Список литератури: 1.Технологии интенсификации учебного процесса в образовательном учреждении: диссертация ... кандидата педагогических наук: 13.00.01 / Безбородова Светлана Валентиновна; [Место защиты: Нижегор. гос. архитектур.-строит. ун-т] - Нижний Новгород, 2008 - 206 с.2.*Безбородова С.В., Котляр Л.М.* Технология интенсификации учебного процесса в средней профессиональной школе в условиях модернизации образования // Фундаментальные исследования. – 2007. – № 12 – С. 352-354. 3.*Ризун Н.О.* Кибернетический поход к построению научно-инновационного многоуровневого комплекса интенсификации учебного процесса в вузе (Аспект структуризации системы) / Н.О. Різун // "Східно-Європейський журнал передових технологій", № 4/9 (52), 2011 р. – С.65-69. 4.*Ризун Н.О.* Эвристический алгоритм совершенствования технологии оценки качества тестовых заданий. "Східно-Європейський журнал передових технологій", №3/11 (45), 2010 р. – с.40-49.5.*Ризун Н.О.* Концепция построения экспертной системы поддержки принятия решений по управлению учебным процессом в ВУЗе. / Ризун Н.О // Вісник НТУ "ХПИ". Збірник наукових праць. Тематичний випуск: Інформатика і моделювання. – Харків: НТУ "ХПІ". – 2011. – № 17. – С. 135 – 142. 6.*Тараненко Ю.К., Ризун Н.О.* Спосіб проведення комп'ютерного тестування знань студентів. [Текст]: патент на корисну модель 58657 Україна: МПК G06F 7/00; Замовник та патентовласник: Тараненко Ю.К., Ризун Н.О. № u 2010 09376, заявл. 26.07.2010, опубл. 26.04.2011, Бюл. № 8, 2011 р. – 14 с. 7.*Тараненко Ю.К., Ризун Н.О.* Спосіб виміру рівня знань учнів при комп'ютерному тестуванні [Текст]: патент на корисну модель № 51559 Україна: МПК G06F 7/00; Замовник та патентовласник: Тараненко Ю.К., Ризун Н.О. № u 200913726, заявл. 28.12.2009, опубл. 26.07.2010, Бюл. № 14, 2010 р.

Поступила в редколлегию 21.076.2011

УДК 621.391

А. В.ПЕРСИКОВ, доц., ХНУРЭ, Харьков
А. С. ЕРЕМЕНКО, с.н.с, канд. техн. наук, ХНУРЭ, Харьков

СИСТЕМА ОЦЕНИВАНИЯ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ТРАФИКА NGN

В статті аналізуються недоліки сучасних систем криптографічного захисту трафіку. Розглядаються питання розробки системи оцінювання ефективності впровадження нових алгоритмів та модифікації мережевих протоколів із урахуванням параметрів, які задаються в згоді про якість обслуговування.
Ключові слова: криптографія, керування, алгоритм, трафік

В статье анализируются недостатки современных систем криптографической защиты трафика. Рассматриваются вопросы разработки системы оценивания эффективности внедрения новых алгоритмов и модификации сетевых протоколов с учетом параметров, задаваемых в соглашении о качестве обслуживания.
Ключевые слова: криптография, управление, алгоритм, трафик

In the article the shortcomings of modern cryptographic systems for the traffic security are analyzed. The issues of development assessment system efficiency of the implementation of new algorithms and modifying network protocols within the parameters defined in the agreement about the quality of service are considered.
Key words: cryptography, control, algorithm, traffic

Введение

Современные телекоммуникационные сети (ТС), такие как NGN (сеть следующего поколения, next generation network) являются распределенными системами, обеспечивающими взаимодействие множества слабосвязанных объектов, с помощью универсальной транспортной сети, способной передавать разнотипные данные с определенными параметрами качества обслуживания (КО) в соответствии с соглашением о качестве обслуживания (service level agreement, SLA) [4, 5]. Одной из базовых задач, регламентируемой стандартами построения NGN [5,6], является задача реализации функций информационной безопасности (ИБ), а, конкретно, обеспечение доверия (путем реализации взаимной сильной аутентификации [15]) и защищенного обмена данными (путем реализации конфиденциальности и целостности). Эти задачи решаются в основном криптографическими методами [6] – реализацией определенных алгоритмов преобразования данных (шифрование / расшифрование / хэширование) и процедур управления ключами (генерация, хранение, передача, согласование, депонирование, уничтожение).

Стойкость системы обеспечения ИБ эквивалентна минимальной стойкости алгоритмов, входящих в протокол защищенного обмена данными и выражается в количестве ресурсов, необходимых для подбора ключа преобразования данных. На сегодняшний день стойкость набора алгоритмов, используемых в NGN и других публичных сетях (например, набор Suite B [8]), достаточна для противодействия экстенсивному криптоанализу [14], однако, отмечая устойчивый рост вычислительной мощности компьютерных систем, вызванный улучшением технологии производства процессоров общего назначения и криптографических процессоров, а также увеличение числа элементарных вычислителей (ядер), способных к синхронной обработке данных [1], можно поставить под сомнение временные рамки использования рекомендуемых наборов алгоритмов [1] (пессимистические прогнозы – до 2015 года, оптимистические – до 2025 года). Вследствие постоянного улучшения методов криптоанализа [15], разумным является ориентация на даты, определяемые пессимистическими прогнозами.

Поскольку сети NGN являются молодым развивающимся типом сетей, использование которого прогнозируется до 2040 года [13], видится, актуальным рассмотрение проблемы замены алгоритмов криптографической защиты. Данная проблема, однако, не решается лишь разработкой алгоритмов с улучшенными характеристиками: внутренней конструкцией, распараллеливаемостью операций, увеличенной разрядностью ключа; необходимо также рассмотрение вопросов улучшения протоколов защищенного обмена данными в сети для их адаптации к передаче разнотипного трафика, характерного для NGN. Рассмотрению схемы оценивания соответствия систем криптографической защиты и посвящена данная работа.

2. Анализ особенностей современных стеков протоколов криптографической защиты в открытых сетях

Наиболее популярными стеками протоколов, обеспечивающими защищенный обмен данными в открытых сетях, таких как Интернет или другие сети на основе технологии коммутации пакетов (основа транспортной сети NGN),

являются IPsec, TLS, L2TP и PPTP (таблица 1). Реализуя функции, определенные в стеке, становится возможным формирование криптографически защищенного канала (согласования параметров и выделение ресурсов для соединения типа «точка-точка»), реализации взаимной аутентификации объектов, а также конфиденциальности и целостности данных. Процесс аутентификации для вышеобозначенных стеков протоколов строго не определяется в каждом из стеков и существует возможность свободного выбора способа, шаблона или протокола аутентификации (таблица 2).

Таблица 1.Стандарты сообщества Интернет, описывающие стеки протоколов защищенной передачи данных

Технология криптографически защищенного канала	Нормативный документ, описывающий реализацию технологии
TLS (прикладной уровень)	RFC 2716, RFC 3546, RFC 4347, RFC 5246, RFC 5878, RFC 6042, RFC 6066
IPsec (сетевой уровень)	RFC 4301-4312, RFC 4894, RFC 5386, RFC 5660, RFC 5856
PPTP (транспортный уровень)	RFC 2637
L2TP (канальный уровень, использование функций IPsec)	RFC 2661, RFC 3193, RFC 3931, RFC 5641

Все криптографические преобразования необходимо проводить в границах криптографического модуля (КМ), который должен реализовываться в соответствии со стандартом FIPS 140-2 (3) [2]. Способность КМ обрабатывать потоки данных, характерные для сети NGN [9] будет обусловлена средней скоростью выполнения преобразований на всем множестве ключей и процедурой управления ключами в распределенной системе, где присутствуют значительные временные задержки обмена данными [16].

Таблица 2.Стандарты сообщества Интернет, описывающие технологии аутентификации и контроля доступа к объектам

Технология	Нормативный документ, описывающий реализацию технологии
Аутентификация S/KEY	RFC 1760
Аутентификация в рамках протокола «точка-точка»	RFC 1334, RFC 1994, RFC 2484
Аутентификация/контроль доступа RADIUS	RFC 2138, RFC 2139, RFC 2865, RFC 2866, RFC 5090, RFC 5607
Масштабируемый контроль доступа Diameter	RFC 3588, RFC 4005, RFC 4006, RFC 4072, RFC 5224, RFC 5624
Аутентификация EAP	RFC 1748, RFC 2716, RFC 2284, RFC 3748, RFC 5247
Аутентификация и механизм мандатного доступа Kerberos	RFC 4120, RFC 4430, RFC 4537
Контроль доступа SOCKS	RFC 1928, RFC 1929, RFC 1961, RFC 3089
Аутентификация X.509	RFC 2459, RFC 2528, RFC 3647, RFC 4210,

