BLOG

128 RAZÕES PARA ENCRIPTAR DADOS NA IOT

O processo que garante a segura transmissão de dados está dependente de uma robusta e fiável encriptação dos dados a transmitir entre as diferentes plataformas/dispositivos.

A importância da informação e a sua privacidade é uma temática que tem centenas de anos. Prova disso são os sistemas de encriptação de mensagens concebidos pelos nossos antepassados, em eras onde o fluxo de dados era bastante inferior ao atual e onde o índice tecnológico era consideravelmente reduzido.

Provavelmente o sistema de encriptação que se tornou pioneiro na sua época, foi a máquina Enigma, usada pelos alemães na 2ª Guerra Mundial para proteger o conteúdo das suas comunicações. Desde então as metodologias de proteção de dados progrediram numa escala ascendente nos vários contextos, até à encriptação utilizada na era digital.

VISÃO

Quantidades massivas de dados são geradas diariamente por uma infinidade de dispositivos dispersos pelo globo. A inequívoca globalização da rede obriga a que as comunicações estabelecidas tendam a ser o mais seguras possível para assegurar a fiabilidade da informação e o cumprimento das políticas de privacidade dos dados das entidades e pessoas e permitir aos utilizadores uma experiência online mais segura. Os dados circulam pelos mais diversos tipos de redes, traduzindo-se numa clara exposição da informação a quem intencionalmente ou não, lhe possa aceder. O processo que garante a segura transmissão de dados está dependente de uma robusta e fiável encriptação dos dados a transmitir entre as diferentes

plataformas/dispositivos, através de complexos algoritmos de encriptação, gerados para movimentar todo o tipo de informação.

AES – O QUE É?

O algoritmo de encriptação de dados **Advanced Encryption Standard** (AES) foi desenvolvido entre os anos 1997 e 2001 pelo **National Institute Of Standards and Technology** (NIST) no seguimento da procura por um sucessor para o bloco de encriptação Data Encryption Standard (DES) que foi assistindo a uma deterioração das suas capacidades fruto do avanço tecnológico. Após a avaliação do sistema de encriptação do AES e respetivos testes de performance, a sua inclusão em sistemas tecnológicos de entidades como a **National Secutiry Agency**, geralmente denominada pelo seu acrónimo NSA e o **Governo dos Estados Unidos da América** evidenciou a confiança depositada neste algoritmo e a sua afirmação como processo de incrementação de segurança na transmissão de dados.

AES é um algoritmo de encriptação padrão mais usado a nível global para proteção de dados que suporta chaves de 128, 192 e 256 bits de comprimento. Define-se como um sistema de cifra de bloco simétrico. O que tem de diferente em relação aos blocos assimétricos? Sucintamente, torna o processo de encriptação e desencriptação mais rápido derivado da baixa utilização de recursos computacionais e tem como condição base da sua utilização, a aplicação da mesma chave para encriptação e desencriptação da mensagem.

A escolha da chave para a encriptação determina quantos rounds serão necessários para transpor o texto simples através da cifra e resultar no texto encriptado. As chaves de 128 bits requerem 10 rounds, por sua vez, a chave de 192 bits requer 12 rounds e uma chave de 256 bits necessitará de 14 rounds. Quanto mais longa for a chave selecionada, mais segura se torna a encriptação. Contudo, o processo requer mais tempo para estar concluído, tanto na encriptação como na desencriptação.

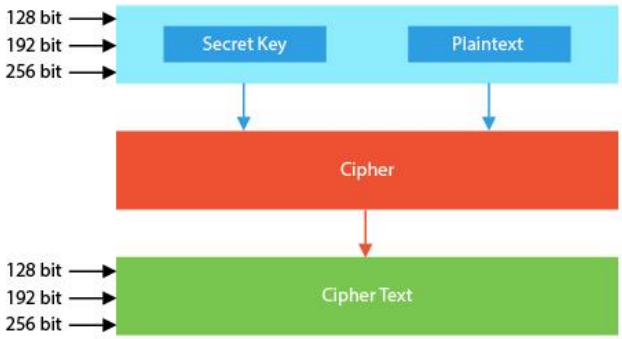

Figura 1 - Esquema gráfica da encriptação do algoritma AES

Algumas utilizações comuns do algoritmo AES:

- VPN's (exemplo: **ExpressVPN** – utiliza a encriptação AES 256 bits para o controlo de canal);

- Ferramentas de compressão (exemplo: **WinRAR** - utiliza a encriptação AES 256 bits na aplicação de passwords a ficheiros comprimidos);

- Aplicações de mensagens (exemplo: **WhatsApp** – usa a encriptação AES 256 bits para a transferência de ficheiros de mídia);

Para experienciar a aplicação do algoritmo de encriptação AES, a DevGlan desenvolveu uma **ferramenta online** que permite simular a codificação e descodificação de informação. Podemos aferir a complexidade da informação encriptada e com que facilidade a mesma pode ser desencriptada tendo acesso aos recursos de desencriptação necessários.

