Publicação do Comitê Gestor da Internet no Brasil

[Revista] .br

ed.13 | ano 08 | 2017

Inteligência artificial torna-se mais sofisticada

MÁQUINAS QUE "PENSAM" E FALAM

Avanços da interface de voz e da computação cognitiva aproximam homens e máquinas

Provedores regionais
Pequenas empresas levam banda larga ao interior

Navegação segura
Escolha da rede privada virtual exige cuidado

Computador quântico
Routo Terada fala sobre o futuro da criptografia

Editorial

Eis o número 13 da revista.br. Para os gregos, 13 é um número de azar porque a quarta cruzada tomou Constantinopla numa terça-feira, 13 de abril de 1204. Já para Zagallo e para os italianos, é um número de sorte. Na dúvida, seguiremos em frente!

E seguir em frente é tratar do que está no horizonte próximo, nem sempre previsível, nem sempre fácil de absorver. Há avanços importantes, talvez inquietantes, em inteligência artificial, em robótica, em coisas que escutam, falam e... aprendem. Estamos cada vez mais cercados por algoritmos, cujo objetivo é tornar nossas ações mais confortáveis e simples, mas cujas consequências podem ser bem menos previsíveis ou propícias.

No progresso mais chão, os telecentros continuam a desempenhar seu papel de prover acesso aos ainda não totalmente incluídos na sociedade da informação e da interação. Os que vivem em grandes centros nem sempre se dão conta da utilidade dos telecentros para muitos. Onde há escassez de Internet, há telecentros. Eles fazem parte do ecossistema que permite o acesso à Internet, desde os grandes provedores de acesso, passando pelos pequenos mas vitais provedores locais, que atuam em áreas de menor interesse econômico, mas certamente tão importantes socialmente como as demais.

Alguns temas técnicos como os envolvidos em captação de áudio e vídeo também são assunto. Dispositivos que atuam no setor audiovisual são cada vez mais acessíveis e sua oferta tem crescido de forma muito rápida. Canais virtuais, VPNs, sua robustez e eventuais riscos envolvidos também têm seu espaço.

Finalmente, sobre criptografia temos uma excelente entrevista com o professor Routo Terada, do IME/USP, completando esta edição. Um profissional que se envolveu com o desenvolvimento da área da computação acadêmica sempre com muito sucesso, e que hoje é uma referência.

Boa leitura!

DEMI GETSCHKO
Editor chefe

Expediente

EDITOR CHEFE
Demi Getschko

CONSELHO EDITORIAL
Carlos Afonso
Eduardo Parajo
Lisandro Granville
Hartmut Glaser

COMUNICAÇÃO NIC.BR
Gerente de Comunicação
Caroline D'Avo

Coordenador de Comunicação
Everton Teles Rodrigues

Assistente de Comunicação
Soraia Marino

REDAÇÃO
Editor
Renato Cruz

Editora de Arte
Maricy Rabelo

Designers
Klezer Uehara e Giuliano Galvez

Colaboradores
Carolina Silva, Demi Getschko, Fábio Barros, Mariana Lima, Nilton Tuna Mateus e Roberta Prescott

