СИСТЕМА МОНИТОРИНГА ОС WINDOWS SERVER. КЛИЕНТСКАЯ КОМПОНЕНТА

А.М. КАДАН, А.А. ШАГУН

Задача создания системы мониторинга сетевого компьютерного оборудования достаточно актуальна, так как система мониторинга является неотъемлемой компонентой политики безопасности любой компании: позволяет решать задачи, связанные с планированием роста сети, поиском и устранением ошибок на серверном и сетевом оборудовании, анализом сетевого трафика.

В докладе представлена клиентская компонента системы мониторинга, разработанная для использования в расмках ОС Windows Server, которая реалзует возможность постоянного наблюдения за состоянием узлов компьютерной сети: выполнять проверку доступности сетевых ресурсов, служб, следить за работой серверного и коммуникационного оборудования; в случае нарушения нормальной работы уведомлять администратора, используя различные средства оповещения.

При разработке данной системы были учтены недостатки известных решений. Главными преимуществами разработанной системы мониторинга ОС Windows Server является: простота настройки; легковесность решения; набор дополнительных функций, не имеющих аналогов. Эффективность разработанной системы продемонстрирована в сравнении с существующими решениями. Подтверждено, что разработанная система мониторинга в большинстве ситуаций потребляет меньше памяти и создаёт меньше нагрузки на процессор.

Оценивая функциональность, следует отметить, что в разработанной системе реализованы функции, которые отсутствуют в ее аналогах: мониторинг DHCP (система наблюдает за состоянием свободного пула адресов и ищет несанкционированные получения адреса); мониторинг DNS (анализ активных зон и уведомление пользователя об изменениях в них); мониторинг домена Active Directory (контроль над изменением групп пользователей, прав пользователей) и пр.

ГЕНЕРАЦИЯ СЛОВАРЕЙ НА ОСНОВЕ ИЕРАРХИЧЕСКИХ ПРАВИЛ В ЗАДАЧАХ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ

А.М. КАДАН, Т.А. ПОШВА

Наиболее достоверную информацию, касающуюся компьютерных преступлений, позволяет получить компьютерно-техническая экспертиза. Данный вид исследования широко применяется при рассмотрении дел в гражданском и уголовном судопроизводстве и является одним из самых актуальных и востребованных.

Основной проблемой, с которой сталкивается эксперт при исследовании информации, является её недоступность. Зачастую важная информация защищена паролем и хранится в зашифрованном виде, и получить доступ к такой информации, без каких-либо знаний о ключе шифрования невозможно.

При, наличии каких-либо данных о составителе пароля для взлома защищённой информации применяется метод атаки по словарю. В отличие от атаки полным перебором, проверяются не все возможные варианты, а лишь уже отобранные по специальным правилам до этого и загружаемые из списка слов, или словаря. Словарь генерируется из информации известной о составителе пароля или о самом пароле.

В докладе рассматривается разновидность простой словарной атаки и модели правил, которые позволяют пользователю задавать свои собственные варианты мутации элементов словаря. Рассмотрены системы иерархических разнородных правил, с помощью которых может быть описан механизм организации атаки. Выделены иерархические правила фильтрации — разнотипные иерархические правила, которые применяются к выходному

набору комбинаций слов (при генерации словаря), и иерархические правила мутации, определяющие схему модификации элементов словаря в ходе атаки. Рассмотренные модели используются для организации атак по словарю и могут находить применение в задачах раскрытия и расследования компьютерных преступлений, предполагающих обеспечение доступа к закрытой паролем информации.

ТЕСТИРОВАНИЯ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ ЭЛЕКТРОННЫХ ПЛАСТИКОВЫХ КАРТ ПО МЕТОДОЛОГИИ NIST

Н.Г. КИЕВЕЦ

Обсуждаются результаты тестирования генераторов случайных чисел (ГСЧ) электронных пластиковых карт (ЭПК) с помощью созданного программно-аппаратного комплекса (АПК) и методологии NIST версии 2010 г., реализованной в системе MATLAB. Анализировалась последовательность длиной 1000192 бит, сформированная из ключей длиной 256 бит, используемых для шифрования по ГОСТ 28147-89. В целях экономии временных ресурсов для тестов, не требующих последовательностей в один миллион бит, была использована начальная часть сформированной последовательности длиной 128000 бит. Частотный тест в подпоследовательностях проводился для последовательности, составленной из первых 100 ключей.

Многократное тестирование с помощью вышеуказанных методик позволило определить требования к параметрам тестирования. Так, прохождение частотного теста в подпоследовательностях при длине подпоследовательности, равной 256 бит, говорит о том, что в каждом из ключей исследуемой последовательности количество единиц примерно равно количеству нулей. В тесте пересекающихся шаблонов длина подпоследовательности была взята равной 256 бит. Тест «блоков» в подпоследовательностях и универсальный статистический тест Маурера четко определяют значение длины подпоследовательности в зависимости от длины тестируемой последовательности. С учетом параметров, рекомендуемых NIST, для теста непересекающихся шаблонов выбрана длина шаблона m=8, так как длина ключа кратна этому значению.

При уровне значимости α=0,01, рекомендуемом NIST, ГСЧ ЭПК прошел все 15 тестов и может быть использован в носителях ключевой информации.

О СВОЙСТВАХ ДЕКАРТОВЫХ ПРОИЗВЕДЕНИЙ НЕПРИМИТИВНЫХ КОДОВ ХЕММИНГА

В.А. ЛИПНИЦКИЙ, А.А. БЕРЕЗОВСКИЙ

Развитие помехоустойчивого кодирования происходит в преодолении противоречивых требований к кодам: высокая скорость передачи информации в сочетании с необходимостью коррекции ошибок большой кратности. Выполнение последнего требования неизбежно вязнет в громоздких процедурах декодирования.

Существует мнение, что коды произведения могут дать неплохой выход из сложившейся ситуации. Теоретический анализ демонстрирует неплохие свойства кодов произведений с сомножителями — непримитивными кодами Хемминга. Проведенные компьютерные расчеты подтверждают теоретические выводы. Правда, обнаружился любопытный факт — при формировании кодов произведений следует избегать самодвойственных неприводимых примитивных полиномов: коды произведения на их основе имеют аномально высокую размерность, но их минимальное расстояние меньше теоретически рассчитанного.