Diretrizes de Segurança em IoT para Operadoras de Rede

Diretrizes de Segurança em IoT para Operadoras de Rede

Versão 2.0

31 de outubro de 2017

Este é um documento de referência permanente e não vinculante da GSMA

Classificação de segurança: não confidencial

Aviso de direitos autorais

Aviso legal

Aviso antitruste

Sumário

1 Introdução

1.1 Panorama

Este documento fornece diretrizes de segurança de alto nível para operadoras de rede que pretendem prestar serviços aos provedores de serviços de IoT para garantir a segurança do sistema e a privacidade dos dados. Essas recomendações baseiam-se em sistemas e tecnologias facilmente disponíveis e já em uso.

1.2 Estrutura do documento

Este documento destina-se a operadoras de rede e provedores de serviços de IoT. Os leitores deste documento também podem se interessar pela leitura de outros textos do conjunto de documentos das Diretrizes de Segurança para IOT da GSMA [11], conforme mostrado abaixo.

Figura 1 - Estrutura do documento da GSMA "Diretrizes de segurança para IoT"

1.3 Propósito e escopo do documento

Este documento deve funcionar como um checklist nos acordos de fornecimento entre os provedores de serviços de IoT e suas operadoras da rede parceiras.

O escopo do documento é limitado a:

- Diretrizes de segurança relacionadas aos serviços de IoT
- Recomendações relativas aos serviços de segurança oferecidos por uma operadora de rede
- Tecnologias de rede celular

Este documento não se destina a criar novas especificações ou padrões de IoT, mas fará referência às soluções, padrões e práticas recomendadas atualmente disponíveis.

Este documento não se destina a acelerar a obsolescência dos serviços de IoT existentes. A compatibilidade com versões anteriores dos serviços de IoT da operadora de rede deve ser mantida enquanto forem considerados adequadamente protegidos.

Este documento não aborda os problemas de segurança associados às interfaces e às APIs implementadas na plataforma de serviços de IoT (ou plataforma de gerenciamento de conectividade IoT) para que ela compartilhe seus dados com os usuários finais (por exemplo, para compartilhar dados com um usuário final por meio de um smartphone ou aplicação para PC) ou outras entidades dentro do ecossistema. Essas interfaces e APIs devem ser protegidas usando as “melhores práticas” em tecnologias e protocolos de segurança de internet.

Note-se que a adesão às leis e regulamentos nacionais para um determinado território pode, quando necessário, anular as diretrizes estabelecidas neste documento.

1.4 Público-alvo

O principal público-alvo para este documento é:

- Em primeiro lugar, as operadoras de rede que desejam oferecer serviços a prestadores de serviços de IoT
- Em segundo lugar, empresas e organizações que procuram desenvolver novos e inovadores produtos e serviços conectados (a chamada "Internet das Coisas") utilizando redes celulares ou de linha fixa. Neste documento, nos referimos a essas empresas como "provedores de serviços de IoT"

1.5 Definições

Termo	Descrição
Relatório de Identificação do Host do Dispositivo	Capacidade de um endpoint de relatar as informações do host para uma operadora de rede. Veja as Diretrizes de Eficiência de Conexão da GSMA [17].
Diâmetro	O diâmetro é um protocolo de autenticação, autorização e contabilidade para redes de computadores. Veja IETF RFC 6733 [18].
Endpoint	Um endpoint, em IoT, é um dispositivo de computação física que executa uma função ou tarefa como parte de um produto ou serviço conectado à internet. Consulte a seção 3 do CLP.13 [29] para obter uma descrição das três classes comuns de dispositivos IoT e exemplos de cada classe de endpoint.
Gateway	Um endpoint de alta complexidade que normalmente serve para interligar endpoints de baixa complexidade (conectados por meio de uma rede local) e uma WAN. Consulte CLP.13 [29] para obter mais informações.
Internet das Coisas	A Internet das Coisas (IoT) descreve a coordenação de várias máquinas, dispositivos e aplicações conectados à internet por meio de múltiplas redes. Esses dispositivos incluem objetos comuns, como tablets e eletrônicos de consumo, e outras máquinas, como veículos, monitores e sensores dotados de recursos de comunicação que lhes permitem enviar e receber dados.
Plataforma de Gerenciamento de Conectividade em IoT	Esse sistema é geralmente hospedado pela operadora de rede para permitir a autogestão de assinaturas e planos de preços de IoT pelo provedor de serviços de IoT.
Serviço de IoT	Qualquer programa de computador que aproveite dados de dispositivos IoT para executar o serviço.

Termo	Descrição
Plataforma de Serviço de IoT	A plataforma de serviço é hospedada pelo provedor de serviços de IoT, que se comunica com um endpoint para fornecer um serviço IoT.
Provedor de Serviço de IoT	Empresas ou organizações que buscam desenvolver novos e inovadores produtos e serviços de IoT conectados. O provedor pode ser uma operadora de rede.
Endpoint de Baixa Complexidade	Normalmente este é um dispositivo limitado (por exemplo, sensor ou atuador) que se conecta a um serviço IoT por meio de um gateway.
Operadora de rede	A operadora da rede de comunicação que está conectando o endpoint IoT à plataforma de serviço IoT.
UICC	Uma plataforma de elemento seguro, especificada no ETSI TS 102 221, que pode suportar múltiplas redes padronizadas ou aplicações de autenticação de serviço em domínios de segurança separados criptograficamente. Pode ser integrada em formatos incorporados e especificados no ETSI TS 102 671.
WAN	Rede de telecomunicações que se estende por uma grande distância geográfica.

1.6 Abreviaturas

Termo	Descrição
3GPP	3rd Generation Project Partnership
AKA	Autenticação e acordo de chave
APDU	Unidade de Dados do Protocolo de Aplicação
API	Interface do Programa de Aplicações
APN	Nome do Ponto de Acesso
BGP	Protocolo de Gateway de Borda
CEIR	Registro Centralizado de Identidade do Equipamento
CERT	Grupo de Respostas a Incidentes de Segurança em Computadores
DNS	Sistema de Nomes de Domínio
DoS	Negação de Serviço
DPA	Acordo de Processamento de Dados
EAB	Restrição de Acesso Estendida
EAP	Protocolo de Autenticação Estendida
EID	Identidade eUICC
ETSI	Instituto Europeu de Normas de Telecomunicações
EU	União Europeia
eUICC	Embedded UICC
FASG	Grupo de Fraude e Segurança
GCF	Fórum de Certificação Global
GGSN	Nó de Suporte do Gateway GPRS
GPRS	General Packet Radio Service

Termo	Descrição
GRX	Troca de Roaming GPRS
GSM	Global System for Mobile Communication
GSMA	GSM Association
GTP	Protocolo de Tunneling GPRS
HLR	Registro de Localização Residencial
HSS	Servidor de Assinante Doméstico
ICCID	Identidade do Cartão de Circuito Integrado
IMEI	Identidade de Equipamento de Estação Móvel Internacional
IMSI	Identidade de Assinante Móvel Internacional
IoT	Internet das Coisas
IP	Protocolo de internet
IPSec	Segurança do Protocolo de Internet
L2TP	Protocolo de Encapsulamento da Camada Dois
LBO	Pausa Local
LPWAN	Redes de Longo Alcance e Baixa Potência
LTE	Evolução a Longo Prazo
M2M	Máquina a Máquina
MAP	Parte de Aplicação Móvel
MME	Entidade de gestão de mobilidade
OMA	Open Mobile Alliance
OSS	Sistema de Suporte de Operações
OTA	Over The Air
PTCRB	Originalmente significava PCS Type Certification Review Board, mas não é mais utilizável.
RAN	Rede de Acesso por Rádio
SAS	Plano de Credenciamento de Segurança
SGSN	Servindo o Nó de Suporte GPRS
SIM	Módulo de Identidade do Assinante
SMS	Serviço de Mensagens Curtas
SoR	Direcionamento de Roaming
SS7	Sistema de Sinalização nº 7
UMTS	Serviço Universal de Telecomunicações Móveis
USSD	Dados de Serviços Suplementares Não Estruturados
VLR	Registro de Localização do Visitante
VPN	Rede Virtual Privada
VoLTE	Voz sobre LTE
WAN	Rede de Longo Alcance

