Segurança para a Internet das Coisas: Uma Solução para Comunicação Criptografada entre Dispositivos

Erik Henrique de Oliveira Zambeli - RA: 1749927

[1]Universidade Tecnológica Federal do Paraná (UTFPR)
Campus Cornélio Procópio – PR – Brazil

Abstract. *resumo..*

Resumo. *resumo..*

1. Introdução

2. Referencial Teórico

Criptografia é uma palavra grega formada pela junção dos termos Kryptos e Grapho (grafia, escrita). Ela utiliza uma sequência de passos que servem para transformar um texto claro em texto codificado que aparenta ser um texto gerado aleatoriamente sem possuir sentido algum. A ação de transformar dados para uma forma ilegível é denominada cifra ou cifragem, e busca garantir a privacidade. O processo inverso da cifragem é chamado de decifragem. Quando utilizamos o processo de cifragem e decifragem, necessitamos de informações confidenciais, chamadas chaves [STALLINGS 2014]. Existem dois tipos de chaves:

Chave Simétrica: É também conhecida como criptografia de chave privada. O emissor usa uma chave para cifrar a mensagem, e o receptor utiliza a mesma chave para decifrá-la.

Chave Assimétrica: Conhecida como criptografia de chave pública. Este tipo de criptografia, usamos duas chaves distintas, de modo a obtermos comunicação segura através de canais de comunicação inseguros. Trata-se de uma técnica de criptografia assimétrica pelo fato de usar um par de chaves distintos.

2.1. Algoritmos criptográficos

Os algoritmos criptográficos podem ser implementados em hardware (para performance) ou software (para flexibilidade), mais a maior parte do tratamento esta relacionado aos algoritmos e protocolos, que são independentes da implementação real [TANENBAUM 2003].Podemos dizer que um algoritmo de criptografia é um procedimento matemático que contém uma entrada (dados a serem cifrados), efetua um processamento matemático com base em uma chave, e gera uma saída.

2.1.1. Criptografia Simétrica

A criptografia simétrica é conhecida por criptografia de chave secreta. Este modelo usa uma única chave que é partilhada entre o emissor e o receptor figura, 1. Desta forma, a chave que é usada para cifrar é a mesma que é usada para decifrar. Quando uma pessoa quer se comunicar de forma segura com outra pessoa, as maquinas já devem conhecer

a chave secreta ou a chave utilizada para cifrar a mensagem deve ser enviada pela rede. Este processo é chamado de “distribuição de chaves”. Algoritmos que usam criptografia simétrica tendem a ser mais rápidos, no entanto não são tão seguros, uma vez que a chave usada para cifrar a informação é partilhada entre as várias máquinas da rede. A maior dificuldade do método é a distribuição segura das chaves[BURNETT 2002].

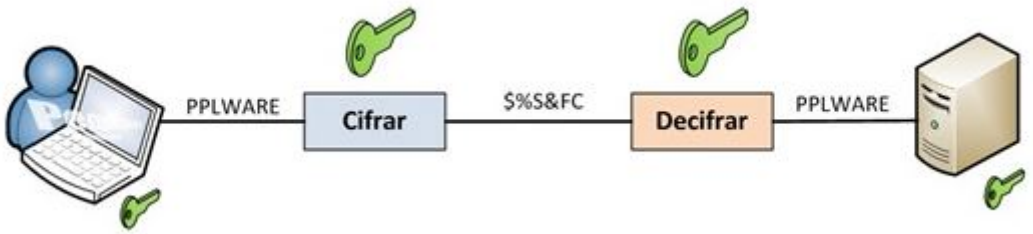

Figure 1. Funcionamento Criptografia Simétrica

2.1.2. Algoritmos de Criptografia Simétrica

Os algoritmos DES , 3DES e AES são alguns dos que utilizam a criptografia simétrica. Podemos analisar outros algoritmos de chave privada ou criptografia simétrica de forma resumida na Tabela 1:

Table 1. Principais algoritmos de chave privada ou criptografia simétrica

Algoritmo	Bits	Descrição
AES	128	O Advanced Encryption Standard (AES) é uma cifra de bloco, anunciado pelo National Institute of Standards and Technology (NIST) em 2003, fruto de concurso para escolha de um novo algoritmo de chave simétrica para proteger informações do governo federal, sendo adotado como padrão pelo governo dos Estados Unidos, é um dos algoritmos mais populares, desde 2006, usado para criptografia de chave simétrica, sendo considerado como o padrão substituto do DES. O AES tem um tamanho de bloco fixo em 128 bits e uma chave com tamanho de 128, 192 ou 256 bits, ele é rápido tanto em software quanto em hardware, é relativamente fácil de executar e requer pouca memória.
DES	56	O Data Encryption Standard (DES) foi o algoritmo simétrico mais disseminado no mundo, até a padronização do AES. Foi criado pela IBM em 1977 e, apesar de permitir cerca de 72 quadrilhões de combinações, seu tamanho de chave (56 bits) é considerado pequeno, tendo sido quebrado por ”força bruta” em 1997 em um desafio lançado na Internet. O NIST que lançou o desafio mencionado, recertificou o DES pela última vez em 1993, passando então a recomendar o 3DES.

3DES	112 ou 168	O 3DES é uma simples variação do DES, utilizando o em três ciframentos suscessivos, podendo empregar uma versão com duas ou com três chaves diferentes. É seguro, porém muito lento para ser um algoritmo padrão.
IDEA	128	O International Data Encryption Algorithm (IDEA) foi criado em 1991 por James Massey e Xuejia Lai e possui patente da suíça ASCOM Systec. O algoritmo é estruturado seguindo as mesmas linhas gerais do DES. Mas na maioria dos microprocessadores, uma implementação por software do IDEA é mais rápida do que uma implementação por software do DES. O IDEA é utilizado principalmente no mercado financeiro e no PGP, o programa para criptografia de e-mail pessoal mais disseminado no mundo.

Fonte:[STALLINGS 2014]

2.1.3. Criptografia Assimétrica

A criptografia assimétrica,conhecida por criptografia de chaves públicas, faz p uso de pares de chaves para criptografar ou descriptografar. As duas chaves são relacionadas através de um processo matemático, usando funções unidirecionais para a codificação da informação. A chave pública que, como o nome já diz, qualquer um pode conhecer e ter acesso, é usada para cifrar, enquanto a chave privada, é usada para decifrar. Uma mensagem cifrada com uma chave pública somente poderá ser decifrada com o uso da chave privada com a qual está relacionada. O método traz segurança, pois não é necessário compartilhar a chave privada. Em contrapartida, o tempo de processamento de mensagens com criptografia assimétrica é muito maior do que com criptografia simétrica [BURNETT 2002]. Na Figura 2 é demonstrado o processo.

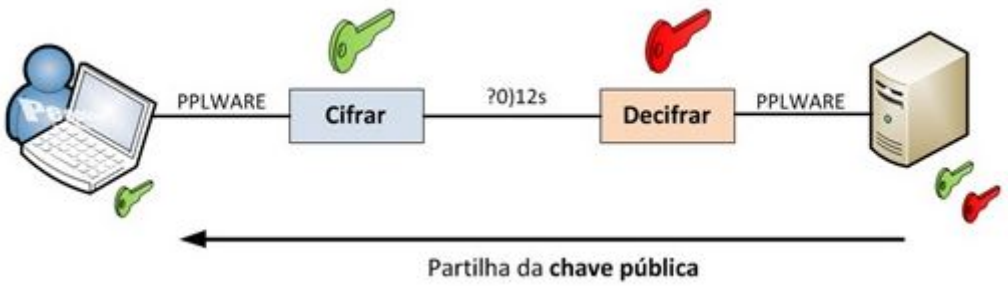

Figure 2. Funcionamento Criptografia assimétrica

2.1.4. Algoritmos de Criptografia Assimétrica

A grande dificuldade deste sistema é a complexidade no desenvolvimento dos algoritmos que devem reconhecer a dupla de chaves existentes e relacionar as mesmas no momento certo, o que reverte num grande poder de processamento computacional para este trabalho [STALLINGS 2014]. A analise dos principais algoritmos de chave pública ou criptografia assimétrica de forma resumida na Tabela 2.

Table 2. Principais algoritmos de chaves públicas ou criptografia assimétrica

Algoritmo	Descrição
RSA	O RSA é um algoritmo assimétrico que possui este nome devido a seus inventores: Ron Rivest, Adi Shamir e Len Adleman, que o criaram em 1977 no MIT. Atualmente, é o algoritmo de chave pública mais amplamente utilizado, além de ser uma das mais poderosas formas de criptografia de chave pública conhecidas até o momento. O RSA utiliza números primos. A premissa por trás do RSA consiste na facilidade de multiplicar dois números primos para obter um terceiro número, mas muito difícil de recuperar os dois primos a partir daquele terceiro número. Isto é conhecido como fatoração. Por exemplo, os fatores primos de 3.337 são 47 e 71. Gerar a chave pública envolve multiplicar dois primos grandes; qualquer um pode fazer isto. Derivar a chave privada a partir da chave pública envolve fatorar um grande número. Se o número for grande o suficiente e bem escolhido, então ninguém pode fazer isto em uma quantidade de tempo razoável. Assim, a segurança do RSA baseia se na dificuldade de fatoração de números grandes. Deste modo, a fatoração representa um limite superior do tempo necessário para quebrar o algoritmo. Uma chave RSA de 512 bits foi quebrada em 1999 pelo Instituto Nacional de Pesquisa da Holanda, com o apoio de cientistas de mais 6 países. Levou cerca de 7 meses e foram utilizadas 300 estações de trabalho para a quebra. No Brasil, o RSA é utilizado pela ICP-Brasil, no seu sistema de emissão de certificados digitais, e a partir do dia 1º de janeiro de 2012, as chaves utilizadas pelas autoridades certificadoras do país, passam a serem emitidas com o comprimento de 4.096bits, em vez dos 2.048bits atuais.
ElGamal	O El Gamal é outro algoritmo de chave pública utilizado para gerenciamento de chaves. Sua matemática difere da utilizada no RSA, mas também é um sistema comutativo. O algoritmo envolve a manipulação matemática de grandes quantidades numéricas. Sua segurança advém de algo denominado problema do logaritmo discreto. Assim, o ElGamal obtém sua segurança da dificuldade de calcular logaritmos discretos em um corpo finito, o que lembra bastante o problema da fatoração.
Diffie - Hellman	Também baseado no problema do logaritmo discreto, e o criptosistema de chave pública mais antigo ainda em uso. O conceito de chave pública, aliás foi introduzido pelos autores deste criptosistema em 1976. Contudo, ele não permite nem ciframento nem assinatura digital. O sistema foi projetado para permitir a dois indivíduos entrarem em um acordo ao compartilharem um segredo tal como uma chave, muito embora eles somente troquem mensagens em público.

Fonte: [STALLINGS 2014]

3. Aplicação

Nesse capitulo será apresentado a utilização da comunicação criptografada para internet das coisas no mercado e ambiente usual, apresentando uma contextualização dos principais perigos em sistemas conectados a internet das coisas.

3.1. Contexto

A internet das coisas trará muitas mudanças à nível global, transformando a forma como nos relacionamos com o mundo e impactando diretamente nossas vidas, o meio ambiente, os negócios e nossa segurança.

Suponha uma casa em que todos os sistemas estejam conectados, desde os eletrodomésticos à rede elétrica até os dados do dono da casa. Sendo assim, se um hacker encontrar uma vulnerabilidade em algum desses sistemas e conseguir invadir a geladeira, por exemplo, o mesmo poderá usá-la de porta de entrada para acessar outros sistemas dentro da casa. O grande problema por trás é que tendo acesso aos sistemas da casa, o hacker poderá roubar dados, alterar informações e danificar o ambiente. Isso pode ter inúmeros impactos e problemas ao dono da casa. As coisas conectadas podem servir tanto como aliadas quanto alvos em ataques, mais o grau de risco em que os sistemas estão expostos aumenta à medida que mais dispositivos são conectados à rede.

A partir dessas discussões percebe-se que a interne das coisas possibilita um mar de oportunidades que deve ser observado de perto por todas as indústrias e mercados. Entretanto, para que as coisas conectadas tragam mais benefícios, é necessário que as questões de segurança estejam presentes em todas as etapas de implantação dessa tecnologia.

3.2. Ferramenta De Mercado

Com os aplicativos sendo parte da rotina dos usuários, visto que o uso é bastante frequente, é mais do que normal que as empresas invistam em segurança. Neste contexto, acaba figurando a criptografia dos apps. Nos dias atuais, o mecanismo foi empregado de modo a proteger os dados dos usuários, sobretudo de invasores. O sistema Android, por exemplo, já oferece essa tecnologia em sua linguagem de programação e aplicativos como o WhatsApp, Telegram, e Followzup por exemplo, são alguns dos que usam a criptografia.

No geral, o sistema do aplicativo codifica informações do próprio aparelho, de modo a impedir que hackers invadam os dados e as usem de modo indevido. Resumindo, há uma espécie de chave colocada pelo próprio usuário que impede o uso desses dados. Essa proteção vai muito além das senhas de desbloqueio do aparelho, já que são mantidas por aplicativos.

