использования UAC-совместимого инсталлятора.

UAC также помогает контролировать доступ к ценной информации, находящейся в папке «Мои документы». Теперь, если пользователь не является создателем файла, он не сможет его ни прочесть, ни изменить, ни удалить, т.е., другими словами, доступ к файлам других пользователей закрыт.

Когда обычные пользователи пытаются выполнить задачу, требующую административных привилегий (например, установка нового приложения или изменение важных системных настроек), им предлагается ввести пароль администратора. IT-администраторы имеют возможность отключить процедуру ввода пароля администратора для обычных пользователей, сокращая тем самым риск несанкционированных действий со стороны последних. Во-вторых, UAC позволяет пользователям с административными привилегиями работать в более безопасной среде путем ограничения (по умолчанию) доступа к критичным ресурсам и функциям системы. Если для выполнения какой-либо задачи требуются повышенные привилегии, система предупредит вас об этом с помощью окна с предложением подтверждения выполнения данной задачи.

Интерфейс пользователя ОС Windows Vista включает в себя ряд улучшений, призванных облегчить пользователям определение тех задач, которые требуют административных привилегий. Эти улучшения проявляются в виде описания запрашиваемых действий, а также в маркировании административных действий значком в виде щита (см. рис).



UAC помогает существующим приложениям работать с правами стандартного пользователя без модификаций, путем предоставления им специальной платформы, которая помогает последним обойтись без использования административных привилегий в обычных ситуациях. Например, чтобы обеспечить нормальную работу приложений, требующих для своего выполнения административных привилегий, Windows Vista содержит механизм виртуализации файловой системы и реестра. Данный механизм перенаправляет запросы чтения и записи из защищенных областей в какое-либо место внутри профиля пользователя, таким образом, приложение работает корректно, не влияя на ресурсы других пользователей или систему вцелом. Это сокращает риск нарушения безопасности, потому что приложения никогда не получат доступ к ресурсам, требующим прав администратора для доступа. Однако Microsoft рекомендует использовать данное решение для приложений только как временный выход из ситуации, пока не найдется замена, не требующая административных привилегий и корректно работающая под UAC.

Необходимо отметить, что Microsoft предлагает ряд инструментов, технологий и ресурсов, чтобы помочь производителям составлять новые программы, корректно работающие под UAC. Например, инструмент Standart User Analyzer позволяет определить, будет ли корректно работать то или иное приложение с правами стандартного пользователя или же нет.

Благодаря включению UAC в бета-версию Windows Vista, Microsoft получила ценную информацию от пользователей, что привело в последствии к ряду улучшений в компоненте UAC второй бета-версии Windows Vista. Вот основные улучшения UAC во второй бета-версии Windows Vista:

- Сокращение числа объектов Панели управления, которые требуют административных привилегий для доступа (объекты Мышь и Клавиатура, Инфракрасный порт и Bluetooth).

- Планировщик заданий теперь не требует административных привилегий

- Применены исправления к сотням приложений, с целью их корректной работы без ввода пароля администратора

Диалоговые окна UAC также подверглись пересмотру. Теперь они более точно указывают на программу, запрашивающую права администратора, а также помогают определить программы, которые потенциально опасны для системы. Microsoft будет продолжать улучшать компонент UAC, удалять ненужные диалоговые окна вплоть до финального выпуска Windows Vista, используя данные, полученные от пользователей.

Отзывы пользователей применяются для точного определения числа всплывающих сообщений (подсказок), которые появятся в пост-бета2 версии Windows Vista, известной как кандидат № 1 на широкомасштабный выпуск (Release Candidate №1). В этой версии Windows Vista их будет даже меньше, чем во второй бета-версии. Например, предполагается удалить сообщение для администраторов, когда они удаляют ярлыки на общем рабочем столе, а также сообщение, которое появляется, когда пользователь получает критичные обновления с Windows Update.

