Հայաստանի Հանրապետության գիտությունների ազգային ակադեմիա
Երիտասարդ գիտաշխատողների հոդվածների ժողովածու
Национальная Академия наук Республики Армения, Сборник статей молодых научных сотрудников
National Academy of Sciences of Armenia, Collection of articles of the young researchers

Ֆիզիկամաթեմատիկական գիտություններ | Физико-математические науки | Physico-mathematical sciences
1(2), 2001
ՏՆՏԵՂԱՏԵՍԻԿԱ | ИНФОРМАТИКА | INFORMATICS

СИСТЕМА РАЗГРАНИЧЕНИЯ ДОСТУПА ДЛЯ ПОЛЬЗОВАТЕЛЕЙ НЕКОТОРЫХ РАСПРЕДЕЛЕННЫХ ПРИЛОЖЕНИЙ, ПОДКЛЮЧЕННЫХ ЧЕРЕЗ INTERNET

Авакян А.

Ереванский государственный университет

В работе рассматриваются вопросы построения систем разграничения доступа для внешних пользователей в специальных типах распределенных приложений. Приводятся расширения внутренней системы защиты (Internal Security System) для пользователей, подключенных через глобальные компьютерные сети. Рассмотрен ограниченный способ обращения внешних пользователей к ресурсам системы. Этот способ реализован в виде отдельной подсистемы External Security System, основными структурными единицами которой являются формы запросов и ответов.

Ավագյան Ա. **Internet-ի միջոցով որոշ տեղաբաշխված կիրառություններից օգտվողների արտոնությունների սահմանափակման համակարգ:** Դիտարկված է որոշ տեղաբաշխված կիրառությունների համակարգերից օգտվելու արտոնությունների սահմանափակման ներքին համակարգի ընդլայնումը գլոբալ համակարգչային ցանցերի միջոցով արտաքին օգտագործողների համար: Այն իրականացված է առանձին ենթահամակարգի ձևով, որի հիմքային օբյեկտներն են հարցման և պատասխանի շաբլոնները, որոնք և սույնով են դիմողների արտոնությունների դիֆերենցումը:

Avagyan A. **Access differentiation system for users connected through Internet in some distributed applications.** An extension of internal security system for users connected via global computer networks is considered with in a framework of specific distributed applications. Form for request and responds provided access differentiation are described.

ВВЕДЕНИЕ. В больницах в течение последнего десятилетия было установлено множество персональных компьютеров (PC), в большинстве случаев используемых как терминал [1, 2]. В немногих случаях использовалась более сложная связь между PC и информационной системой больницы (HIS – Hospital Information System), которая обычно реализовывалась посредством специализированного программного обеспечения. Вход в систему осуществлялся посредством набора пароля, что обеспечивало приемлемую защиту. Хотя в этой ситуации степень риска увеличивалась, сеть могла бы управляться достаточно хорошо и без существующих дополнительных средств [3].

В дальнейшем было разработано несколько различных типов больничных информационных систем. Связь с HIS устанавливалась главным образом для того, чтобы получить данные идентификации пациента из HIS, но иногда и для более сложного взаимодействия.

За последние годы ситуация значительно изменилась из-за удобного интерфейса и новых функций взаимодействия, бурного развития глобальных сетей, доступных массовому пользователю, средств работы с сетями и увеличения потребностей в использовании PC. Сеть диктовала требования на новые меры защиты:

- межсетевое взаимодействие может быть реализовано только при достаточных гарантиях для соответствующей защиты;
- часть локальных систем, которые могут быть связаны с центральной HIS обмена данных, не поддается контролю или ограничению;
- доступность новых систем значительно увеличивает количество пользователей и, следовательно, потребность в защищенных и эффективных средствах обмена данных с HIS;
- непосредственное использование средств PC центральной HIS более существенным способом, чем терминал.