1.7 Referências

Ref	Nº do Doc.	Título
[1]	ETSI TS 102 225	Estrutura de Pacotes Segura para Aplicações Baseadas em UICC www.etsi.org
[2]	ETSI TS 102 226	Estrutura Remota de APDU para Aplicações Baseadas em UICC www.etsi.org
[3]	3GPP TS 31.102	Características da aplicação USIM (Universal Subscriber Identity Module) www.3gpp.org
[4]	N/A	Especificação Aberta de API Móvel www.simalliance.org
[5]	OMA DM	Gerenciamento de Dispositivos OMA www.openmobilealliance.org
[6]	OMA FUMO	Objeto de Gerenciamento de Atualização de Firmware OMA www.openmobilealliance.org
[7]	GSMA SGP.02	Arquitetura de Aprovisionamento Remoto para Especificação Técnica do Embedded UICC (eSIM) www.gsma.com
[8]	ETSI TS 102 310	Suporte ao Protocolo de Autenticação Extensível no UICC www.etsi.org
[9]	3GPP TS 23.122	Funções do Non-Access-Stratum (NAS) relacionadas à Estação Móvel (MS) em Modo Inativo www.3gpp.org
[10]	NISTIR 7298	Glossário dos Principais Termos de Segurança da Informação www.nist.gov
[11]	GSMA CLP.11	Documento de Panorama de Diretrizes de Segurança em IoT https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[12]	n/a	Apresentando o Mobile Connect - o novo padrão em autenticação digital https://www.gsma.com/identity/mobile-connect
[13]	3GPP TS 34.xxx	Especificações da Série 3GPP 34 www.3gpp.org/DynaReport/34-series.htm
[14]	3GPP TS 37.xxx	Especificações da Série 3GPP 37 www.3gpp.org/DynaReport/37-series.htm
[15]	3GPP TS 31.xxx	Especificações da Série 3GPP 33 www.3gpp.org/DynaReport/31-series.htm
[16]	GSMA FS.04	Esquema de Credenciamento de Segurança para Produção de UICC http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/security-accreditation-scheme
[17]	GSMA CLP.03	Diretrizes de Eficiência de Conexão de Dispositivos IoT https://www.gsma.com/iot/iot-device-connection-efficiency-guidelines/

Ref	Nº do Doc.	Título
[18]	IETF RFC 6733	Protocolo Diameter www.ietf.org
[19]	ETSI TS 102 690	Comunicações Máquina a Máquina (M2M); Arquitetura Funcional www.etsi.org
[20]	TR-069	Protocolo de Gerenciamento de WAN CPE www.broadband-forum.org
[21]	n/a	Conexão de ID Aberto openid.net/connect/
[22]	n/a	Aliança FIDO (Identidade Rápida On-line) fidoalliance.org/
[23]	ETSI TS 102 204	Comércio Móvel (M-COMM); Serviço de Assinatura Móvel; Interface de Serviço Web www.etsi.ord
[24]	n/a	Instituto Nacional de Padrões e Tecnologia (NIST) www.nist.gov
[25]	n/a	Rede Europeia de Excelência em Criptologia (ECRYPT) www.ecrypt.eu.org
[26]	GSMA CLP.12	Diretrizes de Segurança em IoT para Ecossistema de Serviço IoT https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[27]	IETF RFC 5448	Método Aprimorado de Protocolo de Autenticação Extensível para Autenticação de 3ª Geração e Acordo de Chave (EAP-AKA) tools.ietf.org/html/rfc5448
[28]	IETF RFC 4186	Método de Protocolo de Autenticação Extensível para GSM para Módulos de Identidade do Assinante de Comunicações Móveis (EAP-SIM) tools.ietf.org/html/rfc4186
[29]	GSMA CLP.13	Diretrizes de Segurança em IoT para Ecossistema de Endpoint IoT https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[30]	n/a	Segurança sem fio em redes LTE www.gsma.com/membership/wp-content/uploads/2012/11/SenzaFili_WirelessSecurity_121029_FINAL.pdf
[31]	n/a	Especificações oneM2M www.oneM2M.org
[32]	GSMA CLP.17	Checklist de Verificação de Segurança em IoT https://www.gsma.com/iot/iot-security-assessment/
[33]	n/a	Comparação de Segurança de Tecnologia LPWA. Um white paper da Franklin Heath Ltd https://goo.gl/JIOlr6
[34]	CLP.28	Guia de Implantação NB-IoT www.gsma.com/iot

Ref	Nº do Doc.	Título
[35]	CLP.29	Guia de Implantação LTE-M www.gsma.com/iot
[36]	3GPP TS33.163	Segurança Eficiente para Bateria de Dispositivos (BEST) de Comunicação de Máquina (MTC) com Baixa Taxa de Transmissão www.3GPP.org

2 Recursos do serviço de IoT que as operadoras de rede podem proteger

Os recursos de segurança que precisam ser implementados para proteger adequadamente os ativos do serviço IoT são específicos para cada caso. Portanto, continua sendo responsabilidade do provedor de serviços de IoT usar os processos adequados de avaliação de impacto de risco e privacidade para obter suas necessidades específicas de segurança. As operadoras de rede e os provedores de serviços de IoT geralmente compartilham requisitos de segurança semelhantes para proteger seus ativos, portanto, faz sentido que eles potencializem soluções de segurança comuns em vez de implementar infraestruturas de segurança duplicadas (e possivelmente redundantes). Além disso, em muitos casos, as operadoras de rede serão também provedores de serviços de IoT.

Os serviços de segurança fornecidos pelas operadoras de rede podem desempenhar um papel fundamental na garantia dos ativos usados para fornecer um serviço de IoT. Estes podem incluir:

- Os dados do serviço de IoT são enviados entre um endpoint IoT e a plataforma de serviço de IoT - isso inclui dados primários confidenciais (por exemplo, dados relacionados ao usuário final) e dados comercialmente exploráveis (por exemplo, dados de controle do atuador) que também podem ter algum impacto sobre a privacidade secundária
- Os recursos de segurança (IMSI, keysets, etc.) e as configurações de rede (APN, valores do temporizador, etc.) utilizados nos endpoints (incluindo os dispositivos gateway)
- As informações comerciais do fornecedor de serviços de IoT, incluindo a reputação da marca, os dados do cliente / usuário sob a responsabilidade da empresa, informações estratégicas, dados financeiros e registros de saúde, etc
- Infraestruturas de negócios do provedor de serviço de IoT, plataformas de serviços, redes corporativas e outros elementos da rede privada
- Infraestruturas públicas de data center (ou seja, compartilhadas) fornecidas pela operadora de rede e usadas pelo serviço de IoT. Isso pode incluir serviços públicos, hospedagem, infraestruturas de virtualização, instalações da nuvem, etc
- Infraestrutura de rede de comunicações, incluindo redes de acesso por rádio, rede central, redes de backbone, funções básicas de serviço (DNS, BGP, etc.), acesso e agregação de redes fixas e celulares, etc.

3 Princípios de segurança de rede

Mecanismos de segurança adequados e confiáveis devem ser implementados pelas operadoras em suas redes.

Nesta seção descreve-se como as redes podem agregar valor ao ecossistema de IoT.

Mecanismos de segurança mais fundamentais fornecidos por uma rede de comunicação:

- Identificação e autenticação das entidades envolvidas no serviço de IoT (ou seja, gateways, endpoints, rede doméstica, redes de roaming, plataformas de serviço)
- Controle de acesso para as diferentes entidades que precisam ser conectadas para criar o serviço de IoT
- Proteção de dados para garantir a segurança (confidencialidade, integridade, disponibilidade, autenticidade) e privacidade das informações da rede para o serviço de IoT
- Processos e mecanismos para garantir a disponibilidade de recursos de rede e protegê-los contra ataques (por exemplo, implementando firewall apropriado, prevenção de intrusão e tecnologias de filtragem de dados)

3.1 Identificação de segurança de usuário, aplicações, endpoints, redes e plataformas de serviços

A identificação consiste em fornecer identificadores únicos para as entidades dentro do serviço de IoT e correlacionando essas identidades eletrônicas com identidades reais e juridicamente vinculativas.

Com um celular conectado a um serviço de IoT, os endpoints são identificados usando IMSI e / ou IMEI (EIDs também podem ser usados para dispositivos com eUICCs). As redes são identificadas usando códigos de rede e códigos do país. Cada método de fornecer identidade tem níveis variáveis de garantia segura associados a ele.

A identidade desempenha um papel crucial no processo de autenticação, uma vez que a autenticação segura só pode ser alcançada com base em uma identidade segura. Portanto, é essencial que as identidades (por exemplo, IMSI, IMEI ou ICCID) emitidas e usadas dentro de um serviço de IoT estejam protegidas de forma segura contra roubo, modificações e personificação.