Защита доступа к сети (Network Access Protection, NAP)

NAP – это система, которая позволяет системным администраторам быть уверенным в том, что в сети находятся только «здоровые» машины. Под понятием «здоровые» подразумеваются машины со всеми необходимыми обновлениями ПО, антивирусных баз и т.д. Если компьютер, не соответствует требованиям, предъявляемым NAP, он объявляется «нездоровым», ему не разрешается доступ к сети, до тех пор, пока все требования NAP не будут выполнены.

Защита от вредоносного кода и компьютерных атак

Центр безопасности Windows (Windows Security Center, WSC)

В 2004 году компания Microsoft включила в операционную систему Windows XP SP2 компонент WSC. Загружаясь как фоновый процесс, WSC в Windows XP постоянно проверял и показывал состояние трех наиболее важных аспектов безопасности: межсетевого экрана, антивирусного ПО, автоматических обновлений.

Windows Vista также содержит WSC, однако, последний имеет ряд улучшений таких как отображение состояния антишпионского ПО, настроек защиты Internet Explorer и UAC. WSC может следить за состоянием защитного ПО третьих производителей, работающих на данном компьютере. В случае если защитное ПО выключено либо требует установки обновлений, WSC предупреждает пользователя об этом.

Windows Defender

Windows Defender – компонент который защищает компьютер от руткитов, кейлоггеров, шпионов, adware, bots и другого вредоносного ПО. (Windows Defender не защищает от червей и вирусов).

Windows Defender содержит 9 агентов безопасности, которые постоянно наблюдают за теми критическими областями ОС, которые наиболее часто пытается изменить вредоносное ПО. К таким областям ОС относятся:

- Автозагрузка. Агент безопасности постоянно наблюдает за списком программ, которым позволено загружаться при старте системы. Таким образом, реализуется защита от вредоносного ПО, которое пытается загрузиться вместе с системой.

- Настройки безопасности системы. Агент безопасности постоянно проверяет настройки безопасности Windows. Не секрет, что некоторое вредоносное ПО старается изменить настройки безопасности с целью облегчения вредного воздействия на ОС. Агент безопасности этой области не позволит неавторизованному ПО изменить настройки безопасности.

- Аддоны Internet Explorer. Агент безопасности следит за приложениями, которые загружаются вместе с браузером. Spyware и другое вредоносное ПО может маскироваться под аддоны Internet Explorer и загружаться без вашего ведома. Агент безопасности не позволит загрузиться такому виду вредоносного ПО.

- Настройки Internet Explorer. Агент безопасности следит за настройками безопасности браузера, потому что вредоносное ПО может попытаться изменить их.

- Загрузки Internet Explorer (Internet Explorer Downloads). Агент безопасности следит за файлами и приложениями, предназначенными для работы с IE (например ActiveX controls). Браузер может загрузить, установить и запустить данные файлы без вашего ведома. Вредоносное ПО может быть включено в такого рода файлы и загрузиться на компьютере-жертве, но агент безопасности защитит и от этой напасти.

- Службы и драйверы. Агент безопасности данной области наблюдает за состоянием служб и драйверов во время их взаимодействия с ОС и приложениями. Поскольку службы и драйверы выполняют важнейшие функции, они имеют доступ к важным областям ОС. Вредоносное ПО может использовать службы для доступа к компьютеру, а также с целью маскировки под нормальные компоненты системы.

- Выполнение приложений (Application Execution). Агент безопасности следит за приложениями во время их выполнения. Spyware и другое вредоносное ПО, используя уязвимости приложений, может нанести вред. Например, spyware может загрузиться во время запуска часто используемого вами приложения. Windows Defender предупредит вас о подозрительном поведении приложений.

- Регистрация приложений (Application Registration). Агент безопасности данной области постоянно наблюдает за инструментами и файлами ОС, где приложения регистрируются с целью загрузки. Spyware и другое вредоносное ПО может зарегистрировать приложение с целью загрузки без вашего ведома и периодически собирать с помощью него вашу личную информацию. Данный агент, сообщит пользователю об обнаружении нового приложения, пытающегося зарегистрироваться с целью загрузки.

