A importância da criptografia na segurança de dados

Universidade de Aveiro

Tiago Fernandes, Simone Pascoal

A importância da criptografia na segurança de dados

Dept. de Eletrónica, Telecomunicações e Informática
Universidade de Aveiro

Tiago Fernandes, Simone Pascoal
(120271) tiagoafernandes@ua.pt, (79319) simone.pascoal@ua.pt

25 de novembro de 2023

Resumo

A criptografia está presente em todos os sistemas informáticos e usados desde sempre. Colocar a informação de modo a que pareça ser um conjunto de caracteres aleatório é uma das melhores maneiras de proteção de dados, a encriptação é usada em trasações e comunicações seguras. Desde antes de cristo, com metodos usando papel e caneta, à segunda guerra mundial, com as comunicações entre soldados, e até agora, com metodos para enviar ficheiros com chaves publicas e mensagens digitais, a criptografia sempre foi o método mais usado para esconder dados sensiveis e cada vez mais de uma maneira mais complexa e que demora bastante tempo ou até impossivel de descodificar. Invasores podem usar a encriptação de maneira não ética, escondendo as informações de dados do dono sendo assim quase impossivel reverter o processo e os criminosos pedem uma quantia monetária para desvendarem a *key* à vitima desse ataque *ransomware*. Por tanto, a criptografia é um método bastante importante na segurança de dados, porém um sistema informático é 100 por cento eficaz com a junção de outros métodos de proteção ,senão torna-se um alvo fácil de ataques para tentar desvendar qual a chave usada para criptografar e assim facilitando os invasores a recolher dados sensiveis.

Agradecimentos

Eventuais agradecimentos. Comentar bloco caso não existam agradecimentos a fazer.

Índice

Capítulo 1

Introdução

Vivemos numa era em que a crescente **digitalização** tem proporcionado uma série de vantagens, tais como, comunicação mais rápida e acessível, fácil acesso à informação, possibilidade de teletrabalho, entre outras, mas também tem suscitado preocupações relacionadas com a segurança e privacidade dos dados sensíveis. Diariamente, uma quantidade significativa de informação, tanto de empresas como de pessoas particulares, é armazenada e partilhada digitalmente, tornando-se assim mais vulnerável à interceção por parte de terceiros mal-intencionados [1], [2].

Atualmente, são cada vez mais frequentes as ameaças cibernéticas e os casos de violação de dados, e é neste contexto que se reveste de extrema importância a utilização de tecnologias, como a criptografia, para salvaguardar a confidencialidade, autenticidade, integridade e não repúdio das informações. A decisão para a escolha deste tema foi motivada pela crescente preocupação global com a segurança da informação [1], [2].

A criptografia é uma solução que converte informações confidenciais num formato ilegível que apenas o destinatário consegue decifrar, conferindo uma proteção importante contra a pirataria informática e garantindo uma maior proteção às empresas e indivíduos. Assim, a escolha deste tema relaciona-se com a urgência de abordar a importância de preservar a segurança de dados, reconhecendo o papel da criptografia como salvaguarda contra ameaças digitais, garantindo a confidencialidade dos dados num mundo cada vez mais interconectado [1], [2].

Este trabalho está dividido em cinco capítulos.

Depois desta introdução, no Capítulo 2, são abordados os principais métodos de criptografia, focando na distinção entre criptografia simétrica e assimétrica, e apresentando alguns exemplos representativos de algoritmos em cada uma dessas técnicas. No Seção 3.2 são apresentados os resultados obtidos com estatísticas de falhas de segurança e eficácia. Depois no Capítulo 4 onde serão mostrados benefícios da criptografia e dificuldades na sua aplicação. Finalmente no Capítulo 5 onde concluimos o trabalho com apreciações finais.

Capítulo 2

Metodologia

2.1 Principais métodos de criptografia

Existem diversos métodos de criptografia, sendo notáveis a criptografia simétrica e a criptografia assimétrica.

A criptografia simétrica baseia-se no uso de uma única chave secreta, utilizada tanto para cifrar como para decifrar informações específicas. Esta técnica distingue-se não apenas pela sua rapidez, mas também pela robustez criptográfica presente em cada bit da chave. Contudo, a sua principal vulnerabilidade reside na necessidade de compartilhar a chave de forma segura [3].