Um problema prático que o provedor de serviço de IoT pode enfrentar é que seu serviço pode exigir comunicações com muitas plataformas de serviços de IoT, e cada uma delas pode exigir uma identificação única e separada. Cada identidade usada para estabelecer um link de comunicação para cada plataforma de serviços de IoT precisará ser provisionada, armazenada e gerenciada de forma segura pelo serviço IoT.

Quando for apropriado para o serviço de IoT, as operadoras de rede recomendam o uso de mecanismos baseados no UICC para identificar de forma segura os endpoints. As operadoras de rede também podem ampliar a funcionalidade de armazenamento seguro fornecido pelo UICC para o provedor de serviço de IoT, o que permite que eles armazenem identidades adicionais no UICC relacionadas ao serviço de IoT. Esta técnica pode ser aplicada a endpoints celulares e não-celulares (por exemplo, EAP-AKA [27]).

Os serviços de "Single sign-on" também podem ser fornecidos pelas operadoras de rede para permitir que os endpoints estabeleçam e comprovem sua identidade uma vez e, em seguida, se conectem a várias plataformas de serviços de IoT sem mais inconvenientes. Os compromissos de segurança e os riscos de usar esse serviço devem ser considerados em várias plataformas.

3.2 Autenticação segura de usuários, aplicações, endpoints, redes e plataformas de serviços

De acordo com o NIST [10], "autenticação" é "verificar a identidade de um usuário, processo ou dispositivo de endpoint, muitas vezes como pré-requisito para permitir o acesso a recursos em um sistema de informações".

As operadoras de rede podem fornecer serviços para garantir que os usuários, aplicações, endpoints, redes e plataformas de serviços associados a um serviço de IoT sejam autenticados com segurança

A autenticação possui uma propriedade relacionada - a de não repúdio. De acordo com o NIST [10], uma definição de não repúdio é: "a garantia de que o remetente de informações possui um comprovante de entrega e o destinatário possui a prova da identidade do remetente, portanto, não pode, em um segundo momento, negar ter processado a informação". Não repúdio equivale a afirmar que a autenticidade não foi violada ao identificar a origem dessa transação ou mensagem.

3.3 Fornecimento de canais de comunicação seguros

As operadoras de rede fornecem mecanismos de segurança de comunicações para redes fixas e celulares de longa distância, garantindo a integridade, confidencialidade e autenticidade das comunicações “best in class”. Quando apropriado, as operadoras de rede podem fornecer e gerenciar conexões seguras para redes corporativas usando redes privadas virtuais (VPNs) e conexões de internet criptografadas.

O objetivo de um canal de comunicação seguro é garantir que os dados enviados pelo canal não sejam processados, utilizados ou transmitidos sem o conhecimento e o consentimento da pessoa em causa. As tecnologias de criptografia desempenham um papel crucial na transmissão segura de dados, garantindo as propriedades de confidencialidade, integridade e autenticidade. A criptografia deve ser apropriada para o sistema que está sendo projetado e implantado, levando em consideração endpoints de baixa complexidade, aspectos de rede (como restrições de backhaul de satélite) e o serviço fornecido.

As operadoras de rede podem fornecer criptografia de dados aos provedores de serviços IoT para garantir a integridade da comunicação e a resiliência da rede.

As operadoras de rede tradicionalmente fornecem infraestrutura de telecomunicações públicas ou uma mistura de infraestrutura de rede pública e privada. Muitas operadoras de rede podem garantir que os dados do cliente/usuário que transitam na infraestrutura de rede pública sejam criptografados entre o ponto em que os dados entram na infraestrutura da rede pública até o ponto em que saem da rede. Quando necessário, as operadoras de rede também podem ajudar os provedores de serviços de IoT a implantar ou derivar suas

próprias credenciais de criptografia para garantir a confidencialidade dos dados de IoT durante o trânsito pela infraestrutura da operadora de rede

As operadoras de rede podem fornecer aos seus clientes redes privadas nas quais canais de comunicação dedicados são fornecidos para o uso de um único cliente para garantir que nenhum dado atravesse uma rede pública como a internet. Tais redes privadas poderiam ser criadas:

1. Pelo uso de um protocolo de tunelamento, como Layer Two Tunneling Protocol (L2TP), protegido por protocolos como Internet Protocol Security (IPsec) ou
2. Pelo fornecimento aos clientes de segurança ponta a ponta entre o UE e o servidor de aplicações, por exemplo, BEST [36] ou
3. Pela criação de uma rede dedicada para o serviço de IoT implantando uma instância separada da rede core compartilhada com rede de rádio - conforme o exemplo abaixo.

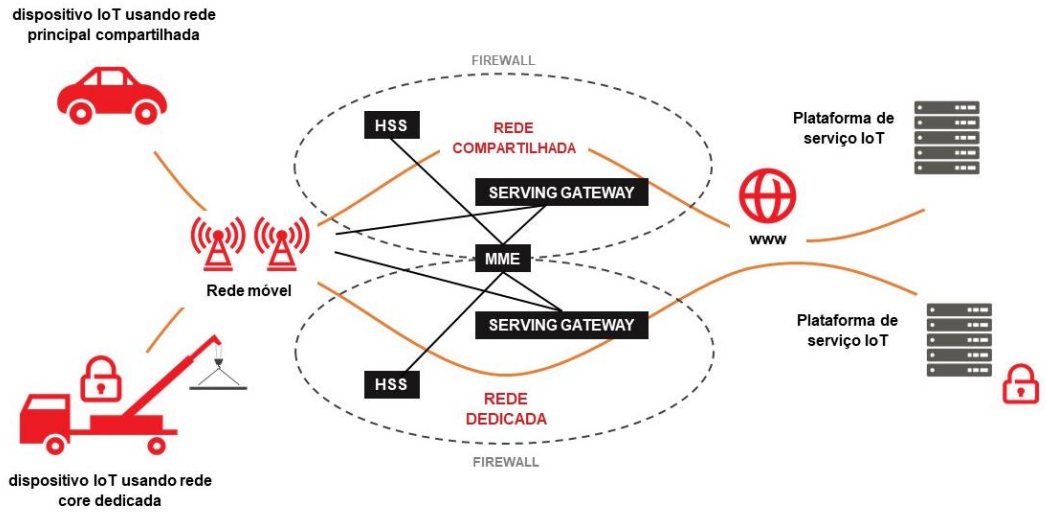


Figura 2 – Exemplo de configuração de rede privada

3.4 Garantia de disponibilidade de canais de comunicação

De acordo com o NIST [10], "disponibilidade" é a propriedade de ser acessível e utilizável mediante demanda por uma entidade autorizada.

As operadoras de rede podem fornecer disponibilidade de rede aos provedores de serviços de IoT. Os mecanismos mais fundamentais para que as operadoras de rede forneçam disponibilidade de rede são os seguintes:

3.4.1 Uso de espectro licenciado

As operadoras de rede integrantes da GSMA operarão redes usando espectro licenciado dedicado sob os termos das licenças emitidas por seus reguladores nacionais. O uso do espectro licenciado garante que a interferência de outras tecnologias de rádio seja reduzida ao mínimo, pois qualquer uso não autorizado desse espectro será objeto de processo. As operadoras de rede, juntamente com os reguladores nacionais, procurarão quaisquer fontes de interferência não autorizadas para garantir que a disponibilidade da rede não seja impactada.

O uso do espectro licenciado, que fornece bandas de rádio dedicadas para a operadora utilizar sua rede, garante que a operadora assegure uma cobertura cuidadosa e planejamento de capacidade para obter a máxima disponibilidade de serviço para seus clientes.

3.4.2 Implementação de tecnologias de rede padronizadas e comprovadas

As operadoras de rede que fazem parte da GSMA implementam tecnologias de rede padronizadas, como GSM, UMTS e LTE, conforme especificado por órgãos de padrões como o 3GPP. O uso de tecnologias padronizadas não só assegura a interoperabilidade entre as operadoras de rede, como também garante que o padrão esteja sujeito a análise durante sua criação para garantir a robustez da tecnologia.

3.4.3 Implementação de tecnologias de rede testadas e certificadas

Muitas partes da rede de uma operadora serão testadas e certificadas de acordo com os padrões internacionais de teste. Os endpoints de alta complexidade e os módulos de comunicação que eles contêm estarão sujeitos às especificações de teste 3GPP [13] via GCF, PTCRB e teste de aceitação da operadora de rede. As redes de acesso de rádio (RAN) estarão sujeitas às especificações de teste 3GPP [14] por meio do teste de aceitação da operadora de rede. Os UICCs estarão sujeitos às especificações do teste 3GPP [15] por meio de testes de aceitação da operadora de rede e, além disso, podem estar sujeitos à certificação GSMA SAS [16].