Все эти условия также требуют новых средств защиты.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. *Источники принципов разграничения доступа.*

Как правило, права доступа к медицинским данным внутри больницы регулируются государственными нормативными актами "Правил секретности". Они основаны на большом наборе моделей, построенном Советом здравоохранения, и Законе регистрации персональных данных и Законе о Контракте лечения. Они совместимы с европейскими правилами, особенно с Соглашением 108 Совета Европы [4]. Планируется адаптация законопроектов европейских стран для соответствия недавней Директиве ЕВРОПЕЙСКОГО ЭКОНОМИЧЕСКОГО СООБЩЕСТВА о Защите данных [5]; ожидается, что это не вызовет серьезных адаптаций в локальных Правилах секретности.

Правила секретности определяют цель и контекст регистрации, тип включенных данных, права предметов данных, права доступа. Они действительны для любой зарегистрированной информации о здравоохранении в больницах: и на бумаге, и в электронной форме.

1.2. ***Правила управления разграничением доступа.***

Правила основаны на знании принципа и применяются к профессиональным работникам здравоохранения, работающим внутри больницы. Общие правила могут быть детализированы до уровня клинических отделов, которые рассматриваются как наименьший практический модуль для лечения пациента.

Доступ можно предоставлять по всем типам информационных данных о здравоохранении:

Использование персональных данных для целей исследования требует согласия пациентов.

Только по некоторым явно определенным условиям или данным возможны исключения.

1.3. ***Управление разграничением доступа.***

Вообще управление доступом в HIS основано на механизме пароля. Как правило, системы разграничения доступа требуют, чтобы пароль регулярно изменялся пользователем. Кроме регулярных проверок, всегда должны быть возможности проверки доступа для действий, выполняемых внутри HIS посредством защищенной регистрации нового пользователя на вход из терминалов.

Внутренняя сеть больниц обычно отделяется от межсетевого центра посредством используемых программных инструментальных средств Firewall [6].

2. ПОСТАНОВКА ЗАДАЧИ

В работе рассматриваются вопросы построения систем разграничения доступа для внешних пользователей в рядах специальных типов распределенных приложений, подобных виртуальной операционной для оперативных вмешательств на среднем ухе [7, 8].

Методика построения и тестирования данных систем описана в настоящем сборнике [9].

Средства и механизмы разграничения доступа для пользователей локальной больничной сети ISS описаны в настоящем сборнике [10].

В настоящей работе приводятся расширения (ISS) для пользователей, подключенных через глобальные компьютерные сети.

3. РАСШИРЕНИЕ ISS ДЛЯ ВНЕШНИХ ПОЛЬЗОВАТЕЛЕЙ

Прямое добавление внешних пользователей во внутреннюю систему защиты (ISS), путем увеличения параметров защиты, не представляется целесообразным ввиду следующего принципиального ограничения:

- внешние подключения происходят через существующие глобальные компьютерные сети и, в частности, через наиболее распространенную сеть Internet. Принципиальные трудности построения эффективных методов защиты этих сетей приводят к значительному ухудшению характеристик ISS и многочисленным возможностям ее взлома пользователями Internet [6, 11].

Поэтому нами выбран ограниченный способ обращения внешних пользователей к ресурсам системы, основанный на следующих положениях:

- внешний пользователь имеет право доступа только к информации, которая выставлена в виде формы запроса для обращения извне;
- запрос со стороны внешнего пользователя может поступить только в ответ на извещение о предоставлении такой информации;
- предоставленная информация изолирована от БД локальных пользователей;
- ответы внешних пользователей регистрируются в форме ответа на запрос и заносятся в БД только в виде добавлений, после предварительного тестирования и проверки.

Этот способ реализован в виде отдельной подсистемы External Security System (ESS), основными структурными единицами которой являются формы запросов и ответов.

Экземпляр формы формируется на основе образца (Template) формы. Многообразие образцов форм и взаимосвязанность между ними определяет естественную иерархию. Проектирование и тестирование СРД над иерархией образцов форм запросов и ответов происходит согласно общей методике построения защиты для класса функциональных ресурсов системы. Далее будет рассматриваться только проектирование СРД над экземплярами форм.