- Windows Add-ons. Агент безопасности следит за так называемыми аддонами, также известными как программные утилиты для Windows. Аддоны позволяют настроить такие аспекты ОС, как безопасность, производительность, мультимедиа. Однако аддоны могут устанавливать ПО, которое будет собирать информацию о вас и о вашем компьютере.

Безопасность Internet Explorer 7

Большой шаг в сторону повышения безопасности браузера и безопасности личных данных был сделан в Microsoft Internet Explorer® 7. Этот новый браузер дает пользователям уверенность в безопасности пребывания в Internet, одновременно защищая личные пользовательские данные от фишинговых атак (phishing attacks) и мошеннических веб-сайтов. Основные улучшения касаются защищенного режима браузера (Protected Mode), который активирует систему защиты браузера, помогая противостоять хакерам, стремящимся завладеть браузером и исполнить вредоносный код. Новая опция Fix My Settings (исправь мои настройки) помогает пользователю поддерживать защиту на должном уровне, когда происходит установка и использование различных Интернет-приложений. Панель Статус безопасности (Security Status Bar) позволяет пользователям быстро отличать нормальные веб-сайты от подозрительных или вредоносных, а компонент Microsoft Phishing Filter предупреждает пользователей при просмотре веб-страниц об известных фишинговых веб-сайтах.

Улучшения межсетевого экрана Windows

Как и в Windows XP SP2, межсетевой экран в Windows Vista включен по умолчанию и начинает защищать пользовательский компьютер с момента загрузки операционной системы. Теперь межсетевой экран способен фильтровать и входящий, и исходящий трафик. Он помогает также защититься от вредного воздействия системных ресурсов, если они ведут себя непредсказуемо (возможно в случае работы вредоносного кода). Например, если системная служба сконфигурирована таким образом, чтобы посылать сообщения в сеть через определенный порт, но пытается это сделать через другой, межсетевой экран Windows, может запретить отправку данных сообщений, тем самым обеспечивая защиту от распространения вредоносного ПО.

Защита данных

BitLocker Drive Encryption (Шифрованиетома)

BitLocker Drive Encryption – инструмент, позволяющий защитить конфиденциальную информацию на диске, путем его шифрования. В случае, если диск, защищенный с помощью технологии BitLocker украден или, например, списан, то информацию на нем прочесть не удастся, поскольку все содержимое диска зашифровано.

Технология BitLocker использует TPM (Trusted Platform Module) – специальный чип, который необходим для безопасного хранения ключевой информации, а также для разграничения доступа к системе. Во время загрузки Windows проверяется целостность системных файлов и данных. Если файлы были изменены, ОС не загрузится. BitLocker поддерживает централизованное хранение ключей в Active Directory, в то же время позволяя системным администраторам хранить ключи шифрования и на USB-устройствах.

BitLocker позволяет изменить стандартный процесс загрузки ОС. Дело в том, что загрузка ОС может блокироваться до тех пор, пока пользователь не введет PIN-код или не вставит USB-устройство с ключами дешифрования. Эти дополнительные меры безопасности обеспечивают так называемую мультифакторную аутентификацию (многоуровневую).

BitLocker Drive Encryption будет доступен для клиентских машин в версиях Windows Vista Enterprise и Ultimate.

Улучшенияв EFS (Encrypting File System)

В Windows Vista EFS поддерживает хранение пользовательских ключей и ключей восстановления на смарт-картах. Кроме того, EFS в Windows Vista может быть использована для шифрования файла подкачки (эта опция может быть активирована системным администратором через групповую политику). Кэш на стороне клиента, в котором сохраняются копии документов с сервера также может быть зашифрован с помощью EFS. В этом случае даже локальный администратор, не обладая пользовательским секретным ключом, не сможет расшифровать файлы пользователя.

В Групповую Политику был добавлен ряд опций, по поддержке EFS. К ним относятся опции включения возможности шифрования файла подкачки, сохранения ключей на смарт-картах, ограничения минимальной длины ключа и т.д.

Кроме вышеперечисленного, существует возможность шифрования пользовательских файлов «на лету» при сохранении их на сервере Longhorn. Такая операция необходима, когда нет доверия к серверу.