3.4.4 Topografias e configuração de rede resiliente

As operadoras de rede fornecem redes resilientes que implementam e desenvolvem a redundância e o isolamento geográfico necessários para garantir a máxima disponibilidade com o menor tempo de inatividade. Todos os elementos da rede são cuidadosamente configurados e monitorados para garantir uma satisfação da rigorosa qualidade do serviço e dos acordos de nível de serviço.

3.4.5 Monitoramento e gerenciamento de recursos de rede em tempo real

As operadoras de rede implementam centros de operações de última geração que monitoram o desempenho de suas redes 24/7 e em tempo real para gerenciar o tráfego de rede, responder à demanda e corrigir falhas. Informações adicionais podem ser encontradas na seção 4.10

3.4.6 Gerenciamento de ameaças e compartilhamento de informações

O Grupo de Fraude e Segurança da GSMA (FASG, da sigla em inglês) fornece um ambiente aberto, receptivo e confiável para todas as operadoras de rede, a fim de compartilhar informações de fraude e informações de segurança e incidentes de forma oportuna e responsável. O grupo avalia o panorama global de ameaças de fraude e segurança, analisa os riscos associados às operadoras de rede e seus clientes, define e prioriza as ações atenuantes apropriadas.

3.4.7 Serviços de roaming

Devido ao uso de tecnologias padronizadas de rede e endpoints e serviços de interconexão, operadoras de rede podem oferecer serviços de roaming, aprimorando ainda mais a cobertura e disponibilidade de rede para seus clientes.

3.4.8 Monitoramento e gerenciamento de desempenho do endpoint

As operadoras de rede podem medir o desempenho dos endpoints que se conectam às suas redes para isolar os que podem estar criando excessivas interferências de rádio (por exemplo, por não conformidade com as regulamentações nacionais) ou tráfego de sinalização de rede (por exemplo, por não estar de acordo com as Diretrizes de Eficiência de Conexão da GSMA [17]) que, por sua vez, podem estar degradando o desempenho da rede como um todo. Os endpoints podem, portanto, ser monitorados, desconectados ou podem ter o firmware atualizado quando o comportamento anormal é detectado.

4 Considerações sobre privacidade

Para perceber as oportunidades que a IoT oferece, é importante que os consumidores confiem nos provedores que estão entregando serviços de IoT e coletando dados sobre eles. A GSMA e seus membros acreditam que a confiança dos consumidores só pode ser totalmente alcançada quando os usuários sentem que sua privacidade é devidamente respeitada e protegida.

Já existem leis bem estabelecidas de proteção de dados e privacidade em todo o mundo que foram aplicadas e cumpridas pelas operadoras de rede. As operadoras acreditam que é possível aplicar os regulamentos e princípios de proteção de dados existentes para atender às necessidades de privacidade no contexto dos serviços e tecnologias de IoT.

No entanto, os serviços de IoT normalmente envolvem operadoras que trabalham em conjunto com provedores parceiros de serviços de IoT. É importante que haja clareza regulatória e segurança jurídica em relação aos serviços de IoT e que os regulamentos de proteção de privacidade e dados sejam aplicados de forma consistente e neutra para todos os provedores de serviços.

As operadoras de rede devem estar cientes de que, se processarem dados, precisam assinar um Acordo de Processamento de Dados (DPA) com o provedor de serviços de IoT. As práticas de proteção e segurança de dados desenvolvidas para um determinado serviço de IoT devem refletir o risco como um todo para a privacidade de um indivíduo e o contexto em que os dados sobre o indivíduo são coletados, distribuídos e usados. Todas as intervenções regulamentares devem ser limitadas às áreas onde os riscos identificados emergem e as medidas existentes são insuficientes para abordá-las. Por exemplo, o OneM2M (através do TS-0003 [31]) permite que a operadora desempenhe o papel de gerenciador de privacidade para um provedor de serviços.

As operadoras de rede podem aproveitar sua ampla experiência em abordar problemas de privacidade e segurança e trabalhar em colaboração com os provedores de serviços de IoT, para incorporar privacidade e segurança nas tecnologias de IoT e na experiência do consumidor. Essa colaboração garantirá que os provedores de serviços de IoT possam identificar e mitigar os riscos de privacidade dos consumidores relevantes no contexto do serviço que está sendo entregue.

Para mais informações, consulte os Princípios de Privacidade dos Serviços Móveis da GSMA
http://www.gsma.com/publicpolicy/mobile-and-privacy/mobile-privacy-principles

5 Serviços fornecidos pelas operadoras de rede

As operadoras de rede podem fornecer redes celulares de longa distância (WANs) seguras aos provedores de serviços de IoT.

Esta seção contém recomendações de melhores práticas ao conectar serviços de IoT a redes de longa distância. Quando apropriado, as recomendações serão independentes da tecnologia utilizada, mas também usarão as melhores práticas de redes celulares e outros tipos de rede.

5.1 Procedimentos seguros de gerenciamento de assinatura

Esta seção contém recomendações sobre como as assinaturas do provedor de serviços de IoT devem ser gerenciadas pelas operadoras de rede:

- A operadora de rede ou o provedor de serviços de IoT deve realizar uma avaliação dos serviços de rede necessários para habilitar o serviço de IoT (voz, dados, SMS, etc.) agora e no futuro.
- Com base nesta avaliação, a operadora de rede deve trabalhar de acordo com o "princípio de privilégio mínimo" e fornecer assinaturas do provedor de serviços de IoT com apenas os serviços necessários para o serviço específico. Por exemplo:
    - Os serviços de IoT que usam apenas portadores de dados não devem ser provisionados com serviços de voz e SMS
    - Quando um endpoint só se conecta a uma plataforma de serviço de IoT conhecida, a assinatura associada a esse dispositivo deve apenas permitir a conexão a uma lista branca conhecida por intervalos de endereços IP (ou domínios).
    - Se o serviço de IoT usar voz ou SMS, o uso de uma lista de discagem fixa pré-configurada deve ser considerado.
- As operadoras de rede devem implementar processos seguros de inscrição para assinaturas IoT que habilitem serviços críticos de IoT (por exemplo, para as assinaturas associadas a serviços de saúde). Esses serviços não devem ser arbitrariamente desconectados.
- As operadoras de rede devem identificar os UICCs usados para os serviços de IoT dos UICCs tradicionais usados para fornecer serviços tradicionais e, se exigido pelo provedor de serviços de IoT, separá-los adequadamente.
    - Se os UICCs usados para os serviços de IoT forem segregados dos UICCs usados para “aparelhos” tradicionais, isso fornecerá uma base para um gerenciamento mais seguro e eficiente das assinaturas associadas pela operadora de rede. Por exemplo, uma operadora de rede pode considerar o uso de um HLR / HSS separado para endpoints que tenham vida útil estendida e estejam mais bem configurados para suportar esses UICCs por um período muito longo (ou seja, muitos anos).

5.1.1 Fornecimento e gerenciamento de UICC

5.1.1.1 Gerenciamento remoto de UICC (Over the air)

Os endpoints IoT não são fisicamente acessíveis em alguns cenários. Para poder realizar alterações no UICC remotamente, o gerenciamento over the air do UICC deve ser suportado pela operadora de rede. Os mecanismos de segurança over the air do UICC devem seguir as especificações mais recentes do ETSI [1] [2] e 3GPP [3] e usar o nível de segurança mais apropriado para o serviço de IoT.

Os endpoints IoT devem suportar os comandos APDU necessários reconhecidos pelo UICC para garantir que a execução over the air do comando UICC seja bem-sucedida.

5.1.1.2 UICC não removível

A operadora de rede deve fornecer UICCs não removíveis (por exemplo, formato da máquina) para os serviços de IoT, em que o modelo de ameaça de serviço sugere que o endpoint esteja vulnerável a modificações físicas. Medidas adicionais de segurança devem ser aplicadas para detectar e reagir a tal ameaça.

5.1.1.3 Gerenciamento remoto de UICCs Integrados (eUICCs)

A operadora de rede deve fornecer gerenciamento remoto seguro de UICCs não removíveis (por exemplo, eUICCs) para serviços de IoT que exigem que os endpoints estejam localizados em locais remotos ou de difícil acesso.

Por exemplo, para provedores de serviços de IoT que precisam gerenciar um grande número de eUICCs em endpoints dos quais o provedor de serviços de IoT não é o proprietário e não pode acessar facilmente (por exemplo, um carro).

