Rio de Janeiro, 2018

Chaves Embaixo do Tapete:

exigências de acesso a todos os dados e comunicações pelo governo geram insegurança

Tradução do artigo Keys Under Doormats

Instituto
de Tecnologia
& Sociedade
do Rio

Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, Daniel J. Weitzner

Chaves embaixo do Tapete:

exigências de acesso a todos os dados e comunicações pelo governo geram insegurança

Tradução brasileira

Por Instituto de Tecnologia e Sociedade do Rio (ITS Rio)

Chaves embaixo do Tapete
"Keys Under Doormats"

EXIGÊNCIAS DE ACESSO A TODOS OS DADOS E COMUNICAÇÕES PELO GOVERNO GERAM INSEGURANÇA

Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, Daniel J. Weitzner

Tradução:

Ronivaldo Sales, Flavio Jardim, Ana Lara Mangeth, Gabriella Cantanhede e Eduardo Magrani

Resumo

Há vinte anos, os órgãos que fiscalizam a execução e aplicação da lei exerceram pressão política a fim de exigir que os serviços de comunicação e de dados desenvolvessem seus produtos de forma a garantir que tais órgãos obtivessem acesso a todos os dados. Após um longo debate e intensas previsões de que os canais de aplicação da lei "ficariam limitados", essas tentativas de regulamentar a Internet emergente foram abandonadas. Nos anos que se seguiram, a inovação na Internet prosperou, e esses órgãos encontraram meios novos e mais eficazes de acessar quantidades muito maiores de dados. Hoje, estamos novamente sendo solicitados a promover normas voltadas ao fornecimento de mecanismos de acesso excepcional. Neste relatório, um grupo de cientistas da computação e especialistas em segurança, muitos dos quais participaram de um estudo em 1997 sobre esses mesmos temas, se reuniram para explorar os prováveis efeitos da imposição de mandatos de acesso extraordinários.

Constatamos que o dano que poderia ser causado pelos requisitos de acesso excepcional feitos por órgãos fiscalizadores seria ainda mais intenso hoje do que há 20 anos. Considerando o crescente custo econômico e social da insegurança básica do atual ambiente da Internet, qualquer proposta que altere a dinâmica de segurança *online* deve ser abordada com cautela. Um acesso excepcional forçaria os desenvolvedores de sistemas de Internet a reverterem as práticas de *forward secrecy* que procuram minimizar o impacto na privacidade do usuário quando os sistemas são violados. A complexidade do ambiente atual da Internet, com milhões de aplicativos e serviços conectados globalmente, significa que os novos requisitos propostos por órgãos de aplicação da lei provavelmente introduzirão falhas de segurança imprevistas e difíceis de detectar. Além dessas e outras vulnerabilidades técnicas, a perspectiva de sistemas de acesso excepcional implantados globalmente gera questões difíceis sobre como tal ambiente seria governado e como garantir que tais sistemas respeitariam os direitos humanos e o Estado de direito.

7 de julho de 2015

Sumário executivo

Os líderes ligados à política e à execução e cumprimento da lei nos Estados Unidos e no Reino Unido fizeram um apelo para que os sistemas de Internet fossem reprojetados a fim de garantir o acesso do governo às informações - inclusive àquelas encriptadas. Eles argumentam que o crescente uso de encriptação irá neutralizar sua capacidade investigativa, propondo, assim, que os sistemas de comunicação e de armazenamento de dados sejam projetados para permitir o acesso excepcional por órgãos de aplicação da lei. Essas propostas são inviáveis na prática e suscitam sérias questões legais e éticas, bem como provocariam um retrocesso na segurança, em uma época na qual as vulnerabilidades da Internet causam gravíssimos danos econômicos.

Como cientistas da computação, com ampla experiência em segurança e sistemas, acreditamos que o ideal de cumprimento da lei não levou em conta os riscos inerentes a sistemas de acesso excepcional. Com base em nossa considerável experiência em aplicações do mundo real, sabemos que tais riscos se escondem nos detalhes técnicos. No presente relatório, examinamos se é viável, do ponto de vista técnico e operacional, atender aos apelos dos órgãos de aplicação da lei por acesso excepcional, sem causar vulnerabilidades de segurança em larga escala. Não contestamos as pretensões desses órgãos no sentido de executar ordens legais de vigilância desde que cumpram os requisitos de direitos humanos e do Estado de direito. Recomendamos enfaticamente que qualquer um que proponha regulamentos apresente primeiro requisitos técnicos e concretos, para que a indústria, os acadêmicos e o público possam verificar as deficiências técnicas e os custos ocultos.

Muitos de nós trabalhamos juntos, em 1997, para responder a uma proposta semelhante, porém mais estreita e mais bem definida, denominada *"Clipper Chip"* [1]. A proposta do *Clipper* buscou fazer com que todos os sistemas de encriptação forte mantivessem uma cópia das chaves necessárias para desencriptar informações com um terceiro confiável que forneceria as chaves para os órgãos de aplicação da lei, mediante a devida autorização legal. Naquela ocasião, constatamos que estava fora do alcance da tecnologia de ponta disponível incorporar sistemas de custódia de chaves em escala. Os governos continuaram a pressionar pela custódia de chaves, mas as empresas de Internet resistiram com sucesso, com base na elevada despesa e nas questões de governança e de risco. O *Clipper Chip* acabou sendo abandonado. Um conjunto muito mais restrito de requisitos de acesso à aplicação da lei foi imposto, mas apenas em sistemas de telecomunicações regulamentados. Ainda assim, em um número pequeno, porém preocupante de casos, fraquezas relacionadas a esses requisitos surgiram e foram exploradas por atores estatais, entre outros. Esses problemas teriam sido piores se a custódia de chaves tivesse sido implementada de forma ampla. Se todas as aplicações de

informação tivessem que ser projetadas e certificadas para acesso excepcional, é improvável que empresas como o Facebook e o Twitter existissem, por exemplo. Outra lição importante dos anos de 1990 é que o declínio na capacidade de vigilância, previsto pelos órgãos de aplicação da lei há 20 anos, não aconteceu. De fato, em 1992, a Unidade de Telefonia Avançada do FBI alertou que dentro de três anos as interceptações do Título III seriam inúteis: não mais de 40% dessas seriam inteligíveis e, no pior dos casos, todas poderiam ser inúteis [2]. O mundo não ficou sem capacidade de interceptação. Pelo contrário, a aplicação da lei dispõe agora de recursos de vigilância muito melhores e mais eficazes do que naquela época.

O presente relatório se propõe a analisar similarmente o requisito recentemente proposto de acesso excepcional às comunicações dentro da infraestrutura de informação global mais complexa da atualidade. Constatamos que isso representaria riscos de segurança muito graves, comprometeria a inovação e implicaria em questões controversas para os direitos humanos e as relações internacionais.

Existem três problemas gerais. Primeiro, fornecer acesso excepcional a comunicações forçaria uma reviravolta com relação às melhores práticas que estão sendo implantadas para tornar a Internet mais segura. Essas práticas abrangem o *forward secrecy* – em que as chaves de desencriptação são excluídas imediatamente após o uso, de forma que o furto da chave de encriptação utilizada por um servidor de comunicações não comprometa as comunicações prévias ou posteriores. Uma técnica relacionada, a *encriptação autenticada*, usa a mesma chave temporária para garantir a confidencialidade e verificar se a mensagem não foi falsificada ou adulterada.

Segundo, incorporar acesso excepcional aumentaria substancialmente a complexidade do sistema. Pesquisadores de segurança dentro e fora do governo concordam que a complexidade constitui o inimigo da segurança - cada novo recurso pode interagir com os outros para criar vulnerabilidades. Para obter um acesso excepcional e amplo, novos recursos de tecnologia teriam que ser implantados e testados com literalmente centenas de milhares de desenvolvedores em todo o mundo. Este é um ambiente muito mais complexo do que a vigilância eletrônica agora implantada nas telecomunicações e serviços de acesso à Internet. Esses tendem a usar tecnologias semelhantes, e são mais propensos a ter meios para gerenciar vulnerabilidades que podem surgir de novos recursos. Funcionalidades que permitem o acesso excepcional, para fins de aplicação da lei em várias aplicações de computação móvel e de Internet, poderiam ser particularmente problemáticas porque seu uso seria tipicamente indetectável, e tornaria os testes de segurança difíceis e menos eficazes.

Em terceiro lugar, o acesso excepcional criaria alvos concentrados que poderiam atrair maus atores. As credenciais de segurança que desbloqueiam os dados teriam que ser retidas pelo provedor da plataforma, órgãos de execução ou aplicação da lei ou algum outro terceiro confiável. Se as chaves dos órgãos de aplicação da lei garantissem o acesso

total, um invasor que obtivesse acesso a essas chaves teria o mesmo privilégio. Além disso, a necessidade declarada do órgão competente de obter acesso rápido aos dados inviabilizaria o armazenamento de chaves *off-line* ou a divisão de chaves entre os vários proprietários de chaves, como engenheiros de segurança normalmente fariam com credenciais de valor extremamente alto. Ataques recentes ao Escritório de Gestão de Pessoal dos Estados Unidos (*United States Government Office of Personnel Management* "OPM") mostram o nível de danos que podem ser causados quando muitas organizações dependem de uma única instituição que possua vulnerabilidades de segurança. No caso do OPM, várias agências federais perderam dados sensíveis devido a sua infraestrutura vulnerável. Se os provedores de serviços estabelecerem requisitos incorretos de acesso excepcional, a segurança de todos os seus usuários estará em risco.

Nossa análise se aplica não apenas a sistemas que fornecem acesso a dados encriptados, mas também a sistemas que fornecem acesso direto a textos simples (*plaintext*). Por exemplo, os órgãos de aplicação da lei exigiram que as redes sociais permitissem acesso rápido e automatizado aos seus dados. Um *backdoor* na aplicação da lei em uma rede social também constitui uma vulnerabilidade, exposta a ataques e abusos. De fato, o banco de dados que continha alvos de vigilância do Google foi monitorado por agentes chineses que invadiram o sistema, supostamente para fins de contrainteligência [3].

