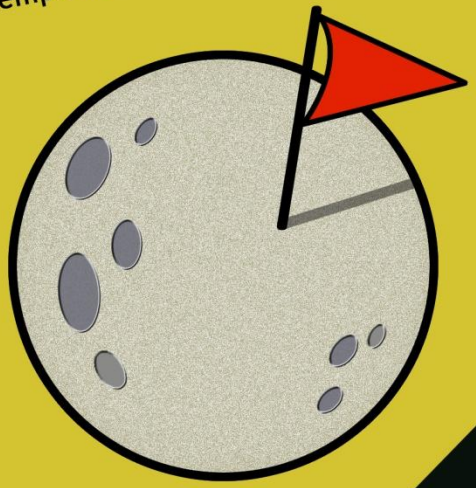
CYBERLAW by CIJIC

DIREITO: A PENSAR TECNOLOGICAMENTE

Em pleno século XXI, o ciberespaço assume-se como o novo plano da acção. Este, representa, entre outras dimensões, um conjunto cada vez mais alargado e eficiente de meios de comunicação e de informação ao serviço do Homem. A sociedade hodierna, inebriada por esta revolução tecnológica, numa quase-metamorfose híbrida, adapta-se a esta tecno-dependência. Mas, será que compreendemos, minimamente, o advento do ciberespaço e do tempo moderno em que vivemos?



CIJIC
Centro de Investigação Jurídica do Ciberespaço
da Faculdade de Direito de Lisboa

FACULDADE DE DIREITO
UNIVERSIDADE DE LISBOA

CYBERLAW by CIJIC

CYBERLAW by CIJIC Revista científica sobre *cyberlaw* | Número 01 janeiro 2016 | Grátis

DIREITO: A PENSAR TECNOLOGICAMENTE

cyber espaço
novas fronteiras

cyber ataques
algumas estratégias de mitigação

cyber segurança
preocupação global

outros
- direito constitucional do Inimigo
- obscurantismo
- DOTMLPI-I
- ENISA


CYBERLAW
by CIJIC

CYBERLAW by CIJIC

CIBERSEGURANÇA E OBSCURANTISMO

CIBERSECURITY AND OBSCURANTISM

CARLOS CALEIRO [1]

e

ANDRÉ SOUTO [2 3]

[1] Instituto Superior Técnico; SQIG – Instituto de Telecomunicações. Correio Eletrónico: ccal@math.tecnico.ulisboa.pt

[2] Instituto Superior Técnico; SQIG – Instituto de Telecomunicações. Correio Eletrónico: a.souto@math.tecnico.ulisboa.pt

[3] Pelo apoio financeiro, os autores estão gratos ao projeto FEDER/FCT PEst-OE/EEI/LA0008/2013 do Instituto de Telecomunicações. A. Souto agradece ainda à FCT a bolsa de Pós doutoramento SFRH/BPD/76231/2011.

SUMÁRIO: 1. INTRODUÇÃO; 2. O PRINCÍPIO DE *KERCKHOFFS*; 3. CRIPTOLOGIA E CIBER(IN)SEGURANÇA; 4. A VULNERABILIDADE *LOGJAM*; 5. CONCLUSÕES

RESUMO

Com a democratização das telecomunicações e tecnologias da informação, a cibersegurança tornou-se, para além de uma preocupação global, um dos alvos mais insistentes de teorias da conspiração. Na transição de séculos de obscurantismo para o carácter universal que a segurança de informação hoje detém, tornou-se inevitável o conflito entre cibercrime e cibervigilância, e direitos fundamentais como a privacidade e a liberdade de expressão. Discutimos esta tensão colocando em perspetiva desenvolvimentos recentes, em particular a vulnerabilidade *Logjam* e o seu encaixe com revelações do caso *Snowden*, concluindo que a cibersegurança deverá sair da era da obscuridade, por via da crescente literacia científica e interdisciplinar, e tornar-se num esforço que deve ser partilhado por todos.

Palavras-Chave: Cibersegurança; Criptografia; Princípio de *Kerckhoffs*; Protocolo de *Diffie-Hellman*; *Logjam*.

ABSTRACT

As a consequence of the democratic access to telecommunication and information technologies, cybersecurity has become not just a global concern but also a preferred target of conspiracy theories. Along with the transition from centuries of obscurantism to the current universality of information security issues, came an unavoidable conflict between cyber crime and surveillance, and fundamental rights like privacy and freedom of speech. We discuss this tension, putting in perspective recent developments, and in particular the recent Logjam vulnerabilities and their fit with the Snowden affair, to conclude that cybersecurity must leave the age of obscurity, through increased scientific interdisciplinary literacy, and become an effort to be shared by all.

Keywords: Cibersecurity; Cryptography; Kerckhoffs' Principle; Diffie-Hellman's Protocol; Logjam.

1.INTRODUÇÃO

Entrámos, quase sem darmos conta, na era digital. A velocidade a que os avanços tecnológicos inundam (e mudam) as nossas vidas, o tecido económico, os meios de governação, a organização política e militar dos estados, é avassaladora. Esta revolução tem um impacto bem vincado na forma como os diferentes atores se relacionam, e traz-nos para o limiar de um futuro onde a informação (e a forma como a comunicamos) é o bem mais precioso, que todos querem obter, preservar e usar em seu proveito. A cibersegurança é hoje, portanto, um tema inultrapassável, que a todos diz respeito. E se, em termos estritamente técnicos, é uma disciplina que se insere nas tecnologias de comunicação, informática, engenharia, física e matemática, a sua ubiquidade e implicações tornam-na naturalmente interdisciplinar, tocando igualmente as ciências sociais e humanas, nomeadamente a economia e o direito.

