September, 10 - December, 15, 2020

Conference Proceedings

BRIDGE TO SCIENCE: RESEARCH WORKS

San Francisco, USA

LINGUISTIC BASIS OF TEACHING ORAL COMMUNICATION OF STUDENTS IN GERMAN LANGUAGE LESSONS *65*
Maxmurova Mavjuda Halimovna
LEXICAL-STYLISTIC GRADUINOMY IN UZBEK, ENGLISH, RUSSIAN *67*
Ne'matova Mohibegim Fazliddinovna
THE PEDAGOGICAL SKILL OF A MODERN TEACHER *70*
Haydarov Muzaffar O'rmonovich
GRAMMAR TRANSLATION PROBLEMS *72*
Ibragimova Madinabonu Karimovna
THE ROLE AND SIGNIFICANCE OF CONDUCTING ART IN THE SYSTEM OF MUSIC EDUCATION *74*
Maftuna Komiljonovna Alimbayeva, Madina Uzakovna Teshayeva
CONCERT GENRE INTERPRETATION PROBLEMS (IN THE EXAMPLE OF A CONCERTO BY FRANCIS POULENC FOR PIANO AND ORCHESTRA) *76*
Maftuna Komiljonovna Alimbayeva, Madina Uzakovna Teshayev
APPLICATION OF PEDAGOGICAL TECHNOLOGIES IN ENGLISH LESSONS *78*
Pulatova Shakhzoda Khaydarovna
PSYCHOLOGICAL AND PEDAGOGICAL FOUNDATIONS OF TEACHING A FOREIGN LANGUAGE *80*
Tolibova Nodira Nusratovna
PHRASEOLOGISMS OF THE ENGLISH LANGUAGE WITH PROPER NAMES *82*
Mirkhadjaeva Mahliyo Islomovna
PROBLEMS OF CORRECT SPONUNCEMENT IN TEACHING ENGLISH *84*
Bakhronova Zulfiya Ravshanovna
PROFESSIONAL COMPETENCE OF A FOREIGN LANGUAGE TEACHER *86*
Bobokulova Gulrukh Sharipovna
PHRASEOLOGICAL VARIANTS IN THE GERMAN LANGUAGE *88*
Samadova Sevar Akhatovna
ORGANIZATION OF GERMAN LANGUAGE PHRASEOLOGY TRAINING *90*
Mirzaeva Mukhayo Ruzievna
TYPES OF DICTIONARIES AND THEIR STRUCTURE *92*
Khusenova Mehriniso Uktamovna
ENCRYPTION IS A KEY ELEMENT OF INTEGRATED SECURITY *94*
Ataeva Gulsina Israilovna, Shokirov Obidzhon
THE USE OF INTEGRATED TECHNOLOGIES IN THE EDUCATIONAL PROCESS *97*
Ismoilova Mahsuma Narziqulovna, Barrayeva Sevara Shoim qizi, Samiyeva Gulshan Alisher qizi
SPREAD OF CORRUPT PRACTICIES IN THE RUSSIAN REGIONS *99*
Boris Zalivanskiy, Elena Samokhvalova
USE OF ETHNO-ARTISTIC TECHNOLOGIES IN THE WORLD ART LESSONS *102*
Julia Mikhailova
MASS ONLINE COURSES AS ONE OF THE INNOVATIVE WAYS OF LEARNING IN THE MODERN HIGHER EDUCATION SYSTEM *105*
Nadezhda Kornienko, Anastasia Miroshnikova, Elena Malyshkina
DISTANCE LEARNING FOR MEDICAL UNIVERSITY STUDENTS: PLUS AND MINUS *107*
Natalia Bratchikova
SARS-COV-2 and CARDIOVASCULAR SYSTEM *109*
Arina Vyuzhanina, Sergey Jeyranyan, Polina Plotnikov, Elena Udina
STUDY OF THE ORGANIZATION OF VOLUNTEER ACTIVITIES IN THE TERRITORY OF THE PERM KRAI DURING THE PERIOD OF COVID-19 NEW CORONAVIRAL INFECTION *112*
Vladislava Galanova
CLINICAL FEATURES OF THE COURSE OF COVID-19 IN PATIENT WITH END-STAGE OF CHRONIC KIDNEY DISEASE (CLINICAL CASE) *114*
Anastasia Gantseva, Danil Udin
ANALYSIS OF THE DEMAND AND PURCHASE OF MEDICINES DURING THE COVID 19 PANDEMIC *117*
Grebneva Marina, Maksimova Vladislava, Maria Kurilyak
ANALYSIS OF THE HEALTH STATE OF 4 COURSES STUDENT IN THE PERIOD OF DISTANCE LEARNING *120*
Nataliya Zhdanova, Elizaveta Sheveleva, Maria Kurilyak
COURSE OF NEW CORONAVIRUS INFECTION IN PERM REGION *123*
Zhelnina Angelina
HOW DOES COVID-19 PROGRESS WITH OBESITY *125*
Mariya Kanaeva, Maria Kurilyak