O maior impedimento para acesso excepcional pode ser a jurisdição. Incorporar acesso excepcional já seria arriscado o suficiente, mesmo que apenas um órgão do mundo o possuísse. Mas, esta não é apenas uma questão dos Estados Unidos. O governo do Reino Unido promete editar legislação que obrigue os provedores de serviços de comunicações, incluindo corporações sediadas nos EUA, a conceder acesso aos órgãos de aplicação da lei do Reino Unido, e outros países certamente seguirão o exemplo. A China já sugeriu que pode exigir acesso excepcional. Se um desenvolvedor com sede na Inglaterra implanta um aplicativo de mensagens usado por cidadãos da China, este deve fornecer acesso excepcional aos órgãos de aplicação da lei chineses? Quais países têm respeito suficiente pelo Estado de direito para participar de uma estrutura internacional de acesso excepcional? Como essas determinações seriam feitas? Como seriam dadas as aprovações em tempo hábil para os milhões de novos produtos com capacidade de comunicação? E como esse novo ecossistema de vigilância seria financiado e supervisionado? Os governos dos Estados Unidos e do Reino Unido têm se empenhado muito para manter a governança da Internet transparente, em face de demandas de países autoritários que defendem o controle estatal. A pressão por acesso excepcional não representa uma forte inversão política?

A necessidade de lidar com essas questões legais e políticas poderia alterar a Internet da noite para o dia, de seu atual modelo aberto e empreendedor, para uma indústria altamente regulada. Enfrentar essas questões requer mais do que nossa *expertise* técnica

como cientistas da computação, mas essas devem ser respondidas antes de se implementar técnicas de acesso excepcional.

No corpo deste relatório, procuramos estabelecer as bases para este necessário debate, apresentando o contexto histórico do denominado acesso excepcional, resumindo as demandas dos órgãos de cumprimento ou execução da lei a partir de nosso entendimento, e depois discutindo-as com base nos dois tipos de plataforma mais populares, que estão em rápido crescimento: serviços de mensagens e dispositivos eletrônicos pessoais, como *smartphones* e *tablets*. Finalmente, estabelecemos em detalhes as questões para as quais os formuladores de políticas devem exigir respostas se a demanda por acesso excepcional prevalecer. Sem uma proposta técnica concreta e sem respostas adequadas às questões levantadas neste relatório, os legisladores devem rejeitar imediatamente qualquer proposta de retorno à política de controle de criptografia que falhou nos anos de 1990.

Índice

1 Contexto do atual debate sobre acesso excepcional

O debate sobre encriptação foi reaberto no ano passado com o diretor do FBI, James Comey, e o primeiro-ministro do Reino Unido, David Cameron, advertindo que, assim como ocorreu no início da década de 1990, a encriptação ameaça os mecanismos de aplicação da lei, e defendendo que os provedores de serviços que usam encriptação sejam obrigados legalmente a fornecer acesso a chaves ou a texto simples em resposta a mandados devidamente autorizados. Por isso, convocamos o nosso grupo de especialistas para reexaminar o impacto do acesso excepcional obrigatório no ambiente atual da Internet.[1]

Na década de 1990, os governos dos Estados Unidos e de vários outros países industrializados defenderam o enfraquecimento da encriptação. Alegando que seu uso generalizado seria desastroso em termos de aplicação da lei, o governo dos EUA propôs o uso do *Clipper Chip*, um dispositivo de encriptação contendo uma chave mestra do governo para permitir-lhe acesso a comunicações encriptadas. Outros governos seguiram o exemplo com propostas de licenciamento de encriptação, que exigiriam cópias de chaves a serem mantidas sob custódia por terceiros confiáveis – empresas que seriam confiáveis para entregar chaves por determinação da lei. O debate envolveu a indústria, ONGs, a academia e outros. A maioria dos autores do presente artigo elaborou um relatório sobre as questões relacionadas à custódia de chaves e encriptação por terceiros confiáveis, analisando a dificuldade técnica, os riscos acrescidos e os custos prováveis do referido sistema de custódia de chaves [1]. O esforço pelo uso do sistema mencionado foi abandonado em 2000, em decorrência da pressão feita pela indústria durante o *boom* das empresas "pontocom" e por causa da resistência política da União Europeia, entre outros motivos.

[1] Seguimos o relatório 1996 *National Academies CRISIS*, usando a expressão "acesso excepcional" para "enfatizar que a situação não é aquela que foi incluída dentro dos limites pretendidos da transação original". [4, p. 80]

1.1 Resumo do atual debate

O debate atual sobre política pública é dificultado pelo fato de que os órgãos de aplicação da lei não forneceram uma declaração suficientemente completa de seus requisitos para especialistas técnicos ou legisladores analisarem. A seguinte exortação do diretor do FBI dos Estados Unidos, James Comey, é a que consideramos mais próxima:

> "Não estamos buscando uma abordagem *backdoor*. Pretendemos usar a abordagem *frontdoor*, com clareza e transparência, e com orientações claras e previstas na lei. Sentimo-nos plenamente confortáveis em relação a ordens judiciais e processos legais – As abordagens *frontdoor* são as que fornecem as provas e informações de que precisamos para investigar crimes e prevenir ataques terroristas."
>
> "Os adversários cibernéticos irão explorar qualquer vulnerabilidade que encontrarem. Contudo, é mais sensato abordar quaisquer riscos de segurança desenvolvendo soluções de interceptação durante a fase de *design*, em vez de recorrer a uma solução de *patchwork* quando os órgãos se apresentarem após os acontecimentos. E com encriptação sofisticada, pode não haver solução, deixando o governo em um beco sem saída – tudo em nome da privacidade e da segurança da rede." [5]

O primeiro-ministro David Cameron simplesmente quer que a polícia tenha acesso a tudo. Falando na ocasião dos assassinatos do Charlie Hebdo em Paris, ele disse:

> "No nosso país, queremos permitir um meio de comunicação entre pessoas que, mesmo em situações extremas, e com um mandado assinado pessoalmente pelo secretário de administração interna, não possa ser lido? . . . A questão permanece: Vamos permitir um meio de comunicação no qual isso simplesmente não pode ser feito? Minha resposta para essa pergunta é: Não, não devemos". [6]

Sendo assim, devemos perguntar se é possível introduzir tal acesso excepcional sem criar riscos inaceitáveis. Para entender as questões técnicas e operacionais, primeiro revisamos os resultados do nosso relatório de 1997 e consideramos o que mudou desde então. Em seguida, tentamos esclarecer os requisitos ideais para os órgãos de aplicação da lei e entender os tipos de riscos que provavelmente surgirão se esses requisitos genéricos forem amplamente impostos no ambiente global da Internet. Depois, apresentamos dois cenários tecnológicos típicos do panorama frente à moderna vigilância eletrônica. Combinando o que é conhecido publicamente hoje sobre as práticas de vigilância com os requisitos legais comuns, somos capazes de apresentar cenários que ilustram muitos dos principais riscos que o acesso excepcional implicará.

Não temos a intenção de sugerir que a nossa própria interpretação do que Comey indicou como requisitos sirvam de base para a regulação, mas apenas que sejam um ponto de partida para a discussão. Se as autoridades do Reino Unido ou dos Estados Unidos discordam de nossa interpretação, solicitamos-lhes que declarem explicitamente suas exigências. Só assim, uma análise técnica rigorosa pode ser conduzida de maneira aberta e transparente. Essa análise é crucial em um mundo completamente dependente de comunicações seguras em todos os aspectos da vida cotidiana, desde a infraestrutura crítica das nações, até as questões relacionadas aos governos, à privacidade pessoal e a todos os assuntos de negócios, do trivial ao global.

1.2 Resultados da análise de 1997 sobre sistemas de custódia de chaves

Iniciamos com a revisão das observações referentes aos riscos dos sistemas de recuperação/custódia de chaves de um artigo que muitos de nós redigimos há quase 20 anos [1]. Muitos de nós nos reunimos para examinar os riscos de segurança concernentes à garantia de acesso dos órgãos de aplicação da lei a informações encriptadas. Observamos que qualquer sistema de custódia de chaves apresentava requisitos básicos que impunham custos substanciais aos usuários finais, e que esses custos seriam muito elevados para implementar. Para que os órgãos obtivessem acesso rápido e confiável ao texto simples, cada sistema de custódia de chaves exigia a existência de chaves secretas altamente sensíveis, mas permanentemente disponíveis. Esse requisito, por si só, inevitavelmente leva a um aumento do risco de exposição, a uma maior complexidade de software e a altos custos econômicos.

A primeira desvantagem é o aumento do risco de um incidente de segurança. A organização que possui a chave de custódia poderá se deparar com um membro interno mal-intencionado que abuse de seu poder ou compartilhe a chave da organização. Mesmo partindo-se do pressuposto de que determinado órgão é honesto, há uma questão de competência: os ataques cibernéticos aos proprietários das chaves podem facilmente resultar em perdas catastróficas.

A complexidade adicional de um sistema de custódia de chaves agrava esses riscos. À época, todas as soluções para a custódia de chaves propostas abertamente tinham grandes falhas que podiam ser exploradas; até mesmo a encriptação normal era difícil de implementar apropriadamente, e a custódia de chaves tornava as coisas muito mais difíceis. Outra fonte de complexidade foi a escala de um sistema universal de recuperação de chaves – o número de agentes, produtos e usuários envolvidos seria imenso, exigindo um sistema de custódia muito além da tecnologia da época. Além disso, a custódia de chaves ameaçava aumentar a complexidade operacional: várias instituições teriam que

negociar, de forma segura e protegida, questões de direcionamento, autenticação, validade e transferência de informações para acesso a informações legais.

Todos os fatores acima aumentam os custos. Os riscos de exposição, por exemplo, mudam o cenário com relação a ameaças para as organizações, que devem então se preocupar com divulgações equivocadas ou fraudulentas. O governo teria aumentado a burocracia para testar e aprovar os principais sistemas de recuperação de chaves. Os fornecedores de software teriam que arcar com o ônus pelo aumento dos custos de engenharia. Em 1997, observamos que os sistemas que permitissem acesso excepcional a chaves seriam inerentemente menos seguros, mais caros e muito mais complexos do que aqueles que não dispusessem do mesmo. Esse resultado ajudou os formuladores de políticas a decidirem contra o acesso excepcional obrigatório.

1.3 O que mudou e o que se manteve desde os anos de 1990?

É impossível operar a Internet comercial ou outra rede global de comunicações, mesmo em níveis modestos de segurança, sem o uso de encriptação. Um amplo debate nas décadas de 1980 e 1990 sobre o papel da encriptação já havia chegado a essa conclusão. Hoje, a importância técnica fundamental da criptografia forte e as dificuldades inerentes à limitação de seu uso para atender aos objetivos de aplicação da lei permanecem as mesmas. O que mudou é que a escala e o escopo dos sistemas dependentes de encriptação forte são muito maiores, e nossa sociedade é muito mais dependente de redes digitais distantes que estão sob ataques diários.