Imagens:
Shutterstock

.br é uma publicação do Comitê Gestor da Internet no Brasil

JORNALISTA RESPONSÁVEL
Renato Cruz
MTB 025.958

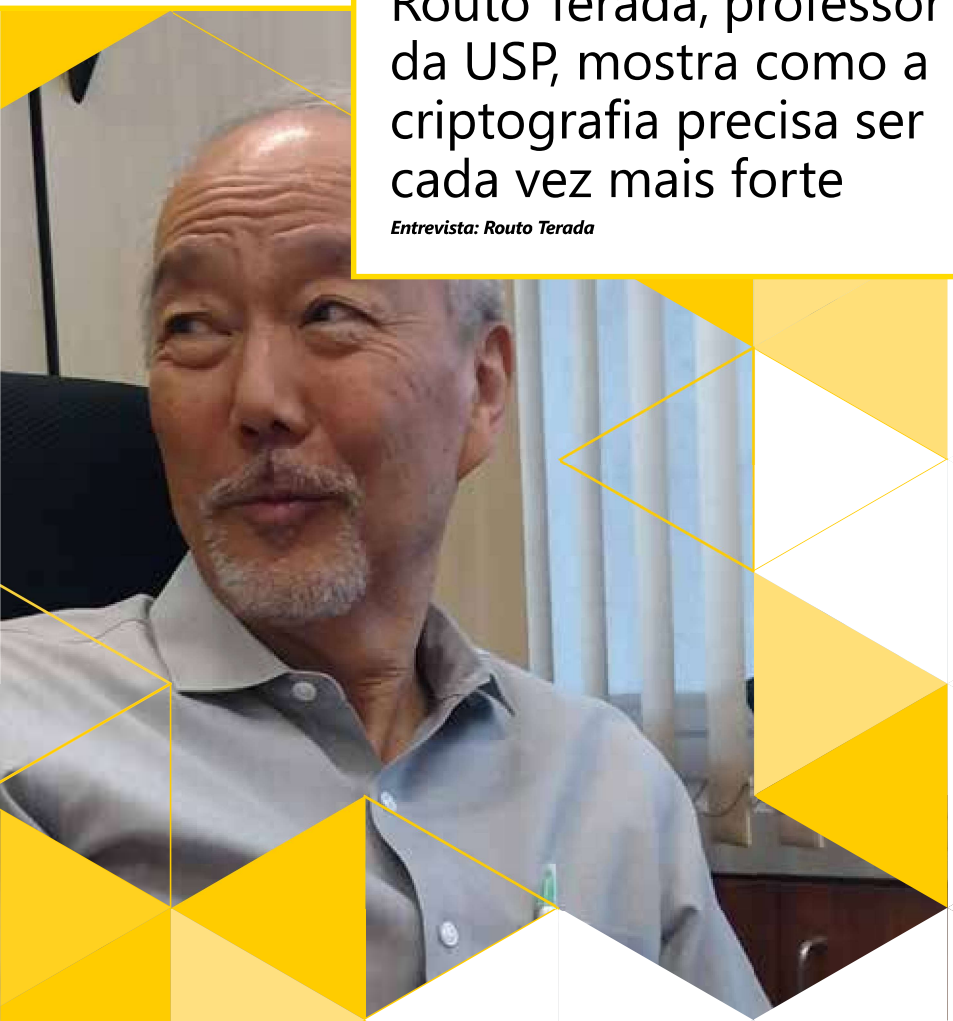
Conversa com o Leitor
Para falar com a Revista .br, escreva para @comuNICbr e imprensa@nic.br

Como fica a segurança na era do **computador quântico**

Texto Renato Cruz

Routo Terada, professor da USP, mostra como a criptografia precisa ser cada vez mais forte

Entrevista: Routo Terada



Segurança absoluta não existe. Nem por isso estudiosos e pesquisadores deixam de buscar soluções cada vez mais sofisticadas para proteger as informações digitais. Isso inclui projetar até um futuro em que a computação quântica promete velocidades de processamento capazes de tornar obsoletas as chaves calculadas hoje pelo clássico RSA, algoritmo de criptografia desenvolvido no fim dos anos 1970 por três cientistas do Instituto de Tecnologia de Massachusetts (MIT, na sigla em inglês).

No Brasil, Routo Terada, professor titular no Departamento de Ciência da Computação da Universidade de São Paulo, PhD em ciência da computação pela Universidade de Wisconsin, trabalha com criptografia na pós-graduação da USP desde 1980, quando o tema começou a ganhar importância no Brasil com a propagação da Internet e o surgimento dos negócios virtuais. Nesta entrevista, Terada conta sua experiência, fala dos pontos fortes e fracos dos sistemas de segurança, avalia a questão da privacidade, relata as condições do mercado e dos profissionais e recomenda mais investimento na área acadêmica, vítima da crise que assola a USP e outras grandes universidades brasileiras.

Antes da Web, qual era a principal aplicação da criptografia?

R.T_ As aplicações concentravam-se principalmente nas áreas militar e diplomática. Mas as funções matemáticas – o algoritmo – eram secretas. A famosa máquina Enigma, usada pelos nazistas na Segunda Guerra, continha um algoritmo totalmente desconhecido integrado ao circuito eletromecânico.

Quando o algoritmo deixou de ser secreto?

R.T_ Com o RSA, a fundamentação matemática é clara. Qualquer pessoa pode estudar, saber como funciona e qual é a justificativa matemática para a chave privada ser difícil de recalcular ou mesmo adivinhar. Não existe chave totalmente protegida, mas do ponto de vista computacional é inviável quebrá-la. O pressuposto é que a criptografia seja muito forte mesmo para um adversário que disponha de recursos computacionais e conhecimento matemático bastante sólido.