A criptografia simétrica pode adotar várias abordagens, incluindo as cifras de blocos (block ciphers) e as cifras contínuas (stream ciphers). No âmbito das cifras de blocos, a criptografia realiza-se de forma repetida, encriptando conjuntos de dados (blocos) em cada ronda. Por outro lado, nas cifras contínuas, a criptografia processa-se bit a bit, originando uma sequência contínua de dados encriptados, designada por "stream" [3].

No âmbito das cifras de blocos, destaca-se o amplamente utilizado algoritmo AES (Advanced Encryption Standard), desenvolvido por Joan Daemen e Vincent Rijmen em 1998, o qual oferece suporte a chaves de 128, 192 e 256 bits. O AES encripta um bloco de dados de 128 bits que é organizado numa matriz 4x4, também conhecida por estado. A matriz de estado é sujeita a várias rondas de transformação, sendo o número de rondas determinado pelo tamanho da chave (10 para 128 bits, 12 para 192 bits e 14 para 256 bits). Após a adição inicial da chave, onde é realizada a soma entre chave da ronda e a matriz de estado, através do uso de um "ou exclusivo" (XOR), o estado passa por operações tais como, SubBytes (substituição de bytes utilizando a função não linear SBox), ShiftRows (troca da posição dos bytes de cada linha do estado, com rotações à esquerda), MixColumns (multiplicação das colunas do estado pela matriz seguinte) e AddRoundKey (XOR com a chave da ronda). A última ronda é distinta, sem operações MixColumns. A desencriptação inverte essas operações, incluindo InvSubBytes, InvShiftRows e InvMixColumns, com a última ronda

diferenciada pela ausência de InvMixColumns. Cada ronda utiliza uma rede de permutação e substituição, tornando o AES adequado para implementação em ambientes tanto de hardware quanto de software [1], [4], [5]. No contexto das cifras contínuas, o algoritmo ChaCha20, desenvolvido por Daniel J. Bernstein em 2008, destaca-se pela sua fiabilidade e velocidade superior, quando comparada ao AES em sistemas desprovidos de aceleradores de hardware [6], [7]. Ao utilizar uma chave secreta de 256 bits e um valor aleatório ou pseudo-aleatório adicional conhecido como nonce de 96 bits, o ChaCha20 gera um keystream essencial para o processo de criptografia. O nonce desempenha um papel crucial, pois não pode ser repetido após a geração de um keystream, garantindo a segurança do algoritmo contra-ataques de repetição. O ChaCha20 é capaz de gerar uma grande quantidade de matrizes 4x4 distintas, a partir da chave e do nonce, que são utilizadas para criar o keystream. Esse keystream é dividido em chaves de criptografia, cada uma com o mesmo número de bits da mensagem original. O processo de encriptação envolve uma operação XOR entre a mensagem original e a chave de criptografia, resultando na mensagem cifrada. Tanto o emissor quanto o recetor são capazes de gerar o mesmo keystream. Desta forma, o recetor, conhecendo a mesma chave secreta e nonce, pode realizar uma operação XOR entre a mensagem cifrada e a chave de criptografia, recuperando a mensagem original [7], [8].

Na criptografia assimétrica, também conhecida como criptografia de chave pública, cada utilizador detém um par de chaves: uma chave pública, divulgada publicamente, e uma chave privada, mantida em segredo. Ambas as chaves são necessárias para realizar operações, como a assinatura digital, onde os dados são encriptados com a chave privada para garantir a autenticidade do remetente. Por exemplo, um envelope digital, que inclui uma mensagem assinada pela chave pública do destinatário, atua como meio de controlo de acesso, assegurando que somente o destinatário pretendido tenha a capacidade de desencriptar a mensagem, uma vez que detém a chave privada necessária para o efeito. A criptografia assimétrica é frequentemente empregue na troca de chaves, estabelecendo a base para a utilização subsequente da criptografia simétrica na comunicação, em que uma parte gera uma chave secreta, cifra-a com a chave pública do destinatário, e este decifra-a utilizando a sua chave privada. Esta técnica de criptografia é utilizada para garantir a segurança em emails, na internet e noutros sistemas que requerem uma troca segura de chaves através da rede pública [9].

