Руслан Богатырев

Защищенные операционные системы

Источник: Открытые системы, #04/2001

Безопасность компьютерных систем была и остается головной болью для тех, кому небезразлична судьба важной информации, влияющей на принятие решений, управление финансами, распределение ресурсов и т. п. Годы идут, а число желающих воспользоваться плодами чужого труда или же нанести умышленный ущерб не уменьшается, а непрерывно возрастает. Более того, благодаря возможности быстрого и широкого распространения «передового опыта» по преодолению защитных барьеров, ввиду явной беспечности многих владельцев информации и редкого соблюдения принципа неотвратимости наказания весь мир столкнулся с серьезной и жестокой болезнью. Имя ее неизвестно, но опасность ее очевидна. Она в скрытой форме поразила огромную территорию и теперь грозит перерасти в настоящую эпидемию.

Еще никогда в истории реальный мир так не зависел от мира искусственного, придуманного и построенного самим человеком. Не позаботившись должным образом об организации действенной защиты своих творений, мы во благо развития цивилизации стремимся все глубже связать информационными каналами два этих мироздания, обеспечить максимальное проникновение более несовершенного мира в менее несовершенный. Компьютерная эволюция уже преодолела три важных этапа:

1) концентрацию вычислительных и информационных ресурсов (в эпоху мэйнфреймов);
2) обеспечение технической доступности компьютерных мощностей для массовой аудитории (в эпоху ПК);
3) ломку естественных границ пространства и времени в масштабах мировой экономики и политики (в эпоху Internet).

Единая цифровая форма представления в огромной степени облегчила решение многих практических задач, но при этом поневоле создала почву для нанесения максимального ущерба с минимальными затратами. Более того, в силу унификации информационного обмена и простоты работы с программными инструментами вред может осуществить даже неискушенный человек. Только лишь столкнувшись с проблемой СПИД, мы смогли осознать, что наш организм обладает своей многоуровневой защитой, где иммунитет играет едва ли не ключевую роль. Отсутствие в компьютерном мире подобного всепроникающего защитного барьера не в столь уж отдаленном будущем обещает принести проблемы такого масштаба, по сравнению с которыми беды, вызванные современными эпидемиями, покажутся мелкими и незначительными. Наступает время всерьез задуматься над тем, что без возведения искусственных барьеров, без создания аналогов локальной иммунной защиты для ПО дальше двигаться вперед становится все опаснее.

Когда речь заходит о проблемах информационной безопасности, прибегают обычно к простому и проверенному сценарию: сначала хорошенько запугать аудиторию цифрами и фактами, характеризующими масштабы и природу грозящей опасности, а затем приступить к основной части — к изложению рецептов чудодейственных «препаратов», устраняющих ряд упомянутых симптомов. Отдавая дань традиции, не будем чересчур далеко отходить от проторенного пути. Однако вряд ли имеет смысл лукавить: проблем здесь куда больше, чем решений. Так что в зону нашего внимания попадут в основном болевые точки компьютерных конфигураций — их операционных систем.

По данным годового отчета «2001 Computer Crime and Security Survey» [4] Института компьютерной безопасности в Сан-Франциско и ФБР, финансовые потери от компьютерных преступлений в США за минувший год выросли на 43% с 265,6 млн. долл. до 377,8 млн. При этом 85% респондентов из 538, в основном из промышленных и государственных структур, заявили о фактах нарушения компьютерной безопасности, причем не только из-за атак злоумышленников. Почти 64% были озабочены понесенными убытками, но лишь 35% смогли оценить их в денежном выражении. Около 70% респондентов заявили, что чаще всего атакам подвергались Internet-каналы, а 31% показали, что атакам подвергались внутрикорпоративные системы. Случаи вторжения извне подтверждали 40% респондентов (в 2000 г. — 25%), а 38% фиксировали отказ в обслуживании (27% в 2000 г.). На нарушение привилегий из-за злоупотребления сотрудниками работой в Сети жаловались 91% респондентов, а 94% обнаружили в своих системах вирусы (в 2000 г. это отмечали 85%).