A abrangência e relevância que hoje se reconhece ao tema advêm da popularização das tecnologias de informação e comunicação, no âmbito das economias globais e abertas do final do século XX, em forte contraste com o passado. É desta rutura, nascida da conjugação dos desenvolvimentos em tecnologias de informação, do surgimento da denominada criptografia moderna, e da globalização económica, que se desenvolve (pelo menos) nas sociedades democráticas um crescente interesse científico pela cibersegurança. A segurança de informação já não é hoje um problema restrito aos estados e às organizações militares, ou à proteção de infraestruturas críticas, propriedade industrial ou fluxos de comércio internacional. A questão abrange também tudo aquilo que hoje se denomina por *internet* das coisas: o nosso automóvel, a nossa casa, os dispositivos médicos que usamos, e uma crescente quantidade de outras dimensões das nossas vidas, para além do nosso computador pessoal ou telemóvel.

No entanto, o caminho da luz nesta área de fulcral importância está ainda no seu início. A era moderna da criptografia nasce apenas no final do século XX com o trabalho seminal de *Whitfield Diffie* e *Martin Hellman* [1], que passa a possibilitar o acordo secreto de chaves criptográficas à distância e em canais de comunicação públicos. É este avanço que permite a explosão do ciberespaço, em frente de onda com a globalização das redes de comunicação e a popularização dos computadores. Os já conhecidos resultados matemáticos de *Claude Shannon* [2] sobre a

(im)possibilidade de segurança perfeita são o ingrediente final que nos traz à formulação de cibersegurança que hoje conhecemos.

Após séculos de permanência dos assuntos da segurança de informação na esfera militar e securitária, é natural que surjam conflitos com direitos fundamentais, como a privacidade e a liberdade de expressão, seja por ausência ou fraca regulamentação, excesso de zelo ou outras razões menos claras. Fenómenos como a cibervigilância, particularmente exacerbados na sequência dos atentados terroristas de Nova Iorque, EUA em Setembro de 2001 (uma discussão que se reavivou na sequência dos recentes atos terroristas de Paris, França em Novembro de 2015), ou o combate ao cibercrime, acabam inevitavelmente por conduzir a abusos, ou pelo menos a teorias da conspiração, a que casos como o de *Edward Snowden* [3] dão eco e expressão.

Em Maio deste ano, um coletivo de 14 cientistas de institutos de investigação e universidades francesas e norte-americanas descobriu e divulgou uma vulnerabilidade bastante preocupante, a que chamaram *Logjam* [4], com o potencial de comprometer uma larga percentagem das comunicações e servidores a nível mundial [5]. Este ataque coloca em causa a segurança de um dos componentes mais fundamentais da criptografia moderna - o protocolo de acordo de chaves de *Diffie-Hellman*. O ataque não determina fraquezas na matemática subjacente (tanto quanto se sabe, impoluta), mas explora uma conjugação de defeitos na sua implementação e utilização por parte dos protocolos criptográficos mais comuns. É hoje considerado (fortemente) plausível que esta vulnerabilidade fosse conhecida e explorada durante anos, pelo menos pela agência norte-americana de segurança (NSA) num seu programa de cibervigilância de massas. Claro que a emergência destes factos retira credibilidade às entidades envolvidas, para além de suscitar fundadas dúvidas sobre a eficácia da estratégia utilizada. Conhecer uma vulnerabilidade (séria) e optar, intencionalmente, por explorá-la, ao invés de a divulgar e mitigar, abre um perigoso caminho que pode permitir a exploração da mesma vulnerabilidade por terceiros, desde que bem equipados, mas quiçá pior intencionados.

Para além de vários outros casos pouco exemplares há também, felizmente, uma miríade de exemplos recentes que trazem à evidência as vantagens da clarificação. A discussão científica aprofundada e alargada destas matérias, no seio das sociedades ocidentais modernas, terá forçosamente de nos conduzir, por via da literacia sobre o ciberespaço, a um contexto onde, na ausência de soluções perfeitas, todos sejamos

abertamente corresponsáveis e ciberconscientes. Neste artigo, usaremos a descoberta da vulnerabilidade Logjam, na sua dimensão técnica e no seu impacto político, como paradigma das boas práticas a que, julgamos, estaremos inevitavelmente condenados, em defesa de um Princípio de *Kerckhoffs* generalizado (Kerckhoffs, 1883).

O artigo está estruturado da seguinte forma: na Secção 2 abordaremos, em perspetiva histórica, o conflito entre obscurantismo científico e segurança de informação, com ênfase nos bons exemplos recentes de aplicação do Princípio de Kerckhoffs; na Secção 3 daremos uma panorâmica da importância da criptologia em cibersegurança, enquadrando a sua relevância para a vulnerabilidade Logjam recentemente descoberta; consubstanciando o carácter técnico desta vulnerabilidade, a Secção 4 analisará a forma como uma conjugação de fraquezas (infeliz, ou talvez intencional) contribuiu para a vulnerabilidade em questão, bem como o papel fundamental da investigação científica na sua descoberta e mitigação; concluiremos, na Secção 5, defendendo o progresso científico, a ciberliteracia e a responsabilidade partilhada como pilares fundamentais da cibersegurança do futuro.

