CRIPTOGRAFIA: MAIS DO QUE UMA NECESSIDADE, UM IMPERATIVO*

Antonio Tadeu Matias da Silva - Universidade do Estado de Minas Gerais

Juarez Lopez Filho - Universidade do Estado de Minas Gerais

Matheus Ananias de Souza - Universidade do Estado de Minas Gerais

Lucas Borcard Cancela - Universidade do Estado de Minas Gerais

Resumo: O presente trabalho apresenta a criptografia como uma técnica primordial aos sistemas de informação, pois, em sua essência, as tecnologias de informação e comunicação carregam consigo a premência da velocidade. Assim sendo, torna-se passível de carregar em seu bojo não apenas benefícios, mas, também mazelas, dentre as quais, aparecerá em destaque ao longo deste artigo, uma que é resultado imediato deste mundo tão efêmero - a ausência de segurança - logo, o uso da criptografia na transmissão de dados é praticamente uma norma, a qual não pode ser deixada em segundo plano de maneira alguma. No atual contexto da globalização, onde a informação é o bem mais precioso, o uso ou não da criptografia pode significar a diferença entre fracasso e sucesso. Portanto, o objetivo deste trabalho é abordar a criptografia como importante ferramenta na segurança de rede. A metodologia utilizada foi a revisão bibliográfica.

PALAVRAS-CHAVE: Criptografia; Segurança; Rede; Internet.

INTRODUÇÃO

Desde os primórdios da história humana a comunicação se tornou uma necessidade, de um modo totalmente diferente do restante dos animais, visto que as articulações entre símbolos e significados passaram a ganhar nível de complexidade mais bem elaborado. O grande problema do processo de comunicação é que, apesar de ser um ato social, por diversos motivos, razões ou interesses, diversas vezes esse processo necessita de certo sigilo, seja por questões de confrontos, quer seja para evitar a perda de algum recurso.

Nesse entremeio surge a ideia de criptografar mensagens, ou seja, criar métodos os quais permitam que apenas o emissor e o receptor do conteúdo da comunicação o possa entender. Primeiramente não se iniciou com o processo de codificação/decodificação de mensagens, mas, um sutil escamoteamento dos tão preciosos recados – tatuagens no couro cabeludo ou por baixo das armaduras são exemplos desta técnica.

Os sistemas de codificação tal qual conhecemos hoje evoluíram muito a partir da 2ª Guerra Mundial, quando mensagens cifradas eram passadas entre aliados no front de batalha e até mesmo em além-mar. Decodificar esses conteúdos significou a vitória em uma série de batalhas, bem como, em grande medida, até mesmo a derrocada final de quem teve o seu conteúdo desvendado.

A tecnologia que evoluiu destes processos criou bases para o que é hoje a moderna criptografia, as quais estão presentes nos mais diversos afazeres do nosso dia-a-dia, desde os mais corriqueiros até os mais complexos - desde acessar um e-mail, fazer realizar uma transferência bancária entre investimentos localizados em bolsas de valores em pontos antípodos do mundo.

Neste trabalho, também, será estudado uma temática que envolve diretamente em seu uso a criptografia, que é o uso de bitcoins; uma espécie de moeda virtual que corre em paralelo ao sistema financeiro, sem que para isso não perca em si mesma a sua noção de valor,

tanto que, suas operações demandam segurança, portanto, criptografia.

1. CONCEITUAÇÕES DE CRIPTOGRAFIA E O SEU USO NOS BITCOINS

A etimologia do vocábulo criptografia revela a sua razão de ser - do grego: *kryptós*, "escondido", e *gráphein*, "escrita" - é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta"), o que a torna difícil de ser lida por alguém não autorizado. Assim sendo, só o receptor da mensagem pode ler a informação com facilidade.

Para tanto, cada vez mais é necessário que esses dados sejam armazenados ou transportados de maneira segura, de modo a dificultar a invasão dos dados, criando-se chaves de segurança para proteger nossas informações pessoais em transações, tais como contas bancárias, conversas pessoais, segredos profissionais, dados sigilosos, etc. Acerca disto, (Costa et alli., 2012) afirmam que:

“Conectar-se em rede significa possibilitar condições específicas de controle com acesso externo aos recursos no contexto computacional, principalmente às informações. As falhas decorrentes da ausência de medidas de segurança para proteção permitem condições de controle e acesso que podem ser exploradas por usuários externos ou internos ao sistema de computação, obtendo acesso não autorizado. As falhas no sistema podem ser causadas por impactos de diferentes níveis havendo uma ambivalência, partindo desde uma simples ameaça, até uma ação que comprometa a imagem corporativa, chegando a perdas financeiras e de mercado em longo prazo”.