Um exemplo notável de criptografia assimétrica é a técnica conhecida como criptografia de curva elíptica. Neste método, uma função unidirecional é utilizada, baseada na aplicação de logaritmos discretos a curvas elípticas. Esta técnica oferece uma segurança por bit superior quando comparada a sistemas que utilizam logaritmos discretos ou fatorização de números primos. Adicionalmente, este algoritmo requer menos recursos computacionais devido à utilização de chaves mais curtas, tornando-se uma opção eficiente para dispositivos com baixo consumo de energia [3].

Capítulo 3

Resultados

3.1 Estatísticas de comprometimento de dados antes e após a aplicação da criptografia

Há milhares de anos atrás a criptografia era de fácil entendimento, pois eram métodos que usavam papel e caneta. No inicio do século XX, muito depois da revolução industrial, começaram por criar métodos mais complexos com máquinas mecânicas e, com o inicio da eletrônica, a complexidade aumentou para que seja impossivel desencriptar algo com papel e caneta. A criptografia mais complexa só era usada em governos e em missões militares, para a sua comunicação, por exemplo, na Segunda Guerra Mundial. Antes da aplicação de criptografia os dados estavam, significativamente, mais expostos, causando um aumento de comprometimento de dados. Depois da aplicação completa, os dados não são mostrados mesmo quando interceptados, se um *hacker* aceder aos seus ficheiros, não vai conseguir ler os dados, pois estão criptografados, e muitos outros beneficios. Por isso, a aplicação da criptografia é importante, mas tem de se combinada com outros métodos. É de salientar que cada vez mais os ataques aumentam, logo não há uma aproximação percentual da relação da criptografia com invasões.[10]

3.2 Casos de sucesso da criptografia

Como foi dito anteriormente, a criptografia é usada em muitas situações, por exemplo, antes de cristo com a cifra de César, na Segunda Guerra Mundial, Transferencia de arquivos importantes com chaves publicas, entre outros. A cifra de César foi muito usada para serem transmitidas cartas com mensagens importantes. A criptografia ajudou os soldados na Segunda Guerra Mundial, pois faziam comunicação com os soldados aliados sem que os inimigos descodificassem a mensagem [11], depois para melhorar essa comunicação e incluir ficheiros foi criado a chave publica e os protocologos para trasações financeiras e

trocas de informação sensivel. Em 2016, o FBI teve que *hackear* um iphone de um atirador de San Bernardino que matou 14 pessoas, pois para a proteção do utilizador do Iphone a Apple usa criptografia ao mais alto nivel que nem eles podem fornecer tais informações, mais tarde, a Apple processou o FBI e a equipa de invasores por ter entrado no Iphone.[12] Recentemente, nos anos 2000 e em diante, com a ascenssão das criptomoedas coma tecnologia *blockchain* permite a segurança das transações das moedas virtuais.

Capítulo 4

Análise

4.1 Benefícios da criptografia

A criptografia oferece-nos muitos beneficios, tendo em conta que os dados estão em constante movimento, seja por mensagens, transações financeiras, transações wifi e muitas outras formas de comunicação. A criptografia em conjunto com outras formas de proteção de dados, como autenticação e segurança no *backend*, pode segurar que os dados comunicados entre dispositivos ou servidores não sejam expostos.

Os pincipais beneficios da criptografia são a garantia da integridade dos dados movimentados, além de impedir terceiros mal intencionados, ainda protege para que os dados não sejam alterados, para fins de fraudes e extorsões. E o mais discutido, a proteção contra interceções de comunicação. Muitas entidades exigem criptografia forte, melhorando ainda mais os beneficios, como entidades de saúde, que usam dados pessoais sensiveis, transações de cartão de cédito e débitp e os dados de transação de varejo.[13]

4.2 Desafios enfrentados na aplicação da criptografia

A aplicação da criptografia é fundamental em segurança, porém com uso indevido pode fazer grandes estragos.