No início dos anos de 1990, a comercialização da Internet era frustrada pelos controles do governo dos EUA sobre encriptação – controles que, em muitos aspectos, eram contraproducentes para os interesses comerciais e de segurança nacional em longo prazo. Um estudo de 1996 da Academia Nacional de Ciências dos Estados Unidos concluiu que, “Em última análise, as vantagens do uso mais difundido da criptografia superam as desvantagens” [4, p. 6]. [7]. Quatro anos depois, diversos motivos fizeram com que os EUA afrouxassem os controles de exportação sobre encriptação, em resposta: a) às pressões da indústria; b) ao afrouxamento dos controles criptográficos de exportação pela União Europeia; c) aos controles criptográficos de exportação declarados inconstitucionais pelos tribunais dos EUA; d) à crescente dependência das comunicações eletrônicas e do comércio.

As Guerras Criptográficas, na verdade, tiveram início na década de 1970, com conflitos sobre se as empresas de computadores, como IBM e Digital Equipment Corporation, poderiam exportar hardware e software com encriptação forte, e sobre se os acadêmicos poderiam publicar livremente pesquisas criptográficas. E permaneceram, durante a década de 1980, sobre se a *National Security Agency* (NSA) ou o Instituto Nacional de

Padrões e Tecnologia (*National Institute of Standards and Technology* - NIST) controlaria o desenvolvimento de padrões criptográficos para o lado da segurança não nacional do governo (o NIST recebeu a autoridade conforme a Lei de Segurança dos Computadores de 1987). Estas entraram em vigor durante a década de 1990 quando o governo dos EUA, em grande parte mediante o uso de controles de exportação, procurou impedir que empresas como Microsoft e Netscape usassem criptografia forte em navegadores da Web e outros softwares que estavam na base da Internet em crescimento. O fim das guerras – ou o aparente fim – veio por causa do *boom* da Internet.

De muitas maneiras, os argumentos são os mesmos de duas décadas atrás. Padrões criptográficos do governo dos EUA – o Padrão de Encriptação de Dados, na ocasião; atualmente, o Padrão Avançado de Encriptação, – são amplamente utilizados tanto internamente quanto no exterior. Sabemos mais agora sobre como construir sistemas criptográficos fortes, embora periodicamente nos surpreendamos com quebras de segurança. No entanto, o verdadeiro desafio da segurança não é a matemática dos sistemas criptográficos, e sim a engenharia, especificamente o design e a implementação de sistemas de software complexos. Dois grandes esforços do governo, *healthcare.gov* e o programa Trilogia do FBI, demonstram as dificuldades que a escala e a integração do sistema representam na construção de grandes sistemas de software. O *healthcare.gov*, *site* que implementa o programa de saúde da presidência, apresentou sérias falhas em seus primeiros dias, sendo incapaz de servir mais do que uma pequena porcentagem de usuários [8]. Uma década antes, cinco anos de esforço foram necessários para construir um sistema eletrônico de arquivos de processos para o FBI – tentativa esta que custou US$ 170 milhões, e foi abandonada por ser considerada impraticável [9].

De certa forma, o pior ainda não aconteceu – a rede elétrica, o sistema financeiro, a infraestrutura crítica em geral e muitos outros sistemas funcionam usando de maneira confiável softwares complexos. Mas, por outro lado, o pior ocorre diariamente. Violações recentes com vistas a ganhos financeiros incluem: T.J. Maxx, furto de 45 milhões de registros de cartão de crédito [10]; Heartland Payment Systems, comprometimento de 100 milhões de cartões de crédito [11]; Target, comprometimento de 40 milhões de cartões de crédito; Anthem, coleta de nomes, endereços, datas de nascimento, informação sobre emprego e rendimentos, e registros de previdência social de 80 milhões de pessoas que poderiam resultar em usurpação de identidades [12].

Os ataques a órgãos governamentais também estão aumentando. Uma série de 2003 invasões, visando *sites* militares dos EUA, coletou dados sensíveis, como especificações para sistemas de planejamento de missão de helicópteros do Exército, software de planejamento de voo da Força Aérea e do Exército e esquemas para a *Mars Orbiter Lander* [13]. Esses furtos não foram apenas da base industrial de defesa, mas envolveram também as indústrias farmacêutica, de Internet, de biotecnologia e de energia. Em 2010, o então subsecretário de Defesa William Lynn concluiu: “Embora a ameaça à propriedade

intelectual seja menos dramática do que a ameaça à infraestrutura nacional crítica, pode ser a ameaça cibernética mais significativa que os Estados Unidos enfrentarão a longo prazo ”[14].

Os ataques cibernéticos norte-coreanos realizados em dezembro de 2014 contra a Sony, o primeiro deles por um Estado-nação, resultaram em grandes manchetes. No entanto, o furto em 2011 das *seed keys* da RSA/EMC – chaves iniciais usadas para gerar outras chaves – em *tokens* de *hardware* usados para fornecer autenticação de dois fatores [15], e o recente furto de registros de funcionários do Escritório de Administração de Pessoal dos EUA são questões muito mais sérias. O primeiro comprometeu a infraestrutura técnica de sistemas seguros, enquanto o segundo, ao fornecer a estranhos informações pessoais de usuários do governo, acabou criando um impulso para potenciais ataques internos por muitos anos a frente, comprometendo a infraestrutura social necessária para apoiar sistemas governamentais seguros – incluindo qualquer futuro sistema de acesso excepcional. E, embora os ataques contra infraestruturas críticas não tenham sido significativos, o potencial para isso foi demonstrado em casos de teste [16] e em um ataque real a uma usina siderúrgica alemã que causou danos significativos a um alto-forno [17].

Como o acesso excepcional coloca em risco a segurança da infraestrutura da Internet, os efeitos serão sentidos tanto pelos órgãos governamentais quanto pelo setor privado. Por causa do custo e da velocidade de inovação do Vale do Silício, a partir de meados dos anos de 1990, o governo dos EUA avançou em direção a uma estratégia comercial de produtos prontos para uso (*comercial off the shelf* - COTS) para equipamentos de tecnologia da informação, incluindo dispositivos de comunicação. Em 2002, Richard George, diretor técnico da Information Assurance, disse a um público da Black Hat que “a Agência de Segurança Nacional dos Estados Unidos (*National Security Agency* – NSA) tem uma estratégia de COTS, que é: quando existirem produtos prontos para uso com os recursos necessários, incentivaremos sua utilização, quando e onde for apropriado...”[18]. Tal solução de COTS faz sentido, é claro, somente se as tecnologias do setor privado que o governo usa forem seguras.

As tecnologias de comunicação projetadas para atender aos requisitos do governo para *backdoors* de acesso legal se mostraram inseguras. Durante dez meses, entre 2004 e 2005, 100 membros seniores do governo grego (incluindo o primeiro-ministro, o chefe do Ministério da Defesa Nacional e o chefe do Ministério da Justiça) foram grampeados por partes desconhecidas mediante acesso legal incorporado a uma central telefônica pertencente à Vodafone Greece [19]. Em 2010, um pesquisador da IBM observou que uma

arquitetura da Cisco para interceptação legal em redes IP era insegura.[2] Esta arquitetura era pública há vários anos, e versões inseguras tinham sido implementadas por várias operadoras na Europa [20]. E quando a NSA examinou as centrais telefônicas construídas para cumprir o acesso obrigatório do governo por escutas telefônicas, detectou problemas de segurança em *todas* as centrais submetidas a testes [21]. Incorporar requisitos de acesso excepcional à tecnologia de comunicações implicará ainda mais esse tipo de problema, colocando em risco não apenas os sistemas do setor privado, mas também os do governo.

Com relação ao acesso pelos órgãos de aplicação da lei e segurança de sistemas, o vice-presidente do *Joint Chiefs of Staff*, almirante James A. Winnefeld, comentou recentemente: "Mas acho que todos nós venceríamos se nossas redes fossem mais seguras. Eu prefiro um cenário onde temos redes seguras, porém com maiores desafios em termos de inteligência para o Mike [diretor da NSA, Mike Rogers] resolver, a um cenário onde as redes são muito vulneráveis e com um problema fácil para o Mike. E não se trata apenas de ser a coisa certa a se fazer, mas também se deve ao fato do nosso país ser o mais vulnerável do mundo, devido à dependência que temos do ciberespaço. Também estou muito confiante de que Mike conta com alguns colaboradores inteligentes, bem qualificados para acabar desempenhando um bom trabalho".

Embora o debate sobre o acesso obrigatório pelos órgãos de aplicação da lei não seja novo, ele adquire uma urgência ainda maior no mundo de hoje. Dada a nossa crescente dependência da Internet e a necessidade urgente de tornar esta e outras infraestruturas digitais mais seguras, qualquer movimento no sentido de uma menor segurança deve ser encarado com extremo ceticismo. Em outras ocasiões, ao considerar esta questão, governos de todo o mundo chegaram à conclusão de que projetar provisões de acesso excepcional a sistemas vitais aumentaria o risco de segurança e comprometeria a inovação. Conforme ainda será demonstrado no presente artigo científico, tais medidas são ainda mais arriscadas atualmente.

[2] Cabe ressaltar que o projeto do roteador foi baseado em padrões estabelecidos pelo Instituto Europeu de Normalização das Telecomunicações.

2 Cenários

As autoridades responsáveis pela aplicação da lei apresentaram um requisito muito amplo de acesso excepcional. No entanto, faltam muitos detalhes, incluindo a gama de sistemas aos quais tais requisitos se aplicariam, a aplicação extraterritorial, e se as comunicações anônimas seriam permitidas, entre outras variáveis. Para analisar a gama de riscos de segurança que podem surgir em aplicativos e serviços comumente usados, examinamos dois cenários conhecidos: serviços de mensagens encriptadas em tempo real e dispositivos, como *smartphones*, que usam encriptação forte para bloquear o acesso ao dispositivo.

2.1 Cenário 1: permitindo acesso excepcional a aplicativos de mensagens encriptadas e distribuídas globalmente

Imagine um aplicativo global de mensagens massivamente distribuído na Internet usando encriptação de ponta a ponta. Muitos exemplos de tais sistemas realmente existem, incluindo o *Signal*, que está disponível no iPhone e Android, *Off-the-Record (OTR)*, um *plug-in* de habilitação de criptografia para muitos programas populares de bate-papo por computador, sendo o *TextSecure* e o *WhatsApp* frequentemente citados. Seria possível fornecer um aplicativo seguro que, ao mesmo tempo, atenda aos requisitos de acesso excepcional dos órgãos de aplicação da lei?

