BOLETIM

OBSERVATÓRIO DE CIBERSEGURANÇA

OUTUBRO 2023 | nº 4/2023

DESTAQUES

Criptografia

A criptografia é um termo usado para descrever o desenvolvimento e análise de mecanismos, baseados em técnicas matemáticas, que visam garantir serviços de segurança fundamentais tais como a confidencialidade, a integridade e a autenticidade de dados (Martin, 2018). Estando na base de muitas tecnologias de segurança da informação, a criptografia é essencial para garantir a segurança das nossas comunicações e transações digitais.

Confidencialidade

A cifragem é o processo de transformar informação tornando-a ininteligível para todos exceto os que conhecerem a sua chave criptográfica. Em esquemas simétricos, o processo de cifragem e decifragem é controlado pela mesma chave privada. Em esquemas de chave pública, a informação é cifrada com uma chave pública, mas decifrada com uma chave privada. A cifragem é fundamental para a implementação do protocolo HTTPS.

Integridade

As funções *hash* criptográficas são utilizadas para garantir a integridade dos dados, tais como *software*, a inviolabilidade de provas em tribunal, assim como para a validação de *passwords* de forma segura. Sistemas de assinatura digital baseados em criptografia de chave pública são fundamentais para a segurança das relações jurídicas no ambiente digital.

PANORÂMICA

A robustez da criptografia de chave pública assenta no facto de ser computacionalmente muito difícil determinar a chave privada a partir da chave pública, nomeadamente por envolver a factorização de números muito grandes (Observatório de Cibersegurança, 2023). Contudo, esta operação torna-se mais fácil com um algoritmo de factorização quântico (Shor, 1994), pondo assim em risco a maioria dos sistemas criptográficos atuais.

Protocolo criptográfico	Tipo	Objectivo	Impacto da computação quântica
SHA-2, SHA-3	---	Funções de Hash	Requer o uso de chaves mais longas
AES	Chave simétrica	Encriptação	Requer o uso de chaves mais longas
RSA	Chave pública	Assinaturas, Geração de chaves criptográficas	Protocolo inseguro
ECDSA, ECHD (Elliptic Curve Cryptography)	Chave pública	Assinaturas, Geração de chaves criptográficas	Protocolo inseguro
DSA (Finite Field Cryptography)	Chave pública	Assinaturas, Geração de chaves criptográficas	Protocolo inseguro

Impacto esperado da computação quântica nos protocolos criptográficos atuais (Observatório de Cibersegurança, 2023)

Os esquemas de cifragem simétrica e funções *hash* criptográficas também serão afetados por este desenvolvimento tecnológico, contudo, menos (ENISA, 2021). Por exemplo, estimava-se que um adversário teria de gerar em média $2^{n/2}$ valores *hash* de n-bits (Martin, 2012) para encontrar uma colisão entre dois valores *hash*, todavia, prevê-se que os algoritmos quânticos possam reduzir este valor para $2^{n/3}$ tentativas (Brassard et al., 1997).

Com os avanços observados na computação quântica, a corrida para o desenvolvimento e standardização de protocolos de cifragem resilientes a ataques quânticos começou em 2016 (ENISA, 2021). O National Institute for Standards and Technology (NIST) já identificou quatro protocolos de cifragem pós-quânticos e espera-se que estes possam ser utilizados já em 2024.

PERSPETIVA

1 Se a criptografia é utilizada para proteger certos dados, então o controlo sobre o acesso aos mesmos recairá sobre quem controla a criptografia. Se, por um lado, a robustez dos sistemas criptográficos é essencial para garantir a segurança e privacidade das nossas interações *online*, por outro, dificulta o combate ao crime que, cada vez mais, depende de provas digitais (Conselho da União Europeia, 2020).

2 Tem-se discutido diferentes abordagens para lidar com a questão do controlo do uso da criptografia em diferentes jurisdições (Andrews, 2000). Nomeadamente, através da i) introdução de *backdoors*; ii) do controlo de exportações de sistemas criptográficos; ou iii) da retenção obrigatória de chaves criptográficas (*key escrow*) utilizadas para cifrar texto, ou do texto original antes de ser cifrado, por parte de plataformas.