Даже из этих скупых цифр видна явно негативная тенденция — Internet не только возводит мосты между странами и континентами, но и приближает преступника к жертве. Перефразируя известное изречение, можно сказать, что если вы не интересуетесь киберкриминалом, очень скоро киберкриминал заинтересуется вами. Если оставить в стороне извечные вопросы разведки и промышленного шпионажа и сосредоточиться только на «бытовой» стороне дела, то одними из ведущих проблем в области информационной безопасности в минувшем году стали атаки на платежные системы, дискредитация компаний (отказ в обслуживании), производственный саботаж, вскрытие корпоративных секретов, нарушение прав интеллектуальной собственности. По оценкам отдела по науке и технологиям при Президенте США, ежегодный урон, наносимый американскому бизнесу компьютерными злоумышленниками в последние годы, достигал 100 млрд. долл. Потери от несанкционированного доступа к информации, связанной с деятельностью финансовых институтов США, составляли не менее 1 млрд. долл. в год. Таким образом, американский бизнес вплотную подошел к тому рубежу, когда своевременное и адекватное решение вопросов безопасности для него становится экономически целесообразным.

UNIX в контексте безопасности

История ОС неотделима от истории и эволюции самих компьютеров. Так уж сложилось, что именно клоны UNIX доминируют сегодня на рынке корпоративных систем и стали связующим звеном между миром персональных и высокопроизводительных компьютеров. К сожалению, Unix страдает серьезными недостатками, а феномен Linux [3], заставил по-иному взглянуть на многие проблемы, в том числе и на проблемы информационной безопасности.

UNIX не имеет четкого механизма, обеспечивающего целостность пользовательских программ и файлов, не обеспечивает управление доступом для отдельного пользователя; разграничение прав ведется в рамках групп. В обычном варианте UNIX не столь уж трудно стороннему человеку захватить полномочия суперпользователя. Учет и контроль действий пользователя, особенно при работе с критичными для безопасности ресурсами, также не является сильным местом обычного UNIX. Конечно, определенными усилиями по конфигурированию со стороны системного администратора некоторые изъяны можно устранить. Но, в общем, картина не выглядит обнадеживающей [1, 2].

В работе [6] сотрудников Агентства национальной безопасности США приводится подробный анализ проблем, стоящих перед существующим поколением операционных систем в плане компьютерной безопасности. Основной вывод: нужны новые специально спроектированные защищенные ОС. В частности, авторы говорят о том, что система Kerberos, протоколы SSL и IPSEC в значительной степени уязвимы в силу того, что при невозможности обеспечить наличие достоверного ПО на концах соединения защита становится иллюзорной.

Вот что сказал в своем недавнем интервью Элиас Леви (Aleph1), модератор известного списка рассылки BugTraq, посвященного проблемам компьютерной безопасности: «Я считаю, что модель безопасности в UNIX чересчур упрощенная. Подход «все или ничего» оказывается никуда не годным по сравнению с принципом наименьших полномочий (least privilege)... Достоверная вычислительная база (Trusted Computing Base) никогда не предоставит всего того, что требовалось бы пользователю. С другой стороны, я нахожу, что большинство реализаций механизмов принудительного управления доступом (mandatory access control), привилегиями и т. д. слишком усложнены... В конечном итоге трудно предсказать те взаимодействия, которые приведут к появлению слабых мест. Вспомним хотя бы проблему sendmail, которая появилась в результате полномочий, внедренных в ядро Linux».

Леви призывает отказаться от практики «латания дыр» и начать строить новую ОС, изначально удовлетворяющую требованиям безопасности.

Это перекликается с наметившимся сегодня интересом к достоверным (trusted) и защищенным (secure) операционным системам. Требования к безопасности должны быть определяющими в проектировании ОС, а не вводиться как вспомогательные службы.