Normalmente, as operadoras usam as plataformas de gerenciamento de conectividade IoT para monitorar e gerenciar os serviços de comunicação para dispositivos IoT por (e)UICCs

A operadora de rede deve suportar a arquitetura de provisionamento remoto da GSMA para Especificações Técnicas de Embedded UICC [7].

5.1.1.4 Serviços baseados em UICC

Uma operadora de rede pode fornecer serviços baseados em UICC ao provedor de serviços de IoT. Isso possibilita que o provedor de serviços de IoT use o UICC como uma plataforma segura e inviolável para seus serviços de IoT. Tais serviços baseados em UICC são geralmente desenvolvidos em JavaCardTM e são interoperáveis entre todos os cartões UICC compatíveis com JavaCardTM. Um exemplo de tal aplicação para um endpoint poderia ser o monitoramento e o relatório da qualidade da rede. O recurso de resistência à violação fornecido pela plataforma UICC é altamente valioso para endpoints que podem ser acessados fisicamente por invasores. Alavancar o UICC como um elemento seguro comum para todas as partes interessadas também pode tornar a segurança de endpoints IoT mais custo-eficiente.

O UICC também pode ser usado para armazenamento resistente a violações de dados confidenciais para serviços de IoT, incluindo chaves de segurança controladas pelo provedor de serviços de IoT. O ETSI TS 102 225 [1] aproveita o recurso de Gerenciamento Confidencial de Conteúdo de Cartão da especificação da Plataforma Global de Especificação de Cartão para permitir que os provedores de serviços de IoT gerenciem independentemente seu próprio domínio de segurança em um UICC.

Um provedor de serviços ou operadora de rede IoT pode pedir ao fornecedor do UICC para criar esses domínios de segurança dentro do UICC. O emissor do UICC deve garantir que ele esteja protegido por chaves de segurança adequadas e que o endpoint pode executar os comandos APDU necessários para acessá-la.

Além disso, o UICC também pode ser usado para criptografar (usando chaves de segurança armazenadas) e enviar conteúdo confidencial para os serviços de IoT ou

fornecer serviços de segurança para aplicações baseadas em endpoints por meio de serviços como Open Mobile API [4] ou oneM2M TS-0003 [31].

5.1.1.5 Garantia de produção e aprovisionamento do UICC

Uma operadora de rede deve obter seus UICCs de fabricantes cujos processos de fabricação e provisionamento são acreditados de acordo com o SAS (Security Accreditation Scheme) da GSMA [16].

5.2 Autenticação de rede e algoritmos de criptografia

Esta seção contém recomendações e boas práticas para autenticação de rede e criptografia de link para diferentes redes de longa distância.

A operadora de rede deve implementar algoritmos de autenticação de rede que atendam às expectativas de tempo de vida dos endpoints do provedor de serviços de IoT.

Operadoras de rede fornecem vários tipos de serviços de comunicação que podem ser usados por um serviço de IoT, como conectividade de dados USSD, SMS e IP. Neste documento, apenas a conectividade de dados IP é discutida, pois é a forma de serviço de comunicação mais utilizada pelos serviços de IoT.

O USSD e o SMS são usados por muitos serviços de IoT existentes, mas é importante destacar que USSD e SMS têm recursos de suporte de segurança limitados em comparação com a conectividade de dados IP. Em geral, o tráfego USSD e SMS não é, por padrão, criptograficamente protegido de ponta a ponta pela operadora de rede e por mecanismos de proteção criptográfica para garantir que a confidencialidade e a integridade sejam preservadas em mensagens SMS. Provedores de serviços de IoT que usam USSD ou SMS para sua comunicação precisam estar cientes das vulnerabilidades associadas a USSD e SMS e, quando possível, implementar criptografia adicional à camada de serviço.

5.2.1 Segurança de sistemas GSM / GPRS (2G)

As operadoras de rede que fornecem redes GSM / GPRS devem:

- Usar uma codificação mínima de 128 bits A5/3 para proteger o link entre o endpoint e a estação base. Sempre que possível, as operadoras de rede devem evitar A5 / 1 e A5 / 2 ou usar links não criptografados.
- Usar o algoritmo de autenticação MILENAGE. As operadoras de rede devem evitar o COMP128-1 e o COMP128-2 e considerar o suporte ao algoritmo de autenticação TUAK
- Tomar as medidas apropriadas para abordar e mitigar ataques falsos a estações base

Nos sistemas GSM / GPRS a rede não é autenticada pelo endpoint, apenas o dispositivo é autenticado pela rede. Portanto, em sistemas GSM / GPRS recomenda-se a criptografia de ponta a ponta na camada de serviço. Deve-se levar em consideração o processamento prático, as limitações dos endpoints e as restrições de largura de banda de rede em soluções fornecidas como serviços de IoT.

Em sistemas GSM / GPRS, o túnel GTP entre SGSN e GGSN criado na rede GRX não é encriptado. A operadora de rede deve confirmar a segurança desse link garantindo que a rede GRX seja gerenciada como uma rede privada.

5.2.2 Segurança dos sistemas UMTS (3G)

As redes UMTS permitem autenticação mútua, ou seja, tanto o endpoint é autenticado pela rede, quanto esta é autenticada pelo endpoint.

As operadoras que possuem redes UMTS devem dar suporte ao algoritmo de autenticação e geração de chave MILENAGE. E devem suportar os algoritmos Kasumi de encriptação para confidencialidade e integridade.

Operadoras de rede devem considerar o suporte ao algoritmo de autenticação TUAK.

5.2.3 Segurança em sistemas LTE (4G)

As operadoras de rede que fornecem rede LTE devem dar suporte ao algoritmo de autenticação MILENAGE e aos algoritmos de criptografia LTE EEA1, EEA2 ou EEA3.

As operadoras de rede devem considerar o suporte ao algoritmo de autenticação TUAK.

É aconselhável que as operadoras de rede revisem o *white paper* “Segurança wireless em redes LTE”, da GSMA [30].

5.2.4 Segurança de redes de longo alcance e baixa potência

Várias tecnologias de rede de longa alcance e baixa potência (LPWA) foram implantadas por diversas operadoras de rede. Uma lista completa e atualizada de implementações de rede LPWA pode ser encontrada no site da GSMA: www.gsma.com/iot

Guias de implantação para NB-IoT [34] e LTE-M [35] podem ser encontrados no site da GSMA para ajudar a garantir a implantação consistente dessas tecnologias de uma perspectiva de rede e de dispositivo.

Em maio de 2017, o analista de segurança Franklin Heath divulgou um relatório independente intitulado “Comparação de Segurança de Tecnologia LPWA” [33] entre os recursos de segurança de cinco tecnologias de rede de longa distância e baixa potência para vários casos típicos de uso em IoT, como agricultura inteligente, iluminação de rua inteligente, detectores de fumaça, medidores de água e outros medidores inteligentes. O relatório avalia os recursos de segurança de três tecnologias móveis para IoT sob o padrão 3GPP que operam em espectro licenciado, nomeadamente: LTE-M, NB-IoT e EC-GSM-IoT, bem como tecnologias de espectro não licenciadas LoRaWAN e Sigfox. O relatório pode ser baixado em: https://goo.gl/JIOlr6 [33].

O relatório argumenta que as organizações devem descobrir qual o nível de segurança que necessitam, além de outras considerações como custo, duração da bateria e cobertura de rede ao considerar uma solução LPWA. Ele destaca como as necessidades de segurança de IoT são orientadas em grande parte por questões de privacidade e segurança, e que qualquer implantação usando tecnologias LPWA deve estar sujeita a uma verificação de riscos de segurança por ferramentas como a avaliação de segurança em IoT da GSMA [32].

Alguns fatores importantes de segurança de rede destacados no relatório e que devem ser considerados em qualquer avaliação incluem:

- Largura de banda, incluindo taxas máximas de downlink e uplink de dados - isso pode limitar os recursos de segurança que podem ser suportados pela rede LPWA ou implementados na camada de aplicação.
- Downlink diário e taxa de transferência de uplink - os dispositivos LPWA normalmente não transmitem ou recebem dados o tempo todo, o que pode afetar os recursos de segurança, como atualizações de segurança over the air.
- Autenticação - Dispositivo, Assinante e Rede - A conectividade de rede segura requer que várias partes diferentes se autentiquem entre si, como o dispositivo, o assinante e o provedor de rede - a tecnologia deve proteger contra 'spoofing' dessas partes por agentes mal-intencionados.
- Confidencialidade dos dados - A criptografia é normalmente usada para impedir que os dados sejam interceptados por um hacker. A confiança nisso pode ser aumentada pelo estabelecimento de segurança de ponta a ponta na camada de aplicação.
- Provisionamento de chaves - Técnicas criptográficas para autenticação, confidencialidade e integridade dependem de chaves criptográficas compartilhadas com segurança entre as partes.
- Equipamentos Certificados - Em muitos mercados, existem requisitos legais para dispositivos com transmissão de rádio serem aprovados ou certificados antes de sua comercialização. Esta é uma oportunidade para verificar os recursos de segurança.
- Rede IP - O uso de IP pode possibilitar ataques a dispositivos da internet e os recursos de segurança IP devem ser considerados.

O relatório conclui que vários recursos de segurança, possivelmente importantes das tecnologias LPWA, são, de certa forma, opcionais, pois podem ser diretamente habilitados pela operadora de rede ou dependem de outras escolhas feitas pela operadora. As operadoras de rede devem garantir que estão cientes das consequências para a segurança das escolhas que fazem em sua configuração de rede e que o status dessas opções seja claramente comunicado aos seus clientes. Algumas opções também estão sob o controle do fabricante do dispositivo (como incluir ou não um elemento seguro fixo como um eUICC não removível) e o dever de comunicar para seus clientes as implicações disso sobre a segurança.

Considerações de segurança no uso de uma tecnologia LPWA incluem:

Para todas as tecnologias de rede LPWA:

- Se uma camada de rede IP é implementada na camada de link.
- Se um elemento seguro está presente e, em caso afirmativo, se ele é removível.
- Até que ponto a integridade dos dados é garantida.
- Se quaisquer algoritmos ou comprimentos de chave suportados pela tecnologia estão na lista negra ou devem ser preteridos (como chaves de criptografia de 64 bits para GPRS).

Para tecnologias de rede 3GPP LPWA (ou seja, NB-IoT e LTE-M):

- Se há suporte ao aprovisionamento remoto de SIM (RSP).

- Quais algoritmos de integridade (EIAx / GIAx) e algoritmos de confidencialidade (EEAx / GEAx) são implementados e permitidos.

Para LoRaWAN:

- Se ABP (ativação por personalização) ou ativação over the air for implementado e, se para a ativação over the air um AppKey pode ser compartilhado entre dispositivos.

Para SigFox:

- Ao usar a rede SigFox, deve-se levar em conta que a criptografia de carga útil é opcional, mas disponível. Portanto, um chip criptografado certificado pela Sigfox deve ser usado para ativar a criptografia AES 128 e manter os dados confidenciais over the air.

Para todos os dispositivos LPWA:

- Qual formulário (se houver) de certificação de segurança foi realizado.

5.3 Segurança de redes fixas

Recomendações para configuração padrão de redes Wi-Fi sob o controle de uma operadora de rede ou de um provedor de serviços de IoT incluem autenticação EAP-SIM [28] ou EAP-AKA [27] e podem contar com a estrutura EIC UICC do ETSI TS 102 310 [8].

5.4 Priorização de tráfego

As operadoras de rede podem fornecer níveis de qualidade de serviço apropriados ao serviço de IoT que está sendo fornecido.

5.5 Segurança de backhaul

Os padrões 3GPP que especificam GSM, UMTS e LTE não exigem o uso de enlaces de backhaul criptografados. Além disso, o compartilhamento de RAN e backhaul entre diferentes operadoras de rede pode introduzir vulnerabilidades de segurança adicionais.

A operadora de rede deve implementar a criptografia de backhaul para redes GSM, UMTS e LTE para dados do usuário final e tráfego de dados do plano de sinalização.

5.6 Roaming

As operadoras de rede podem fornecer aos provedores de serviços de IoT uma área de cobertura móvel internacional por meio do uso de serviços de roaming.

As redes de roaming podem ser vulneráveis a violações de segurança devido à relativa abertura das funções de interconexão SS7 / diâmetro usadas para conectar as redes domésticas e de roaming. Isso é de particular relevância para os serviços de IoT, devido à proporção possivelmente alta de endpoints que estão em roaming. Existem algumas razões para a alta porcentagem de endpoints em roaming. Em primeiro lugar, muitos endpoints são fabricados em um local e distribuídos globalmente. Portanto, em muitos casos, substituir um UICC não é prático ou não é possível no caso de UICC embutido. Em segundo lugar, em muitos casos, o status de roaming é preferível à conectividade local, devido à possível

cobertura múltipla de várias redes de roaming. A formação de alianças globais com UICCs globais e acordos de roaming dedicados à IoT facilitam a situação de roaming permanente, quando permitido pela legislação local.

As operadoras de rede devem considerar como proteger seus HLRs e VLRs contra ataques de negação de serviço (incluindo ataques DoS não intencionais), solicitações de fontes não autorizadas e exploração de serviços de “direcionamento de roaming”.

O roaming é facilitado pelos protocolos de sinalização entre operadoras de rede que são trocados entre as entidades core da rede móvel:

1. Entre o VLR ou o SGSN na rede de roaming (visitada) e o HLR na rede doméstica - o protocolo MAP (Mobile Application Part) (para redes CDMA, o IS41 é semelhante ao MAP).
2. Entre o MME na rede de roaming LTE e o HSS na rede doméstica LTE - o protocolo Diameter (certas variantes como o S6a).
3. Entre o SGSN / S-GW na rede visitada e GGSN / P-GW na rede doméstica - a transferência de dados de roaming usando GTP (GPRS Tunneling Protocol).

Esta seção se concentra em problemas de segurança de roaming relacionados aos serviços de IoT. As questões gerais de segurança de roaming são cobertas pelo GSMA FASG (Grupo de Fraude e Segurança) e seus subgrupos. Assim, questões como o registro duplo em roaming, recebidas de dois VLRs diferentes localizados em países diferentes - um cenário clássico de fraude de roaming - estão fora do escopo deste documento.

5.6.1 Signaling storm e ataques em roaming

A IoT possui requisitos de segurança adicionais aos da rede móvel, devido à distinta natureza dos endpoints e ao possível alto nível de criticidade do serviço. Ao servir um grande número de endpoints, a rede móvel é exposta a “signaling storms”. Um ataque intencionalmente malicioso de negação de serviço é apenas uma das razões para tais tempestades. Um problema de falha de energia, desastre natural ou cobertura em determinada área de uma rede móvel de serviço pode ser comum em muitos países e, portanto, causar tais problemas. Todos os medidores inteligentes de roaming e outros endpoints localizados nessa área tentarão se deslocar para outra rede de roaming, simultaneamente. Tal cenário cria uma “signaling storm” e impõe um risco severo ao HLR / HSS residencial. O 3GPP TS 23.122 [9] define um serviço de Extended Access Barring (EAB) para abordar tais cenários: operadoras de rede podem restringir o acesso da rede aos endpoints configurados para EAB, além de mecanismos de controle de acesso comuns e específicos de domínio. A configuração do EAB pode ser executada no UICC ou no próprio dispositivo. Os gateways de segurança de rede devem ser configurados para ataques de negação de serviço intencionais.

Também pode haver necessidade da operadora de rede doméstica (junto com o provedor de serviços de IoT) distinguir entre endpoints de baixa prioridade e endpoints fundamentais. Por exemplo, pode ser necessário que os dispositivos de assistência médica continuem a manter o serviço sob tempestades de sinalização e ataques de negação de serviço. A rede pode ter necessidade de rejeitar o registro de endpoints de "baixa prioridade" em roaming sob condições de sinalização de tempestade, mas permitir o registro de dispositivos de "alta prioridade". O mecanismo de rejeição implementado pode ser acompanhado de um

temporizador de desligamento, a fim de auxiliar o endpoint na tentativa de registro, após a tempestade de sinalização.

A recomendação seria que as operadoras de rede exibissem todas as mensagens de roaming recebidas de redes domésticas/parceiros de roaming. Além de bloquear mensagens de redes domésticas/parceiros de roaming não autorizados/falsificados, é necessário filtrar as mensagens de acordo com a prioridade do endpoint. Em ataques de sinalização de tempestade/negação de serviço, é necessário permitir mensagens de dispositivos críticos/de alta prioridade ou rejeitar mensagens de dispositivos não críticos. Métodos de rejeição são necessários para adiar as tentativas de registro e outras atividades por um determinado período.

5.6.2 Gestão de roaming baseada em segurança (SoR)

Outro caso de uso de segurança que pode ser executado por uma operadora de rede é a Gestão de Roaming (SoR, da sigla em inglês) dos endpoints IoT para fins de segurança. A rejeição de um update de localização sem um temporizador de back-office obriga o endpoint a tentar novamente e, finalmente, tentar o registro de uma rede de roaming (visitada) diferente. Outro método para SoR é over the air, usando listas preferenciais de roaming UICC e outros parâmetros armazenados no UICC. Os recursos de atualização over the air do UICC permitem que a rede doméstica atualize as listas de roaming preferenciais, que determinam a prioridade das redes durante o processo de seleção de uma rede de roaming. A rede doméstica também pode atualizar a memória do endpoint com a nova lista e fazer com que o endpoint pesquise uma nova rede instantaneamente.

No caso de ser detectado um risco de segurança em uma rede visitada específica, a rede doméstica pode decidir transferir seus endpoints em roaming outbound para outra rede visitada, usando o mecanismo SoR. Essa transferência ativa de endpoints pode ser feita na próxima tentativa de registro do endpoint ou ad-hoc usando os serviços SIM over the air. Um risco de segurança relacionado a uma rede visitada específica pode ser detectado se um problema for relatado por um número relativamente alto de endpoints em roaming nessa rede ou informações recebidas por outras entradas.

5.6.3 Negação de serviço de roaming de dados

Os ataques de negação de serviço não se limitam ao espaço de sinalização de mobilidade, o roaming de dados também é um possível campo para tempestades de sinalização. A maioria dos dados de roaming é roteada da rede visitada SGSN (S-GW no caso de LTE) para a rede doméstica GGSN (P-GW para LTE). O caso de LBO (Local Breakout), onde os dados são roteados da rede visitada diretamente para a internet raramente é implementado. No futuro, a situação pode mudar, devido a regulamentações, como a regulamentação da UE que permitiu o serviço LBO desde julho de 2014, LTE e especialmente VoLTE (Voz sobre LTE), onde as chamadas de voz feitas na rede de roaming podem ser manipuladas pelo doméstico P-GW (como é o caso das chamadas regulares de voz por comutação de circuitos feitas em uma rede visitada).

Signaling storms podem acontecer quando o domicílio GGSN/P-GW é inundado com pedidos de novas sessões de dados. O protocolo GPRS cria um túnel seguro entre o endpoint e o GGSN, e uma solicitação para uma nova sessão (Create-PDP-Context) resulta na configuração de um túnel e na alocação de um endereço IP para o endpoint. Quando os

dispositivos de IoT não se comportam de maneira customizada, eles podem gerar disparos de solicitações para novas sessões de dados, conforme observado anteriormente. Ataques de negação de serviço podem ser gerados por um número relativamente pequeno de endpoints, criando várias solicitações para novas sessões de dados em paralelo. Os servidores GGSN / P-GW são limitados em sua capacidade e devem ser protegidos contra tais tempestades.

Para evitar signaling storms, as operadoras de rede podem, com base em uma política de segurança, impedir que certos dispositivos se conectem à sua rede, alterando o perfil de comunicação dos dispositivos afetados ou promulgando políticas de segurança dentro do núcleo de pacotes da rede.

Os endpoints críticos devem receber um serviço também sob ataques de negação de serviço, enquanto os pedidos de endpoints de prioridade mais baixa são adiados por um determinado período de atraso.

5.7 Gerenciamento de endpoints e gateways

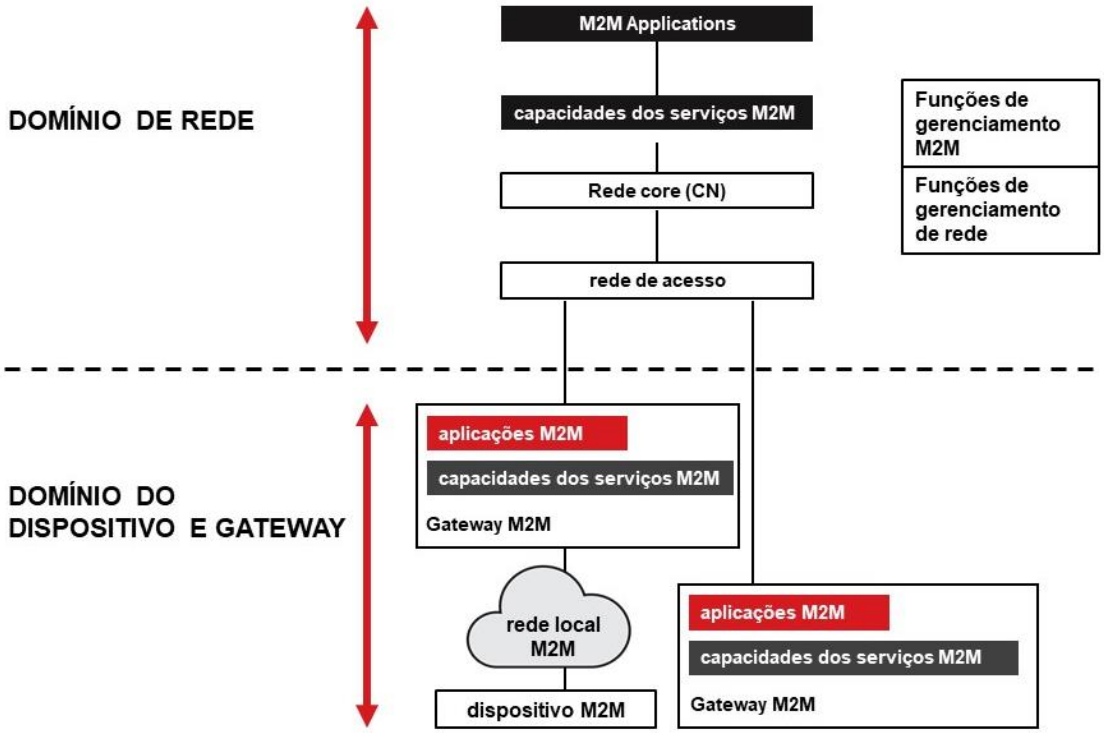
Deve-se observar que as medidas de segurança de hardware e software, incluindo os consoles de gerenciamento de configuração local para endpoints e gateways, estão além do escopo deste documento. Esta seção aborda aspectos relacionados à rede. Consulte o documento da GSMA “Panorama das diretrizes de segurança de IoT do CLP.11” [11] para obter as diretrizes de segurança relacionadas a endpoints.

5.7.1 Gerenciamento de endpoints

As operadoras de rede podem oferecer aos provedores de serviços de IoT recursos básicos para configurar e gerenciar com segurança dispositivos e assinaturas de endpoint, adotando alguns dos princípios e tecnologias desenvolvidos para o gerenciamento de dispositivos móveis "tradicionais". Os endpoints que usam um UICC para registrar e conectar-se a uma rede celular podem ser gerenciados usando as plataformas de gerenciamento de conectividade, as plataformas de gerenciamento de dispositivos e as plataformas de gerenciamento UICC existentes hoje.

Além dessa capacidade básica de gerenciamento de endpoints, a funcionalidade de gerenciamento de endpoints mais complexa e específica pode ser fornecida por meio de platafoma de serviços de IoT.

Um exemplo de uma arquitetura típica de gerenciamento de endpoints é mostrado abaixo e é retirado dos princípios de comunicação ETSI M2M [19].



a) - Arquitetura de alto nível do ETSI para gerenciamento de dispositivos M2M

Os blocos azuis indicam o que é tradicionalmente gerenciado pelas plataformas de gerenciamento de dispositivos existentes da operadora de rede e os blocos vermelhos indicam o componente de serviço que é gerenciado pela plataforma de serviço de IoT.

As operadoras de rede podem realizar algumas das funções de gerenciamento de dispositivos indicadas em vermelho a pedido do provedor de serviços de IoT.

5.7.2 Gerenciamento de gateway

O uso de gateway possivelmente introduz mais um nível de complexidade ao gerenciamento de dispositivos no provedor de serviços de IoT. Em alguns casos, o gateway IoT pode ser um dispositivo baseado em UICC que se conecta a uma rede celular, em outros casos, linhas fixas são usadas.

O gateway deve ser um objeto gerenciado, para que seja monitorado e atualizado com novo firmware ou software, caso seja necessário. Protocolos para fornecer firmware seguro e atualizações de software e mecanismos seguros de integração de software e sistemas devem ser usados para proteger a interconexão do gateway ao backbone da rede.

As operadoras de rede podem fornecer e gerenciar gateways seguros em nome do provedor de serviços de IoT, que permitem que os endpoints se conectem de forma segura e se integrem melhor aos mecanismos de segurança de rede de longa distância da operadora de rede.