International Conference. September, 10 - December, 15, 2020. San Francisco, California, USA

BRIDGE TO SCIENCE: RESEARCH WORKS • Conference Proceedings

DOI: http://doi.org/10.15350/L_2/7

Research Article

ENCRYPTION IS A KEY ELEMENT OF INTEGRATED SECURITY

Ataeva Gulsina Israilovna[1]
Shokirov Obidzhon[2]

[1]Senior Lecturer, Department of Information Technologies, Bukhara State University, Uzbekistan.
[2]Student of the Physics and Mathematics Faculty, Bukhara State University,

DOI: http://doi.org/10.15350/L_2/7/39

Abstract.

The importance of encryption. Encryption is a key element of end-to-end data-centric security. End-to-end encryption ensures your data is as secure as possible, whether it's on the public or private cloud, on your device, or on the go.

Key words: codes, cipher, cryptography, encrypted traffic, data.

Мир управляется кодами и шифрами. От электронной почты до банкоматов, развлечений и покупок в Интернете - криптография присутствует в каждый момент нашего бодрствования. Фактически, жизнь, которую мы знаем, без неё была бы практически невозможна.

Криптография - это наука о секретной коммуникации. Её основная цель - обеспечить связь по незащищенному каналу таким образом, чтобы потенциальный противник не мог понять, что передаётся.

Глобальное распространение кибератак привело к тому, что один конкретный компонент криптографии - шифрование - стал критически важным в усилиях по защите конфиденциальных данных и интеллектуальной собственности (IP).

Ущерб от утечки данных. Недостаточная безопасность и нетерпеливые киберпреступники привели к тому, что количество утечек корпоративных данных растет угрожающими темпами. Ошеломляющее количество пострадавших клиентов - и финансовые потери - продолжают вызывать потрясение в деловом мире и угрожать доверию пользователей. Многие производители подключенных устройств предпочитают использовать более дешевые микросхемы, а не чипы с более высоким уровнем безопасности.

Важность шифрования. Шифрование - ключевой элемент комплексной безопасности, ориентированной на данные. Сквозное шифрование обеспечивает максимальную защиту данных независимо от того, находятся ли данные в общедоступном или частном облаке, на устройстве или в пути. Это может быть бесценным в усилиях по борьбе с продвинутыми угрозами, защите от взломов с помощью Интернета вещей и соблюдению нормативных требований. Но большое разнообразие вариантов развертывания на предприятии может пугать, и компании не используют его эффективно.

Основы. Шифрование - это процесс, основанный на математическом алгоритме (известном как шифр), который делает информацию скрытой или секретной. Незашифрованные данные называются обычным текстом; зашифрованные данные называются зашифрованным текстом. Чтобы шифрование работало, требуется код (или ключ), чтобы сделать информацию доступной для предполагаемых получателей.

Выбор того, что зашифровать. Прежде чем предприятия смогут решить, как шифровать, они должны определить, что шифровать.

Разработка программы шифрования должна быть частью общего процесса планирования управления рисками и данными. Комплексный подход, который конкретно рассматривает, какие наборы данных - структурированные или

DOI: http://doi.org/10.15350/L_2/7

неструктурированные - должны быть зашифрованы и как должно работать управление ключами, повысит эффективность и результативность IT-организации.

Не существует единого универсального стандарта для постоянного шифрования всех данных во всех системах. Успешный подход будет зависеть от чувствительности и уровня риска информации вашей организации и ее методов хранения данных. Первым шагом является понимание различных типов шифрования, а также того, что шифрование может и чего не может.

Три состояния данных. Чтобы данные были безопасными, они должны быть защищены на протяжении всего жизненного цикла. Поэтому важно учитывать состояние данных, которые вы пытаетесь защитить:

1.Данные в неактивном состоянии: в вашем хранилище или на настольных компьютерах, ноутбуках, мобильных телефонах, планшетах и Iot-устройствах.

2.Данные в движении: передаются по сети.

3.Данные в использовании: в процессе создания, обновления, стирания или просмотра.

Каждый тип данных представляет собой уникальную проблему. И у каждого могут быть разные инструменты и методологии, которые можно использовать для его защиты.

Типы шифрования для неактивных данных включают следующее:

- Полное шифрование диска (FDE) для защиты конечных точек
- Полнодисковое шифрование с предзагрузочной аутентификацией (FDE w / PBA) для защиты конечных точек
- Аппаратный модуль безопасности (HSM) для защиты жизненного цикла управления ключами
- Зашифрованная файловая система (EFS) для защиты хранилища
- Виртуальное шифрование для защиты хранилища
- Шифрование файлов и папок (FFE) для защиты неструктурированных данных
- Шифрование базы данных для защиты структурированных данных

Типы шифрования для данных в движении включают (но не ограничиваются) следующие:

- Виртуальная частная сеть (VPN) для удаленного доступа
- Защищенный доступ Wi-Fi (WPA / WPA2) для беспроводного доступа
- Уровень защищенных сокетов (SSL) для связи веб-браузера с сервером
- Secure Shell (SSH) для безопасного удаленного системного администрирования

Наиболее распространенным методом защиты данных в движении является использование виртуальной частной сети на уровне защищенных сокетов (SSL VPN). Такие технологии, как SSL VPN, имеют решающее значение для защиты от атак типа «злоумышленник в середине» и перехватчиков пакетов.

Проблема использования данных. Облачные вычисления создали потребность в защите используемых данных, поскольку сторонние поставщики все чаще размещают и обрабатывают данные. Но труднее всего защитить **используемые данные**, поскольку они почти всегда должны быть расшифрованы и, следовательно, открыты для использования. Это открывает серверы для атаки с помощью метода, называемого очисткой RAM, который проверяет память работающего веб-сервера и извлекает данные, пока они находятся в обработанном незашифрованном состоянии.

Поскольку ключи дешифрования и дешифрованные данные должны быть полностью недоступны для злоумышленника, чтобы шифрование обеспечивало безопасность, альтернативные средства управления обычно предоставляются в среде, где используются либо ключи, либо данные. Предприятиям, развертывающим облачные сервисы, следует искать распределенное решение, такое как HSM, чтобы хранить ключи в безопасности и вне контроля поставщика услуг. Компании, занимающиеся безопасностью, начинают устранять пробелы в безопасности шифрования используемых данных, вводя новые продукты, такие как «полностью гомоморфное» шифрование, которое потенциально может обеспечить неограниченный анализ зашифрованной информации, а также полное шифрование памяти, которое ограничивает открытые текстовые данные.

DOI: http://doi.org/10.15350/L_2/7

References

Adamenko M.V. - Fundamentals of classical cryptology: secrets of ciphers and codes - Publishing house "DMK Press" - 2016 – 296p.

Atayeva G.I., Raxmatova Sh. Problems of information security: electronic signature as one of the ways of protecting information // Scientific reports of Bukhara State University – 2018 – 4(1), 39-44p.

G.A. Isroilovna, L.Y. Djalolovna. Methods and algorithms of computer graphics // Scientific reports of Bukhara State University – 2020 – 4 (1), 43-47p.

Ataeva G.I., Utepbergenova G. Information Security, // SCIENTIST OF XXI CENTURY – 2017- 1 (4), 60-62p.