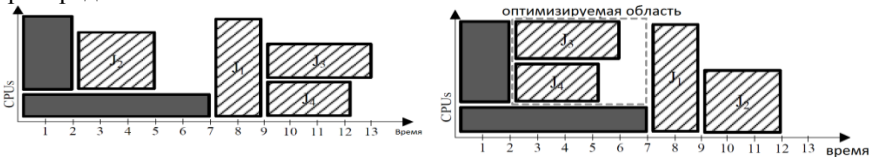
Предлагается вероятностная модель планирования выполнения работ, в основе которой лежит оценка следующих вероятностей: вероятности планирования работы в качестве приоритетной задачи; вероятности планирования работы в качестве обратно заполненной задачи; вероятности завершения выполняемой работы в данный момент времени; вероятности освобождения заданного количества процессоров выполняемыми работами в данный момент времени; вероятности возникновения события освобождения работами процессоров. Для каждой из вероятностей получены численные соотношения, выполняющиеся при определенных допущениях.

Разработано программное обеспечение, позволяющее для множества выполняемых работ и списка работ, поставленных в очередь на выполнение, оценивать вероятности выбора работ из очереди с целью их постановки на выполнение в качестве приоритетной работы либо в качестве обратно заполненной работы. Проведены вычислительные эксперименты, показывающие способность предлагаемой вероятностной модели улучшить работу алгоритма Backfill в плане загрузки ресурсов распределенной вычислительной системы.



а) б)

Рис.1. Планы выполнения работ, построенные алгоритмом Backfill

Работа выполнена при участии и под руководством А.А. Прихожего.

УДК 681.3

Защита локальной сети, необходимый минимум

Шевчик Р. В.
Белорусский национальный технический университет

При построении безопасной локальной вычислительной сети (LAN) следует минимизировать количество служб и сервисов, предоставляемых сетью, используемых клиентами из сети Интернет. Архитектура LAN в обязательном порядке должна предусматривать наличие DMZ — демилитаризованной зоны, контролируемой межсетевым экраном. Крайне желательно наличие NAT (система переадресации выполняет функцию сокрытия адресов внутренних систем). Установка самых последних обновлений строго обязательна.

Даже если система имеет самые последние обновления, с момента обнаружения новой уязвимости и до момента выхода заплатки «умные люди» успевают написать эксплоит или создать «червя». Как на сервере, так и на рабочих станциях должно быть установлено антивирусное ПО со свежими базами. Если до сих пор используется файловая система FAT32, ее следует сменить на NTFS. NTFS более безопасна: она позволяет разграничить доступ к ресурсам ПК и значительно усложнит процесс локального и сетевого взлома паролей базы SAM.

В свойствах подключения крайне желательно оставить только самое необходимое, а именно TCP/IP. «Службу доступа к файлам и принтерам сети Microsoft» необходимо отключить (касается машин, не предоставляющих SMS-доступ), чтобы не облегчать задачу всем любителям «дефолтовых» C$, D$, ADMIN$ и т.д. Все неиспользуемые сервисы желательно выключить. Это не только повысит производительность вашей системы, но и автоматически закроет множество открытых портов.

Удалите лишние учетные записи (такие, как HelpAssistant и SUPPORT_388945a0), запретите локальный и сетевой вход для всех пользователей, оставив только используемых на данной машине. Пользователя «Администратор» лучше переименовать. Открытые по умолчанию ресурсы C$, D$, ADMIN$ желательно отключить (созданием параметра DWORD по адресу HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\lanmanserver\parameters).

В локальной сети не стоит забывать и о снифферах, с помощью которых ваши пароли могут стать «общественным достоянием» (не секрет, что пароли таких сервисов, как FTP и Telnet, передаются по LAN в открытом виде). Используя сниффер, даже зашифрованные пароли легко взломать. Выход — построение локальной сети не на хабах (сетевые пакеты, которые получает хаб, распределяются по всем адресам независимо от места назначения), а на свитчах (используется технология доставки пакетов «по адресу»). Применение свитчей значительно усложняет процесс перехвата сетевых паролей и делает злоумышленника «видимым» (перехват паролей возможен даже при использовании свитчей, но в этом случае машина злоумышленника вынуждена генерировать ARP-пакеты — технология ARP-poizoning), используя стандартный набор для антисниффинга.

Литература:

1. Взлом и защита локальной сети [Электронный ресурс] / nestor — Электронные данные. — Режим доступа: http://www.nestor.minsk.by/kg/ 2007/29/kg72917.html — Дата доступа: 9.05.2015.