4. ФОРМА ОБМЕНА

Интерфейс взаимодействия с внешними пользователями организован в виде обмена форм запросов и ответов по инициативе внутреннего пользователя.

4.1. ***Форма запроса*** внутреннего пользователя формируется на основе специального образца запроса, по заявке внутреннего пользователя, в которой указаны:

- ID внутреннего пользователя (ID_Internal User);
- обязательные объекты для запроса;

- необязательные объекты (если есть);
- список внешних пользователей, которым будет пересылаться запрос.

4.2 ***Форма ответа на запрос.*** Образец запроса однозначно определяет образец ответа. После получения запроса и обработки информации внешний пользователь заполняет ответные поля и помещает их в очередь ответов (Answer Box). В форме ответа указаны:

- ID внешнего пользователя (ID External User);
- обязательные объекты ответа;
- необязательные объекты (если есть).

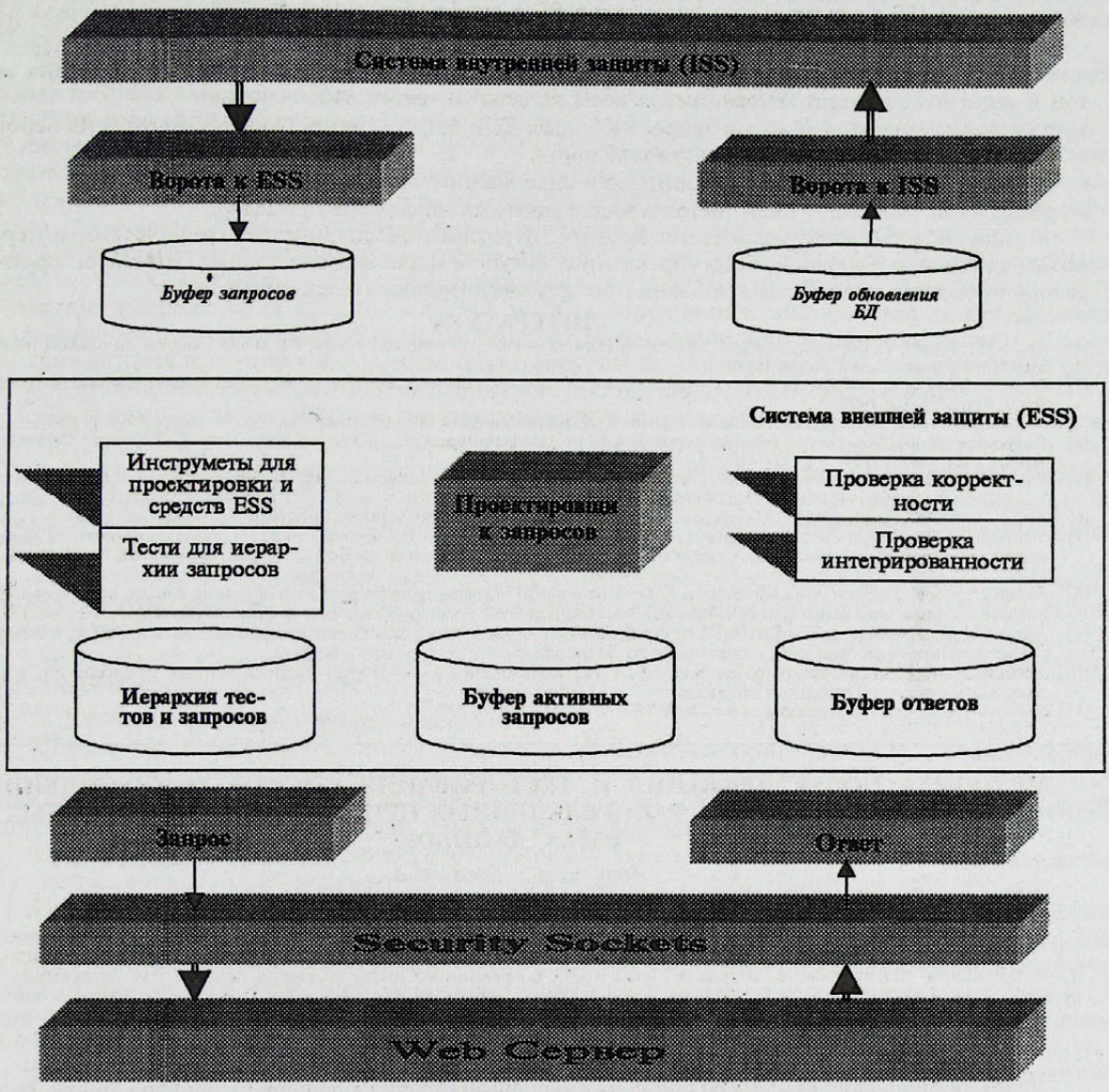

Рис. 1. Схема взаимодействия ISS с ESS.

5. МЕХАНИЗМЫ ВЗАИМОДЕЙСТВИЯ

5.1. ***Заполнение и проверка формы запроса.*** По инициативе внутреннего пользователя формируется заявка на запрос. Если пользователю разрешена пересылка всех обязательных объектов, то данные объекты копируются в отдельный буфер ESS (Buffer of Active Requests). К ним добавляются внешние связки (на Hypertext Markup Language (HTML) форме запроса), а также те имеющиеся необязательные поля, которые разрешены к пересылке.

5.2. ***Выставление информации запроса и посылка уведомления о запросе.***

Форма запроса помещается в ящик пользователя (User Box) и для уведомления о предлагаемом запросе, посылается почтовое сообщение (Mail Message) внешним пользователям (External Users).

5.3. ***Обработка запроса внешними пользователями и высылка образца ответа.*** После обработки информации запроса внешний пользователь заполняет обязательные поля образца ответа и посылает ответ в почтовый ящик ответов (Answer Box).