2.O PRINCÍPIO DE KERCKHOFFS

Sendo verdade que a comunicação de informação confidencial não é um exclusivo dos nossos dias, havendo exemplos conhecidos no antigo Egito com cerca de 4000 anos, é inegável que até à emergência da era digital nas últimas décadas do século XX se tratou de uma questão "apenas" relevante em contextos militares ou de soberania (e a partir do fim do século XIX também de algumas, poucas, grandes indústrias). Até há pouco mais de 50 anos atrás podemos afirmar que se vivia, globalmente, em regime de total obscurantismo no que diz respeito à segurança de informação, cujas técnicas eram do conhecimento quase exclusivo de algumas elites. Se a princípio a segurança de informação se sustentava no analfabetismo da maioria das populações, mais tarde passou a suportar-se na suposta dificuldade do comum mortal em executar corretamente operações matemáticas relativamente simples, e no obscurantismo que rodeava as técnicas utilizadas, conhecidas apenas dos iniciados. No entanto, a História foi-nos ensinando a olhar para estas questões com mais seriedade (ver por exemplo [7]).

A melhor forma de conceber sistemas criptográficos seguros era já objeto de discussão no final do século XIX, nomeadamente nos trabalhos do linguista e criptógrafo holandês Auguste Kerckhoffs [6]. Precursor da análise de boas práticas para a construção de sistemas criptográficos seguros, válidas até hoje, Kerckhoffs afirmou que a segurança dos mesmos não deve ser baseada no obscurantismo e portanto no desconhecimento das técnicas de cifra utilizadas. Em contraponto, e numa perspetiva completamente contrária, propôs que um sistema deverá ser seguro mesmo que o adversário conheça tudo sobre ele, incluindo as técnicas, o processo de cifra e até mesmo o próprio criptograma, isto é, a mensagem cifrada, ficando apenas incógnita a chave usada para cifrar.

Hoje conhecido como Princípio de Kerckhoffs, esta proposta é comummente considerada como a negação de todas as abordagens à segurança por obscuridade. Isto não significa que princípios menos transparentes de segurança de informação por obscuridade não continuem a ser usados até hoje, nem mesmo que essas abordagens sejam necessariamente menos seguras, mas a prática demonstra que há uma marcada distinção, em termos de qualidade da segurança de informação, quando os métodos propostos são publicamente discutidos, analisados e validados, e todos os detalhes de desenho dos sistemas são cuidadosamente justificados e verificados. Apesar desta evidência, ou talvez contribuindo ainda mais para salientar a sua importância, há diversos episódios relevantes que vale a pena recordar.

O papel crucial que a criptografia e a capacidade de criptanálise desempenharam no desenlace da II Guerra Mundial (ver [8] e [9]), bem como o contexto de guerra fria que se lhe seguiu, contribuíram de forma vincada para a obscuridade do tema. A criptografia foi classificada como arma de guerra pelos EUA e, a partir de 1949, a livre circulação de sistemas criptográficos foi regulada internacionalmente pelos países da OTAN ao abrigo do *Coordinating Committee for Multilateral Export Controls* (CoCom) [10].

É neste contexto que se dá a popularização das telecomunicações e tecnologias de informação, a partir da década de 1970 e no último estertor da guerra fria, no âmbito de economias globais e abertas em forte contraste com o passado. É desta rutura, nascida da conjugação dos desenvolvimentos em tecnologias de informação, do surgimento da denominada criptografia moderna e da globalização económica que se desenvolve (pelo menos) nas sociedades democráticas um crescente interesse

científico pela cibersegurança. A segurança de informação deixara de ser um problema restrito aos estados e organizações militares, ou à proteção de infraestruturas críticas e propriedade industrial, passando a abranger uma fatia muito significativa da economia mundial e da vida de todos nós.

Em 1991 dá-se um caso particularmente revelador do clima securitário que envolvia (e sempre envolverá) a segurança de informação, mas também de como a luz começava a raiar. *Phil Zimmermann*, informático norte-americano, decide disponibilizar publicamente um conjunto de implementações de sistemas criptográficos que pudessem ser utilizados pelo utilizador comum, que denominou de *Pretty Good Privacy* (PGP) [11]. Os seus programas rapidamente extravasaram as fronteiras territoriais dos EUA e *Zimmermann* acabou por ser acusado de traição. O processo foi arquivado em 1996, talvez por ser impossível conter o inevitável, e o PGP ainda hoje está disponível para quem o quiser usar [12].

Tendo ficado obsoleto por ser demasiado restritivo, na sequência do caso PGP e dado o fim da guerra fria, o controlo de importação/exportação de métodos criptográficos é hoje regulado internacionalmente pelo *Wassenaar Arrangement* [13], que substitui o CoCom a partir de 1996. Ainda assim é bom salientar, até por ser relevante para o que se segue, que praticamente até ao início do século XXI, todos os sistemas informáticos exportados pelos EUA comportavam criptografia propositadamente enfraquecida, de acordo com as normas então vigentes.