Os gateways que se comunicam usando conectividade de rede fixa podem ser gerenciados remotamente usando o protocolo de gerenciamento de rede de longa distância (WAN) Broadband Forum TR-069 Customer Premises Equipment (CPE) [20].

Os gateways que se conectam usando conectividade de rede celular podem ser gerenciados remotamente usando os protocolos OMA Device Management (DM) e Firmware Update Management Object (FUMO) [5] [6].

5.7.3 Lista negra de endpoints IoT

As operadoras de rede devem implementar listas negras e a conexão do dispositivo IoT ao banco de dados CEIR (Central Equipment Identity Register) da GSMA. O CEIR é um banco de dados central, administrado pela GSMA, contendo IMEIs associados a dispositivos e endpoints perdidos ou roubados que não devem ter acesso à rede. Uma vez que um IMEI é inserido no CEIR, o endpoint que contém o IMEI será colocado na lista negra por todas as operadoras de rede que coletarem esses dados e implementarão a lista negra local com base no uso de registros de identidade de equipamentos (EIRs).

As operadoras de rede também podem implementar uma “lista cinza” localizada do dispositivo para permitir a suspensão temporária de dispositivos “suspeitos” enquanto a operadora de rede investiga a natureza de tais dispositivos antes de qualquer lista negra. Deve-se notar que, para serviços críticos, como assistência médica, o bloqueio de um IMEI pode não ser desejável ou possível. É importante que os detalhes dos endpoints conectados sejam claramente compreendidos pelas operadoras de rede, até o ponto em que a verdadeira aplicação (ou host) de um endpoint possa ser discernida. Os endpoints que utilizam o IMEI emitido para um fornecedor de módulo de comunicações devem suportar o Relatório de Identificação de Host de Dispositivo, que é um recurso que permite que o dispositivo do Ponto de Endereçamento informe as informações do host para a operadora de rede. O Relatório de Identificação do Host do Dispositivo é descrito nas Diretrizes de Eficiência de Conexão da GSMA [17].

5.8 Outros serviços relacionados à segurança

5.8.1 Serviços de nuvem / Gerenciamento de dados

As operadoras de rede podem fornecer aos clientes as plataformas de serviços de IoT da nuvem hospedada para implementar os serviços de IoT e também fornecer serviços para armazenar e gerenciar os dados produzidos por esses serviços.

As operadoras de rede podem fornecer uma nuvem privada ou uma infraestrutura de nuvem compartilhada, dependendo dos requisitos do provedor de serviços de IoT.

5.8.2 Segurança baseada em analytics

As operadoras de rede podem fornecer serviços de análise de dados e inspeção profunda de pacotes para identificar ameaças e anomalias nos dados gerados pelos serviços de IoT. Um exemplo poderia ser uma operadora que executasse periodicamente uma inspeção profunda de pacotes para cadeias específicas, como números de seguridade social e coordenadas de GPS. Isso poderia indicar que tais informações não estão protegidas adequadamente e alertar o provedor de serviços de IoT responsável pelo vazamento.

Isso é vantajoso para a IoT, pois os dispositivos e serviços do endpoint de baixa complexidade não podem fornecer essa funcionalidade por conta própria. As operadoras de rede podem fornecer aos provedores de serviços da IoT visibilidade do status de segurança, ameaças e ataques identificados, bem como uma verificação geral de integridade da

segurança. Esses serviços de introspecção são vitais para garantir que as ameaças não sejam infiltradas “dentro do canal”, particularmente onde os serviços de dados são criptografados. Os serviços fornecidos incluem:

- Uso de detecção de anomalias e aprendizado de máquina para identificar problemas
- Criação de sistemas de proteção contra intrusões em diagnósticos de endpoints em tempo real
- Fornecimento de painel para fácil visualização e identificação de anomalias
- Fornecimento de meios automatizados para sinalizar e bloquear conexões suspeitas
- Fornecimento de análise de ameaças de serviços baseados em nuvem

5.8.3 Gerenciamento de rede segura

As operadoras de rede podem fornecer redes que são gerenciadas e mantidas com segurança.

- Canais de backup em caso de falha no link físico ou lógico
- Identifique falha de link como evidência de possível violação de segurança
- Implemente políticas de roaming com impacto na segurança e integridade
- Gerenciamento de UICC/SIM
- Gestão de informação segura
- Participação em CERTs e compartilhamento de informações sobre ameaças para mitigar e prevenir futuros ataques.
- Proteção contra ataques de negação de serviço
- Realizar verificações periódicas de segurança / avaliações de vulnerabilidades
- Gerenciamento e manuseio de requisitos regulatórios relacionados à segurança de rede
- Restringir as opções de comunicação ao mínimo necessário para um determinado serviço de IoT

5.8.4 Plataforma segura de gerenciamento de conectividade em IoT

As operadoras de rede estão usando cada vez mais o core de rede dedicado e a infraestrutura de OSS para gerenciar as assinaturas de IoT e os planos de preços de maneira eficiente e escalonável. O acesso a essa infraestrutura é frequentemente exposto ao cliente comercial da operadora (ou seja, um provedor de serviços de IoT) para que ele possa autogerenciar suas assinaturas (isso inclui a ativação do serviço, a suspensão, etc. individualmente ou em massa).

As diretrizes da plataforma de serviços oferecidas no CLP 12 “Diretrizes de segurança em IoT para o ecossistema IoT” [26] fornecem orientações valiosas que podem beneficiar a operadora de rede que dispõe de suporte para plataformas de gerenciamento de conectividade em IoT. Essas diretrizes contêm as seguintes recomendações:

- As operadoras de rede devem garantir que o acesso ao portal da internet da plataforma de gerenciamento de conectividade em IoT, que pode ser hospedado pela operadora de rede ou pela nuvem, use a criptografia 'best in class' conforme as diretrizes publicadas recentemente por organizações como NIST [24] e ECRYPT2 [25]

- As operadoras de rede devem garantir que o acesso ao portal da internet da plataforma de gerenciamento de conectividade em IoT use procedimentos padrão de "melhores práticas" para criação, atualização e redefinição de senhas

5.8.5 Gerenciamento de certificados

Operadoras de rede podem fornecer serviços de gerenciamento de certificado X.509.

5.8.6 Altenticação multifatorial

Os serviços de autenticação multifatorial normalmente exigem que um usuário se autentique usando um token eletrônico, além de um nome de usuário e senha. Como tal, a autenticação de vários fatores pode fornecer proteção adicional contra o acesso aos serviços de IoT de usuários não autorizados.

A iniciativa Mobile Connect da GSMA [12], juntamente com OpenID Connect [21], FIDO [22] e ETSI MSS [23] são exemplos de habilitadores de autenticação multifatorial que podem permitir a um provedor de serviços de IoT obter autenticação e informações comerciais adicionais. O usuário final, neste contexto, é um ser humano que pode fornecer informações a uma plataforma de serviços de IoT para dispor de diferentes níveis de garantia. Exemplos incluem inserir um PIN e fornecer uma assinatura biométrica.

Embora a maioria das soluções de autenticação multifatorial sejam usadas atualmente para habilitar serviços tradicionais de “smartphone”, essas tecnologias podem ser aplicadas aos serviços de IoT que exigem a garantia de autorização humana para determinadas tarefas, como executar uma operação de conexão de rede, atualização de software ou reinicialização forçada.

Por exemplo, usando a autenticação multifatorial, uma identidade móvel poderia ser usada adicionada a um gateway dentro de um carro conectado. Nesse caso, a infraestrutura de autenticação multifatorial pode funcionar como uma camada de autorização adicional para que os ocupantes do carro tenham acesso aos serviços de infoentretenimento e pagamento dentro do carro.

Anexo A Gerenciamento do documento

A.1 Histórico do documento

Versão	Data	Breve descrição da mudança	Autoridade de aprovação	Editor / Empresa
1.0	08-Fev-2016	Novo PRD CLP.14	PSMC	Ian Smith GSMA
1.1	17-Nov-2016	Referências ao esquema GSMA IoT Security Assessment adicionado. Correções editoriais menores.	PSMC	Ian Smith GSMA
2.0	30-Set-2017	Alteração principal para adicionar referências do LPWA	Grupo de segurança IoT	Rob Childs GSMA

A.2 Outras informações

Tipo	Descrição
Proprietário do documento	Programa de IoT da GSMA
Contato	Rob Childs – GSMA

É nossa intenção fornecer um produto de qualidade para seu uso. Se você encontrar algum erro ou omissão, entre em contato conosco com seus comentários. Você pode nos notificar em prd@gsma.com

Seus comentários ou sugestões e perguntas são sempre bem-vindas.