technology review.es
Published by MIT

Segunda-feira, 05 de agosto de 2013

Avanços na Matemática Trazem a Tona a Perspectiva de uma Crise de Segurança da Internet

Avanços acadêmicos sugerem que os sistemas de criptografia que protegem as comunicações on-line podem ser prejudicados em poucos anos.
Por Tom Simonite

Os sistemas de criptografia usados para proteger as contas bancárias on-line e manter comunicações críticas privadas podem ser desfeitos em poucos anos, pesquisadores de segurança alertaram na Conferência Black Hat, em Las Vegas na última Quinta-Feira. Avanços em pesquisa no campo da matemática feitos nos últimos seis meses poderiam sustentar maneiras práticas e rápidas para decodificar dados criptografados que são considerados inquebráveis hoje.

Alex Stamos, diretor chefe de tecnologia da empresa de segurança on-line Artemis, liderou uma apresentação descrevendo como ele e outros três pesquisadores de segurança estudaram recentes publicações do mundo insular de pesquisa cryptopgráfica acadêmica, que abrange as tendências em atacar esquemas de criptografia mais comuns.

"Nossa conclusão é de que há uma pequena, mas definitiva chance de que RSA e o clássico Diffie-Hellman não poderão ser usadas para fins de criptografia em quatro a cinco anos" disse Stamos, referindo-se os dois métodos de criptografia mais usados.

Qualquer indício de que esses métodos poderiam ser prejudicados devem ser levados a sério, disse Stamos. Eles são usados para proteger bancos on-line, comércio on-line e e-mails, bem como mecanismos que assegurem que as atualizações baixadas por sistemas operacionais como Windows e OSX são genuínos. O resultado dos dois métodos de criptografia serem quebrados seria, disse Stamos "um fracasso total de confiança na Internet."

Ambas a criptografia RSA e Diffie-Hellman são sustentadas por um desafio matemático conhecido como o problema do logaritmo discreto. Esse problema é difícil de resolver computacionalmente, assegurando que os dados encriptados só podem ser decodificadas rapidamente com o conhecimento da chave secreta usada para codificar as informações. Decifrar a criptografia RSA ou Diffie-Hellman hoje requer o uso de grandes recursos de computação por períodos de tempo significativos.

No entanto, é possível que os algoritmos capazes de resolver o problema do logaritmo discreto rapidamente possam existir. "Contamos com que o algoritmo eficiente não seja encontrado", disse Jarved Samuel, um criptógrafo que trabalha para a consultoria de segurança ISEC Partners e que apresentou ao lado de Stamos. "Se for encontrado o sistema de criptografia está quebrado."

No início deste ano, o acadêmico francês Antoine Joux publicou dois artigos que sugerem que tal algoritmo pode ser encontrado logo. "Isso é algo importante, já que houve progresso marginal por 25 anos", disse Samuel. "Isso vai estimular pesquisadores a olhar mais de perto para o problema e provavelmente resultará em mais progresso."

Uma razão para acreditar que o progresso será rápido, diz Samuel, é que os avanços do Joux não foram baseados em inventar técnicas completamente novas. Em vez disso, ele aplicou truques conhecidos que não haviam sido utilizados com esse problema específico. Quebrar a criptografia RSA exigiria um pouco mais de trabalho adicional, nota Samuel, porque depende menos diretamente do problema do logaritmo discreto do que a criptografia Diffie-Hellman.

No entanto, Stamos acredita que assim que um matemático publicar uma técnica boa o suficiente, seria rapidamente usada em ataques online. "Joux ou um desses caras poderiam ter um avanço, jogá-lo em uma listas de discussão sobre criptografia e uma implementação prática pode ser criada em um ou dois dias", disse ele.

Philippe Courtot, CEO da empresa de segurança Qualys, destacou a apresentação de Stamos em um breve discurso que abriu a Conferência Black Hat na quarta-feira. "O protocolo RSA, que é a base da segurança na Internet é susceptível de ser decifrado em um futuro muito próximo", disse ele, observando que enquanto a indústria de segurança de computadores foi sustentada por apenas um punhado de esquemas de chave de criptografia "somos muito lentos em adaptá-los."

Stamos pediu para o setor de segurança pensar em como se afastar de Diffie-Hellman e RSA e, especificamente, para usar uma alternativa conhecida como criptografia de curva elíptica (ECC), que é significativamente mais jovem, mas conta com desafios matemáticos mais difíceis para proteger os dados criptografados.

A Agência de Segurança Nacional dos EUA há anos tem recomendado a ECC como a proteção criptográfica mais confiável disponível. Em 2005, a agência lançou um kit de ferramentas chamado SuiteB com algoritmos de criptografia para ser usado para proteger as informações do governo. SuiteB faz uso da ECC e evita RSA e Diffie-Hellman. Um kit de ferramentas de criptografia secreto, SuiteA, é usado internamente pela NSA e também se acredita que ele seja baseado em ECC.

O governo russo também se afastou da RSA para dados sensíveis e declassificou o seu próprio kit de ferramentas de criptografia que utiliza ECC. Quando a Rússia precisava renovar o método para a identificação de seus domínios Web .ru, ele insistiu que seus algoritmos ECC fossem usados.

Implementações da ECC foram pioneiras e patenteadas por uma empresa chamada Certicom que é agora uma subsidiária da fabricante do telefone BlackBerry. Embora o governo dos EUA tenha adquirido licenças que permitam o uso da ECC por si e seus contratantes, outras empresas que querem usar ECC terão de fazer acordos caros com a Certicom para evitar ações judiciais. Em 2007 Certicom processou a Sony por usar ECC em software para DVDs BlueRay sem licenciar suas patentes. Sony inicialmente tentou ter algumas patentes invalidadas em juízo, antes de aceitar um acordo fora dos tribunais em 2009.

Stamos pediu ao BlackBerry que mudasse sua política em relação às patentes da Certicom, sugerindo que poderia permitir o uso livre delas para sistemas baseados em SuiteB usando ECC, mas ainda tem receitas significativas a partir de outros casos de uso. "Não há uma empresa no mundo que tenha a oportunidade de que o BlackBerry tem agora", disse ele, acrescentando que, se a RSA e Diffie-Hellman fossem decifradas, o governo dos EUA provavelmente derrubaria patentes da Certicom no interesse nacional. "Se o cryptopocalipse acontece, essas patentes não vãovovdurar."

Algumas pessoas na comunidade de segurança especulam que os criptógrafos da NSA já podem ter descoberto a forma de quebrar muitos esquemas de criptografia mais comuns. O sofisticado malware Flame descoberto no ano passado contou com uma técnica matemática completamente nova para derrotar um método de criptografia usado para verificar algumas atualizações de software como originárias da Microsoft, permitindo ao Flame se camuflar como software legítimo. Presume-se que o Flame tenha sido criado por um governo, talvez o dos Estados Unidos, e Stamos brincou dizendo que ele se originou com alguém que tinha recursos significativos de computação "em seu porão, em Maryland," o estado onde o NSA e muitos empreiteiros da defesa se baseiam.

No entanto, Moxie Marlinspike, co-fundador do Whisper Systems, que desenvolve aplicativos para chamadas e mensagens de textos criptografadas em smartphones, disse ao MIT Technology Review, antes da palestra de Stamos que ele acreditava que a vanguarda da pesquisa criptográfica a maior parte dela permanece em aberto. "Eu não acho que eles estão à nossa frente", disse ele, referindo-se ao governo. Tabelas salariais federais, que são públicos, estão muito aquém daquelas do setor privado, Marlinspike apontou, algo que ele acredita que mantém os melhores talentos de criptografia no setor privado.