	RFC 4211, RFC 4212, RFC 5708, RFC 6187

Эффективным с точки зрения распараллеливания алгоритмов обеспечения конфиденциальности и целостности будет использование шифрования в режиме счетчика и выработки кода аутентичности путем выполнения хэш-функции в специальном режиме (с введением в расчеты зависимости от секретной компоненты и обрезки цифрового отпечатка) [15]. Это позволит уменьшить задержку преобразования данных на сетевых элементах (в основном, пограничных маршрутизаторах [12]) за счет использования современных многоядерных и многопроцессорных систем.

Таблица 3.Основные особенности протоколов организации криптографически защищенных каналов

Протокол/характеристика	TLS	IPsec	PPTP	L2TP
Аутентификация	обязательна для реализации, но есть вариант NULL		не обязательна для реализации	
Выделенный транспортный протокол передачи управляющей информации	нет	нет	TCP	нет
Транспортный протокол	любой	любой	TCP	UDP, ATM, FR
Криптографические примитивы (управления ключами / шифрование)	асимм. / симм.	асимм. / любой	не определены	
Алгоритм шифрования	да	да	сквозная передача шифрованного трафика	
Тэг целостности	ЭЦП, MAC	MAC		
Использование произвольного механизма аутентификации	нет	да	да	да, типа CHAP
Масштабируемость системы управления ключами	да	да	нет	нет
Возможность перешифрования	нет	да	нет	нет
Буферизация данных	да	да	нет	нет
Возможность настройки дисциплины обслуживания данных	нет			
Действия при потере трафика возлагаются на	TCP	Протокол вышестоящего уровня		
Переменный объем данных для формирования тега целостности	нет			
Способ обработки данных при использовании множества алгоритмов	Многоконвейерный		Возможность отсутствует	
Обработка данных в соответствии с параметрами КО	нет, реализуется отдельным протоколом, управляющим обработкой данных			

Поддержка передачи данных в соответствии с параметрами КО	нет, реализуется отдельным протоколом, управляющим передачей данных

Анализ стандартов, описывающих стеки протоколов (таблица 3) показал, что в протоколах формирования криптозащищенного канала отсутствуют механизмы обеспечения качества обслуживания при передаче и обработке данных, что приведет к неспособности защищенной системы гарантировать соблюдение SLA. Использование специальных протоколов, направленных на реализацию концепции Traffic Engineering [7] (например, MPLS), а также специализированных дисциплин обслуживания пакетов [12], не позволит гибко настраивать систему ИБ, вследствие ориентации протоколов на процесс передачи данных, а не их обработку (а задержки в ТС и изменение характера трафика возникает именно вследствие применения криптографических преобразований, т.е. обработки данных).

Следует также отметить, что все популярные протоколы не поддерживают использование произвольной дисциплины обслуживания данных, а PPTP и L2TP также не поддерживают буферизацию данных. Эти особенности не позволяют использовать возможности современных КМ, такие как большой объем памяти для буферизации обработанных данных и приоритетная многоканальная обработка данных [15].

3. Схема оценивания эффективности внедрения новых алгоритмов

В результате анализа стандартов RFC и NIST [16], регламентирующих реализацию методов криптографической защиты в телекоммуникационных и информационных системах, была разработана и предложена следующая схема оценивания эффективности внедрения новых методов криптографической защиты (рис.).

Блок задач 1. Разработка метода управления должна быть изначально согласована с ограничениями, выдвигаемыми типом сервиса, сетью и показателями SLA x_j ($x_j^{\min} \le x_j \le x_j^{\max}$), $j = \overline{1..n}$, где n – количество рассматриваемых показателей. Подробное описание и аналитические выражения для определения показателей SLA приведены в [3], однако, вследствие разнотипности показателей, различия диапазонов значений и условий превышения/недостижимости, данные показатели должны быть

Рис. Универсальная схема оценивания эффективности

унифицированы и, внедрения новых методов криптографической защиты по возможности, нормированы. Данная процедура может быть выполнена путем шкалирования [10].

На один физический интерфейс и процессор КМ могут поступать различные виды информации [6]:

1) управляющая – например, сигнальный трафик NGN;
2) служебная – например, уведомления о статусе выполнения операций в сети;
3) криптографические ключи – информация, используемая для уникального преобразования данных;
4) трафик реального времени – медиаданные, критичные к изменению временных характеристик трафика;
5) остальной трафик – данные, не критичные к изменению временных характеристик трафика.