EFS будет доступна в версиях Windows Vista Business, Enterprise и Ultimate.

Контроль USB-устройств

Не секрет, что бесконтрольное использование USB-накопителей может привести к утечке конфиденциальной информации из организации, к заражению компьютера вредоносным ПО и другим малоприятным последствиям. Именно поэтому в ОС Windows Vista реализован механизм контроля использования USB-устройств.

Посредством Групповой Политики Windows Vista позволяет системным администраторам блокировать установку неавторизованных USB-устройств в компьютер. Данная политика может применяться как к отдельному компьютеру, так и к множеству компьютеров по всей сети. У администраторов в руках находятся весьма гибкий инструмент по настройке политики запрета USB-устройств. Например, можно разрешить установку только определенного класса устройств, таких как принтеры, запретить установку любых типов USB-накопителей или запретить установку любых неавторизованных устройств. Данные политики можно перекрывать путем ввода пароля администратора для установки того или иного устройства. И, наконец, можно открывать доступ по чтению/записи к устройствам для определенных пользователей или компьютеров.

Windows 7

Что нового на фронте безопасности в Windows 7?

Полнофункциональная' публичная бета версия Windows 7 была выпущена 9 января, и ИТ индустрия преисполнилась шумихой об изменениях интерфейса, но что же творится внутри? Какие изменения были внесены в область ОС и ее сетевой безопасности? В этой курсовой работе мы рассмотрим функции безопасности Windows 7, а также зададимся вопросом, стоит ли чисто с точки безопасности переходить на новую версию операционной системы. Мы будем концентрировать свое внимание на изменениях, коснувшихся интерфейса управления безопасностью, изменениях в User Account Control, усовершенствовании BitLocker, также познакомимся с AppLocker и новой биометрической инфраструктурой (Biometric Framework).

Проблемы с безопасностью в Vista

В ответ на жалобы о том, что Windows была не безопасна, компания Microsoft сконцентрировала большую часть своего внимания на безопасности во время создания Windows Vista. Шифрование дисков BitLocker, родительский контроль, встроенная утилита против вредоносного ПО (Windows Defender), усовершенствования в брандмауэре Windows, Data Prevention Execution (DEP), защищенный режим IE, защита служб, новая функция управления цифровыми правами, обновление Crypto API, клиент Network Access Protection (NAP), усовершенствование Encrypting File System (EFS), политики ограничения софта и многие другие усовершенствования функций безопасности были представлены в Vista. Service Pack 1 добавил дополнительные усовершенствования в области безопасности, включая мультифакторную аутентификацию для BitLocker, перестроенный Random Number Generator (RNG), подписание файлов Remote Desktop Protocol (RDP), и т.д.

Однако функцией безопасности, которую быстрее всего заметили (и возненавидели) пользователи, стала функция User Account Control (UAC), посредством которой все учетные записи пользователей, включая учетные записи администраторов, запускаются в стандартном режиме по умолчанию и требуют повышения уровня прав в случае необходимости более высоких привилегий. Сама природа UAC, наряду с функцией Secure Desktop, которая блокировала доступ вредоносному ПО к компьютеру, требуя прав администратора и назойливо затемняя монитор, была основной жалобой по поводу Vista.

Команда разработчиков Windows 7 столкнулась с трудностью создания ОС, которая будет столь же безопасна, или даже более безопасна, чем Vista, но в то же время сделает безопасность более прозрачной для пользователей.

Итак, прощай Центр безопасности, привет Центр действий

Центр безопасности (Security Center), располагавшийся в панели управления и предназначавшийся для предоставления управления параметрами безопасности из одного места, использовался в Windows XP SP2, а затем в Vista. В Windows 7, добавлено еще больше централизации. Теперь центра безопасности больше нет, а на его место пришел новый Центр действий (Action Center). Здесь вы найдете оповещения, которые не только связаны с безопасностью, но и касающиеся обновлений Windows Update, диагностики, NAP, резервного копирования и восстановления, диагностирования и исправления проблем, как показано на рисунке 1.