Dois organismos norte-americanos desempenham até hoje um papel particularmente importante, pela sua liderança nesta área: a *National Security Agency* (NSA), e o *National Bureau of Standards* (NBS) hoje denominado *National Institute for Standards and Technology* (NIST). É pela pressão crescente da necessidade global de dispor de sistemas de cifra robustos que é certificado pelo NBS em 1977 o *Data Encryption Standard* (DES) (National Institute of Standards and Technology, 1977), o primeiro *standard* de criptografia dita simétrica. Construído sob a custódia da NSA, o DES foi sempre severamente criticado por haver diversos elementos obscuros no seu desenho, nunca devidamente explicados, que foram dando azo a diversas teorias da conspiração sobre a possibilidade de o sistema conter vulnerabilidades não divulgadas que a NSA poderia explorar. Apesar disso, o DES foi usado intensivamente em todo o mundo, sem problemas de maior, até ser substituído por um novo *standard* em 2001. Pode até dizer-se que o escrutínio do DES ela comunidade científica desempenhou

um papel crucial nos avanços na ciência da cibersegurança das últimas décadas. Curiosamente, ou talvez como concessão inevitável ao Princípio de *Kerckhoffs*, o processo de seleção pelo NIST do novo *standard*, a cifra *Advanced Encryption Standard* (AES) [15], foi absolutamente distinto, exemplarmente aberto e profundamente escrutinado. Em 1997 realizou-se uma chamada internacional para apresentação de propostas, que foram sendo discutidas, debatidas, analisadas e escrutinadas pela comunidade internacional, ao longo de quatro anos, até ser finalmente escolhido um vencedor: a cifra *Rijndael* proposta por dois cientistas belgas. O processo repetiu-se, em 2015, para a seleção do novo *standard Secure Hash Algorithm* (SHA-3) [16], uma função de dispersão utilizada, por exemplo, em sistemas de assinatura digital.

Apesar dos bons exemplos citados e de outros, os problemas de cibersegurança não deixaram de existir, nem os princípios obscurantistas foram eliminados definitivamente, e as teorias da conspiração não pararam de crescer. Em 2013, na sequência da revelação de inúmeros segredos da NSA pelo seu ex-funcionário *Edward Snowden* [3], tornou-se público que os EUA tinham ativo um programa de cibervigilância de massas que lhes permitia analisar comunicações cifradas (quase todas, hoje em dia, mesmo que não tenhamos consciência disso). Esta perspetiva deu azo a todo o tipo de especulações sobre os mecanismos que poderiam estar a ser usados, e que iam desde a ficção científica à mistificação, passando também por algumas possibilidades mais sérias, envolvendo a inclusão de potenciais portas de escuta (*backdoors*) em *software* e *hardware* comercial de uso generalizado, ou a exploração de avanços não divulgados na matemática das cifras, ou mesmo da concepção em segredo de computadores quânticos. Finalmente, o artigo que divulga a vulnerabilidade Logjam [4, 5] vem trazer luz a esta questão, numa articulação engenhosa de pequenas vulnerabilidades que estão perfeitamente em linha com as capacidades da NSA, e que discutiremos de seguida.

3.CRIPTOLOGIA E CIBER(IN)SEGURANÇA

A vulnerabilidade *LogJam* enquadra-se num tipo de ataque muito sério à privacidade das comunicações. Nomeadamente, a vulnerabilidade permite violar a

segurança de uma das peças mais fundamentais da cibersegurança moderna: o protocolo de acordo de chaves de *Diffie-Hellman*. O referido protocolo permite o estabelecimento de uma comunicação privada via *internet* entre duas partes, sendo utilizado massivamente em quase todos os sistemas de comunicação que necessitem de qualquer tipo de privacidade. É através dele que as partes acordam uma chave secreta que usarão daí em diante em comunicações cifradas/privadas entre si. Sem ele, a menos que as partes se encontrem previamente, não é possível, na prática, estabelecer ligações privadas. A ideia de *Diffie* e *Hellman* está presente em quase todos os protocolos de comunicação segura, incluindo TLS, HTTPS, SSH, IPSec, SMTPS ou IKE, utilizados para estabelecer ligações remotas entre servidores e clientes, redes VPN, ou servidores de correio electrónico IMAP e POP [5]. A confiança que é depositada na segurança do protocolo de Diffie-Hellman é sustentada na firme opinião dos especialistas, que consideram estarmos cientificamente ainda muito longe de sabermos resolver eficientemente o problema do logaritmo discreto, em que o protocolo se baseia. Ou seja, a criptanálise eficiente do problema do logaritmo discreto está bastante para além do alcance do conhecimento matemático atual.

O problema do logaritmo discreto é um dos mais populares exemplos daquilo que, na criptografia moderna, se acredita ser uma função de sentido único. A designação provém do facto de, dado um valor (mensagem), ser computacionalmente simples calcular o valor da sua imagem (cifra), mas ser computacionalmente difícil inverter o processo (criptanálise) sem conhecimento adicional (sobre a chave utilizada na cifra). De acordo com a moderna teoria da complexidade computacional, isto não invalida a possibilidade de fazer criptanálise do sistema, mas implica que não possa ser feita em tempo útil para parâmetros de segurança suficientemente grandes (tamanho das chaves). Intuitivamente, uma função de sentido único pode ser comparada a uma construção Lego. Na verdade, dada uma construção já pronta, determinar o conjunto de peças que lhe deu origem é fácil (basta desmontar a construção). Contudo, dadas as peças, refazer a construção pode ser muito trabalhoso.