A criptografia é um ramo da Matemática, portanto seus métodos são muito antigos, logo, suas análises e proposições apareceram bem antes que a Ciência da Computação. De fato, o estudo da criptografia cobre bem mais do que apenas da cifragem e da decifragem. É um ramo especializado da teoria da informação com muitas contribuições de outros campos da matemática e do conhecimento, incluindo autores como Maquiavel, Sun Tzu e Karlvon Clausewitz. Mas, em se falando de ciência da computação, a criptografia garante basicamente quatro objetivos principais, os quais foram enumerados por (Reisswitz, 2012):

1 - *confidencialidade da mensagem*: só o destinatário autorizado deve ser capaz de extrair o conteúdo da mensagem da sua forma cifrada. Além disso, a obtenção de informação sobre o conteúdo da mensagem (como uma distribuição estatística de certos caracteres) não deve ser possível, uma vez que, se o for, torna mais fácil a análise criptográfica.

2 - *integridade da mensagem*: o destinatário deverá ser capaz de verificar se a mensagem foi alterada durante a transmissão.

3 - *autenticação do remetente*: o destinatário deverá ser capaz de verificar que se o remetente é realmente quem diz ser.

4 - *não repúdio ou irretratabilidade do remetente*: não deverá ser possível ao remetente negar a autoria de sua mensagem.

Esta listagem, em resumo, enumera um conjunto de objetivos a serem alcançados

pela criptografia, mas, não significa que um algoritmo dará necessariamente conta de todas essas características e objetivos. Em geral, atuam especificamente em uma ou mais características. Acerca deste fato (Reisswitz, 2012) afirma:

“Mesmo em sistemas criptográficos bem concebidos, bem implementados e usados adequadamente, alguns dos objetivos acima não são práticos (ou mesmo desejáveis) em algumas circunstâncias. Por exemplo, o remetente de uma mensagem pode querer permanecer anônimo, ou o sistema pode destinar-se a um ambiente com recursos computacionais limitados.”

Desse modo, a criptografia trabalha com uma série de chaves simétricas e assimétricas, que tal qual a uma chave numa fechadura trabalha no algoritmo para proteger o acesso ao conteúdo. Ainda sobre este fato (Reisswitz, 2012) afirma:

“Chave Criptográfica é uma com valor secreto, a qual interage com o algoritmo de encriptação. A fechadura da porta da frente da sua casa tem uma série de pinos. Cada um desses pinos possui múltiplas posições possíveis. Quando alguém põe a chave na fechadura, cada um dos pinos é movido para uma posição específica. Se as posições ditadas pela chave são as que a fechadura precisa para ser aberta, ela abre, caso contrário, não.”

Do mesmo modo funciona um algoritmo de encriptação, tanto no modo assimétrico, com a sua chave pública, quanto no modo simétrico, com uma chave particular. Nesse entremeio surgiram os DES simples, os triplos, os AES, etc. que evoluem ainda mais o poder de segurança, mas, que muitas vezes acabam por aumentar a necessidade de processamento e de memória.

Nesse panorama de segurança de redes, do uso da criptografia surge os Bitocins. O Bitcoin é uma criptomoeda descentralizada que visa facilitar transações de financeiras no ambiente virtual, de forma segura e independente de qualquer instituição financeira, como o sistema bancário. Sobre isto, (Oliveira et alli, 2014) afirmam:

“A ausência de um controle central mediado por um governo ou instituição financeira agregando seus impostos e taxas administrativas, bem como a manutenção da privacidade durante seu uso e o fato de serem objetos totalmente digitais, confere o crescente aumento de popularidade ao Bitcoin, se mostrando como uma alternativa as moedas convencionais e mais adequado as novas tecnologias da informação e comunicação”.