5.4. ***Получение и проверка ответов.*** Проверяется соответствие очередного ответа с данными образцов и тестов запроса. Результаты проверки ответа посылаются внутреннему пользователю. В случае неудовлетворения тот же вопрос помещается в User Box пользователя и посылается почтовое сообщение о результате проверки ответа.

5.5. ***Добавление ответа в БД.*** После положительного тестирования и проверки документы через шлюзы ISS автоматически заносятся в БД в виде добавления.

6. СИНТЕЗ РЕЗУЛЬТИРУЮЩЕЙ СИСТЕМЫ ЗАЩИТЫ

Результирующая система состоит из системы защиты и ActiveX элемента управления защитой и тестами. Результат генерации системы защиты и тестов, включающий:

- создание структур шаблонов запроса (Request Templet) и ответов (Answer Templet) на основе выбранных схем базовых структур шаблонов;
- создание и настройку схем алгоритмов в виде хранимых на сервере процедур;
- создание и настройку схем тестов в виде хранимых на сервере процедур.

ActiveX элементом управления защитой и тестами обеспечивается графический интерфейс пользователя для динамического управления доступом и для запуска тестов. Позволяет администратору проводить сеанс редактирования полномочий пользователей системы.

ЛИТЕРАТУРА

[1] *Kiuchi T., Sakurai T.* University Medical Information Network – Past , Present, and Future, 9th World Congress on Medical Informatics, Medinfo '98, Seoul, Korea, August 1998.

[2] *Hode T., Wattling D. and Alvarez R.* The Canadian Health Information Framework, 9th World Congress on Medical Informatics, Medinfo '98, Seoul, Korea, August 1998.

[3] *Norifusa M.* Internet security: difficulties and solutions. International Journal of Medical Informatics, Vol. 49, March, 1998, p. 69-74.

[4] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe* Convention 108, January 1981, –ISBN (1982) 92–871–0022–5.

[5] European Commission Directive 95/46/EC, On the Protection of Individuáls with Regard to: the Processing of Personal Data and on the Free Movement of such Data, OJ L281/31–50, 24 October 1995.