Para fornecer acesso aos dados encriptados pelos órgãos de aplicação da lei, uma das abordagens naturais consiste em fornecer à autoridade competente acesso direto às chaves que podem ser usadas para desencriptar os dados e há um mecanismo frequentemente sugerido e aparentemente bastante atraente para custodiar as chaves de desencriptação. Os dados normalmente são encriptados – para armazenamento ou transmissão – com uma chave simétrica,[3] e muitos protocolos de transmissão de dados (por exemplo, o protocolo TLS - *Transport Layer Security* ou Segurança da Camada de Transporte) podem operar de forma que os dados a serem enviados sejam encriptados com uma chave simétrica que, por sua vez, é encriptada com uma chave pública[4] associada ao destinatário pretendido. Essa chave simétrica encriptada, em seguida, é transferida

[3] Uma chave simétrica é aquela usada para encriptação e desencriptação.

[4] Uma chave pública é usada para encriptar dados que podem ser desencriptados somente por uma entidade que possui uma chave privada associada.

com os dados encriptados, e o destinatário acessa os dados usando primeiramente sua chave privada para desencriptar a chave simétrica e, em seguida, usando a chave simétrica para desencriptar os dados.

O mais indicado é incrementar isso fazendo a encriptação da chave simétrica uma segunda vez – dessa vez, com uma custódia especial de chaves públicas. Se os dados forem transmitidos, duas encriptações da chave simétrica acompanham os dados – uma com a chave pública do destinatário pretendido e a outra com uma chave pública associada a um agente de custódia. Se os dados forem encriptados com uma chave simétrica para armazenamento em vez de transmissão, a chave simétrica poderá ser encriptada com a chave pública de um agente de custódia, e essa chave custodiada poderá permanecer com os dados encriptados. Se uma entidade de aplicação da lei obtiver esses dados encriptados durante a transmissão ou a partir do armazenamento, o agente de custódia poderá ser inscrito para desencriptar a chave simétrica que poderia, então, ser usada para desencriptar os dados.

Observam-se, no entanto, três principais impedimentos ao usar essa abordagem para custódia por parte de terceiros. Dois são técnicos e o terceiro é processual. O primeiro obstáculo técnico é que, embora o modo de encriptar uma chave simétrica com chave pública seja de uso comum, as empresas afastam-se agressivamente desse modelo em função de uma vulnerabilidade prática significativa: *se a chave privada de uma entidade for violada, todos os dados protegidos com essa chave pública serão imediatamente comprometidos*. Como não é prudente supor que uma rede nunca será violada, uma única falha nunca deve comprometer todos os dados que já foram encriptados.

Assim, as empresas convergem para o *forward secrecy*, uma abordagem que reduz muito a exposição de uma entidade que foi prejudicada. Com o *forward secrecy*, uma nova chave é negociada a cada transação e as chaves de longo prazo são usadas somente para autenticação.

Essas chaves de transação (ou *sessão*) são descartadas após cada transação – o que reduz significativamente a exposição de uma entidade que tenha sido comprometida. Quando um sistema com *forward secrecy* é usado, invasores que infringem uma rede e obtêm acesso às chaves só conseguirão desencriptar dados a partir do momento da violação até que esta seja descoberta e corrigida; os dados históricos permanecem seguros. Além disso, como as chaves de sessão são destruídas imediatamente após a conclusão de cada transação, o invasor deve inserir-se no processo de cada transação em tempo real para conseguir obter as chaves e comprometer os dados.[5]

[5] A falta de *forward secrecy* foi identificada no documento de 1997 [1] como uma fraqueza dos sistemas de custódia de chaves à época.

Os benefícios da segurança indicam claramente a razão pela qual as empresas estão mudando rapidamente para sistemas que fornecem *forward secrecy*.[6] No entanto, o requisito de custódia de chaves cria uma vulnerabilidade a longo prazo: Se *qualquer* uma das chaves de custódia privadas for comprometida *alguma vez*, todos os dados utilizados mediante o uso da chave comprometida ficarão permanentemente comprometidos. Ou seja, para atender à necessidade de acesso oculto de terceiros por órgãos de aplicação da lei, as mensagens terão que ser deixadas expostas a ataques por qualquer um que obtiver uma cópia de uma das muitas cópias das chaves desses órgãos. *Assim, todos os métodos conhecidos para obtenção de custódia por terceiros são incompatíveis com o forward secrecy*.

Inovações que proporcionam melhor *forward secrecy* também oferecem suporte a uma ampla tendência social: os usuários estão migrando em massa para comunicações mais efêmeras. O que justifica a mudança para esse tipo de comunicação vai desde decisões práticas de empresas, até a proteção de informações de uso exclusivo de espionagem industrial até indivíduos que buscam proteger sua capacidade de comunicação anônima e evitar ataques de governos repressivos. Muitas empresas excluem e-mails após 90 dias, enquanto as pessoas mudam do e-mail para o bate-papo, usando serviços como o *Snapchat*, nos quais as mensagens desaparecem após a leitura. Empresas líderes como Twitter, Microsoft e Facebook apoiam a mudança para mensagens temporárias e o uso de mecanismos modernos de segurança como suporte. Esse desenvolvimento social e técnico não é compatível com a manutenção de meios para fornecer acesso excepcional.

O segundo obstáculo técnico é que a prática recomendada atual consiste em usar frequentemente *encriptação autenticada*, que fornece a *autenticação* (assegurando que a entidade no outro lado da comunicação é quem você espera, e que a mensagem não sofra alteração após o envio), bem como a *confidencialidade* (protegendo a privacidade das comunicações, incluindo dados financeiros, médicos e outros dados pessoais). No entanto, a divulgação da chave para encriptação autenticada a um terceiro significa que o destinatário da mensagem não estará mais provido de garantia técnica para a integridade da comunicação; a divulgação da chave permite que o terceiro não apenas *leia* o tráfego encriptado, mas também *forje* o tráfego para o destinatário e faça com que ele pareça vir do remetente original. Assim, divulgar a chave a um terceiro cria uma nova vulnerabilidade de segurança. Remetendo-nos aos métodos de encriptação dos anos de 1990, com chaves separadas para encriptação e autenticação, isto não apenas dobraria o

---

Desde então, a necessidade de sigilo aumentou substancialmente.

[6] Ver [22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32].

esforço computacional necessário, mas traria muitas oportunidades para erros de projeto e implementação que viriam a causar vulnerabilidades.

O terceiro principal obstáculo para a custódia de chaves de terceiros é procedimental, e se resume a uma pergunta simples: Quem controlaria as chaves retidas? Dentro dos Estados Unidos, pode-se postular que o FBI ou alguma outra entidade federal designada tenha a chave privada necessária para obter acesso a dados, e que mecanismos judiciais seriam construídos para permitir seu uso pela multiplicidade de entidades de aplicação da lei federais, estaduais e locais. Entretanto, isso deixa sem resposta a questão do que acontece fora das fronteiras de uma nação. Organizações públicas e privadas alemãs e francesas estariam dispostas a usar sistemas que dariam ao governo dos EUA acesso a seus dados – especialmente quando eles poderiam, ao invés disso, usar sistemas construídos localmente? E a Rússia? Os dados encriptados transmitidos entre os EUA e a China precisariam ter chaves custodiadas pelos dois governos? Poderia um agente de custódia individual ser considerado aceitável para ambos os governos? Em caso afirmativo, o acesso seria concedido a apenas um dos dois governos ou ambos precisariam concordar com uma determinada solicitação?

Essas questões difíceis devem ser respondidas antes que qualquer sistema de acesso excepcional seja implementado. Tal arquitetura exigiria acordos globais sobre como a custódia deveria ser estruturada, muitas vezes contra os melhores interesses e objetivos internos de certos países, juntamente com mandados em praticamente todas as nações para vender e usar apenas sistemas compatíveis.

2.2 Cenário 2: acesso excepcional a textos simples em dispositivos encriptados, como *smartphones*

Imagine um fornecedor de plataformas de *smartphones* que procura atender às demandas excepcionais das autoridades de aplicação da lei. Quando essas autoridades recolhem um dispositivo, talvez de uma cena de crime e obtêm a autorização legal necessária (nos Estados Unidos, isso seria um mandado resultante da *Riley v. Califórnia*), o agente coleta um número de identificação único do dispositivo por meio de algum mecanismo de serviço e, em seguida, envia uma solicitação ao fornecedor da plataforma para desbloquear o dispositivo remotamente ou fornecer as chaves necessárias para a autoridade competente desbloqueá-lo localmente.

À primeira vista, fornecer acesso a textos simples em dispositivos – discos rígidos de *laptops*, *smartphones*, *tablets* – é intuitivo. Na verdade, diversas corporações já fazem a custódia das chaves de encriptação do dispositivo. No entanto, e pelo fato de ocorrer frequentemente, não é fácil expandir de um mecanismo corporativo para um mecanismo global.

Ao encriptar os dados armazenados no dispositivo, a senha inserida pelo usuário geralmente não é usada diretamente como uma chave de encriptação. Há muitas razões para isso; de uma perspectiva de usabilidade, o mais importante é facilitar a mudança de senha para o usuário. Se a chave fosse usada diretamente, o processo de desencriptar e voltar a encriptar todo o dispositivo seria demorado por conta da alteração da senha. Em vez disso, uma chave aleatória é usada para encriptação em massa; a chave fornecida pelo usuário (chamada "Chave de Encriptação de Chave" – ou *KEK*, do termo em inglês *Key-Encrypting Key*) é usada para encriptar a chave aleatória.

Para proteger a senha do usuário contra os ataques de força bruta, o fornecedor do dispositivo pode avançar mais um passo e combiná-lo com um identificador exclusivo específico do dispositivo para produzir a *KEK*. No iPhone, a *KEK* é armazenada em um processador especial resistente a adulterações, que limita a taxa de tentativa (*guess rate*) a uma vez a cada 80 milissegundos. Isso protege os proprietários de dispositivos contra, por exemplo, ladrões que atuam de forma mais sofisticada, eventualmente tentando obter acesso a itens como senhas bancárias. Mas, independentemente de como a *KEK* seja gerada, a obtenção de acesso ao texto simples exige que a chave de encriptação do dispositivo seja encriptada com base em alguma chave ou chaves adicionais. Podem ser chaves de propriedade do fabricante ou pertencentes a um ou mais órgãos de aplicação da lei. Qualquer uma dessas escolhas é problemática [33].

Se for usada uma chave obtida através de um fornecedor, é necessário algum tipo de protocolo de rede para desencriptar a chave do dispositivo. Este pedido deve ser autenticado. Mas como? Como o fornecedor pode ter credenciais seguras para todos os milhares de órgãos fiscalizadores em todo o mundo? Como o resultado pode ser fortemente vinculado ao dispositivo, para evitar que órgãos inescrupulosos solicitem chaves a dispositivos que não estejam em sua posse legal? Estes não são requisitos fáceis de cumprir, especialmente para dispositivos que nem sequer inicializam sem uma chave válida. Eles provavelmente exigirão alterações no hardware de segurança ou no software que os aciona; ambos são difíceis de fazer corretamente. Corrigir falhas – especialmente falhas de segurança – no hardware implantado é caro e muitas vezes inviável.

Fornecer dispositivos com chaves exigidas pelos órgãos competentes é igualmente difícil. Novamente, como o fornecedor pode saber quem forneceu as chaves? Como essas chaves podem ser alteradas?[7] Quantas chaves podem ser instaladas sem causar uma lentidão inaceitável? Outra alternativa é exigir que os órgãos de aplicação da lei enviem os dispositivos de volta ao fornecedor para acesso excepcional via desencriptação. No entanto, ainda será necessário armazenar por longos períodos de tempo chaves que

[7] Observamos que alguns tipos de *malware*, como o Stuxnet e o Duqu 2, dependem de chaves de assinatura de código emitidas para empresas legítimas. Quando uma chave é comprometida, ela deve ser substituída.

possam desencriptar todos os dados confidenciais em dispositivos. Isso apenas desloca para os fabricantes de dispositivos os riscos de proteger essas chaves.

Alguns argumentariam que as chaves por país poderiam ser uma exigência de vendas. Ou seja, todos os dispositivos vendidos nos Estados Unidos deveriam ter, digamos, uma chave pré-instalada fornecida pelo FBI. Isso, no entanto, não é suficiente para dispositivos trazidos por viajantes – e esses são os dispositivos que provavelmente são de interesse em investigações de terrorismo. O requisito de que as chaves sejam instaladas nas fronteiras também é problemático. Não há portas de entrada padrão ou mecanismos de carregamento de chaves; além disso, isso exporia os viajantes norte-americanos a *malwares* instalados por guardas de fronteira em outros países [34, 35].

2.3 Resumo dos riscos dos dois cenários

Projetar acesso excepcional nos serviços e aplicativos de informações atuais resultará em uma série de riscos críticos à segurança. Primeiro, os intensos esforços que a indústria dedica para melhorar a segurança serão prejudicados e revertidos. Fornecer acesso durante qualquer período de tempo a milhares de órgãos de aplicação da lei necessariamente aumentará o risco de que intrusos sequestrem os mecanismos de acesso excepcional. Caso o órgão de aplicação da lei necessite rever os dados encriptados até um ano antes, o valor de um ano de dados será posto em risco. Se esse órgão quiser garantir acesso em tempo real aos fluxos de comunicação, os intrusos também terão mais facilidade para obter acesso em tempo real. Este é um espaço de negociação em que o acesso não pode ser garantido aos órgãos de aplicação da lei sem criar um risco sério de que intrusos criminosos obtenham o mesmo acesso.

Em segundo lugar, o desafio de garantir o acesso a vários órgãos de aplicação da lei em vários países é extremamente complexo. É provável que os custos desse desafio sejam proibitivos e também um problema insolúvel de relações exteriores.

Requisitos simples podem produzir soluções simples (por exemplo, bloqueio de porta). Mas os requisitos de acesso pelos órgãos competentes a dados criptografados são inerentemente complexos e, como já mostramos, quase contraditórios. Requisitos complexos ou quase contraditórios produzem soluções frágeis, muitas vezes inseguras. Como o ex-chefe de pesquisa da NSA declarou em 2013:

> "Quando se trata de segurança, a complexidade não é sua amiga. De fato, foi dito que a complexidade é inimiga da segurança. Este é um aspecto que é frequentemente ressaltado em relação à segurança cibernética em vários contextos, incluindo tecnologia, codificação e política. A ideia básica é simples: à medida que os sistemas de software se tornam mais complexos, eles apresentam mais falhas, e essas falhas

serão exploradas pelos adversários cibernéticos". [36]

Temos uma ilustração muito real do problema da complexidade em uma análise recente de um dos sistemas de segurança mais importantes da Internet: SSL/TLS. O sistema de Segurança da Camada de Transporte (*Transport Layer Security - TLS*) e seu antecessor Camada de Soquete Seguro (*Secure Socket Layer - SSL*) são os mecanismos pelos quais a maior parte da Web faz a encriptação do seu tráfego – sempre que um usuário efetuar login em uma conta bancária, realizar compras eletrônicas ou se comunicar em redes sociais, o usuário está confiando no bom funcionamento dos sistemas SSL/TLS. Tudo que o usuário precisa saber de toda essa complexidade é que o ícone ou a chave devem ser exibidos na janela do navegador. Isso indica que a comunicação entre o usuário e o *site* remoto está protegida contra interceptação.

Infelizmente, escrever código que implemente corretamente esses protocolos criptográficos revelou-se difícil; proteções enfraquecidas tornam o processo ainda mais trabalhoso. Por exemplo, o OpenSSL, software usado por cerca de dois terços dos *sites* para fazer a encriptação TLS, tem sofrido com *bugs* de sistema, resultando em vulnerabilidades catastróficas. O infame *Heartbleed bug* foi causado pela falta de uma verificação de limites perdidos (*missing bounds check*), um erro de programação elementar que permaneceu despercebido no código por dois anos, deixando 17% de todos os *sites* vulneráveis ao furto de dados. Vulnerabilidades mais recentes, no entanto, foram causadas por restrições herdadas da exportação de algoritmos criptográficos, que remontam às Guerras Criptográficas. O fato de haver tantas implementações diferentes de TLS, todas com interoperabilidade para tornar a Web segura, provou ser uma verdadeira fonte de risco de segurança [37]. Os operadores de *sites* estão relutantes em mudar para protocolos mais seguros, caso isso implique na perda, mesmo em um pequeno percentual, de potenciais clientes que ainda utilizam software antigo, evidenciando que as vulnerabilidades deliberadamente introduzidas durante as Guerras Criptográficas persistem até hoje. A introdução de novos requisitos de acesso excepcional e complexos também adicionará mais *bugs* de segurança que ainda permanecerão escondidos em nossa infraestrutura de software por décadas.

Em terceiro lugar, existem riscos mais amplos para a tecnologia de vigilância mal implantada. Mecanismos de acesso excepcional projetados para uso dos órgãos de aplicação da lei foram explorados por atores hostis no passado. Entre 1996 e 2006, verificou-se que informantes de dentro da *Telecom Italia* permitiram a escuta de 6.000 pessoas, incluindo líderes empresariais, financeiros e políticos, juízes e jornalistas [38]. Em um país de 60 milhões de pessoas, isso significa que nenhum grande negócio ou acordo político era realmente privado. A motivação aqui parecia ser dinheiro, incluindo a possibilidade de chantagem. Como em exemplo anterior, de 2004 a 2005, os telefones celulares de 100 membros seniores do governo grego foram grampeados, dentre eles, o

primeiro-ministro, o chefe do Ministério da Defesa Nacional, o chefe do Ministério da Justiça e outros. A *Vodafone Greece* adquiriu uma central telefônica da Ericsson. A empresa de telefonia grega não havia adquirido recursos de escutas telefônicas, mas estes foram adicionados durante uma atualização na central em 2003. Como a *Vodafone Greece* não tinha disponibilizado recursos de interceptação, a empresa não estava habilitada a acessar recursos associados, como auditoria. No entanto, alguém agindo sem autorização legal foi capaz de ativar os recursos de interceptação e mantê-los funcionando por dez meses, sem ser detectado. A vigilância só foi descoberta quando algumas mensagens de texto apresentaram erros. Embora as técnicas utilizadas tenham sido compreendidas, o responsável pela vigilância permanece desconhecido [19].

Em seguida, houve elevação de custos para a economia. O crescimento econômico vem em grande parte da inovação em ciência, tecnologia e processos de negócios. Atualmente, o progresso tecnológico se dá em grande parte sobre a incorporação de inteligência – software e comunicações – em todos os lugares. Produtos e serviços que eram autônomos agora vêm com um aplicativo de celular, um serviço da Web *online* e modelos de negócios que envolvem anúncios ou assinatura. Sendo esses cada vez mais "sociais" e permitindo aos usuários conversar com seus amigos e atraí-los para o *Web marketing* do fornecedor. Países que exigem que esses novos aplicativos e serviços da Web tenham suas funções de comunicação de usuário-para-usuário (*user-to-user*) autorizadas pelo governo estarão em significativa desvantagem. Atualmente, o mundo usa amplamente aplicativos e serviços dos EUA, em vez de aplicativos aprovados pelo governo da Rússia e da China, proporcionando, assim, enorme alavancagem para as empresas dos Estados Unidos.

Finalmente, essa vantagem de mercado oferece benefícios reais não apenas economicamente, mas em relação ao poder de influência e liderança moral. A Internet aberta tem sido uma meta de política externa dos Estados Unidos e de seus aliados por vários bons motivos. A credibilidade do Ocidente nesta questão foi prejudicada pelas revelações de Snowden, mas pode e deve se recuperar. Legisladores não devem arriscar os reais benefícios econômicos, geopolíticos e estratégicos de uma Internet aberta e segura, por ganhos dos órgãos de aplicação da lei que sejam, na melhor das hipóteses, menores e táticos.

3 Riscos de segurança relacionados às exigências de aplicação da lei no *common law* através de acesso excepcional

Haja vista não haver uma declaração específica de requisitos legais para acesso excepcional por órgãos de aplicação e execução da lei, consideramos o que entendemos ser um conjunto muito geral de necessidades de vigilância eletrônica, aplicável em várias jurisdições em todo o mundo. Nosso objetivo aqui é entender a natureza geral dos riscos de segurança associados à aplicação das exigências de acesso excepcional, no contexto das categorias tradicionais de vigilância eletrônica. Órgãos de diferentes países apresentaram exigências diferentes em momentos diferentes, que são tratadas em quatro categorias: acesso a conteúdo de comunicações, acesso a dados de comunicações, acesso ao conteúdo em repouso e ponto de acesso (*endpoint*) secreto. Todos os tipos de acesso devem ser controlados e passíveis de auditoria de acordo com os requisitos legais locais; por exemplo, observando os requisitos legais dos EUA, deve-se respeitar a segurança e a privacidade das comunicações não direcionadas.[8]

3.1 Acesso ao conteúdo de comunicações

A maioria das forças policiais tem permissão para acessar dados suspeitos. Nos países que respeitam o Estado de direito, esse acesso é cuidadosamente regulado por leis e supervisionado por um judiciário independente, embora a maioria da população mundial não desfrute de tais proteções legais. O acesso por parte dos órgãos de aplicação da lei pode ser a um banco de dados central de mensagens não encriptadas, onde isso existe em um provedor central. Não havendo um banco de dados central, como no caso de um telefone ou chamada de vídeo, a polícia deve grampear a comunicação enquanto ela ocorre. Mas como um requisito de acesso excepcional pode ser implementado para permitir o acesso ao conteúdo de comunicações? Se os dados forem encriptados, o mecanismo mais óbvio para permitir o acesso da polícia exigiria que o tráfego entre Alice no país X e Bob no país Y tivesse a chave de sua sessão também encriptada sujeita às chaves públicas das forças policiais em X e Y ou de terceiros de sua confiança. Isso, no entanto, implica em sérios problemas.

Primeiro, qualquer exigência de custódia restringirá outras funcionalidades importantes de segurança, como o *forward secrecy*, o uso de identidades transitórias e a

[8] Nos Estados Unidos, 47 USC 1002(a)(4)

forte privacidade do local. Conforme ilustrado na análise do cenário acima, um requisito de acesso excepcional sobreposto à tradicional vigilância de conteúdo colocará em risco a segurança do mesmo. Quando há condições para fornecer acesso excepcional a órgãos de aplicação da lei, tais condições podem ser indevidamente utilizadas por outros.

Em segundo lugar, a natureza global dos serviços de Internet faz com que a conformidade com as regras de acesso excepcional seja difícil tanto de definir como de aplicar. Se o software vendido no país X copiar todas as chaves para o governo daquele país, os criminosos poderão simplesmente comprar seu software de países que não cooperam; assim, nos Estados Unidos criminosos poderiam adquirir seus softwares da Rússia. E se o software escolher automaticamente quais governos copiar, usando uma técnica como a geolocalização por IP, como evitar ataques baseados na dissimulação de localização? Embora seja possível projetar sistemas de telefonia móvel para que as jurisdições de acolhimento (*host jurisdictions)* tenham acesso ao tráfego (desde que os usuários não recorram ao *VoIP*), essa é uma tarefa muito mais difícil para aplicativos de mensagens de uso geral.

Terceiro, pode ser necessário detectar ou dissuadir empresas que não fornecem acesso excepcional, provocando problemas relacionados à certificação e à aplicação da lei. Por exemplo, se os Estados Unidos ou o Reino Unido proibirem o uso de aplicativos de mensagens não certificados conforme uma nova lei de custódia, esses aplicativos serão bloqueados no *firewall* nacional? O *Tor* será então bloqueado, como na China? Ou será simplesmente um crime usar esse software? E qual é o efeito sobre a inovação se todo novo produto de comunicação tiver que passar por avaliação supervisionada pelo governo contra algum novo perfil de proteção de custódia de chaves?

3.2 Acesso aos dados de comunicações

Os dados de comunicações tradicionalmente significavam registros detalhados de chamadas e (desde que os telefones celulares se tornaram comuns) histórico de localização do autor da chamada; obtidos por intimação de empresas de telefonia e usados na investigação de crimes violentos mais graves, como assassinato, estupro e roubo. Os dados de comunicações permanecem amplamente disponíveis, pois os provedores de serviços os mantêm por algum tempo para fins internos. No entanto, as forças policiais fora dos EUA reclamam que a mudança para serviços globalizados de mensagens dificulta a obtenção de muitos dados. Por exemplo, os e-mails agora são normalmente transmitidos com o uso de encriptação TLS; isto é, a mensagem é encriptada entre o computador do usuário e o provedor de serviços (por exemplo, Google para Gmail, Microsoft para Hotmail, etc.). Assim, para adquirir as comunicações em texto simples, o órgão competente deve apresentar ao provedor de e-mail uma ordem judicial. Uma nova lei de vigilância do Reino

Unido pode exigir que empresas de serviços de mensagens como Apple, Google e Microsoft honrem tais pedidos de forma ágil e direta, como condição para realizar negócios no Reino Unido. Assim, haverá disposições uniformes para o acesso a dados de comunicações sujeitos a disposições para mandados ou intimações, transparência e jurisdição?

Como já observado, determinar a localização não é trivial, e burlar esse processo (usando softwares, *VPNs* e outros proxies estrangeiros) pode ser fácil. Criminosos se voltariam para aplicativos de mensagens não autorizados, levantando questões de aplicação da lei. A aplicação rígida da lei pode impor custos reais à inovação e à indústria em geral.

3.3 Acesso a dados em repouso

Os dados de comunicações são uma instância dentro do problema geral de acesso a dados em repouso. Quase todos os países permitem que suas forças policiais tenham acesso a dados. Onde o Estado de direito básico estiver em vigor, o acesso ocorre mediante a autorização de documento jurídico, como mandado ou intimação, ressalvados determinados limites. Diversas empresas já insistem em obter custódia de chaves usadas para proteger dados corporativos em repouso (como o *BitLocker* em *laptops* corporativos). Portanto, esse é um campo com "solução" de custódia já implantada: um investigador de fraude que deseja acesso a um *laptop* de um comerciante desonesto de Londres pode simplesmente pedir a um policial que envie uma notificação de desencriptação ao CEO do banco. Mas, ainda assim, muitos dos mesmos problemas surgem. Os suspeitos podem usar um software de encriptação que não possua capacidade de custódia, ou que falhe em custodiar a chave adequadamente, ou poderão alegar ter esquecido a senha ou, de fato, ter esquecido. O responsável pela custódia poderá estar em outra jurisdição ou ser uma outra parte adversária em litígios. Em outras palavras, o que funciona razoavelmente bem para fins corporativos, ou em um setor razoavelmente bem regulado em uma única jurisdição, simplesmente não se adapta a um ecossistema global de tecnologias, serviços e sistemas legais altamente diversificados.

Outro caso complexo de acesso a dados em repouso surge quando os dados só estão presentes ou são acessíveis via *laptop* pessoal, *tablet* ou telefone celular do suspeito. Hoje, caso policiais queiram capturar um suspeito usando serviços do *Tor*, eles podem ter que prendê-lo enquanto seu *laptop* estiver aberto em uma sessão ao vivo. Os órgãos policiais em alguns países podem obter um mandado para instalar *malware* no computador de um suspeito. Essas agências prefeririam que as empresas de antivírus não detectassem seu *malware*; alguns podem até esperar que os fornecedores os ajudem, talvez mediante mandado para instalar uma atualização com ferramentas de monitoramento remoto em um dispositivo com número de série específico. Os mesmos problemas surgem com este

tipo de acesso excepcional, e com as questões familiares oriundas do acesso da polícia secreta à residência de um suspeito para realizar buscas secretas, ou instalar dispositivo de escuta. Tal acesso excepcional comprometeria gravemente a confiança e sofreria grande resistência dos fornecedores.

4 Princípios em jogo e perguntas não respondidas

Com a vida e a liberdade das pessoas cada vez mais digital, a questão de se responder às demandas dos órgãos de aplicação da lei para garantir acesso a informações privadas tem uma urgência especial e deve ser avaliada com clareza. Do ponto de vista da política pública, há um argumento para fornecer a esses órgãos as melhores ferramentas possíveis para investigar crimes, respeitando um processo justo e o Estado de direito. Mas uma análise científica cuidadosa do provável impacto de tais demandas deve distinguir o que poderia ser desejável do que é tecnicamente possível. Nesse sentido, uma proposta para regular a encriptação e garantir acesso aos órgãos competentes se assemelha a uma proposta de exigir que todos os aviões possam ser controlados do solo. Embora isso possa ser desejável no caso de um sequestro ou um piloto suicida, uma avaliação clara de como seria possível projetar tal capacidade revela que há enorme complexidade técnica e operacional, escopo internacional, custos elevados e enormes riscos – tanto que tais propostas, embora feitas ocasionalmente, não são realmente levadas a sério.

Mostramos que as exigências atuais dos órgãos de aplicação da lei para acesso excepcional provavelmente envolveriam riscos substanciais de segurança, custos de engenharia e efeitos colaterais. Se os formuladores de políticas acreditarem que ainda é necessário considerar mandados de acesso excepcional, há questões técnicas, operacionais e jurídicas que devem ser respondidas em detalhes antes que a legislação seja elaborada. A partir de nossa análise dos dois cenários e dos requisitos gerais de acesso por parte dos órgãos de aplicação da lei, apresentados anteriormente no documento, oferecemos este conjunto de perguntas.

4.1 Escopo, limitações e liberdades

O primeiro conjunto de perguntas que uma proposta de acesso excepcional deve abordar diz respeito: ao âmbito de aplicação do requisito de acesso excepcional; a quaisquer limitações ao mandado; e a quais liberdades do usuário permaneceriam protegidas sob tais propostas. Perguntas como estas surgem nesta categoria:

1. Todos os sistemas que usam encriptação são cobertos ou apenas alguns? Quais?
2. Todas as comunicações *online* e plataformas de informação precisam fornecer acesso a texto simples, ou simplesmente fornecer chaves para agências que já haviam coletado o texto criptografado usando meios técnicos?
3. Pessoas, corporações, instituições sem fins lucrativos ou governos poderiam implantar serviços adicionais de encriptação sobre esses sistemas com acesso excepcional? Esses sistemas instalados pelo usuário também teriam que atender a

requisitos de acesso excepcional?