Блок задач 2. Определение ограничений на реализацию криптографической защиты связано с блоком 1, поскольку недопустимо одобрение алгоритма или протокола, если его действие не согласовано с набором требований системы управления, архитектурой сети и общей логической структурой протокола и физической структурой системы. В качестве основных показателей SLA относительно криптографических преобразований трафика NGN можно выбрать:

1) операционная эффективная емкость криптографического модуля;
2) накладные расходы на обработку данных;
3) накладные расходы на кодирование данных;
4) задержка обработки пакетов;
5) степень изменения временных характеристик потока данных.

Блок задач 3. Реализация метода в КМ должна отвечать требованиям стандарта FIPS 140-2 (3) и логическая архитектура обработки данных протоколом должна отвечать физической архитектуре КМ.

Блок задач 4. Оценка эффективности реализации может быть проведена путем анализа определенного агрегированного показателя. Основной проблемой данного блока является точное оценивание показателей системы вследствие их значительной корреляции. Однако чем больше физических интерфейсов имеет криптографический модуль, и чем меньше смешение типов данных, передаваемых на физический интерфейс, тем меньше степень влияния одних операций на другие. При определении истинных значений характеристик x_j необходимо стремиться к минимуму среднеквадратичной ошибки оценок данных характеристик $\hat{x}_j$: $\varepsilon^2(\hat{x}) = \sum_{i=1}^{m}\left[\sum_{j=1}^{n} h_{ij}\hat{x}_j - z_i\right] \to \min$. Здесь z_i – наблюдаемые значения характеристик, включая шумы системы, а h_{ij} – матрица обусловленности факторов. Важным моментом является то, что оценивание является косвенным, и $i > j$, т.е. возможно получение значений характеристик без раскрытия внутренней структуры криптографического модуля.

Блок задач 5. Обработка данных должна быть приоритетной в том случае, если один физический интерфейс и процессор используются для обработки ранее

обозначенных видов информации. Задачей планировщика обработки пакетов является переупорядочивание запросов на обработку данных таким образом, чтобы свести к минимуму простой процессора (фактически – минимизировать задержку обработки данных) и при этом соблюсти условие $x_j^{\min} \le x_j \le x_j^{\max}$. Современные модели приоритетного обслуживания [11] оперируют с двумя основными показателями, которые можно легко определить для криптографического преобразования: среднее и статистическая дисперсия, и на их основе формируются алгоритмы переупорядочивания запросов.

Блок задач 6. Оценка эффективности обработки данных является нетривиальной задачей вследствие того, что один КМ может одновременно обрабатывать данные различного предназначения (шифрование данных, перешифрование с целью преобразования форматов, расшифрование с целью анализа и др.). Можно пользоваться универсальным критерием эффективности – если сеть при выбранном способе обработки данных способна удовлетворить критериям SLA, формируемых множеством пользователей, тогда можно считать способ обработки приемлемым. Сложностью определения несоответствия критериям SLA является выбор некомпенсационной метрики несоответствия, где положительный эффект улучшения одних показателей (менее важных) не будет компенсировать отрицательный эффект других показателей (более важных).

Блок задач 7. Перераспределение ресурсов КМ для уменьшения несоответствия показателям SLA подразумевает:

−достижение максимальной степени использования ресурсов модуля;

−избежать конфликтов различных информационных потоков за резервирование ресурсов КМ;

−обеспечить выполнение условий обслуживания информационных потоков в режиме реального времени;

−обеспечить соблюдение условий договора с абонентом относительно параметров сервиса (соглашения об уровне услуг, SLA).

Такое перераспределение возможно лишь при согласованности возможностей сетевых протоколов и логической и физической архитектур КМ.

4. Выводы

В работе были проанализированы различные технологии организации криптографически защищенного канала, рассмотрены протоколы проведения аутентификации объектов ТС, выделены общие черты и различия при обработке стеками протоколов множества видов трафика, передаваемого в транспортной сети NGN. Было выделено, что проанализированные протоколы, ориентированы на совместную обработку различных типов данных с помощью единого процессора, однако FIPS 140-2 (3) запрещает такой способ обработки данных для конфиденциальной информации. Поэтому необходим пересмотр протоколов с целью разделения информационных потоков, что позволит протоколам быть одобренными для реализации в сетях, где циркулирует информация с ограниченным доступом и увеличить скорость системы обработки информации за счет одновременного проведения операций над множеством потоков данных.