Qual é o tamanho dessa chave?

R.T_ Atualmente, no RSA, trabalhamos com 1.024 bits. Em nível militar passa de 2 mil. Em linguagem leiga, quanto mais longa a chave, mais difícil quebrá-la. O número de combinações possíveis é astronômico. Entretanto, quanto mais longa a chave, mais difícil fazer a gestão.

Por que fica mais difícil?

R.T_ Fica mais difícil a gestão do banco de dados das chaves públicas que a autoridade certificadora deve administrar, fazer troca, remoção (no caso de cancelamento ou prazo de validade expirado), geração de chave etc. Isso também acontece do lado do usuário, em que a gestão é da chave privada, que deve ser administrada e gravada de forma segura pelo *software* do usuário. A chave pública deve também ser administrada pelo lado do usuário, para *double-checking*, sincronização com a chave privada etc.

Quando se fala de crime ou espionagem não se trata necessariamente de quebra da chave, não é?

> "O pressuposto é que a criptografia seja muito forte mesmo para um adversário que disponha de recursos computacionais e conhecimento matemático bastante sólido."
>
> *Routo Terada*

R.T_ Segurança 100% não existe, então há várias formas de burlá-la. A mais simples é o suborno de alguém que esteja trabalhando num banco ou mesmo no provedor de Internet. É o que os americanos chamam de *insider*. Mas aí entramos numa área que poderíamos chamar de engenharia social ou de psicologia humana: disponibiliza-se algo grátis e o presente tem alguma armadilha embutida.

É possível derrotar os criminosos digitais?

R.T_ Estabelecendo um paralelo, temos de um lado as quadrilhas e de outro a polícia que quer impedir o crime. A área de criptografia também é assim. Criamos formas de proteção, e os criminosos tentam burlá-las de alguma maneira. As lojas virtuais, hoje em dia, até deixam de armazenar os dados do cartão de crédito porque não querem ter a responsabilidade de proteger o cartão de milhares de clientes.

Que preocupação o usuário ou uma pequena empresa de e-commerce precisam ter? Que tipo de risco estão correndo?

R.T_ A recomendação padrão é que tenham antivírus. Mas, de novo, há a engenharia social que explora a ingenuidade das pessoas. Se alguém recebe um *e-mail* falso, dizendo "sua conta vai ser fechada se você não mandar sua senha", a pessoa manda. Essa parte de engenharia social é muito complicada.

> "As lojas virtuais, hoje em dia, até deixam de armazenar os dados do cartão de crédito porque não querem ter a responsabilidade de proteger o cartão de milhares de clientes"
>
> *Routo Terada*

O ponto fraco, então, são as pessoas?

R.T_ Sim. Mas não é por isso que vamos restringir o acesso. Por isso existe o *token* [em que o comerciante não tem acesso aos dados do cartão], às vezes uma segunda senha, ou mesmo identificação biométrica. Tudo isso é necessário, mas a vida do cidadão honesto fica mais complicada. Esses bloqueios encarecem o sistema e aumentam o tempo gasto pelo usuário. E, se forem muitos, acabam tornando o processo inviável.

Como fica a segurança em relação à computação quântica?

R.T_ A minha área de pesquisa, atualmente, é de algoritmos que sejam fortes mesmo com a existência do computador quântico. O RSA e outros algoritmos baseados em curvas elípticas são o fundamento de segurança contra ataques na computação convencional. Mas há quem diga que se tornariam inúteis. O pesquisador Peter Shor publicou um algoritmo, teórico, que seria capaz de quebrar a chave RSA e de curvas elípticas em segundos num computador quântico.

Mesmo assim, podem ser mais rápidos que os computadores convencionais?

R.T_ Ainda não existe uma tecnologia que garanta probabilidade alta de chegar ao resultado correto. Tenho notícias de que a IBM já consegue multiplicar 8 bits por 8 bits e na maioria dos casos o resultado é correto. Agora, ir de 8 bits para 16 bits já é um custo maior, e depois (24x24) maior ainda. Por enquanto, o custo é muito alto. Nas conferências internacionais de que tenho participado, especula-se que talvez daqui a cinco anos se consiga multiplicar 32 bits por 32 bits.

Existem substitutos do RSA para trabalhar com computação quântica?

