работает над системой Watson Health. Эта система охватывает огромные сферы здравоохранения, которые занимаются разнообразными направлениями в медицине. Это технологии в геномной инженерии, онкологии и управлении здоровьем населения [4]. Все технологии направлены на изучение особенностей человека, ведь каждый человеческий организм уникален и реагирует на лечение и медицинские препараты по-разному. Если врачам удастся учитывать индивидуальные особенности пациентов, то лечение сложных заболеваний будет гораздо эффективнее. В этом помогают новые возможности для облегчения выполнения задач, которые направлены на обработку медицинских изображений. Система обработки изображений обладает некоторыми возможностями, такими как аналитическая оценка, обобщение данных, персонализация. Более простые функции выполняет система MedWhat, она работает как личный помощник в виде приложения для мобильного телефона со встроенной функцией распознавания речи. Приложение может отвечать на разные поставленные вопросы, а так же оно способно интересоваться самочувствием человека через различные промежутки времени. Для более точных ответов нужно указать свои данные, такие как рост, вес, возраст и медицинские характеристики.

На кафедре информационных систем и технологий развивается направление разработки интеллектуальных информационных систем, способных обрабатывать снимки компьютерной томографии и оказывать помощь специалисту в постановке диагноза на основе анализа изображений снимков и персональных данных пациентов о симптомах заболеваний.

Таким образом, сферы применения искусственного интеллекта достаточно обширны, от использования самостоятельных приложений на смартфоне пациента, которые позволяют определить диагноз «не выходя из дома», до применения программного обеспечения на основе нейронных сетей в специализированных медицинских учреждениях с точной постановкой диагноза.

1. Искусственный интеллект. Десятая национальная конференция по искусственному интеллекту // Т. 1-3. – М.: Наука, 2015. – 359 с.
2. Тьюринг А. Может ли машина мыслить // – М.: Ленанд, Едиториал УРСС, 2016. – 128 с.
3. Применение ИИ в медицине: эффективная диагностика и создание новых лекарств // Новости [Электронный ресурс]. Режим доступа: <https://aiconference.com.ua/ru/news/primenenie-iskusstvennogo-intellekta-v-meditsine-effektivnaya-diagnostics-i-sozdanie-novih-lekarstv-92604>.
4. Watson Health // Новости [Электронный ресурс]. Режим доступа: http://zdrav.expert/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:IBM_Watson_Health.

Мовсарова П.М.¹, Визирова Х.Р.¹, Бийсултанова М.А.¹, Газиева И.И.¹, Даудов И.М.²

Криптографические методы защиты информации и VPN в IP сетях

¹ФГБОУ «Грозненский государственный нефтяной технический университет имени академика М. Д. Миллионщикова»

²ФГБОУ «Чеченский государственный университет»
(Россия, Грозный)

doi: 10.18411/lj-11-2019-38

idsp: ljjournal-11-2019-38

Наше время часто называют переходным от индустриальной к информационной цивилизации. Информационные ресурсы становятся важнейшими из всех видов ресурсов, влияющими на общественный прогресс.

Стремительное развитие компьютерных сетей обеспечивает быстрый доступ к информации и эффективные способы ее передачи, но предполагает наличие адекватных мер защиты от несанкционированного доступа. Средства защиты информации превращаются в один из основных инструментов. Наличие встроенных механизмов защиты информации и эффективность их работы в прикладных системах становятся определяющими факторами при выборе потребителями оптимального решения, разработчики программных средств уделяют этим вопросам особое внимание.

Надлежащий уровень защиты может быть обеспечен с помощью криптографических методов. Первоначальной целью криптографии был перевод данных в нечитаемую форму для сохранения тайны.

Любая современная криптосистема работает по определенной методологии и использует следующие компоненты: алгоритм шифрования; ключи, используемые указанными алгоритмами шифрования; систему управления ключами; незашифрованный (открытый) текст; зашифрованный текст.

Существует два вида методологии с использованием ключей: симметричная - с применением секретного ключа и асимметричная - с открытым ключом.