Критерии и ориентиры в области безопасности

Работы над критериями безопасности систем начались еще в 1967 г. и в 1970 г. появился первый отчет под названием «Security Controls for Computer Systems». В 1983 г. Министерство обороны США выпустило «Orange Book» — книгу в оранжевой обложке под названием «Критерии оценки достоверных компьютерных систем» (Trusted Computer Systems Evaluation Criteria). Область компьютерных сетей в отношении безопасности определялась в так называемых рекомендациях X.800 — Security Architecture for Open Systems Interconnection for CCITT Applications. В «Оранжевой книге» достоверная система определяется как «система, использующая достаточные аппаратные и программные средства для обеспечения одновременной обработки информации разной степени секретности группой пользователей без нарушения прав доступа».

Выделяются два основных критерия оценивания достоверных систем:

1) политика безопасности (набор правил и норм, определяющих дисциплину обработки, защиты и распространения информации, а также выбор конкретных механизмов обеспечения безопасности; это активный компонент защиты);
2) гарантированность (степень доверия, которая может быть оказана конкретной реализации ОС; отражает уровень корректности механизмов безопасности; является пассивным компонентом защиты).

В соответствии с «Оранжевой книгой» выделяются три роли: системный администратор, системный оператор и администратор безопасности. Согласно требованиям TCSEC документация производителя должна включать в себя четыре важных элемента: политику безопасности; интерфейсы достоверной вычислительной базы; механизмы TCB; руководство по эффективному использованию механизмов TCB.

Вообще говоря, в область защищенных компонентов входят не только операционные системы. Так, в частности, в дополнение к «Оранжевой книге» TCSEC, регламентирующей вопросы обеспечения безопасности в ОС, существуют аналогичные документы Национального центра компьютерной безопасности США для СУБД (TDI, «Пурпурная книга») и сетей (TNI, «Красная книга»). Так что «Оранжевая книга» — не единственный, хотя и важный документ. В США давно уже появилась целая серия документов в разноцветных обложках, получившая название «Радуга» (Rainbow Series; www.radium.ncsc.mil/tpep/library/ rainbow). При этом, как видно из врезки, иногда под обложкой одного и того же цвета выступал разный материал.

За пределами США также появились аналоги «Оранжевой книги»: это руководящие документы Гостехкомиссии (1992 г.), а также «Критерий оценки безопасности информационных технологий» (ITSEC — Information Technology Security Evaluation Criteria, 1991), действующий в Великобритании, Германии, Франции и Нидерландах.

Рис.1. Этапы создания «Единых критериев»

Конечно же, в силу необходимости унификации подходов к информационной безопасности в конце концов возникла потребность снять двойственность регулирования, которая отдельно велась в США (TCSEC) и Европе (ITSEC). На рис. 1 показано «генеалогическое древо» принятия нового международного стандарта, получившего название «Единые критерии для оценки безопасности в области информационных технологий» [5]. Чаще всего его называют просто «Common

Criteria» («Единые критерии»), определяющие международный стандарт ISO/IEC 15408, в разработке которого приняли участие Агентство национальной безопасности и Национальный институт стандартов и технологий (США), Группа по безопасности в области электроники и передачи данных (Великобритания), Федеральное агентство в области информационных технологий (Германия), Центральная служба безопасности информационных систем (Франция), Агентство национальной безопасности Нидерландов в области передачи данных, Служба безопасности в области передачи данных (Канада).

Описание Common Criteria V2.1 содержится в трех книгах:

1) Введение и общая модель (CCIMB-99-031).
2) Функциональные требования к безопасности (CCIMB-99-032).
3) Требования к гарантиям безопасности (CCIMB-99-033).

В «Единых критериях» (http://www.commoncriteria.org) выделяются 11 функциональных классов:

1) аудит;
2) криптографическая поддержка;
3) передача данных;
4) защита данных пользователя;
5) идентификация и аутентификация;
6) управление безопасностью;
7) конфиденциальность;
8) защита функций безопасности целевой системы;
9) утилизация ресурсов;
10) доступ к целевой системе;
11) достоверные пути/каналы.

Внутри каждого их этих классов содержится несколько семейств, а в каждом семействе — от одного до нескольких компонентов.