3.3. Followzup

O Followzup é um serviço gratuito para envio de mensagens de texto criptografadas para celulares e outros dispositivos móveis. As mensagens são enviadas em background, a partir de sistemas e websites com o auxílio de APIs, disponíveis em PHP, Java, Ruby, Perl, Python, C# e .NET. As APIs são simples de usar, e com apenas 1 linha de comando a aplicação pode enviar uma mensagem para o celular de um ou mais usuários [FOLLOWZUP 2017].

Além de enviar, os websites Internet também podem receber mensagens dos usuários, originadas a partir de seus dispositivos móveis. A comunicação entre sistemas e dispositivos móveis por meio do Followzup é criptografada com os padrões AES e RSA, e o protocolo aberto do serviço permite o desenvolvimento de APIs para outras linguagens, assim como o desenvolvimento de APPs para diferentes modelos de dispositivos móveis [FOLLOWZUP 2017].

Exemplos de uso:

- Monitorar a atividade de usuários em sistemas e websites;
- Monitorar e enviar alertas sobre ocorrências em sistemas e equipamentos;
- Enviar notícias, dicas, avisos e mensagens publicitárias;
- Receber mensagens de solicitações dos usuários;
- Solicitar respostas de confirmação dos usuários;
- Enviar mensagens associadas a "links" externos;
- Informar e confirmar agendamento de compromissos;
- Informar a realização transações comerciais e financeiras;

As mensagens enviadas por meio do Followzup são criptografadas com os protocolos AES e RSA, garantindo confidencialidade em todo o trajeto percorrido pela informação. Cada aplicação e cada dispositivo móvel possui seu próprio par de chaves assimétricas RSA, e apenas o webservice Followzup pode decriptografar e ter acesso ao conteúdo das requisições.

Cada solicitação encaminhada ao serviço Followzup possui seu próprio número de sequência, garantindo maior segurança na comunicação entre sistemas e dispositivos. Com esse nível adicional de segurança, as requisições eventualmente interceptadas e reenviadas pela rede de acesso, são automaticamente consideradas inválidas pelo serviço.

4. Conclusão

A internet é uma grande rede onde milhares de informações se cruzam o tempo todo e nada impede, mesmo com toda a tecnologia, que certas mensagens possam ser capturadas enquanto circulam na web. Proteger as informações em trânsito é essencial para evitar que dados sigilosos de clientes, ou mensagens estratégicas acabem de posse de cibercriminosos ou pessoas mal-intencionadas. O uso de dispositivos móveis é muito comum. Essas ferramentas possibilitam que os colaboradores acessem dados pessoais e de empresa por meio de qualquer link de internet. O que ocorre é que muitas vezes a navegação pode ser realizada a partir de uma rede pública, como bibliotecas, shoppings centers e outros ambientes que disponibilizam acesso à web. Esse tipo de rede facilita a captura, por parte de criminosos, de senhas, usuários e outros dados importantes que podem ser utilizados em uma futura invasão e roubo de informações. Ao criptografar esses envios apenas o destinatário poderá fazer uso da chave para verificar o conteúdo.

Com a evolução da tecnologia, nada está seguro 100% seguro. Temos como exemplo todas as metodologias e técnicas de criptografia que foram mostradas ao longo do item 2. Cedo ou tarde todas as chaves foram quebradas, ou seja, utilizar da criptografia não garante totalmente o roubo de dados, porém nenhuma outra técnica de segurança da informação é tão eficaz quanto a criptografia. Por isso, pode-se afirmar que mesmo que não se possa obter a total certeza de que seus dados não serão decifrados e roubados por hackers, utilizar da criptografia é a melhor forma de se proteger contra o vazamento.

Referências

BURNETT, S.; PAINE, S. (2002). *Redes de Computadore Criptografia e SegurançãO guia oficial RSA*. Rio de Janeiro: Campus, 1ª edição edition.

FOLLOWZUP (2017). *Comunicação Criptografada Entre Aplicações e Dispositivos Móveis*. http://followzup.com/wiki/doku.php?id=br-000-index, 20 de maio de 2019 edition.

STALLINGS, W. (2014). *Criptografia e Segurança de Redes*. São Paulo: Pearson Education, 2014., 6ª edição edition.

TANENBAUM, A. S. (2003). *Redes de Computadores*. Campus, 4ª edição edition.