Para melhor compreender o protocolo de *Diffie-Hellman* é útil entender melhor o problema do logaritmo discreto: dado um número que sabemos ser uma potência

(módulo um número primo[1]) de uma certa base, determinar qual o expoente. Trata-se de um problema matemático, do domínio da álgebra e teoria de números (vide o texto introdutório [17]).

Os números inteiros (positivos e negativos) podem ser somados entre si, a operação de soma tem elemento neutro (0), e cada número inteiro *a* tem um elemento simétrico -*a* (que somado consigo dá resultado 0). Por esta razão, a estrutura $(\mathbb{Z}, +)$ é denominada um grupo, neste caso infinito. O problema do logaritmo discreto põe-se sobre estruturas de grupo muito semelhantes a esta, mas finitas. Nomeadamente, usa-se aritmética módulo um número positivo fixo n. Consideram-se apenas os valores $0, \dots, n-1$ e a operação de soma é tomada subtraindo n ao resultado, várias vezes se necessário, caso seja maior que $n-1$. Por exemplo, em aritmética módulo $n = 12$ (como nos usuais relógios de ponteiros) tem-se que $10 + 5 = 15 - 12 = 3$. Isto não é surpreendente se pensarmos que se começarmos a ler um livro às 10h da manhã e demorarmos 5h a lê-lo, irão ser 3h da tarde no relógio (15h, na verdade) quando terminarmos.

Outra operação aritmética usual que podemos considerar é a multiplicação. Por exemplo, de novo em aritmética módulo $n = 12$ tem-se que $4 \times 7 = 4$. Podendo parecer estranho, a verdade é que $4 \times 7 = 7 + 7 + 7 + 7 - 12 - 12 = 28 - 24 = 4$. Quando n é um número primo estas estruturas ganham propriedades ainda mais interessantes e $(\mathbb{Z}_n^*, \times)$, que consiste do conjunto de todos os números $1, \dots, n-1$ (excluímos 0) com a operação de multiplicação, torna-se também num grupo (convidamos o leitor a tentar perceber porquê). Mais ainda, estes grupos dizem-se cíclicos pois é possível percorrer todos os seus elementos calculando potências sucessivas de um elemento especial g a que se dá o nome de gerador. Não podemos considerar agora $n = 12$, pois não se trata de um número primo, mas tomando por exemplo $n = 7$, tem-se que $g = 3$ é gerador pois calculando potências sucessivas de 3, módulo 7, obtém-se $3^1 = 3,\ 3^2 = 2,\ 3^3 = 6, 3^4 = 4, 3^5 = 5,\ 3^6 = 1$, sequência que se repetirá se continuarmos o processo.

Podemos agora formular rigorosamente o problema do logaritmo discreto: conhecidos um número primo p e um elemento gerador g, determinar para um número A o valor a do expoente que satisfaz $A = g^a$ em aritmética módulo p. De

[1] Um número diz-se primo se os únicos números que o dividem (exatamente) o número 1 e o próprio número.

facto, este problema parece relativamente simples para $n = 7$, mas a verdade é que não se conhece nenhum método eficiente para calcular o expoente pretendido quando o número primo p considerado é suficientemente grande. O melhor método conhecido para resolver o problema é o denominado *index calculus*, que emana do importante algoritmo de factorização conhecido por *number field sieve* (NFS), um crivo algébrico que executa um número de passos exponencial no tamanho do número primo p considerado, da ordem de $exp\left(\left(2 + o(1)\right)(\log p)^{\frac{1}{3}}(\log\log p)^{\frac{2}{3}}\right)$. O leitor interessado poderá aprofundar os detalhes em [18] ou [19].

É agora simples explicar o protocolo de acordo de chaves de *Diffie-Hellman*. Após a escolha e publicação de um número primo p muito grande (na prática, o leitor pode pensar em p com sendo um número com centenas algarismos) e de um gerador g (de gerador), cada uma das partes, usualmente denominadas de *Alice* e *Bob*, escolhe secretamente um expoente, de entre os números $2, \dots, p - 2$. Após ter escolhido o seu expoente a, a *Alice* calcula $A = g^a$ em aritmética módulo p, e envia o valor A para o *Bob*. Simultânea e simetricamente, o *Bob* escolhe o seu expoente b, calcula $B = g^b$ em aritmética módulo p, e envia o valor B para a *Alice*. Depois desta troca de mensagens, em canais públicos, ambos calculam a chave partilhada $K = A^b = B^a = g^{a \times b}$ que podem de seguida utilizar para cifrar as comunicações entre ambos. Um atacante à escuta terá acesso, sem dificuldade, aos valores de p e g, para além de A e B, mas isso não lhe dá nenhuma vantagem óbvia para o cálculo da chave K. Para tal, o melhor método conhecido consiste em calcular o logaritmo discreto de uma das mensagens, por exemplo A, obtendo a e permitindo-lhe então calcular $K = B^a$, tal como a *Alice* faria.