Criminosos podem aceder dados e criptografá-los para os deixar inacessivel ao dono até que o mesmo pague para saber a *key* da encriptação. Se as chaves de criptografia forem pouco eficazes, invasores podem tentar descobrir e usar a mesma chave para todos os arquivos (se as organizações usarem sempre o mesmo metodo) e assim causar um "desastre natual de compromete os servidores". Com o crescimento da computação quântica e processadores capazes de processar grandes quantidades de informações em um intervalo de tempo reduzido, a desencriptação será muito mais eficaz e por isso só com tecnicas de

criptografia quânticas é que será possivel fazer chaves mais fortes e seguras.[13] Sobre os desafios na criptografia quântica, vemos a dificuldade de a tornar pratica, pois requer a transmição de qubits que são fracos e sensiveis a interferencias, logo a longa distancia, fica bastante complicado funcionar. Para ajudar nesse processo pode ser muito dispendioso. O segundo é estabelecer confiança, pois a criptografia quântica funciona em duas partes e se alguma for interceptada, todo o distema fica comprometido. O terceiro é sobre a falta de um padrão, pois a tecnologia é recente e ainda não há experiencias necessarias para saber a melhor utilização dela.

Capítulo 5

Conclusões

Contribuições dos autores

Indicar a percentagem de contribuição de cada autor.

Tiago Fernandes (TF) , Simone Pascoal (SP) : xx%, yy%

Acrónimos

TF Tiago Fernandes

SP Simone Pascoal

Bibliografia

[1] P. Patil, P. Narayankar, N. D.G. e M. S.M., «A Comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish», *Procedia Computer Science*, vol. 78, pp. 617–624, 2016. DOI: 10.1016/j.procs.2016.02.108. URL: https://www.sciencedirect.com/science/article/pii/S1877050916001101.

[2] M. T. Gençoğlu, «Importance of Cryptography in Information Security», *IOSR Journal of Computer Engineering (IOSR-JCE)*, pp. 65–68, 2019. DOI: 10.9790/0661-2101026568. URL: https://www.researchgate.net/publication/331641251.

[3] E. Conrad, S. Misenar e J. Feldman, «Chapter 3 - Domain 3: Security engineering», em *Eleventh Hour CISSP®*, 3rd, Syngress, 2017, pp. 47–93, ISBN: 978-0-12-811248-9. DOI: 10.1016/B978-0-12-811248-9.00003-6. URL: https://www.sciencedirect.com/science/article/pii/B9780128112489000036.

[4] J. C. C. Resende, *Flexible and compact muti-algorithm cryptographic engine*, 2014. URL: https://scholar.tecnico.ulisboa.pt/records/BskD95YefV8z8ZW4In6pdy4jrKNvzjXQdhyB.

[5] R. A. M. Azevedo, *Implementação de sistemas de encriptação AES Advanced Encryption Standard em hardware para segurança*, 2013.

[6] D. J. Bernstein, «The Salsa20 family of stream ciphers», em *New stream cipher designs: The eSTREAM finalists*, M. Robshaw e O. Billet, eds. Springer Berlin Heidelberg, 2008, pp. 84–97, ISBN: 978-3-540-68351-3. DOI: 10.1007/978-3-540-68351-3_8. URL: https://doi.org/10.1007/978-3-540-68351-3_8.

[7] I. Semenov, *An implementation of ChaCha20 stream cypher in all-programmable SoCs*, 2020.

[8] P. M. Lima, C. K. P. da Silva, C. M. de Farias, L. K. Carvalho e M. V. Moreira, «Uso da cifra de fluxo ChaCha20 em redes de automação»,

[9] L. Johnson, «Chapter 11 - Security component fundamentals for assessment», em *Security controls evaluation, testing, and assessment handbook*, 2nd, Academic Press, 2020, pp. 471–536, ISBN: 978-0-12-818427-1. DOI: 10.1016/B978-0-12-818427-1.00011-2. URL: https://www.sciencedirect.com/science/article/pii/B9780128184271000112.

[10] C. Griffiths, «The Latest 2023 Cyber Crime Statistics»,

[11] nationalmuseum, «War of Secrets: Cryptology in WWII», *nationalmuseum*,

[12] A. Kharpal, «Apple vs FBI: All you need to know», *CNBC*, 2016.

[13] Google, «O que é a criptografia?»,