Empresas & Negócios

Matéria de capa

Foto de Christina Morillo no Pexels


# ESTAMOS CHEGANDO À ERA DA COMPUTAÇÃO CONFIDENCIAL

Leia na página 6

Você já deve ter notado em alguns sites que, ao lado da barra de URL do seu navegador, aparece um cadeado. Esta é uma informação visual para o usuário de que aquela página é segura e que as informações que inserir irão trafegar de forma segura entre seu computador e o servidor do site. É um recurso bastante importante hoje em dia. Ao se logar em algum site, você espera ter garantias de que ninguém vai capturar o seu nome de usuário e sua senha.

**Luiz Jeronymo (*)**

Mais importante ainda, quando estiver num site de comércio eletrônico, você quer ter certeza de que suas informações pessoais (nome, endereço, CPF, número de cartão de crédito etc.) não sejam interceptadas por terceiros. As páginas que apresentam aquele cadeado usam o protocolo HTTPS, que através de certificados criptográficos SSL/TLS, impede que alguém leia ou modifique os dados que você troca com o site. Seu uso, hoje em dia, é tão comum que qualquer proprietário de site que não o use é visto como negligente.

No entanto, o cadeado não te diz nada sobre o que aquele servidor fará com seus dados. Você apenas sabe que está compartilhando seus dados com ele e não com outra pessoa. No mundo dos negócios, onde os dados costumam ser um dos ativos mais valiosos de uma empresa, essa situação não é mais aceitável. Por exemplo, as instituições financeiras têm informações sobre seu cliente, mas realmente gostariam de ter uma visão mais ampla de como ele se comporta no mercado, ao mesmo tempo em que não querem compartilhar dados confidenciais.

Portanto, necessita-se de uma empresa terceirizada neutra para fornecer a função de agregação de informação que nenhuma das instituições confia que qualquer outra executará. Usualmente, cada instituição compartilha confidencialmente suas informações com um bureau de dados de mercado, que extrai inteligência e insights destes conjuntos de dados e então as devolve às instituições. Mas aquele bureau pode fazer o que quiser com aqueles dados. A única proteção real é a sua política de privacidade e sua reputação como empresa confiável.

Cenário semelhante é encontrado em outros segmentos: seguradoras que precisam compartilhar informações sobre sinistros fraudulentos sem violar as regras de confidencialidade; participantes em leilões online que não gostariam que o leiloeiro explorasse o conhecimento de quanto eles pretendem pagar; pacientes que contribuiriam com seus registros para ajudar a combater uma doença, mas ficariam arrasados se as informações sobre sua saúde se tornassem públicas.

Qualquer situação em que você tenha que abrir mão de dados valiosos para receber em troca algum insight mais amplo é provavelmente um exemplo desse fenômeno. E se você pudesse ter certeza do que o computador da outra pessoa fará com seus dados? Você, seus clientes e concorrentes poderiam se beneficiar da inteligência coletiva que surge quando vários conjuntos de dados são reunidos com a certeza de que seus próprios dados permanecerão ocultos para os demais, incluindo quem está hospedando o serviço.

Essa cooperação entre participantes de uma indústria é a promessa central das plataformas blockchain corporativas. Mas e se as empresas precisarem obter inteligência coletiva de dados que precisam permanecer ocultos? O blockchain não traz respostas a essa pergunta. No entanto, integrada a outra tecnologia - como a computação confidencial - esse desafio pode finalmente ser superado.

Curiosamente, as três grandes empresas de chips que estão mais ativas em computação confidencial - ARM, AMD e Intel - chegaram a este ponto de ângulos intrigantemente diferentes. Lembra-se dos velhos tempos em que você podia instalar um novo software e seu PC não inicializava mais? O mesmo não ocorre com os smartphones porque os fabricantes aprenderam a lição e deliberadamente projetaram seus aparelhos para que seja realmente difícil para seus proprietários fazer algo que os impeçam de funcionar.

Este modelo é habilitado, em parte, pela computação confidencial. Para proteger o ecossistema do dispositivo móvel é necessário encontrar uma maneira de proteger o usuário de si mesmo, removendo o controle sobre alguns aspectos da operação do celular. A ARM, cujos designs estão presentes em praticamente todos os celulares do planeta, se concentrou neste problema com sua arquitetura TrustZone, que possibilita aos fabricantes bloquear parte de seus telefones de forma que o usuário não possa bagunçar certas coisas.

Outro problema que a computação confidencial pode ajudar é o das empresas que querem executar seus aplicativos na nuvem. Elas querem fazer upload de seus aplicativos e dados para a nuvem, mas ter 100% de certeza de que o operador daquela nuvem não poderá ver o que está sendo processado. A AMD se concentrou neste problema com sua tecnologia SEV (Secure Encrypted Virtualization), hoje usada pelo Google e outros provedores de nuvem como base de seus serviços, possibilitando que você carregue seu aplicativo e execute-o, inalterado, mas de uma forma que o Google não possa espionar.

Há uma terceira possibilidade de uso da computação confidencial que é ambiciosa e potencialmente revolucionária. Do ponto de vista do provedor de serviços de dados, trata-se de oferecer um serviço no qual os usuários possam saber, com certeza, como seus dados serão tratados. Como explica o CTO da R3, Richard Gendal Brown, é como se inventássemos um "cadeado" que permitisse aos usuários saber o que será feito com seus dados, em vez de apenas dizer quem os está processando.

Isso é totalmente novo e possibilitaria uma classe inteiramente nova de serviços "invioláveis", onde os usuários saberiam como seus dados seriam processados, com a segurança de que o provedor não poderia adulterar o algoritmo para extrair seus segredos sorrateiramente. Isso pode ser feito por meio de enclaves seguros, que criam um ambiente de computação confiável isolado do sistema operacional que o hospeda. Os enclaves podem acessar e realizar cálculos nos dados, enquanto estes dados permanecem criptografados para o sistema operacional hospedeiro.

Pode-se afirmar com exatidão qual código está sendo executado dentro destes enclaves de forma a não haver surpresas. Já há no mercado plataformas que possibilitam (e facilitam) o desenvolvimento de enclaves seguros em linguagens JVM, e são baseadas na terceira grande tecnologia no espaço da computação confidencial, a SGX (Software Guard Extensions) da Intel. Muitos computadores e servidores têm esse recurso escondido dentro deles, mas provavelmente ele não é utilizado: tem sido muito difícil para a maioria dos desenvolvedores explorar essa tecnologia.

A tecnologia SGX "out-of-the-box" não é exatamente amigável, especialmente para desenvolvedores de negócios. Portanto, construir uma plataforma que a torne acessível aos fornecedores independentes de software (ISV) e aos engenheiros que trabalham para eles é de extrema importância. Estamos falando de levar o compartilhamento de dados a um nível totalmente novo, permitindo que várias partes contribuam com dados para uma análise conjunta sem revelar os dados reais a ninguém.

Desenvolvedores de software poderão construir sistemas que possam, de fato, ser auditados remotamente. Sistemas em que os proprietários de dados extremamente valiosos poderão verificar de forma independente o que acontecerá com seus dados antes de enviá-los a um terceiro. É a era da computação confidencial, que já está bastante próxima.

Freepik

**(*) É Sales Engineer da R3 no Brasil (www.r3.com).**