Критерии, сформулированные в TCSEC, ITSEC и CCITSE, определяют разбиение компьютерных систем на 4 уровня безопасности (A, B, C, D) в зависимости от степени достоверности . Уровень A самый высокий. Далее идет уровень B (в порядке понижения безопасности здесь идут классы B3, B2, B1). Затем наиболее распространенный уровень C (классы C2 и C1). Самый нижний уровень — D (системы, которые не смогли получить аттестацию по заявленным выше классам).

Следуя компромиссу между требованиями безопасности, эффективностью системы и ее ценой, подавляющее большинство компаний стремится сегодня получить сертификат по классу C2.

Литература

1. П. Христов. Безопасность данных в ОС UNIX // «Открытые системы», 1993, № 3.
2. В. Галатенко. Информационная безопасность // «Открытые системы», 1995, № 4, 1996, № 1.
3. Р. Богатырев. Linux: истоки новой философии программирования // Мир ПК, 2001, No.1.
4. 2001 Computer Crime and Security Survey // Computer Security Institute, San Francisco, March 12, 2001; http://www.gocsi.com/prelea_000321.htm
5. Common Criteria for Information Technology Security Evaluation (CCITSE) V2.1 // 1998; http://www.radium.ncsc.mil/tpep/library/ccitse/ccitse.html
6. P. Loscocco et al. The Inevitability of Failure: The Flawed Assumptiom of Security in Modern Computing Environments // National Security Agency, 1998.

Тематика набора книг по компьютерной безопасности TCSEC в серии «Радуга»

- TCSEC (1983, 1985, «Оранжевая книга», 5200.28-STD).
- TNI, интерпретация достоверных компьютерных сетей (1987, 1990, «Красная книга», NCSC-TG-005, NCSC-TG-011).
- TDI, интерпретация достоверных СУБД (1991, «Пурпурная книга», NCSC-TG-021).
- Системы формальной верификации (1989, «Пурпурная книга», NCSC-TG-014).
- Производство достоверных систем (1992-1994, «Пурпурные книги», NCSC-TG-024).
- Защита доступа (1992, «Фиолетовая книга», NCSC-TG-028).
- Доверительное распределение (1988, «Темнолиловая книга», NCSC-TG-008).
- Создание документации (1988, «Рубиновая книга», NCSC-TG-007).
- RAMP (1995, «Розовая книга», NCSC-TG-013).
- Анализ тайных каналов (1993, «Светлорозовая книга», NCSC-TG-030).
- Тестирование безопасности (1991, «Яркооранжевая книга», NCSC-TG-023).
- Дискреционное управление доступом (1987, «Неоновая книга», NCSC-TG-003).
- Правила создания руководств пользователя (1991, «Персиковая книга», NCSC-TG-026).
- Управление конфигурациями (1988, «Янтарная книга», NCSC-TG-006).
- Требования к компьютерной безопасности (1985, «Яркожелтая книга», CSC-STD-003-85).
- Технические уточнения для требований к компьютерной безопасности (1985, «Желтая книга», CSC-STD-004-85).
- Достоверное восстановление после сбоев (1991, «Желтая книга», NCSC-TG-022).
- Написание руководств для управления достоверными средствами (1992, «Желто-зеленая книга», NCSC-TG-016).
- Комплектование данных в автоматизированных информационных системах (1991, «Бледнозеленая книга», NCSC-TG-025).
- Управление паролями (1985, «Зеленая книга», CSC-STD-002-85).
- Терминологический словарь в области компьютерной безопасности (1988, «Темнозеленая книга», NCSC-TG-004).
- Моделирование безопасности (1992, «Зеленовато-голубая книга», NCSC-TG-010).
- Компетенция администратора безопасности (1992, «Бирюзовая книга», NCSC-TG-027).
- Идентификация и аутентификация (1991, «Светлоголубая книга», NCSC-TG-017).
- Многократное использование объектов (1992, «Светлоголубая книга», NCSC-TG-018).
- Анкетирование при оценивании достоверных систем (1992, «Голубая книга», NCSC-TG-019).
- Концепции сертификации и аккредитации (1994, «Голубая книга», NCSC-TG-029).
- Оценивание достоверных продуктов (1990, «Яркоголубая книга», NCSC-TG-002).
- Интерпретация подсистем компьютерной безопасности (1988, «Небесноголубая книга», NCSC-TG-009).
- Управление достоверными средствами (1989, «Коричневая книга», NCSC-TG-015).
- Аудит в достоверных системах (1988, «Светлокоричневая книга», NCSC-TG-001).
- TRUSIX (1989, «Серебряная книга», NCSC-TG-020).