[6] *Ingham B. et al.* Supporting Highly Manageably Web Services" Dept. of Computer Sciences, University of Newcastle upon Tune.

[7] *Shoukourian S.K., Shukurian A.K., Avagyan A.A., Vasilyan A.M.* Designing a virtual operating room for prediction of operative interventions under some pathologies of middle ear. A case of the database, 9th World Congress on Medical Informatics, Medinfo '98, Seoul, Korea, August 1998.

[8] *Shoukourian S.K., Vasilyan A.M., Shukurian A.K.* Draft on a virtual operating room for prediction of hearing function changes and operative interventions under some pathologies of middle ear, Proceedings of the International Conference on Critical Technologies, Yerevan, 1995.

[9] *Авакян А.А., Василян А.М.* Методика проектирования и тестирования систем разграничения доступа для некоторых распределенных приложений, основанных на базах данных. – Настоящий сборник.

[10] *Василян А.М.* Система разграничения доступа для пользователей некоторых распределенных приложений, в рамках локальной сети. – Настоящий сборник.

[11] *Gundavaram Sh.* CGI–Programming on the World Wide Web. // O' Relly 1997.

МЕТОДИКА ПРОЕКТИРОВАНИЯ И ТЕСТИРОВАНИЯ СИСТЕМ РАЗГРАНИЧЕНИЯ ДОСТУПА ДЛЯ НЕКОТОРЫХ РАСПРЕДЕЛЕННЫХ ПРИЛОЖЕНИЙ, ОСНОВАННЫХ НА БАЗАХ ДАННЫХ

Авакян А., Василян А.

Ереванский государственный университет

Рассмотрена методика проектирования и тестирования систем разграничения доступа (СРД) для распределенных приложений. Методика основана на комбинации в рамках единой оболочки механизмов и инструментов разграничения доступа в СУБД и ОС, современного инструментария прикладного программирования и формальной верификации, которые обычно используются раздельно. Предложена модель и механизмы их отражения в СУБД с учетом удаленных пользователей, подключенных через глобальные компьютерные сети.

Ավագյան Ա., Վասիլյան Ա. **Տվյալների բազաների վրա հիմնված տեղաբաշխված կիրառությունների համակարգերից օգտվելու արտոնությունների սահմանափակումների ևախագծման և տեստավորման մեթոդիկան:** Դիտարկված է բաշխված կիրառությունների համակարգերից օգտվելու արտոնությունների սահմանափակման նախագծման և տեստավորման մեթոդիկան: Այն հիմնված է Օպերացիոն համակարգերի և Տվյալների Բազաների Կնկավարման Համակարգերի (ՏԲՂՀ) արտոնությունների սահմանափակումի, ինչպես նաև ժամանակակից ծրագրային միջավայրերի և ֆորմալ վերիֆիկացիայի միջոցով կոմբինացված մեկ միասնական մեխանիզմի և գործիքային բաղադրի ստեղծման վրա: Դրանք սովորաբար օգտագործվում են իրարից անջատ: Առաջարկված է համապատասխան մոդելը և ՏԲՂՀ-ի համար նրա արտապատկերման մեխանիզմները, հաշվի են առնված նաև այն օգտագործողները, որոնք միմում են գլոբալ համակարգչային ցանցի միջոցով:

Avagyan A., Vasilyan A. **Methology of designing and testing of systems for access differentiation system in distributed applications built on databases.** The paper suggests a detailed outline of a design and testing methodology for access differentiation systems (ADS) in distributed applications which use databases. The approach combines different protection mechanisms and tools in DBMS, OS and state of the art for application programming tools (object-oriented environments, system description and verification tools, SQL tools), that are usually used separately, in order to provide a practical integrated approach to the development of protection systems for specific applications with a particular emphasis on automation of design, implementation and verification. The appropriate model as well as tools for its mapping to a DMBS are suggested. Remote users connected via global computer networks are considered too.