COMUNICAÇÃO SEM FIOS SEGURA

Globalmente assistimos a um aumento da aplicação de sensores para monitorização de ambientes críticos e controlo de aplicações em redes sem fios. Os dados recolhidos nos diversos terminais devem permanecer legíveis apenas aos seus destinatários para evitar o desvio de informações que possam indiretamente revelar outros dados. Um caso de estudo prático é o exemplo da política de privacidade implementada pela **NSA**, que não publica a informação relativa aos consumos de energia dos seus *data centers* com a intenção de proteger o possível cálculo de recursos computacionais usados.

A proteção da informação providenciada pelas ligações sem fios tem sido alvo de escrutínio quase diário, discussão essa gerada em volta das notícias sobre falhas de segurança em redes sem fios pelo desencadeamento de inúmeros ataques informáticos. Ainda assim, continua a ser maior o número de ligações devidamente seguras do que as que não o são. É uma questão de notoriedade mediática. A vulnerabilidade das redes sem fios é ultrapassada com a implementação de medidas de segurança acrescidas que têm vindo a garantir quase na sua totalidade uma correta e fiável utilização.

Enquanto organização caracterizada pela aposta na investigação e desenvolvimento de soluções sem fios, a segurança e privacidade dos dados recolhidos são para a **Tekon Electronics** uma mais valia que implementa nas suas soluções sem fios com o propósito de proporcionar uma aposta segura a implementar no âmbito industrial. A acuidade dos dados na **Indústria 4.0** fomenta a aplicação de medidas de segurança robustas para a transmissão de dados.

As famílias de produtos sem fios **DUOS** e **PLUS** desenvolvidas com base no conceito tecnológico da **Internet das Coisas** (IoT) transferem a responsabilidade da proteção de dados para o seu processo de comunicação entre as diferentes plataformas. O processo de encriptação de dados recolhidos pelos sensores instalados nos transmissores até à comunicação com o gateway está garantido pela utilização do algoritmo **AES** com uma chave de **128 bits**.

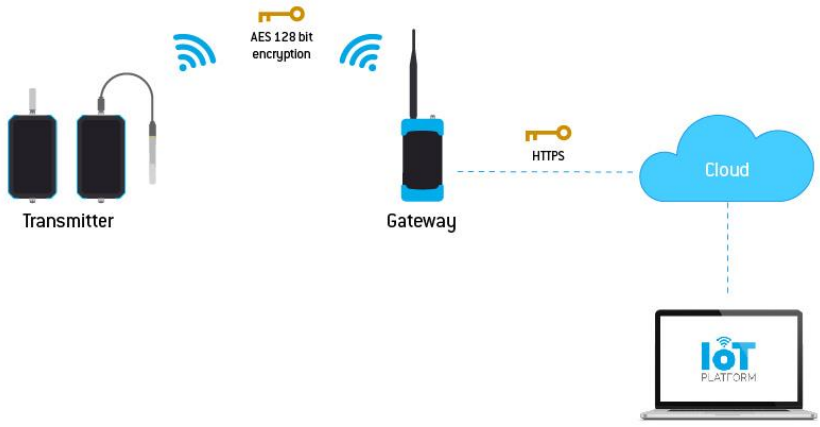

Figura 2 - Demonstração gráfica da encriptação dos dispositivos sem fios da Tekon Electronis

A iniciativa pelo planeamento e desenvolvimento total da solução de dispositivos e da plataforma **IoT**, incute à **Tekon Electronics** a tarefa de assegurar uma legítima e fiável comunicação entre os nossos dispositivos e a *cloud* de partilha de informação. A posterior transferência da informação decorre sobre a responsabilidade de sistemas de segurança definido por terceiros, por já não se enquadrarem em tipologias diretamente relacionadas com a utilização prática das soluções sem fios.

CONCLUSÕES FINAIS

A encriptação de dados continua a ser um tópico principal naquele que é um dos procedimentos que cada vez mais atrai as atenções para si – **a segurança de dados**. O merecido destaque destes sistemas é sinónimo do valor que acrescentam às organizações, evidenciando a sua utilização na modernização da indústria e dos processos produtivos. Desenvolver produtos tecnológicos com o desígnio de oferecer um elevado índice de segurança da transmissão de dados continua a destacar os produtos e serviços IoT presentes no concorrido mercado global.

A ausência de registos válidos que indiquem alguma vulnerabilidade do algoritmo de encriptação **AES** tem contribuído para a solidificação da confiança depositada nesta solução que continua a ser uma escolha pelas entidades de referência nas variadas aplicações tecnológicas do nosso quotidiano.