Рисунок 1: Центр действий централизует многие задачи администрирования, включая безопасность

Более гибкие параметры UAC

В Vista можно было отключать UAC посредством групповой политики, но это было не очень хорошее решение, поскольку оно подвергало вас потенциальному риску атак. Вместо этого можно было устанавливать UAC на повышение уровня прав без запроса подтверждения, что было более удачной мыслью. Однако версии Home операционной системы Vista не включали редактора групповой политики, поэтому для выполнения данной задачи приходилось изменять системный реестр. Компания Microsoft упростила пользователям контроль над поведением UAC в Windows 7.

Заметка: ИТ администраторы вздохнут с облегчением, когда узнают, что пользователи не смогут изменять параметры UAC, не имея привилегий администратора.

В левой панели центра действий есть опция с названием User Account Control Settings. Поведение подсказок UAC настраивается посредством движущегося рычага, который имеет четыре положения:

- Всегда оповещать (Always Notify): вы будете получать уведомление UAC во время установки ПО или внесении изменений в систему
- Оповещать только когда программы пытаются внести изменения (Notify Only When Programs Try to Make Changes): вы будете получать уведомления только в том случае, если программа требует привилегии более высокого уровня, а не когда вы вносите изменения в параметры Windows (этот параметр используется по умолчанию)

- Оповещать только когда программа пытается внести изменения (Не затемнять монитор – (Do Not Dim the Desktop)): то же, что и параметр по умолчанию, за исключением того, что функция Secure Desktop отключена во время оповещения
- Никогда не оповещать (Never Notify): вы не будете получать уведомления ни при внесении изменений в параметры Windows, ни при установке ПО (не рекомендуется)

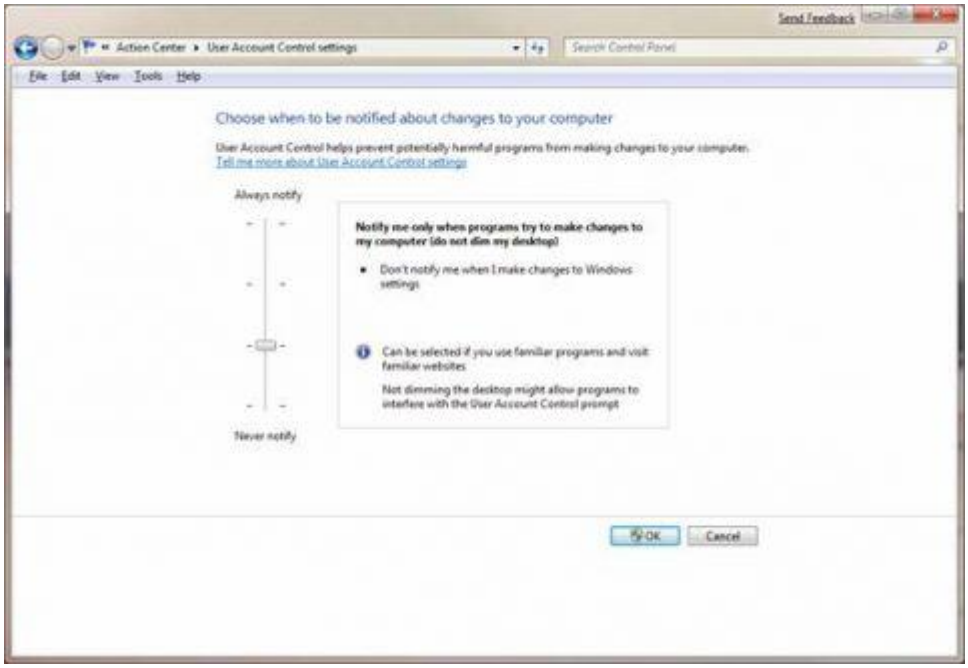


Рисунок 2: Этот слайдер позволяет вам более четко управлять оповещениями UAC в Windows 7

Усовершенствования BitLocker

BitLocker, включенный в версии Vista Enterprise и Ultimate, позволяет шифровать целые тома с помощью AES, либо используя Trusted Platform Module (TPM) чип, которым оснащены некоторые компьютеры, либо USB ключ. Это не позволяет загружать ОС или получать доступ к данным в зашифрованных разделах без авторизации (например, устанавливая различные элементы ОС или их загрузку). Это особенно полезно для мобильных устройств, которые могут быть утеряны или украдены.

В Vista BitLocker изначально мог использоваться только для шифрования разделов, на которые была установлена ОС. Service Pack 1 добавил возможность шифрования нескольких дисков, но его нельзя было использовать для шифрования съемных носителей. В Windows 7, BitLocker был усовершенствован поддержкой шифрования портативных жестких дисков и флеш-карт. Это называется ‘BitLocker to Go’. Эту функцию многие компании очень долго ждали, поскольку хранение уязвимых данных на USB носителях стало очень популярным.

Заметка: можно настраивать политику, которая будет требовать того, чтобы носители были защищены с помощью BitLocker, прежде чем пользователи смогут записывать на них данные.

BitLocker управляется из панели управления, как показано на рисунке 3.

Рисунок 3: В Windows 7 у вас есть возможность использовать BitLocker шифрование на съемных и фиксированных носителях

Можно использовать кодовую фразу для разблокирования диска или смарт-карту и PIN, как показано на рисунке 4.

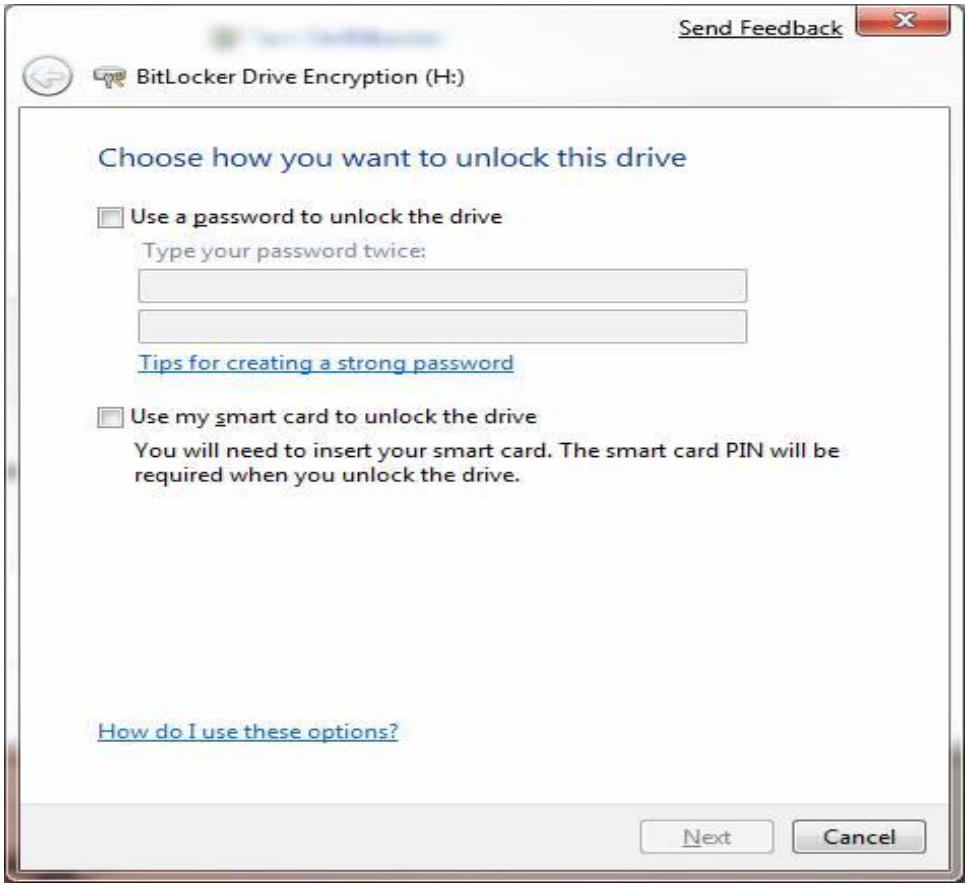


Рисунок 4: Когда вы шифруете диск с помощью BitLocker, можно использовать кодовую фразу или смарт-карту для разблокирования носителя

Можно также устанавливать ключ восстановления, чтобы использовать его для разблокирования носителя, если вы забыли кодовую фразу. Ключ восстановления можно сохранить в файл или распечатать и хранить в надежном месте (или и то, и другое). Может потребоваться время в зависимости от размера носителя. Шифрование 2 GB USB носителя заняло немногим более 9 минут в моей системе. Шкала прогресса будет информировать о продвижении процесса, как показано на рисунке 5.

Рисунок 5: Шкала прогресса информирует вас о выполнении процесса шифрования

AppLocker

Windows 7 имеет еще один «блокиратор»: AppLocker, который представляет собой новую функцию групповой политики. Она позволяет администраторам управлять версиями приложений, которые пользователи могут устанавливать и использовать. Это не позволяет пользователям устанавливать и запускать старые версии приложений, которые могут иметь уязвимости в безопасности.

В предыдущих версиях Windows использовалась политика Software Restriction Policies для управления тем, какие программы пользователи могут запускать. AppLocker является усовершенствованием такого контроля благодаря более простой настройке посредством трех типов правил: Путь (Path), Хэш-значение файла (File Hash) и Публикатор (Publisher). Правила Publisher заменяют правила сертификатов (Certificate Rules) в SRP, и дают вам больше гибкости и возможностей. Их также сложнее обойти.

Биометрическая инфраструктура (Biometric Framework)

В Vista, если вы хотели использовать отпечатки пальцев для входа в систему, вам нужно было использовать ПО производителей датчиков, считывающих отпечатки пальцев. Новая функция безопасности в Windows 7 под названием Biometric Framework, предоставляет собственную поддержку устройств считывания отпечатков пальцев и упрощает разработчикам задачу внедрения биометрической безопасности в своих приложениях. Вы найдете это новое приложение под названием Биометрические устройства (Biometric Devices) в панели управления. Оно используется для управления считыванием отпечатков пальцев, как показано на рисунке 6.

Рисунок 6: Можно управлять биометрическими устройствами из панели управления

Параметры можно настраивать на разрешение входа пользователей в Windows и/или в домен, используя биометрические данные, и для каждого пользователя можно задавать определенный палец.

Заметка: на момент написания этой статьи, сенсоры отпечатков пальцев являются единственными биометрическими устройствами, поддерживаемыми в Windows Biometric Framework.

Служба Windows Biometric Service (WBS) является частью инфраструктуры, управляющей устройствами считывания отпечатков пальцев и действующей в качестве I/O proxy между клиентскими приложениями и биометрическими устройствами, поэтому приложения не имеют прямого доступа к биометрическим данным. Это защищает конфиденциальность пользователей.

Заключение

Что ж, можно сказать, что Microsoft идет по правильному пути, повышая безопасность своих ОС. Будет ли система безопасности удобна, незаметна для пользователя и эффективна? Пока можно сказать, что она неудобна для пользователя из-за обилия ненужных сообщений от UAC, появляющихся на экране.

Хоть Microsoft и работает над этой проблемой, все равно, думаю, часть недовольств останется. Будет ли ПО от Microsoft менее дырявым благодаря SDL? Вопрос остается открытым.

Какие выводы можно сделать?

Microsoft действительно пытается повысить безопасность новой ОС.

Команда разработчиков Windows 7 столкнулась с трудностью создания ОС, которая будет столь же безопасна, или даже более безопасна, чем Vista, но в то же время сделает безопасность более прозрачной для пользователей.