Была предложена схема оценивания эффективности внедрения новых методов криптографической защиты в рамках существующих и разрабатываемых

протоколов обмена данными, с учетом требований, определяемых соглашением о качестве обслуживания информационных потоков. Данная схема может быть использована при тестировании соответствия криптографических алгоритмов, модулей и защищенных протоколов обмена данными и управления ключами общей идеологии информационного обмена в NGN.

Список литературы: 1.Announcing request for candidate algorithm nominations for a new cryptographic hash algorithm (SHA–3) family. Federal Register Vol. 72, No. 212, 2 Nov 2007, 2007. pp. 62212-62220. 2.FIPS-140-3 Draft security requirements for cryptographic modules. National Institute of Standards and Technology, Information Technology Laboratory, 2009, 63 p.3.*Hardy W.* Measurement and evaluation of telecommunications quality of service – John Wiley & Sons. Inc, 2001, 245 p.4.ITU-T P.564 ITU-T Recommendation P.564 (2007), Conformance testing for voice over IP transmission quality assessment models, 2007, 32 p.5.ITU-T Y.2001. Рекомендация МСЭ-Т Y.2001 (2004), Общий обзор СПП, 2004, 32 с.6.ITU-T Y.2704 ITU-T Recommendation Y.2012 (2010), Security mechanisms and procedures for NGN, 2010, 58 p. 7.RFC 3272 Awduche D. Overview and Principles of Internet Traffic Engineering, 2002. – 71 p. 8.RFC 4869 Law L. Suite B Cryptographic Suites for IPsec, 2007. – 8 p.9.Бакланов И.Г. NGN: принципы построения и организации [Текст] – М.: Эко-Трендз, 2008. – 400 с. 10.*Бешелев С.Д.* Математико-статистические методы экспертных оценок [Текст] / С.Д. Бешелев, Ф.Г. Гурвич. – М.: Статистика , 1980. – 263 с. 11.*Бронштейн О.И.*Модели приоритетного обслуживания в информационно-вычислительных системах [Текст] / О.И. Бронштейн, И.М. Духовный. М.: издательство «Наука», 1976. – 220 с.12.*Вегешна Ш.* Качество обслуживания в сетях IP [Текст] : пер. с англ. - М.: Издательский дом «Вильямс», 2003. - 368 с. 13.Исследование рынка услуг связи в России, предоставляемых на базе технологических решений [Электронный ресурс] / NGN J'son & Partners management consultancy. – Режим доступа: http://web.json.ru/markets_research/analytical_reports/detail/?report_id=3904 – 20.07.2011 г. – Загл. с экрана. 14.*Поповский В.В.* Защита информации в телекоммуникационных системах. В 2-х т. [Текст] / В.В. Поповский, А.В. Персиков. - Х.: СМИТ, 2006. 15.*Поповский В.В.* Основы криптографической защиты информации в телекоммуникационных системах. В 2-х т. [Текст] / В.В. Поповский, А.В. Персиков. - Х.: СМИТ, 2010. 16.*Столлингс В.* Криптография и защита сетей: принципы и практика. – М.: Издательский дом «Вильямс», 2001. – 672 с.

Поступила в редколлегию 17.07.2011

УДК 621.391

НАОРС И. АНАД, асп. ХНУРЭ, Харьков
Я.Т. ХУСЕЙН, асп. ХНУРЭ, Харьков

СОВЕРШЕНСТОВАНИЕ МЕХАНИЗМОВ СЛУЧАЙНОГО МНОЖЕСТВЕННОГО ДОСТУПА В СИСТЕМАХ БЕСПРОВОДНОЙ СВЯЗИ

Проведен аналіз алгоритмів множинного випадкового доступу з вирішенням конфлікту, що використовуються в системах абонентного радіодоступу і їх застосовність в типових умовах інтенсивного і нестаціонарного трафіку. Запропонована адаптивна процедура, що містить алгоритм оптимальної стохастичної оцінки і знаходжувач порогу, що сигналізує про необхідність переходу на новий алгоритм.

Проведен анализ алгоритмов множественного случайного доступа с разрешением конфликта, используемые в системах абонентного радиодоступа и их применимость в типовых условиях интенсивного и нестационарного трафика. Предложена адаптивная процедура, содержащая