4. Os sistemas *machine-to-machine* seriam cobertos? E quanto aos sistemas da Internet das Coisas e de controle industrial (SCADA)? Muita troca de informações ocorre de uma máquina para outra, como: a comunicação de dados pessoais de saúde de um sensor para um *smartphone*, dispositivos de detecção agrícola baseados em campo para tratores, ou controles de balanceamento de carga em sistemas de distribuição de energia elétrica, gás, óleo e água.
5. Como as diferenças regulatórias dos países seriam resolvidas? Os desenvolvedores de tecnologia teriam que atender aos requisitos de acesso excepcional pertinentes em cada jurisdição onde seus sistemas são usados? Ou haveria um conjunto globalmente harmonizado de requisitos regulamentares?
6. Como pode o projeto técnico de um sistema de acesso excepcional impedir a vigilância em massa que violaria secretamente os direitos de populações inteiras, embora ainda permitindo a vigilância secreta de poucos suspeitos como uma "exceção" real a uma regra geral de privacidade do cidadão?
7. Haveria uma exceção para pesquisa e ensino?
8. Poderiam as empresas se recusar a cumprir as regras de acesso excepcional baseadas no medo de violações dos direitos humanos?
9. Comunicações anônimas, amplamente reconhecidas como vitais para as sociedades democráticas, seriam permitidas?

4.2 Planejamento e design/projeto

Projetar a tecnologia e planejar os procedimentos administrativos que seriam necessários para implementar um sistema de acesso excepcional abrangente levanta muitas questões:

1. Quais são as estimativas de custo e benefício para esse programa? Nenhum sistema é gratuito e esse pode ser muito caro, especialmente se tiver que acomodar um grande número de provedores, como os atuais milhões de desenvolvedores de aplicativos.
2. Quais medidas de segurança e confiabilidade seriam estabelecidas para o projeto? Como os protótipos do sistema seriam testados? Por quanto tempo as empresas teriam que cumprir regras de acesso excepcional?
3. Como os serviços e produtos existentes seriam tratados se não cumprissem regras de acesso excepcional? Os provedores teriam que reprojetar seus sistemas? E se esses sistemas não puderem acomodar requisitos de acesso excepcional?

4. Quem estaria envolvido no projeto dos sistemas e procedimentos – apenas o governo dos Estados Unidos, ou outros governos seriam convidados a participar? Poderiam fornecedores de tecnologia estrangeiros, como a Huawei, participarem das discussões sobre o projeto?
5. Os detalhes técnicos do programa seriam divulgados e abertos para revisão técnica? Que nível de garantia seria fornecido para o projeto?
6. Observamos que geralmente levam muitos anos para que um protocolo criptográfico seja publicado até que seja considerado seguro o suficiente para uso real. Por exemplo, o protocolo de chave pública *Needham-Schroeder*, publicado pela primeira vez em 1978 [39], só apresentou falhas de segurança comprovadamente em 1995 por Gavin Lowe (17 anos depois!) [40].

4.3 Implementação e operação

Uma vez estabelecidos os regulamentos e definidos os parâmetros técnicos do projeto, restariam dúvidas sobre como os sistemas seriam implementados, quem supervisionaria e regulamentaria as questões de *compliance*, e como o projeto do sistema evoluiria para resolver os inevitáveis erros técnicos e operacionais resultantes. Não conhecemos quaisquer sistemas que tenham sido projetados com perfeição na primeira vez, e é fato que a manutenção, o suporte e a evolução dos sistemas existentes constituem uma despesa importante.

1. Quem supervisionaria as questões de *compliance*? Uma agência reguladora existente, como a FCC, teria jurisdição sobre todo o processo? Como outros países regulamentariam os serviços nacionais e estrangeiros dos EUA? Haveria uma harmonização global da regulamentação e aplicação de normas? A União Internacional de Telecomunicações teria um papel na definição e aplicação de requisitos?
2. Seriam necessários padrões técnicos globais? Como isso seria desenvolvido e aplicado? Como esses padrões seriam alterados/aprimorados/corrigidos? Os organismos tradicionais, como o setor-T da União Internacional das Telecomunicações da ONU e os padrões ISO, ou o mundo passaria a prestar atenção nos organismos de normalização da Internet, como o IETF e Consórcio *World Wide Web*? Como o mundo convergiria para um conjunto de *standards*?
3. O governo dos EUA forneceria bibliotecas de software de referência, implementando a funcionalidade desejada?
4. Programas e aplicativos precisariam ser certificados antes de serem vendidos? Quem

testaria ou certificaria que os programas produzidos estariam operando como pretendido?

5. Quem seria responsável se os mecanismos de divulgação de texto simples apresentassem erros (tanto em termos de projeto como de implementação), causando a divulgação de todas as informações dos cidadãos? De forma mais geral, o que aconteceria quando (e não "se") informações secretas críticas fossem reveladas, como as chaves privadas que permitem que dados encriptados sejam lidos por qualquer pessoa, destruindo a posição privilegiada do órgão de aplicação da lei?
6. Quantas empresas teriam que retirar sua equipe de vendas, com exceção do pessoal local, de dentro dos mercados onde o acesso excepcional fosse obrigatório, de forma conflitante com suas estratégias de negócios ou com os direitos dos usuários em outros países, como o Google já fez no caso da China e da Rússia?

4.4 Verificação, avaliação e evolução

Grandes sistemas existem porque os sistemas bem-sucedidos evoluem e crescem. Normalmente, essa evolução acontece por meio de uma interação orientada pela instituição (empresa de software, agência governamental ou comunidade de código aberto) responsável pelo sistema. Um sistema que evolui sujeito a um conjunto de restrições, como sistemas médicos que precisam manter um plano de segurança ou sistemas de controle de voo que precisam manter não apenas um plano de segurança, mas também precisam atender aos requisitos de desempenho em tempo real, evolui menos rapidamente e com maior custo. Se todos os sistemas que se comunicam deverão, no futuro, evoluir sujeitos a uma restrição de acesso excepcional, haverá custos reais, que serão difíceis de quantificar, já que a questão de quem exatamente seria responsável pelo estabelecimento e policiamento da restrição de acesso excepcional não é clara. No entanto, se essa pergunta for respondida, surgirão mais algumas questões.

1. Qual programa de supervisão seria necessário para monitorar a eficácia, o custo, os benefícios e o abuso em termos de acesso excepcional?
2. Que medidas, em termos de prazo de vigência, seriam incorporadas na legislação para tal programa? Quais condições estariam em vigor para o seu término (por exemplo, por falta de benefício suficiente, por custo excessivo ou por abuso excessivo)?
3. Uma consequência não intencional de tal programa pode ser um uso muito reduzido de criptografia completa. Isso enfraqueceria ainda mais nossa infraestrutura de informações, já frágil e insegura; sendo assim, como incentivamos as empresas a continuarem encriptando as comunicações confidenciais do usuário?

4. Uma outra consequência não intencional de tal programa pode ser tornar os Estados Unidos e outros países participantes menos receptivos à inovação tecnológica. A diminuição ou deslocamento da inovação pode ter consequências para o crescimento econômico e a segurança nacional. Como esses impactos econômicos serão avaliados antes que um programa de acesso excepcional seja exigido? Além disso, que efeito econômico seria considerado muito impactante para que o acesso excepcional fosse considerado válido?

5 Conclusão

Mesmo que os cidadãos precisem da aplicação da lei para se protegerem no mundo digital, todos os formuladores de políticas, empresas, pesquisadores, indivíduos e agentes da lei têm a obrigação de trabalhar para tornar nossa infraestrutura de informação global mais segura e confiável. A análise deste relatório sobre demandas de aplicação da lei para acesso excepcional a comunicações e dados privados mostram que esse acesso abrirá as portas através das quais criminosos e Estados-nação maliciosos podem atacar os próprios indivíduos que a lei procura defender. Os custos seriam substanciais, os danos à inovação severos, e as consequências para o crescimento econômico difíceis de prever. Os custos para a influência dos países desenvolvidos e para nossa autoridade moral também seriam consideráveis. Os formuladores de políticas precisam ter clareza na avaliação dos prováveis custos e benefícios. Não é surpresa que este relatório tenha terminado com mais perguntas do que respostas, já que os requisitos para acesso excepcional ainda são vagos. Se os órgãos de aplicação da lei forem priorizar o acesso excepcional, recomendamos que eles forneçam evidências para documentar seus requisitos e, em seguida, desenvolvam especificações genuínas e detalhadas para o que eles esperam que os mecanismos de acesso excepcional façam. Como cientistas da computação e especialistas em segurança, estamos comprometidos em permanecer engajados no diálogo com todas as partes de nossos governos, para ajudar a discernir o melhor caminho através dessas questões complexas.

6 Referências

[1] H. Abelson, R. N. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P. G. Neumann, R. L. Rivest, J. I. Schiller, *et al.*, *The risks of key recovery, key escrow, and trusted third-party encryption*. 1997. Disponível em: http://academiccommons.columbia.edu/catalog/ac:127127

[2] *Advanced Telephony Unit, Federal Bureau of Investigation, "Telecommunications Overview, slide on Encryption Equipment*. 1992. Disponível em: https: //www.cs.columbia.edu/~smb/Telecommunications Overview 1992.pdf

[3] E. Nakashima. *Chinese hackers who breached Google gained access to sensitive data, U.S. officials say*. The Washington Post, Maio de 2013. Disponível em: https://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/ 2013/05/20/51330428-be34-11e2-89c9-3be8095fe767 story.html

[4] K. W. Dam, H. S. Lin, *et al. Cryptography's role in securing the information society*. National Academies Press. 1996.

[5] James B. Comey. *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?*. Outubro de 2014. Disponível em: https://www.fbi.gov/news/speeches/ going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

[6] David Cameron. *PM: spy agencies need more powers to protect Britain*. Janeiro de 2015. Disponível em: https://embed.theguardian.com/embed/video/uk-news/ video/2015/jan/12/david-cameron-spy-agencies-britain-video

[7] W. Diffie e S. Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, Mass: The MIT Press, Janeiro de 1998.

[8] Paul Ford. *The Obamacare Website Didn't Have to Fail. How to Do Better Next Time*. Outubro de 2013. Disponível em: http://www.bloomberg.com/bw/articles/ 2013-10-16/open-source-everything-the-moral-of-the-healthcare-dot-gov-debacle

[9] D. Eggen and G. Witte. *The FBI's Upgrade That Wasn't*. The Washington Post, Agosto de 2006. Disponível em: http://www.washingtonpost.com/wp-

dyn/content/ article/2006/08/17/AR2006081701485.html

[10] Jaikumar Vijayan. *TJX data breach: At 45.6m card numbers, it's the biggest ever*. Março de 2007. Disponível em: http://www.computerworld.com/article/2544306/ security0/tjx-data-breach--at-45-6m-card-numbers--it-s-the-biggest-ever.html

[11] Brian Krebs. *Security fix payment processor breach may be largest ever*. Janeiro de 2009. Disponível em: http://voices.washingtonpost.com/securityfix/2009/01/ payment processor breach may b.html

[12] R. Abelson and M. Goldstein. *Anthem Hacking Points to Security Vulnerability of Health Care Industry*. The New York Times, Fevereiro de 2015. Disponível em: http://www.nytimes.com/2015/02/06/business/ experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html

[13] N. Thornburgh. *The Invasion of the Chinese Cyberspies*. Time, Agosto de 2005. Disponível em: http://content.time.com/time/magazine/article/0,9171,1098961,00.html

[14] William J. Lynn III. *Defending a New Domain*. Foreign Affairs, Outubro de 2010. Disponível em: https://www.foreignaffairs.com/articles/united-states/ 2010-09-01/defending-new-domain

[15] Arthur Coviello. *Open Letter from Arthur Coviello, Executive Chairman, RSA, Security Division of EMC, to RSA customers*. Março de 2011.

