XXXII Неделя науки СПбГПУ. Материалы межвузовской научно-технической конференции. Ч.V : С.194-195

УДК 004.056

А.П.Лубанец (асп., каф. Телематика), В.С.Заборовский, д.т.н., проф.

УПРАВЛЕНИЕ СИСТЕМАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Для общего случая систем информационной безопасности математически доказано, что основная теорема безопасности (теорема Белла-Лападулы [1]) верна только в случае вырожденной модели возможностей нарушителя, т.е. тогда, когда единственный способ получить сведения о секретной информации — выполнить ее чтение установленным порядком, а единственный способ изменить ее — выполнить запись установленным порядком [2]. В современных информационных системах модель нарушителя нельзя считать вырожденной. Для того чтобы узнать секретную информацию, не обязательно выполнять операцию чтения, эту информацию можно просто найти, используя математические, криптоаналитические и вычислительные инструменты и возможности для реализации атаки с использованием уязвимостей компонентов информационной системы, количество которых увеличивается с каждым годом экспоненциально [3,4]. Именно поэтому система информационной безопасности (СИБ) призвана сделать применение данных инструментов невозможным, а уязвимости – недоступными. Основной упор при этом должен делаться на совершенствование процесса управления системой информационной безопасности, которое, в идеале, должно быть реализовано с выполнением основной теоремы безопасности.

Управление безопасностью в современном понимании заключается в реализации подхода «Три А», в соответствии с которым реализуются три процесса: аутентификации и авторизации пользователя информационной системы или ее объекта и аудите событий, происходящих в ней, и их взаимосвязей (активный аудит). Рассмотренный метод не может ни к коей мере выполнить требования основной теоремы безопасности, а компоненты системы информационной безопасности – обеспечить безопасную циркуляцию информационных потоков. Поэтому в настоящее время наблюдается проработка нового подхода управления безопасностью, заключающегося в одновременном обеспечении целостности, управляемости, доступности и наблюдаемости информационной системы. При этом под целостностью понимается уверенность авторизованного пользователя в том, что получаемая им информация точна и не была случайна изменена. Требование управляемости обеспечивает управляемый доступ и распределение ресурсов информационной системы между пользователями. Доступность системы информационной безопасности должна обеспечиваться таким образом, чтобы пользователь гарантированно имел авторизованный доступ к ресурсам информационной системы в любое время, когда ему это разрешено. И, наконец, наблюдаемость (контроль) системы информационной безопасности заключается в обеспечении прогнозируемого функционирования информационной системы и аудите ее состояний. Разработка архитектуры системы информационной безопасности в контексте приведенных требованиях является сложной научно-технической задачей, один из вариантов решения которой рассматривается в данной работе.

Систему информационной безопасности, отвечающую требованиям обеспечения целостности, управляемости, доступности и наблюдаемости информационной системы, назовем системой гарантированной информационной безопасности (СГИБ). При этом для обеспечения целостности предлагается использовать следующие методы и мероприятия: применять средства криптографической защиты, удовлетворяющие стандартам ГОСТ, внедрять инфраструктуру распределения открытых ключей на базе сертификатов x.509, при

передаче информации в распределенной среде использовать стек защищенных протоколов IPSec, проводить обязательную сертификацию компонентов информационной системы на недокументированные возможностями (НДВ) уполномоченными органами, минимизировать функциональность автоматизированных рабочих мест информационной системы с использованием технологии «тонкого клиента» или при помощи специального программного обеспечения для создания закрытой среды выполнения.

Для обеспечения управляемости СИБ предлагается использовать технологию «единого окна», которая заключается в том, что управление пользователями реализуется централизовано для всех приложений информационной системы с помощью стандартизированной технологии каталогов, поддерживающей протокол LDAP и интегрированной с инфраструктурой распределения открытых ключей. Помимо этого, в политике информационной безопасности должны быть учтены правила «запрещено по умолчанию» и «правило двух ключей» (разделение полномочий системного администратора и администратора информационной безопасности). Управление доступом пользователей к ресурсам информационной системы должно осуществляться в пространстве как можно большей метрики. Это означает, что для локальных сетей необходимо использовать LIP-идентификацию (LIP – Local Identification Parameters – управление доступом осуществляется на основании следующих параметров: VLAN-MAC-IP-TCP/UDP-порт), а для глобальных – GIP-идентификацию (GIP – Global Identification Parameters: SA-IP-TCP/UDP-порт, где SA – Security Association – структура данных защищенного сетевого IPSec-соединения). Приемы обеспечения управляемости СИБ получили название кластера информационной безопасности [5,6].

Доступность СИБ обеспечивается масштабированием компонентов, применением технологий резервирования, функциональной и структурная избыточности.

И, наконец, ключевая характеристика – наблюдаемость СИБ – обеспечивается применением компонент, обеспечивающих скрытое функционирование СИБ, т.е. таких устройств, нахождение в сети которых не идентифицируется известными средствами сканирования (это могут быть межсетевые экраны, экранированные маршрутизаторы, криптошлюзы и т.д.). Для этой же цели используется такие важные технологии как активный аудит и прогнозирование характеристик каналов связи с использованием ряда алгоритмов анализа, основанных на фрактальной природе сетевого трафика.

Примером архитектуры системы, построенной на предлагаемых принципах может быть отраслевая СИБ Минобразования РФ. Важно отметить, что при выполнении всех перечисленных свойств, для СГИБ с некоторыми допущениями возможно доказать теорему о безопасности для невырожденной модели нарушителя.

ЛИТЕРАТУРА:

1. Теория и практика обеспечения информационной безопасности. Под ред. П. Д. Зегжды. — М., Изд-во Агентства «Яхтсмен», 1996.
2. Ростовцев А.Г. Криптография и защита информации // Проблемы информационной безопасности. №2. 2002.
3. В.А. Минаев. Информационная безопасность: российские парадоксы // Системы безопасности. №2. 2003. С. 12-15.
4. Internet Risk Impact Summary for January 1, 2003 – March 31, 2003 // X-Force Global Threat Operations Center Report. Internet Security System Press, 2003. [www.iss.net]
5. Заборовский В., Лубанец А. Кластер информационной безопасности // Бди. 2003. №2. С. 32-35.
6. Лубанец А. Вычислительные кластеры для создания систем информационной безопасности в высокоскоростных компьютерных сетях. // Конфидент. 2003. №2. С. 70-74.