В Windows 7 компания Microsoft продолжила вложение усилий в создание более безопасных операционных систем, прислушиваясь к отзывам пользователей, говорящим о том, как должна работать система безопасности. Представители компании в то же время усовершенствовали некоторые функции безопасности предыдущих версий ОС с точки зрения пользовательского опыта, опыта администраторов и достигнутого уровня безопасности. Для большинства производственных пользователей и сетевых администраторов усовершенствования безопасности Windows 7 станут отличной причиной для перехода на данную ОС

Мое мнение по UAC

По сравнению с Vista конечно есть определенные продвижения, UAC стал менее «раздражающим» в Windows 7, но и замечания все-таки остались. До сих пор он выводит запросы на разрешение для известных, проверенных программ, для компонентов Windows. Уже давно многие разработчики программ безопасности используют свои базы (или белые списки), в которые занесены проверенные, известные программы. Я уверен, что Microsoft обладает всем необходимым, чтобы сделать то же самое. А если все-таки программа неизвестна, то рассматриваемый компонент защиты должен протестировать ее, прежде чем опираться на факт, что он требует поднятия уровня привилегий. В общем, на мой взгляд, Microsoft должны «автоматизировать» этот процесс, чтобы не перекладывать ответственность за принятие решения на пользователя! Если ей все-таки удастся это сделать, тогда UAC действительно станет хорошим средством защиты.

Конечно, безопасность Vista является лишь продолжением начатой работы и во многом напоминает безопасность ее предшественника, она стала более модернизированной, претерпела множество различных изменений в различных областях, но все же это не те изменения, от которых обычный «рядовой» пользователь ощутит выгоду.

Из поколения в поколения Microsoft устраняет недостатки и «дыры» в своих ОС. Так, например, Vista по своей сути более безопасна, нежели Windows XP. Это связано со значительными изменениями, которые Microsoft внесла в платформу Vista. Эти изменения коснулись пользовательских привычек и даже потребовавшие некоторых причудливых переписываний драйверов и т.п.

В то же время улучшения безопасности между Vista и Windows 7 не столь серьезны. В безопасности, как и в других областях, Windows 7 – это Vista, но только лучше.

По словам компании Microsoft, Windows 7 обладает улучшенной безопасностью, надежностью и производительностью. Это действительно так, это подтверждают множество тестов, так и детальный анализ безопасности ОС Vista и «семерки».

Даже, исходя результатов данной курсовой работы, можно сделать аналогичный вывод.

Внедрение в операционную систему таких концепций как защита ядра от исправления, предотвращение выполнения данных, рандомизация адресного пространства, обязательные уровни целостности звучит хорошо, если не учитывать, что ранняя пропаганда Vista тоже рекламировала безопасность операционной системы, однако большинство из этих обещаний провалились при материализации.

Версии

В зависимости от приобретенной версии Windows 7 будут доступны нововведения. Ниже можно ознакомиться с таблицей.

На таблице изображены версии ОС (по горизонтали) и доступные нововведения (по вертикали).

	Starter, Home Basic, Home Premium	Professional	Enterprise	Ultimate
Подключение к домену	-	+	+	+
Remote Desktop	-	+	+	+
BitLocker	-	-	+	+
AppLocker	-	-	+	+

Основное отличие Windows 7 Enterprise и Ultimate заключается в вариантах приобретения (Enterprise нельзя будет купить в розницу) и лицензирования (для Ultimate не предусмотрена возможность volume-лицензирования). Для пользователей, желающих иметь полный функционал без необходимости подписания volume-контракта как раз и предназначена Ultimate-версия — своеобразная Enterprise-версия, предназначенная для домашних пользователей.

Любые новые решения помимо этапа разработки предполагают глубокое тестирование их реализации, именно по этому Microsoft регулярно выкладывает в общий доступ бета-версии своих продуктов. По итогам промежуточных результатах тестирования бета-версии Windows 7 добровольцы нашли более двух тысяч ошибок и недоработок в ОС, которые Microsoft пообещала исправить к моменту выхода окончательной версии. Вместе с тем, новая ОС достаточно стабильна и, в отличие от Vista, на нескольких миллионах компьютерах, использованных для тестирования во всём мире, на 75 % устройств Windows 7 сразу начала нормально работать и только для остальных требовалась загрузка драйверов через Windows Update или с сайта производителя. Такое высокое качество продукта позволяет надеяться на качественную реализацию и рассмотренных технологий, детальное описание которых будет дано в последующих статьях.