Классы безопасности компьютерных систем (TCSEC, Common Criteria)

Класс D. Минимальный уровень безопасности. В этот класс попадают системы, которые были заявлены на сертификацию, но ее не прошли. Пока в данном классе не зарегистрировано ни одной ОС.

Класс C1. Избирательная защита доступа. Предусматривает наличие достоверной вычислительной базы (TCB), выполнение требований к избирательной безопасности. Обеспечивается отделение пользователей от данных (меры по предотвращению считывания или разрушения данных, возможность защиты приватных данных). В настоящее время по этому классу сертификация не предусмотрена.

Класс C2. Управляемая защита доступа. Системы данного класса способны осуществлять более четко выделенный контроль в плане избирательной защиты доступа. Действия пользователя связываются с процедурами идентификации/аутентификации. Наделение и лишение пользователей привилегий доступа. Кроме этого, ведется аудит событий, критичных с точки зрения безопасности, выполняется изоляция ресурсов. По данному классу сертифицированы: AIX 4.3.1, OS/400 V4R4M0 with Feature Code 1920, AOS/VS II, Release 3.10, OpenVMS VAX and Alpha Version 6.1, CA-ACF2 MVS Release 6.1, NT Workstation и NT Server, Ver. 4.0, Guardian-90 w/Safeguard S00.01.

Класс B1. Маркированное обеспечение безопасности. В дополнение к требованиям класса C2 необходимо неформальное описание модели политики безопасности, маркировки данных, а также принудительного управления доступом к поименованным субъектам и объектам. По этому классу сертифицированы: CA-ACF2 MVS Release 6.1 в комплекте с CA-ACF2 MAC, UTS/MLS, Version 2.1.5+ (Amdahl), SEVMS VAX and Alpha Version 6.1, ULTRIX MLS+ Version 2.1 на платформе VAX Station 3100, CX/SX 6.2.1 (Harris Computer Systems), HP-UX BLS release 9.0.9+, Trusted IRIX/B release 4.0.5EPL, OS 1100/2200 Release SB4R7 (Unisys).

Класс B2. Структурированная защита. В этом классе систем TCB должна опираться на четко определенную и документированную формальную модель политики безопасности. Действие избирательного и принудительного управления доступом распространяется на все субъекты и объекты в системе. Выявляются тайные каналы (covert channel). TCB должна четко декомпозироваться на элементы, критичные и некритичные с точки зрения безопасности. Усиливаются механизмы аутентификации. Обеспечивается управление механизмами достоверности в виде поддержки функций системного администратора и оператора. Подразумевается наличие механизмов строгого управления конфигурацией. Система относительно устойчива к вторжению. По данному классу сертифицирована Trusted Xenix 4.0 (Trusted Information Systems).

Класс B3. Домены безопасности. TCB должна удовлетворять требованиям эталонного механизма мониторинга, который контролирует абсолютно весь доступ субъектов к объектам и при этом быть достаточно компактным, чтобы его можно было проанализировать и оттестировать. Требуется наличие администратора по безопасности. Механизмы аудита расширяются до возможностей оповещения о событиях, критичных по отношению к безопасности. Требуются процедуры восстановления системы. Система крайне устойчива к вторжению. По данному классу сертифицирована XTS-300 STOP 5.2.E (Wang Government Services).

Класс A1. Верифицированное проектирование. Данный класс систем функционально эквивалентен классу B3 в том смысле, что не требуется добавления дополнительных архитектурных особенностей или предъявления иных требований к политике безопасности. Существенное отличие состоит в том, что для гарантии корректной реализации TCB требуется наличие формальной спецификации проектирования и соответствующих методов верификации. В данном классе не зарегистрировано ни одной ОС.