При симметричной методологии используется один ключ, с помощью которого производится как шифрование, так и расшифровка посредством одного и того же алгоритма шифрования. Этот ключ передается двум участникам взаимодействия до передачи данных при соблюдении мер безопасности. К достоинствам данной системы можно отнести сравнительное быстроедействие при шифровании и расшифровке передаваемых сообщений, а к недостаткам - то, что безопасно распространять секретные ключи довольно трудно. При асимметричной методологии используются два взаимосвязанных ключа, один из которых является секретным, а другой публикуется в открытых источниках. Данные, зашифрованные одним ключом, могут быть расшифрованы только другим ключом. Главный недостаток - необходимость использования очень больших по размеру ключей для обеспечения безопасности, что негативно отражается на скорости работы алгоритмов шифрования.

Часто обе методологии комбинируются. Например, генерируется симметричный ключ, который передается с помощью алгоритмов асимметричной методологии.

К самым распространенным алгоритмам симметричной методологии можно отнести DES, 3 - DES, RS - 2, RS - 4 и RS - 6. Примеры асимметричной - RSA и ECC. Отдельную позицию занимает популярный алгоритм цифровой подписи DSA.

Многие фирмы, применяя криптографическую защиту в своих прикладных системах, пошли по пути реализации универсальных интерфейсов. В результате такого подхода разработчикам программного обеспечения нет необходимости задумываться над тем, какие именно алгоритмы криптографической защиты будут реализованы в конечном продукте — используются лишь интерфейсы вызовов функций защиты, созданных сторонними производителями. Примером может служить фирма Sun, предлагающая разработчикам программного обеспечения язык Java с широким набором интерфейсов, реализующих основные криптографические алгоритмы и протоколы.

Необходимость защиты может быть обусловлена желанием пользователя - получателя иметь возможность верификации, что дает определенные гарантии подлинности документа или кода. Для обеспечения такого рода безопасности служат цифровые подписи и сертификаты.

Программисты нередко сталкиваются с проблемой большого количества всевозможных интерфейсов в различных языках, в связи с чем появилась потребность в универсальных интерфейсах. Первоначально многие интерфейсы возникали в качестве внутрикорпоративных стандартов — таким образом появились CryptoAPI, Cryptoki,

GCS- CryptoAPI. Интерфейс CryptoAPI ориентирован на использование в ОС MS Windows NT, в то время как остальные не имеют четких ограничений. Порядок взаимодействия приложений с криптографическими модулями операционной системы регламентирует документ MS CryptoAPI. Функции, описанные в нем, поддерживаются Windows9x и Windows NT /2000/XP/. В последних ОС функции CryptoAPI содержатся в модулях `crypt32.dll` и `advapi32.dll`, но они не реализуют криптографических алгоритмов, а обращаются к другим модулям, называемым CSP. Одновременно в операционной системе можно установить несколько CSP. При первом обращении к CryptoAPI прикладная программа выбирает, с каким именно модулем CSP она будет работать в зависимости от того, какие криптографические алгоритмы ей необходимы. CryptoAPI позволяет шифровать данные, подписывать документы цифровой подписью и др. Существуют и встроенные средства, например Microsoft Base Cryptographic Provider. Имеется возможность использовать CryptoAPI в таких программах разработки, как Visual Studio, то есть автоматически осуществляется поддержка таких языков, как Visual C++, Visual Basic, Visual FoxPro и др. С развитием компанией Microsoft языковой платформы .NET большинство языков программирования, поддерживают криптографические методы защиты. Международная организация по стандартизации IETF попыталась создать единый универсальный стандарт, который был назван GSS-API.

Если в языке нет встроенных средств криптографической защиты, то существуют два варианта действий. Во-первых, можно попытаться создать их с нуля, однако это связано с реализацией сравнительно сложных алгоритмов. Во-вторых, можно использовать объектные модули, созданные на основе трансляторов с разных языков программирования, что, несомненно, более перспективно.

Для защиты информации на более низком – сетевом – уровне модели OSI используется технология VPN (Virtual Private Network). VPN предполагает использование криптографических методов защиты для обеспечения конфиденциальности и целостности информации на сетевом уровне с использованием ряда современных протоколов сетевого уровня (IPSec, PPTP, L2TP, L2P) при передаче информации по сетям общего пользования. Шифрование происходит прозрачно для пользователей программными или программно-аппаратными средствами. При этом данные всех сетевых пакетов, начиная с транспортного уровня, шифруются и помещаются в закодированном виде в область данных пакета сетевого уровня. Так образуется скрытый от посторонних «туннель», по которому информация может передаваться в сети общего доступа между узлами воображаемой, виртуальной сети. По сравнению с протоколом SSL VPN предоставляет возможность скрыть от злоумышленника такую информацию, как номера используемых портов, а при использовании механизма туннелирования -и используемые в локальной сети IP-адреса, что затрудняет возможности сканирования сети, поиска слабых мест в ней.

Существуют три основных метода подключения VPN:

- соединением двух сетей, при этом VPN обеспечивается маршрутизаторами или брандмауэрами на границе сети (рис.5.2);
- подключением узла к сети, когда программное обеспечение VPN устанавливается на клиентском компьютере, который подключается к сети;
- подключением через провайдера, когда организацию VPN на коммутируемых линиях связи берет на себя Интернет-провайдер.

Рис. 1. Соединение двух локальных сетей с помощью технологий VPN

Рассмотрим один из протоколов, посредством которого реализуется технология VPN. Стандарт IP Security - это комплект протоколов, касающихся вопросов шифрования, аутентификации и обеспечения защиты при транспортировке IP- пакетов, который должен стать частью разрабатываемого стандарта IPv6. Он включает в себя 3 основных протокола – аутентификации заголовка (Authentication Header, AH), безопасного сокрытия содержимого (Encapsulation Security Payload, ESP) и обмена ключами (Internet Key Exchange, IKE). Протокол AH обеспечивает аутентификацию отправителя пакета и целостность заголовка пакета с использованием механизмов хэширования. Протокол ESP обеспечивает проверку целостности датаграммы пакета и шифрование информации в ней. Он может работать в двух режимах: транспортном и туннельном. В транспортном режиме протокол ESP обеспечивает защиту пакетов (и данных, и заголовков) протоколов более высокого уровня, заголовок пакета IP не защищается. В туннельном режиме ESP обеспечивает связь между двумя шлюзами локальных сетей, защищая информацию в заголовке IP-пакета. В этом режиме IP- пакет полностью кодируется и помещается в область данных пакета, передаваемого между двумя шлюзами. На шлюзе принимающей стороны этот пакет распаковывается и отправляется адресату.

Протокол IKE отвечает за процедуру установки соединения, когда стороны договариваются об используемых криптоалгоритмах, обмениваются сеансовыми ключами шифрования. Протоколы стандарта IPSec используют такие криптоалгоритмы, как DES, TripleDES, AES, SHA, MD5.

Для использования VPN на практике можно использовать аппаратные шлюзы (например, CSP VPN Gate), через которые осуществляется связь с внешней сетью и которые сами реализуют все функции VPN. Для конечного пользователя более простым и дешевым решением может оказаться использование программной реализации, можно, например, воспользоваться встроенными средствами поддержки IPSec в Windows 2000/XP.

Как показывает практика, криптографические методы защиты обеспечивают безопасность на достаточно высоком уровне. Несомненно, что данное направление будет быстро развиваться с появлением новых коммуникационных аппаратно-программных средств. Большинство современных компаний стараются разработать универсальные криптографические интерфейсы и избавить разработчика программного обеспечения от самостоятельных реализаций сложных алгоритмов.

1. Введение в криптографию. Под общ. ред. В. В. Ященко. М.: МЦНМО, «ЧеРо», 2012.
2. Криптографические методы защиты в языках программирования/ В. Рудометов. - Компьютер Пресс № 3, 2013.
3. Алгоритмы шифрования. Специальный справочник – СПб.: БХВ-Петербург, 2009.