Министерство образования и науки Республики Казахстан

Казахстанский филиал Московского государственного университета имени М.В.Ломоносова

Евразийский национальный университет имени Л.Н. Гумилева

Ассамблея народа Казахстана

Международная научная конференции студентов, магистрантов и молодых ученых

«Ломоносов – 2009»

10-11 апреля 2009 года

Конференция посвящается 15-летию инициативы Президента Республики Казахстан Н.А. Назарбаева о создании Евразийского союза

ТЕЗИСЫ ДОКЛАДОВ

I часть

Астана, 2009

УДК 378
ББК 74.58я431
Л 75

Организационный комитет

Сидорович А.В. (председатель), Берсимбаев Р.И., Бекмаганбетов К.А., Власова Г.И., Котлярова Т.Г., Коченов В.Г., Нурсултанов Е.Д., Отелбаев М., Нетесов В.В. (ответственный секретарь).

Л 75 «Ломоносов - 2009»: Международная научная конференция студентов, магистрантов и молодых ученых: Тезисы докладов Международной научной конференции: В 2-х частях. - Астана: Казахстанский филиал МГУ имени М.В.Ломоносова, 2009. – 362с.

ISBN 9965-31-234-6

В сборнике тезисов Международной научной конференции студентов, магистрантов и молодых ученых рассматриваются актуальные вопросы развития математики и информатики, экономики, языкознания и литературоведения, экологии и природопользования и молодежного сотрудничества.

Сборник представляет интерес для научных работников, преподавателей, аспирантов, магистрантов и студентов вузов.

В подготовке сборника к печати принимали участие:

Власова Г.И., Бекмаганбетов К.А., Нетесов В.В., Леонтьева С.В., Сарыбекова Л.О., Абельдинова П.Т., Блинова Г.А., Жайкенова Ж.Б.

4309000000
Л 00(05)-09

УДК 378
ББК 74.58 я431

Тексты тезисов печатаются в авторской редакции

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

функциональности за счет взаимодействия с программным обеспечением независимых поставщиков, а при необходимости и с собственными наработками пользователей;

- **интегрируемость,** то есть система должна интегрировать в единой распределенной информационной среде задачи управления **всеми аспектами деятельности** Вуза;
- **масштабируемость,** как гарантия, что не придется перестраивать систему по мере роста объема обрабатываемой информации и количества одновременно работающих пользователей;
- **переносимость**, или способность работать на различных аппаратных платформах, операционных системах, серверах баз данных;
- **адаптируемость**, то есть возможность легкой настройки на нужды конкретного университета;
- **расширяемость** – возможность наращивания функциональных возможностей системы, не выходя за рамки принятой изначально концепции развития и технологической базы, в соответствии со специфическими потребностями пользователей;
- **локализация,** то есть поддержка национальных требований и стандартов в области бухучета, финансового контроля, документооборота, организации процесса обучения, особенностей системы образования.

В этом докладе я собираюсь осветить несколько ИАСУ из стран СНГ, выделить отличительные особенности и различия, предложить на основе проведенного анализа наиболее оптимальный вариант.

Хаттамалардың дәрменсіздігі мен кеңейтілген шекті автоматты түрі

Бейбітхан Е.
Л.Н. Гумилев атындағы Еуразия ұлттық университетінің магистранты,
Yerkegul_1@mail.ru

Ақпаратты қамтамасыз ету хаттамасының дәрменсіздігі - бұл абоненттердің қолданып жатқан криптографиялық алгоритмдерінің тікелей бұзылуынсыз зиян келтіруіне себепші. Хаттаманың жұмысына және оның талаптарына кедергі келтіру үшін қасқүнемдер қолданатын шабуылдар мен амалдарының түрлері (1-сурет).

1-сурет. Ақпаратты қамтамасыз ету дәрменсіздігін пайда болу себептері

Ортада-адам. Қаскүнем екі абоненттің арасындағы ақпарат алмасу процесіне еніп алады. Ортада адам әдісінің атауы ағылшынның **man-in-the-middle (MINM)** терминінен шыққан. Бұл ашық кілтті криптографиялық алгоритмдерді қолданатын хаттамаларға тиісті.