Neste ponto, revista a matemática subjacente ao protocolo de *Diffie-Hellman* e reafirmada a sua resistência à criptanálise, parece ser extraordinariamente difícil de imaginar em que poderá consistir a vulnerabilidade *Logjam*. É o que veremos de seguida.

4.A VULNERABILIDADE *LOGJAM*

Muito pouco se sabe acerca do verdadeiro conhecimento e poder computacional e intelectual das agências de segurança das grandes potências mundiais, com destaque para a NSA. *Quantos colaboradores tem? Quanto dinheiro investe? Que tecnologias possui?* As respostas a estas perguntas são certamente alguns dos segredos mais bem guardados do mundo, e abundam as teorias da conspiração, algumas decerto com fundamento. No que diz respeito à vulnerabilidade Logjam, em particular, que tipo de abordagem poderá estar por detrás da plausível capacidade para escutar, massivamente, comunicações cifradas com chaves acordadas usando o protocolo de *Diffie-Hellman*?

A resposta não é assim tão difícil de enquadrar. A cibersegurança está assente, para além do fator humano, que nunca é desprezável, em três pilares técnicos essenciais: a matemática da criptanálise, a correção dos protocolos de comunicação que usam as cifras e a boa implementação dessas funcionalidades. Assim sendo, naturalmente, há outras dimensões relevantes a ter em conta. Na verdade, a vulnerabilidade *Logjam* é uma conjugação de deficiências (propositadas ou negligenciadas) quer no desenho lógico dos protocolos de comunicação, quer na implementação das primitivas criptográficas.

Como vimos antes, todo o material criptográfico exportado pelos EUA até ao virar do milénio estava confinado, por lei, a utilizar parâmetros de segurança inseguros (*export grade*, como eram designados). Quase todos os sistemas mais populares exportados usavam, portanto, chaves criptográficas suficientemente pequenas para serem atacadas com a tecnologia de então (e muito mais facilmente com a tecnologia de que dispomos hoje) e, em particular, executavam o protocolo de *Diffie-Hellman* com números primos que não excediam 512 bits (cerca de 150 algarismos). Pode parecer muito (e é, num certo sentido), mas o que os investigadores que descobriram e divulgaram a vulnerabilidade Logjam mostraram é que, na prática e com investimento moderado em tecnologia, é possível resolver o problema do logaritmo discreto para números primos deste calibre em menos de uma semana. Não é demasiado reconfortante, mas ainda assim, tendo em conta os biliões de comunicações que necessitariam de passar por este método de análise, e o facto de pelo padrões aceites hoje se aconselhar a utilização de números primos com pelo

menos 1024 bits (o dobro do tamanho dos anteriores), parece ser um detalhe relativamente inócuo.

É neste ponto que temos de considerar os outros dois contributos decisivos para a vulnerabilidade *Logjam*. Comecemos pelo desenho de várias versões dos protocolos de comunicação, TLS, HTTPS, SSH, IPSec e outros, que utilizam acordo de chaves *à la Diffie-Hellman*. Ao estabelecer contacto entre duas entidades, os protocolos procuram antes de mais acordar quais os algoritmos criptográficos e parâmetros de segurança que vão utilizar. Basicamente, cada máquina envia à outra a lista de algoritmos e parâmetros de segurança que suporta, sendo escolhida por ambos a melhor possibilidade da lista fornecida pelo outro e que o próprio suporta. Sendo uma fase considerada não-crítica, esta fase dos protocolos não é cifrada, o que a torna vulnerável a um simples ataque de *man-in-the-middle*. O atacante intromete-se na comunicação e convence ambos os servidores a utilizar parâmetros de segurança *export grade*, que quase todos os sistemas ainda suportam por uma questão de compatibilidade com o passado e com sistemas mais antigos (infelizmente ainda em uso). Este erro lógico no desenho dos protocolos permite assim que um ataque ao problema do logaritmo discreto possa ser posto em prática, como vimos acima, mas com consequências muito pouco relevantes.

No entanto, há outro ingrediente decisivo para a vulnerabilidade se tornar efetiva que tem a ver com o descuido com que são implementadas as funções criptográficas em muitos sistemas. Como vimos, o protocolo de *Diffie-Hellman* começa por estabelecer, publicamente, um número primo p e um gerador g. Não pretendemos discutir o assunto neste texto, mas existem métodos razoavelmente eficientes para construir números primos grandes de forma aleatória (vide [19]). Ainda assim, por ignorância, negligência, descuido, ou simplesmente por questões de eficiência, muitos sistemas simplificam o problema e utilizam sistematicamente um único número primo p, pré-estabelecido ou normalizado, ou um pequeno conjunto de números primos. Aqui entra o último contributo fundamental dos investigadores que descobriram a vulnerabilidade *Logjam*: ao determinar o logaritmo discreto de A relativamente ao gerador g módulo p, o algoritmo subjacente ao *index calculus* consiste essencialmente na inferência de uma quantidade considerável de relações relevantes, que não dependem do valor A, no fim da qual o expoente a pode ser rapidamente calculado.