O crescimento dessa moeda, desde sua apresentação em 2008, no grupo de discussão The Cryptography Mailing, por um programador japonês ou um grupo de programadores, de pseudônimo Satoshi Nakamoto, não se deu como sucesso ainda por vários fatores: uma das coisa que impede que essa moeda entre em uma grande circulação é o fato de muitas pessoas não confiar nessa moeda digital, vindo a pensar que ela pode ser fraudada, copiada e rouba por piratas da internet (crackers e hackers) de suas respectivas contas. O que não é uma verdade em si, pois como todo e qualquer sistema apresenta falhas, mas, também uma série de qualidades. Dentre elas está o código aberto, que favorece a troca de experiência entre programadores do mundo todo, bem como a criptografia durante o processo. Sobre tal fato, (Oliveira et alli, 2014) reafirmam:

“A criptografia e as redes ponto-a-ponto fundamentam as bases tecnológicas para o desenvolvimento de um novo conceito de moeda, a cripto-moeda, que obedece a um rígido e ao mesmo tempo simples protocolo de funcionamento, que expressa à forma como deve ser emitida, armazenada e transmitida, sendo esta última, análoga a uma operação de enviar e receber e-mails. Outra característica marcante está no uso de tecnologias de fonte aberta, mais conhecidas como *open source* que sustentam essa cripto-moeda chamada Bitcoin”.

O Bitcoin pode ser salvo em computadores ou em pen drives na forma de "arquivos de carteira" ou como "serviços de carteira online", provido por terceiros, e em ambos os casos podem ser enviadas pela internet para qualquer lugar do mundo ou para qualquer pessoa que tenha um "endereço bitcoin", podendo transacionar diretamente uns com os outros, usando criptografia de chave pública, sem intermédio de uma instituição financeira. Transações são verificadas pelos nós da rede P2P, ponto a ponto, e registradas em um banco de dados distribuídos (livro-razão público) de contabilidade pública conhecidos como Blockchain.

Para a segurança, essa moeda oferece uma chave pública a cada transação, que funciona da seguinte forma: a chave pública pode ser usada para verificar se uma assinatura digital foi gerada pela chave privada, bem como codificar dados que somente a chave privada poderá abrir. Ou seja, a chave pública é para o uso dos outros, enquanto a chave privada é usada por você.

A aceitação e adesão ao Bitcoin nas diversas perspectivas impactadas com essa nova tecnologia, pode ser um ótimo investimento para conseguir escapar de inflações e crises financeira que alguns países passam.

CONCLUSÃO

Várias são as possibilidades oferecidas pela rede, algumas muito boas e libertadoras, tais como o uso Bitcoin. Todavia, conforme em vista de tudo que foi explanado até aqui, fica bem claro que a tecnologia de segurança em redes é algo mais do que necessário, para não dizer que é imprescindível, ou até mesmo compulsório.

Neste contexto, as técnicas de criptografia são uma boa aliada na batalha entre o usuário comum, que trafega na rede ao realizar as suas obrigações e os seus afazeres diários, versus o usuário que usurpa informações ao seu favor. Isto tudo ocorre porque existe uma série de ameaças na rede mundial de computadores, desde vírus simples, passando worms e trojans mais robustos, até mesmo existem os spywares bem elaborados que espionam o dia-a-dia de empresas e de cidadãos simples ou chefes de Estado. Além disto, a tecnologia de segurança criptográfica é considerada assim, como a protetora do maior bem da atualidade, pois protege o cerne do paradigma da nossa sociedade – a informação.

REFERÊNCIAS BIBLIOGRÁFICAS

IKEDA, Ana. **Wi-Fi público: saiba como tirar proveito da internet sem fio gratuito. 2013.** Disponível em: <https://goo.gl/Pnai9X>. Acesso em 10 mar. 2017.

JORDÃO, Fabio. **Quais os riscos de usar um WiFi público?. 2013.** Disponível em: <https://goo.gl/HGDF6Y>. Acesso em 9 mar 2017.

OLIVEIRA, F. M. de; TOTTI, M. E. F.; NEY, V. S. P. **Bitcoin: o dinheiro com tecnologia de fonte aberta em rede ponto-a-ponto.** Acessado em

<http://evidosol.textolivre.org/papers/2014/upload/26.pdf> em 20/03/2017.

REISSWITZ, F. **Análise de Sistemas Vol. 2 – Tecnologia Web & Redes**, 2012.

SYMANTEC. **Implementando Uma LAN Sem Fio Segura**, 2006. Disponível em:
http://www.symantec.com/region/br/enterprisesecurity/content/framework/BR_3074.html.
Acesso em 12 mar. 2017.

TAGIAROLI, Guilherme. **Usar rede Wi-Fi aberta oferece riscos aos usuários. 2015.**
<https://goo.gl/QgdSZK>. Acesso em 10 mar. 2017.