R.T_ Existem, mas são algoritmos mais complicados. Demandam chaves muito longas, de megabytes, então, na prática não são viáveis. Há alguns algoritmos que supomos ser fortes mesmo contra um computador quântico, mas não se pode provar. A conjectura é tal que não se consegue, no estado da arte, provar que é falso nem que é verdadeiro. Então, a conjectura é que esses algoritmos são fortes mesmo quando o computador quântico for de fato real.

Quem trabalha com pesquisas nessa área aqui no Brasil?

R.T_ Podemos contar nos dedos. Nós temos um encontro anual, o Simpósio Brasileiro de Segurança, do qual participam dois grupos, um de criptografia e outro de segurança em redes. São basicamente quadros da USP, Unicamp, UnB, UFMG, Federal de Santa Catarina, Federal do Rio Grande do Sul, e um grupo pequeno da Federal da Amazônia. Mas, comparado com o que havia em 1981, quando voltei dos Estados Unidos, cresceu muito.

Como está a situação do Brasil em termos de mercado, empresas e profissionais?

R.T_ Há uma procura muito grande, principalmente na área bancária e financeira e lojas virtuais. Mas falta conhecimento, informação. Às vezes o que é implementado pode ser quebrado facilmente. Os nossos alunos, que têm formação boa, são bastante procurados, mas as empresas têm de pagar um salário maior, o que é um problema.

Há uma discussão muito grande hoje em relação à Internet das coisas. Como o senhor vê essa questão?

R.T_ Essa área é muito complicada, porque o fabricante, por causa da concorrência, acaba implementando artigos baratos para diminuir o preço final, deixando uma vulnerabilidade que é explorada pelos criminosos. Há muita ansiedade por tecnologia avançada, mas que não seja muito cara. E aí aparecem *backdoors* que não estavam previstos.

br *Como o senhor vê a discussão sobre privacidade e segurança, em que as empresas, como WhatsApp, querem preservar a informação do usuário e a polícia quer obter os dados a respeito de criminosos?*

R.T_ O que acontece é que a legislação muitas vezes não prevê certos crimes. O Marco Civil da Internet foi um avanço no sentido de restringir o que o governo pode fazer e definir até onde vai o direito do cidadão. Agora, precisa ser aperfeiçoado. A privacidade, mesmo física, hoje em dia não é muito fácil de preservar – em qualquer lugar há uma câmera. Na Internet é a mesma coisa.

br *O que o governo brasileiro poderia fazer para evitar episódios como o da espionagem da presidente revelada por Edward Snowden?*

R.T_ O Snowden trabalhava na NSA. Ele sabia de tudo. É um exemplo de *insider*. Não tenho muito conhecimento do serviço secreto brasileiro, mas sei que há pesquisadores, pessoas que têm conhecimento matemático, implementam algoritmos etc. Mas são algoritmos secretos. Alguns são *hardwired* [implementados por *hardware*] nos circuitos integrados dos equipamentos. As embaixadas brasileiras têm essas máquinas, usadas também na área militar.

> "O pesquisador Peter Shor publicou um algoritmo, teórico, que seria capaz de quebrar a chave RSA e de curvas elípticas em segundos num computador quântico."
>
> *Routo Terada*

> "A privacidade, mesmo física, hoje em dia não é muito fácil de preservar – em qualquer lugar há uma câmera. Na Internet é a mesma coisa."
>
> *Routo Terada*

br *Quando a espionagem foi revelada, anunciou-se que os e-mails da presidente seriam criptografados. Isso confirma que antes não eram?*

R.T_ Foi uma confissão de que, de fato, não eram. Agora não sei. Sabemos muito pouco do que acontece no governo. Pode ser que já tenha introduzido criptografia, ou esteja usando algum software que já está pronto.

br *Qual é a situação da área acadêmica?*

R.T_ O Brasil, academicamente, precisa ter mais incentivo. A USP, em particular, com essa crise econômica, sofre muito, assim como a Unicamp. E a área de criptografia, apesar do interesse dos alunos, acaba sofrendo também. Mas temos capacitação intelectual. Em 2008 publiquei um livro e isso foi muito bom, porque alunos de outros Estados vêm para cá fazer o mestrado. Temos condições de formar alunos capacitados, de fazer pesquisa, enfim, nós temos condições de avançar junto com outros países.

br *Qual é a situação da área acadêmica?*

R.T_ Em computação, mais de 200. Em criptografia, muito poucos. Mas as perspectivas profissionais são boas. O salário é alto, uma boa motivação.