Desta forma, tendo conhecimento dos poucos números primos de 512 bits usados por uma percentagem assustadoramente grande dos sistemas a nível mundial, os investigadores usaram esta estratégia para pré-calcular toda a informação relevante para, conhecido o valor de A poderem calcular rapidamente a e atacar inelutavelmente a comunicação em tempo real. De notar que mesmo no caso em que as chaves usadas são de 1024 ou 2048 bits (e portanto fora do alcance do ataque proposto), se o conjunto de primos utilizados for pequeno a tarefa de pesquisa é ainda realizável dispondo de recursos computacionais adequados.

Sendo verdade que a conjugação de todos estes elementos é extremamente engenhosa, é certo que agências como a NSA têm certamente o *know-how* para as reconhecer e explorar. Mais, a coincidência de todas estas dimensões não será completamente inocente. Os investigadores que expuseram a vulnerabilidade *Logjam* mostram não só a plausibilidade da estratégia apresentada estar de facto a ser utilizada, mas também que isso é compatível com o nível de influência que a NSA detém junto de um grande número das empresas tecnológicas que produzem e comercializam soluções de segurança informática, e também com o que se sabe sobre o seu orçamento. Havendo ainda assim muitas implementações dos protocolos de comunicação que não são vulneráveis ao ataque de *man-in-the-middle* que permite relaxar o parâmetro de segurança do protocolo de *Diffie-Hellman* para níveis perigosamente baixos, os investigadores sabem ainda que a estratégia é replicável para atacar o problema do logaritmo discreto para primos com 1024 bits, estimando que a pré-computação necessária pode ser realizada, com investimento avultado em capacidade de processamento, mas ainda realizável à escala da NSA, em menos de um ano [4] [5]. Se 10% das comunicações usarem um certo primo p, esse esforço de um ano é depois facilmente recompensado com a escuta de quantidades consideráveis de informação.

Não saberemos ao certo, num futuro próximo, se de facto esta é a estratégia de cibervigilância usada pela NSA, apesar dos indícios que apontam nesse sentido. Tal prática, para além de pôr em causa a proteção dos direitos de cidadãos, empresas e estados, norte-americanos e não só, não contribui para a credibilidade de instituições que se pretendem idóneas, e levanta uma questão ainda mais inquietante: que outros estados poderão dispor de esquemas de vigilância semelhantes, possivelmente explorando exatamente a mesma vulnerabilidade?

5.CONCLUSÕES

Numa época em que as tecnologias de informação e comunicação são quase omnipresentes e se fala cada vez mais na *internet das coisas*, a consciencialização para as questões que envolvem o ciberespaço é cada vez mais pertinente. Segurança e privacidade da informação que circula na rede são um ponto fulcral para utilizadores comuns, estados e empresas. Quão seguras e confidenciais são de facto as comunicações?

Desde o obscurantismo de muitos dos sistemas ainda usados, a ataques que vão sendo conhecidos quase todos os dias, tudo vem contribuindo para minar a confiança dos utilizadores e adensar o clima de suspeição. Só a persistente evolução na forma de pensar as questões da cibersegurança, com o contributo de todos e particularmente das comunidades académicas e científicas, pode alterar este cenário e lançar-nos numa era de crescente iluminismo criptográfico. Alicerçada nos ideais subjacentes à proposta de *Kerckhoffs*, a comunidade começou já a operar esta revolução, propondo a participação de todos no desenho e desenvolvimento de funcionalidade criptográficas e protocolos *open source*, cuja segurança é testada e certificada diariamente por todos os intervenientes.

Neste artigo vimos, através do ataque *Logjam*, como as vulnerabilidades de segurança podem ser subtis, muitas vezes por resultado de interações complexas entre componentes aparentemente inócuas dos sistemas, talvez mesmo deixadas ou promovidas propositadamente por quem de direito para poderem ser usadas para fins menos confessáveis, mas que o esforço de investigadores apostados em transformar o ciberespaço num lugar mais seguro pode ajudar a descobrir e mitigar. É de salientar aqui que a vulnerabilidade *Logjam* foi previamente dada a conhecer pelos investigadores a várias entidades e empresas de relevo, e que muitos dos problemas estão já resolvidos.

Para que este processo seja cada vez mais a norma é essencial investir na investigação científica nesta área verdadeiramente multidisciplinar, apostar na formação de cidadãos cada vez mais competentes e conscientes dos desafios da cibersegurança, e mudar a mentalidade acomodada de que alguma entidade, algures, se encarregará de garantir os nossos direitos, de regular o ciberespaço, e de garantir que estamos seguros. Nesta área, o papel a desempenhar pelas entidades reguladoras, pelos estados ou pelas empresas idóneas é fundamental, mas carece ainda assim de ser

continuamente acompanhado, até porque os problemas de segurança não vão deixar de existir. A cibersegurança deve ser, cada vez mais, uma tarefa partilhada por todos. Só sociedades atentas, conscientes e competentes terão a capacidade de tornar o ciberespaço num lugar mais luminoso.