3 A forma mais controversa de controlo do uso da criptografia passa pela criação de sistemas criptográficos com uma *backdoor*, isto é, pela introdução de alguma fraqueza num algoritmo criptográfico apenas conhecida por quem o desenhou e por quem controla a sua utilização (Martin, 2012). Por exemplo, o gerador de números pseudoaleatórios subjacente ao mecanismo de geração de chaves criptográficas pode ser desenhado de forma a tornar as chaves mais previsíveis (Bernstein et al, 2016).

4 No comércio internacional, os sistemas criptográficos são frequentemente regulados como bens de "duplo uso", estando por isso sujeitos ao controlo de exportações. Um dos controlos utilizados para restringir o uso da criptografia em países terceiros passa pelo estabelecimento de limites máximos ao tamanho das chaves criptográficas, tornando-as assim menos robustas (Martin, 2012; ENISA, 2016).

5 Finalmente, outro **método passa pelo** estabelecimento de regras que obriguem plataformas, que cifram dados, a armazenarem as chaves criptográficas utilizadas para produzir a cifra ou o texto original antes de ser cifrado. Soluções desta natureza têm sido discutidas no contexto da proposta para um regulamento que estabelece regras para prevenir e combater o abuso sexual de crianças (Parlamento Europeu, 2023).

6 Soluções que intencionalmente enfraqueçam sistemas de cifragem para apoiar o combate ao crime resultarão em sistemas criptográficos menos seguros e, por isso, mais propensos ao cibercrime (ENISA e EUROPOL, 2016). Outros métodos de controlo da criptografia poderão também colidir com direitos fundamentais, tendo por isso de ser exercidos sob condições de estrita necessidade e proporcionalidade (Comité Europeu para a Proteção de Dados, 2022).

PUBLICAÇÕES E NOTÍCIAS

A **ENISA**, no dia 31 de agosto, publicou o relatório *Subsea cables: What is at stake?*, sobre cabos submarinos, no qual analisa os principais desafios de cibersegurança associados a este componente crítico da infraestrutura da Internet.

O *Deucalion*, o supercomputador português mais rápido de sempre, foi inaugurado no dia 9 de setembro. Instalado na Universidade do Minho, o Deucalion é capaz de fazer 10 milhões de biliões de cálculos por segundo, vindo por isso multiplicar por dez a capacidade computacional disponível para a academia, empresas e administração pública em Portugal.

Arrancou em outubro a sexta edição do *Mês Europeu da Cibersegurança*, uma iniciativa anual organizada pela ENISA e Comissão Europeia, à qual o CNCS se associa. O mote deste ano, **#BeSmarterThanAHacker**", tem como objetivo sensibilizar os cidadãos e empresas para os comportamentos que devem adotar no que respeita à segurança *online*. Do mesmo modo, outubro é também o *Mês das Competências Digitais*, uma iniciativa do Governo que inclui mais de 40 projetos, programas e iniciativas que promovem a capacitação digital. Utilizando o mote "**#tratarodigitaportu**", esta iniciativa visa também amplificar e divulgar a oferta de capacitação digital disponível para pessoas e organizações em todo o território.

O **Gabinete Cibercrime da Procuradoria-Geral da República**, no dia 3 de outubro, divulgou uma *nota informativa* onde caracteriza e analisa as denúncias de cibercrime recebidas pelo gabinete no primeiro semestre de 2023. Os dados sugerem que a tendência de aumento do número de denúncias, iniciada em 2016, mantém-se, sendo a tipologia criminosa mais denunciada o *phishing*.

Decorreu nos dias 17 e 18 de outubro mais uma edição do *Exercício Nacional de Cibersegurança (ExNCS)*, organizado pelo CNCS em cooperação com a ENISA e com o apoio da Associação Nacional de Municípios portugueses (ANMP) e das 25 Entidades Intermunicipais Portuguesas. A edição deste ano contou com a participação de cerca de 270 municípios e teve como objetivo sensibilizar estas entidades para a cibersegurança, assim como testar a sua capacidade de resposta a incidentes.

A **ENISA**, no dia 19 de outubro, publicou o relatório *ENISA Threat Landscape 2023*, o seu relatório anual sobre o panorama das principais ameaças à cibersegurança na União Europeia. Entre as principais ameaças identificadas, este documento destaca o *ransomware*, o *malware*, a engenharia social, as ameaças aos dados, a desinformação e os ataques a cadeias de fornecimento.

CNCS Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança