НЕОБХОДИМОСТЬ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОПЕРАЦИОННЫХ СИСТЕМ НА СИСТЕМНОМ УРОВНЕ

А.В. Королькова *, Д.С. Кулябов **

(*РУДН, E-mail – akorolkova@sci.pfu.edu.ru,
**РУДН, E-mail – dharma@mx.pfu.edu.ru)

THE NECESSITY OF PROVIDING OPERATING SYSTEMS SECURITY ON A SYSTEM LAYER

A.V. Korolkova, D.S. Kulyabov

The purpose of the work is to attract attention to mandatory models of security. The insufficiency of providing system security on an application layer and the necessity to develop the ways, in which the mandatory security on a system layer is provided, are described in the work.

Любой человек, работающий в сфере информационных технологий, понимает необходимость обеспечения безопасности компьютерных систем. Но попытки обеспечения безопасности страдают от неверного предположения, что адекватная степень защиты может быть достигнута на прикладном уровне совместно с механизмами защиты, существующими в современных операционных системах. Основные усилия направлены на усиление контроля доступа и применение криптографии, что создаёт ложную уверенность в защищённости системы (например, The Next-Generation Secure Computing Base (NGSCB) [1]). Но в реальности необходимо обеспечивать защиту на системном уровне, т.е. развивать т.н. защищённые операционные системы.

Необходимость наличия встроенных средств защиты на уровне операционной системы не вызывает сомнений. Операционная система обеспечивает защиту механизмов прикладного уровня от неправильного использования, обхода или навязывания ложной информации. Если она не сможет удовлетворить этим требованиям, появятся уязвимости в масштабах всей системы.

Существует два подхода к определению мандатных и дис-

крекционных моделей безопасности. Первый базируется на определении TSEC [2] и широко распространён в литературе [3]. Он опирается на модель многоуровневой безопасности Министерства Обороны США. С нашей точки зрения, он слишком узок. Поэтому используется более общий подход [4,5,6].

Мандатной политикой безопасности будем считать любую политику, логика и присвоение атрибутов безопасности которой строго контролируются системным администратором политики безопасности (с помощью мандатной безопасности можно реализовать политики безопасности на уровне предприятия).

Дискреционной политикой безопасности будем считать любую политику, в которой обычные пользователи могут принимать участие в определении функций политики и/или присвоении атрибутов безопасности. В данном случае дискреционная безопасность не является синонимом контроля доступа, основанного на идентификаторе: IBAC (Identity Based Access Control), равно как и любая другая политика безопасности, может быть либо мандатной, либо дискреционной.

Защищенная операционная система должна предоставлять набор средств для задания мандатной политики безопасности операционной системы и перевода этих определений в форму, понятную для нижележащих механизмов обеспечения мандатной безопасности. При отсутствии подобного набора средств не может быть никакой уверенности в том, что механизмы обеспечения мандатной безопасности смогут предоставить желаемые характеристики безопасности.

Современные микроядерные исследовательские операционные системы имеют тенденцию к предоставлению примитивных механизмов защиты, которые могут быть использованы для гибкого построения архитектуры безопасности более высокого уровня. Многие из этих систем, такие как микроядро Fluke и Exokernel, используют механизм привилегий, управляемых на уровне ядра ОС, как механизмы защиты нижнего уровня. Но типичная архитектура привилегий не является адекватной для обеспечения мандатного контроля доступа с высокой степенью гибкости и гарантий. Flask, как вариант микроядра Fluke, предоставляет базовые механизмы мандатной безопасности, аналогичные DTOS, варианта

микроядра Mach; обе системы предоставляют механизмы для обеспечения мандатного разграничения доступа и поддержки мандатной политики безопасности.

Предлагается использовать систему SELinux (как наиболее предпочтительный вариант), базирующуюся на ядре Linux и системе безопасности Flask (на данный момент реализована политика безопасности TE (Type Enforcement)[7,8,9]).

Литература

[1]. Пол Инглэнд, Батлер Лэмпсон, Джон Манферделли, Маркус Пейнадо, Брайан Уиллман. *Доверительная открытая платформа*. // Открытые системы, № 07–08/2003.

[2]. DOD 5200.28-STD. Department of Defense Trusted Computer System Evaluation Criteria, December 1985.

[3]. Д.П. Зегжда, А.М. Ивашко. *Основы безопасности информационных систем*. – М.: Горячая линия – Телеком, 2000. — 452 с.

[4]. D. Ferraiolo and R. Kuhn. *Role-Based Access Control*. Proceedings of the 15th National Computer Security Conference, 1992.

[5]. Secure Computing Corporation. *DTOS General System Security and Assurability Assessment* Report, Technical report MD A904-93-C-4209 CDRL A011 June 1997.

[6]. Peter A. Loscocco, Stephen D. Smalley, Patrick A. Muckelbauer, Ruth C. Taylor, S. Jeff Turner, John F. Farrell. *Assumption of Security in Modern Computing Environments*. Proceedings of the 21st National Information Systems Security Conference, pp. 303–314, October 1998.

[7]. Lee Badger, Daniel F. Sterne, David L. Sherman, Kenneth M. Walker, Sheila A. Haghighat. *A Domain and Type Enforcement UNIX Prototype*. Proceedings of the Fifth USENIX UNIX Security Symposium. Salt Lake City, Utah, June 1995.

[8]. W.E. Boebert and R.Y. Kain, *A Practical Alternative to Hierarchical Integrity Policies.* Proceedings of the 8th National Computer Security Conference, Gaithersburg, MD, p. 18, 1985.

[9.] L. Badger, D.F. Sterne, D.L. Sherman, K.M. Walker, S.A. Haghighat, *Practical Domain and Type Enforcement for UNIX*, IEEE Symposium on Security and Privacy, Oakland CA, May 1995.