Este processo é feito de avanços e recuos, e é ingénuo imaginar que possa chegar o dia, mesmo que longínquo, em que assuntos tão sensíveis como estes serão total e abertamente escrutinados. Mas a verdade é que de cada vez que uma nova vulnerabilidade é descoberta está-se, por um lado, a pôr em causa o sistema, mas por outro a criar oportunidade de colmatar essa falha, tornando o sistema resultante mais resiliente. Não sabemos ao certo se a NSA explorava, de facto, a vulnerabilidade *Logjam*, mas não sobram muitas dúvidas de que usa de facto técnicas de cibervigilância sofisticadas. Não será implausível pensar que outros estados poderosos tenham capacidades similares, e haverá sempre muitos recantos obscuros nesta área. A questão é que proceder de forma pouco transparente acaba por trazer, quase inevitavelmente, mais problemas a jusante. Ainda recentemente o jornal satírico americano *The Onion* sugeria que o estado chinês está com dificuldade em encontrar mão-de-obra qualificada suficiente para explorar todas as vulnerabilidades dos sistemas norte-americanos [20]. Em última análise este é um jogo de equilíbrios difíceis, em que as más práticas não podem trazer bons resultados a prazo, e em que parece claramente preferível divulgar uma vulnerabilidade quando é encontrada, do que explorá-la em segredo. Todos são vulneráveis. Nesta linha, em Agosto deste ano, a NSA publicou uma nota de imprensa em que dá conta da necessidade de se fazer uma aposta séria no desenvolvimento de criptografia resistente à computação quântica. Não tendo dado nenhuma boa justificação para esta aposta, logo surgiu um escrutínio sério por parte dos especialistas sobre o alcance e implicações da afirmação. Estará a NSA em condições de executar ataques quânticos sobre os sistemas? Estará com receio que outros o façam, ou haverá algo mais subtil por detrás desta posição? Vide [21] para uma discussão científica informada sobre o assunto. Certamente, muita água passará debaixo das pontes a propósito deste assunto. Se tudo correr bem, no final, todos saberemos um pouco mais sobre cibersegurança (e computação quântica) e o ciberespaço ter-se-á tornado um lugar um pouco mais seguro.

"*It is a riddle wrapped in a mystery inside an enigma, but perhaps there is a key.*" - *Winston Churchill*, rádio BBC, 1 de Outubro de 1939

Bibliografia

[1] W. Diffie e M. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. 22, n.º 6, p. 644–654, 1976.

[2] C. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, n.º 28, 1949.

[3] Wikipedia a., "Edward Snowden," 2 12 2015. [Online]: https://en.wikipedia.org/wiki/Edward_Snowden. [Acedido em 2 12 2015].

[4] D. Adrian, K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, J. A. Halderman, N. Heninger, D. Springall, E. Thomé, L. Valenta, B. VanderSloot, E. Wustrow, S. Zanella-Béguelin e P. Zimmermann, "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice," em *22nd ACM Conference on Computer and Communications Security (CCS '15)*, Denver, 2015.

[5] D. Adrian, K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, J. A. Halderman, N. Heninger, D. Springall, E. Thomé, L. Valenta, B. VanderSloot, E. Wustrow, S. Zanella-Beguelin and P. Zimmermann, "Weak Diffie-Hellman and the Logjam Attack," Março 2015. [Online]: https://weakdh.org/. [Acedido em 01 12 2015].

[6] A. Kerckhoffs, "La cryptographie militaire," *Journal des sciences militaires*, pp. 161-191, 1883.

[7] S. Singh, The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography, Doubleday, 1999.

[8] Wikipedia b., "Enigma machine," 29 11 2015. [Online]: https://en.wikipedia.org/wiki/Enigma_machine. [Acedido em 2 12 2015].

[9] Wikipedia c., "Cryptanalysis of the Enigma," 12 2015. [Online]: https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma. [Acedido em 02 12 2015].

[10] Wikipedia d., "CoCom - Coordinating Committee for Multilateral Export Controls," 2 09 2015. [Online]: https://en.wikipedia.org/wiki/CoCom. [Acedido em 03 12 2015].

[11] Zimmermann, *Pretty Good Privacy*, 1991.

[12] Open PGP Alliance , "Welcome to The OpenPGP Alliance," 2015. [Online]: http://www.pgpi.org/ [Acedido em 01 12 2015].

[13] The Wassenaar Arrangement , "The Wassenaar Arrangement: On Export Controls for Conventional Arms and Dual-Use Goods and Technologies," 2015. [Online]: http://www.wassenaar.org/ [Acedido em 01 12 2015].

[14] National Institute of Standards and Technology, *Data Encryption Standard*, Federal Information Processing Standards Publication, 1977.

[15] National Institute of Standards and Technology, *ADVANCED ENCRYPTION STANDARD (AES)*, Federal Information Processing Standards

Publication, 2001.

[16] National Institute of Standards and Technology, *Announcing Draft Federal Information Processing Standard (FIPS) 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, and Draft Revision of the Applicability Clause of FIPS 180-4, Secure Hash Standard, and Request for Comments*, Federal Information Processing Standard, 2015.

[17] R. L. Fernandes e M. Ricou, Introdução à álgebra, Lisboa: IST Press, 2014.

[18] H. L. J. A. Lenstra, The development of the number field sieve, Lecture Notes in Mathematics ed., vol. 1554, Springer—Verlag, 1993.

[19] C. C. Richard Pomerance, Prime numbers - A computational perspective, Springer, 2005.

[20] The Onion, "China Unable To Recruit Hackers Fast Enough To Keep Up With Vulnerabilities In U.S. Security Systems," *The onion*, vol. 51, n.º 43, 26 10 2015.

[21] N. Koblitz e A. Menezes, "A riddle wrapped in a enigma," 2015.