Елес уақытын талдау. Бұл шабуылдың класын себепсіз хабарламалардаың ашылып кетуі (oracle) класының арнайы ішкі класына жатқызуға болады Кейде бұл шабуылдар ақпаратты қамтамасыз ету хаттамаларына сәтті шабуыл жасауды жүзеге асыруға жеткілікті болады. SSL/TLS [1] хаттамаларына шабуыл жасау мүмкіндігі мысал бола алады. SSL(англ. Secure Sockets Layer — Сокеттердің қорғалған деңгейі) хаттамасы [2, 3] формальді талдау әдіс көмегімен бірнеше рет талданғанын ескеру керек.

Хабарламалардың шығуы. Бұл әдіс қаскүнемнің абонентке өзінің хабарламасын қайталап жіберуіне негізделген. Шетел әдебиеттерінде осы топқа кіретін шабуылдарды **reflection** деп атайды.

Хабарламаның қайталануы. Қаскүнем бұрын хаттама орындалуы кезінде жіберілген кейбір хабарламалардың жіберілуін қайталауы мүмкін.

Себепсіз хабарламалардың ашылып кетуі. Бұл әдістің мәні қаскүнем кейбір автоматты құрылғыларды немесе абонентті белгілі бір әрекеттің тізбегін орындауға мәжбүр ететіндігі болып табылады. Шетел әдебиеттерінде мұндай құрылғылар мен абоненттерді **oracle** деп атайды.

Хаттаманың параллельді орындалуы. Формальді хаттамалар талдауы бірнеше сессияда параллельді орындалуының рұқсат етілу мүмкіндігі шешілмейтін көптеген хаттамалар типтері үшін күрделі мәселе болып қалады [4].

Математикалық амалдардың ерекшелігін қолдану. Шабуылдың бұл типі ақпаратты қамтамасыз ету хаттамаларында қолданылатын криптографиялық алгоритмдердегі нақты математикалық өзгертулерге байланысты.

Жүйе беделінің түсуі. Уақыт өте келе барлық жүйенің беделі түсетіндігін болжауға болады. Мұның себебі тек қана техникалық жұмыстың жетілмегендігі емес.

Кеңейтілген шекті автомат деп келесі объектілердің жиынтығын айтады [5] $A=(S,S_0,X,Y,O,\delta,\lambda)$, мұнда S – жағдайдың шекті бос емес жиыны; $S_0 \subset S$ - бастапқы жағдайдағы шекті бос емес жиын; X – кіріс мәніндегі шекті бос емес жиын; Y – шығыс мәніндегі шекті бос емес жиын; $O \subset X,Y$ - синхронды мәнінің бірлік жиыны; $\delta : S \times X \to S$ - өту функциясы; $\lambda : S \times X \to Y$ – шығу функциясы; Автоматтың әрбір жағдайы белгілі бір жұмыс кезеңінде ақпараттық алмасуды сипаттайды.

Әдебиет

1. Klima V, Pokoruy O, Rosa T. Attacking RSA – based Sessioris in SSL/TLS. // Presented at CHRS 2003, September 7-11, Cologne, Germany.
2. Mitchell J, Shmatikov V, Stetn U. Finite- Stale Analysis of SSL 3.0. In Proc. 7 tb USENIX Sekurity Syttrposium, pages 201-215, 1998.
3. Paulson L.C. Induelivc analysis of the Internet protocol TLS. // ACM Transactions on Information and System Sekurity, Volume 2, Issue 3, 1999, pp. 332-351.
4. Rasinowitch M, Turuant M. Protokol insecurity with finite number of session is NP-complete // fn 14 IEEE Computer Security Foundations Workshop, pp. 174-190. IEEE Computer Society, 2001.
5. Карпов Ю.Г. Теория автоматов.- СПб., 2002.

Система электронного документооборота в вузе

Галиев Д.С.
Евразийский национальный университет имени Л.Н.Гумилева
daniyar145@rambler.ru

В современном мире новые технологии поражают нас невероятными изобретениями и возможностями. Каждый новый день мы слышим и читаем, видим и пробуем средства, которые еще вчера казались нереальными. Целый мир лихорадочно изобретает новые решения для автоматизации и эффективности рабочих процессов. Повальный ряд предложений ставит нас в затруднительное положение в выборе оптимального программного обеспечения (ПО).

Моя работа посвящена разработке автоматизированной системы управления документами и данными, которая максимально отвечает требованиям современного ВУЗа.

Неоспорима важность сохранности и умелого использования информационных ресурсов для успешного ведения процесса обучения. Способность принять верное решение и вовремя отреагировать на ситуацию, гибко реагировать на все изменения