[16] Jeanne Meserve. *Sources: Staged cyber attack reveals vulnerability in power grid CNN.com*. CNN, Setembro de 2007. Disponível em: http://www.cnn.com/2007/US/ 09/26/power.at.risk/index.html?iref=topnews

[17] K. Zetter. *A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever*. Janeiro de 2015. Disponível em: http://www.wired.com/2015/ 01/german-steel-mill-hack-destruction/

[18] R. George. *Views on the future direction of information assurance*. Julho de 2002. Disponível em: https://www.blackhat.com/presentations/bh-usa-02/bh-us-02-george-keynote.doc

[19] V. Prevelakis and D. Spinellis. *The athens affair*. Spectrum, IEEE, vol. 44, no. 7, pp. 26–33, 2007. Disponível em: http://ieeexplore.ieee.org/xpls/abs all.

jsp?arnumber=4263124

[20] Tom Cross. *Exploring Lawful Intercept to Wiretap the Internet*. Washington, DC, USA, 2010. Disponível em: https://www.blackhat.com/presentations/bh-dc-10/ Cross Tom/BlackHat-DC-2010-Cross-Attacking-LawfulI-Intercept-slides.pdf

[21] Richard George. *Private communication between Richard George, Former Technical Director, Information Assurance Directorate, NSA and Susan Landau*. Dezembro de 2011.

[22] Nicole Perlroth and Vindu Goel. *Twitter Toughening Its Security to Thwart Government Snoops*. Novembro de 2013. Disponível em: http://bits.blogs.nytimes.com/2013/11/22/twitter-toughening-its-security-to-thwart-government-snoops/

[23] Larry Seltzer. *Google moves forward towards a more perfect SSL*. Novembro de 2013. Disponível em: http://www.zdnet.com/article/ google-moves-forward-towards-a-more-perfect-ssl/

[24] D. Gupta. *Google Enables 'Forward Secrecy (PFS)' by 'Default' for HTTPS Services*. Novembro de 2011. Disponível em: http://www.ditii.com/2011/11/23/ google-enables-forward-secrecy-pfs-by-default-for-https-services/

[25] Selena Larson. *After Heartbleed, "Forward Secrecy" Is More Important Than Ever*. Abril de 2014. Disponível em: http://readwrite.com/2014/04/15/ heartbleed-perfect-forward-secrecy-security-encryption

[26] Adam Langley. *Protecting data for the long term with forward secrecy*. Novembro de 2011. Disponível em: http://googleonlinesecurity.blogspot.com/2011/11/ protecting-data-for-long-term-with.html

[27] J. Kiss. *Twitter adds more security to thwart predators and government agencies*. Novembro de 2013. Disponível em: http://www.theguardian.com/technology/2013/nov/ 23/twitter-security-google-facebook-data-nsa

[28] Parker Higgins. *Pushing for Perfect Forward Secrecy, an Important Web Privacy Protection*. Agosto de 2013. Disponível em: https://www.eff.org/deeplinks/2013/ 08/pushing-perfect-forward-secrecy-important-web-privacy-protection

[29] Michael Mimoso. *Microsoft Expands TLS, Forward Secrecy Support*. Julho

de 2014. Disponível em: https: threatpost.com/microsoft-expands-tls-forward-secrecy-support/106965

[30] ____. *Microsoft Brings Perfect Forward Secrecy to Windows | Threatpost | The first stop for security news*. Maio de 2015. Disponível em: https://threatpost. com/new-crypto-suites-bring-perfect-forward-secrecy-to-windows/112783

[31] P. Bright. *Microsoft expands the use of encryption on Outlook, OneDrive*. Julho de 2014. Disponível em: http://arstechnica.com/security/ 2014/07/microsoft-expands-the-use-of-encryption-on-outlook-onedrive/

[32] Liam Tung. *Yahoo finally enables HTTPS encryption for email by default*. Janeiro de 2014. Disponível em: http://www.zdnet.com/article/ yahoo-finally-enables-https-encryption-for-email-by-default/

[33] Apple. *iOS Security on iOS 8.3 or Later*. Tech. Rep., Abril de 2015. Disponível em: https://www.apple.com/business/docs/iOS Security Guide.pdf

[34] N. Perlroth. *Electronic Security a Worry in an Age of Digital Espionage*. The New York Times, Fevereiro de 2012. Disponível em: http://www.nytimes.com/2012/ 02/11/technology/electronic-security-a-worry-in-an-age-of-digital-espionage.html

[35] Ben Thompson. *UAE Blackberry update was spyware*. BBC, Julho de 2009. Disponível em: http://news.bbc.co.uk/2/hi/8161190.stm

[36] Frederick R. Chang. *Is Your Data on the Healthcare.gov Website Secure?*. Written Testimony, U.S. House of Representatives, Novembro de 2013. Disponível em: http://docs.house.gov/meetings/SY/SY00/20131119/101533/ HHRG-113-SY00-Wstate-ChangF-20131119.pdf

[37] B. Beurdouche, K. Bhargavan, A. Delignat-Lavaud, C. Fournet, M. Kohlweiss,

A. Pironti, P.-Y. Strub, and J. K. Zinzindohoue. *A messy state of the union: Taming the composite state machines of TLS*. IEEE Symposium on Security and Privacy, 2015. Disponível em: https://www.smacktls.com/smack.pdf

[38] Piero Colaprico. *Da Telecom dossier sui Ds" Mancini parla dei politici cronaca Repubblica.it*. Janeiro de 2007. Disponível em: http://www.repubblica.it/2006/12/ sezioni/cronaca/sismi-mancini-8/dossier-ds/dossier-ds.html

[39] R. M. Needham and M. D. Schroeder. *Using encryption for authentication in large networks of computers*. Communications of the ACM, vol. 21, no. 12, pp. 993–999, 1978. Disponível em: http://dl.acm.org/citation.cfm?id=359659

[40] G. Lowe. *An Attack on the Needham-Schroeder Public-key Authentication Protocol*. Information Processing Letters, vol. 56, no. 3, pp. 131–133, Novembro de 1995. Disponível em: http://dx.doi.org/10.1016/0020-0190(95)00144-2

7 Biografias dos autores

Harold "Hal" Abelson é professor de engenharia elétrica e ciência da computação no MIT, membro do IEEE e diretor fundador do Creative Commons e da Free *Software* Foundation.

Ross Anderson é professor de engenharia de segurança na Universidade de Cambridge.

Steven M. Bellovin é o Professor Percy K. e Vida LW Hudson de ciência da computação na Columbia University.

Josh Benaloh é criptógrafo sênior da Microsoft Research, sua pesquisa se concentra em protocolos eleitorais verificáveis e tecnologias relacionadas.

Matt Blaze é professor associado de ciência da computação e informação na Universidade da Pensilvânia, onde dirige o Laboratório de Sistemas Distribuídos.

Whitfield "Whit" Diffie é criptógrafo norte-americano, cuja descoberta em 1975 do conceito de criptografia de chave pública abriu a possibilidade de comunicações seguras em escala na Internet.

John Gilmore é um empreendedor e libertário civil. Ele foi um dos primeiros funcionários da Sun Microsystems, e co-fundador da Cygnus Solutions, a Electronic Frontier Foundation, os Cypherpunks e os grupos de notícias alternativos da Internet.

Matthew Green é professor pesquisador do Instituto de Segurança da Informação da Universidade Johns Hopkins. Seu foco de pesquisa é em técnicas criptográficas para manter a privacidade dos usuários e em novas técnicas para implantar protocolos de mensagens seguras.

Peter G. Neumann, cientista-chefe sênior do SRI International Computer Science Lab, e moderador do Fórum de Riscos da ACM há trinta anos.

Susan Landau é professora de política de segurança cibernética no Worcester Polytechnic Institute. É a autora de *Surveillance or Security? The Risks Posed by New Wiretapping Technologies* (MIT Press, 2011) e coautora, com Whitfield Diffie, de *Privacy on the Line: The Politics of Wiretapping and Encryption* (MIT Press, 1998).

Ronald L. Rivest é professor do Instituto MIT e conhecido por sua co-invenção do sistema criptográfico de chave pública RSA, bem como a fundação da RSA Security e da Verisign.

Jeffrey I. Schiller foi diretor da área de segurança do grupo de orientação em engenharia de Internet (1994–2003).

Bruce Schneier é tecnólogo de segurança, autor, membro do Centro Berkman para Internet e Sociedade na Harvard Law School, e o CTO da Resilient Systems, Inc. Ele escreveu vários livros, incluindo *Dados e Golias: As batalhas ocultas para coletar seus dados e controlar seu mundo* (Norton, 2015).

Michael A. Spectre é pesquisador de segurança e candidato a PhD em ciência da computação no laboratório de ciência da computação e inteligência artificial do MIT.

Daniel J. Weitzner é pesquisador-chefe do Laboratório de Inteligência Artificial e Ciência da Computação do MIT e diretor fundador, MIT Cybersecurity e Internet Policy Research Initiative. De 2011 a 2012, ele foi vice-diretor de tecnologia dos Estados Unidos na Casa Branca.

8 Agradecimentos

Os autores agradecem a várias pessoas que foram extremamente úteis na produção deste relatório. Alan Davidson foi fundamental nas primeiras discussões que levaram a este relatório, enquanto ele era vice-presidente e diretor do Open Technology Institute da New America Foundation. Beth Friedman, comunicadora técnica da Resilient Systems, forneceu um essencial apoio de edição. A iniciativa de pesquisa em políticas de Internet e segurança cibernética do MIT ajudou a reunir os autores e a produzir a versão final do relatório.