Panorama das Diretrizes de Segurança para IoT

Panorama das Diretrizes de Segurança para IoT
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 Visão geral executiva

O surgimento da Internet das Coisas (IoT, da sigla em inglês) está criando novos provedores de serviços que procuram desenvolver produtos e serviços inovadores e conectados. Analistas estimam que centenas de milhares de novos serviços de IoT irão conectar bilhões de novos dispositivos IoT na próxima década. Esse rápido crescimento da Internet das Coisas representa uma grande oportunidade, para todos as partes desse novo ecossistema, de expandir ofertas de serviços e aumentar sua base de clientes.

Analistas indicam que os temas de segurança são um inibidor significativo para a implantação de diversos novos serviços de IoT; ao mesmo tempo, o fornecimento de ampla conectividade para uma gama cada vez maior de serviços de IoT aumentará a exposição desse ecossistema a fraudes e ataques. Já há muitas evidências que mostram um interesse cada vez maior dos hackers por essa área.

À medida em que soluções inovadoras para determinados segmentos de mercado são desenvolvidas por novos provedores de serviço, é possível que esses provedores não tenham conhecimento das ameaças que os serviços podem enfrentar. Em alguns casos, o provedor pode não ter desenvolvido um serviço que tenha se conectado a uma rede de comunicações ou à internet anteriormente e eles podem não dispor de habilidades e conhecimentos para mitigar os riscos decorrentes de se permitir o acesso à internet em seus dispositivos. Em contraposição, hackers entendem as fragilidades de segurança da tecnologia, e podem tirar proveito rapidamente se as vulnerabilidades forem expostas. Há uma série de ataques que resultaram em dispositivos comprometidos. Os dispositivos comprometidos podem remover dados, atacar outros dispositivos ou causar interrupção de serviços relacionados ou não relacionados.

Embora muitos prestadores de serviços, como os que atuam nos setores automotivo, de saúde, de eletrônica de consumo e serviços municipais, possam considerar seus requisitos particulares de segurança como exclusivos de seu mercado, geralmente não é esse o caso. Quase todos os serviços de IoT são criados usando componentes, tanto de plataformas de serviço como de dispositivos da ponta - comumente conhecidos como endpoints - que contêm tecnologias semelhantes a muitas outras soluções de comunicação, informática e TI. Além disso, as ameaças que esses diferentes serviços enfrentam, e as possíveis soluções para mitigar essas ameaças, geralmente são muito similares, mesmo que a motivação do invasor e o impacto de falhas de segurança possam variar.

O setor de telecomunicações, representado pela GSMA, tem um longo histórico de produtos e serviços seguros para seus clientes. O fornecimento de produtos e serviços seguros é tanto um processo quanto um objetivo. Vigilância, inovação, capacidade de resposta e melhoria contínua são necessárias para garantir que as soluções sejam capazes de responder às ameaças.

Para ajudar a garantir que os novos serviços de IoT lançados no mercado sejam seguros, as operadoras de rede, juntamente com seus parceiros de rede, serviços e equipamentos de dispositivos, gostariam de compartilhar seus conhecimentos de segurança com prestadores de serviços que procuram desenvolver serviços de IoT.

A GSMA criou, portanto, este conjunto de diretrizes de segurança para ajudar prestadores de serviços que estão buscando desenvolver novos serviços de IoT.

1.2 Série de documentos “Diretrizes de segurança para IoT” da GSMA

Este documento é parte de um conjunto de documentos da GSMA que contém diretrizes de segurança destinadas a ajudar a indústria emergente de Internet das Coisas a estabelecer uma compreensão comum dos problemas de segurança a ela relacionados. Esse conjunto de documentos propõe uma metodologia para o desenvolvimento de serviços seguros de IoT para garantir que as melhores práticas na área sejam implementadas ao longo do ciclo de vida do serviço. Os documentos fornecem recomendações sobre como mitigar ameaças e falhas de segurança comuns dentro dos serviços de IoT.

A estrutura do conjunto de documentos de diretrizes de segurança da GSMA é mostrada abaixo. Recomenda-se que este documento de visão geral seja lido como base antes da leitura dos demais documentos.

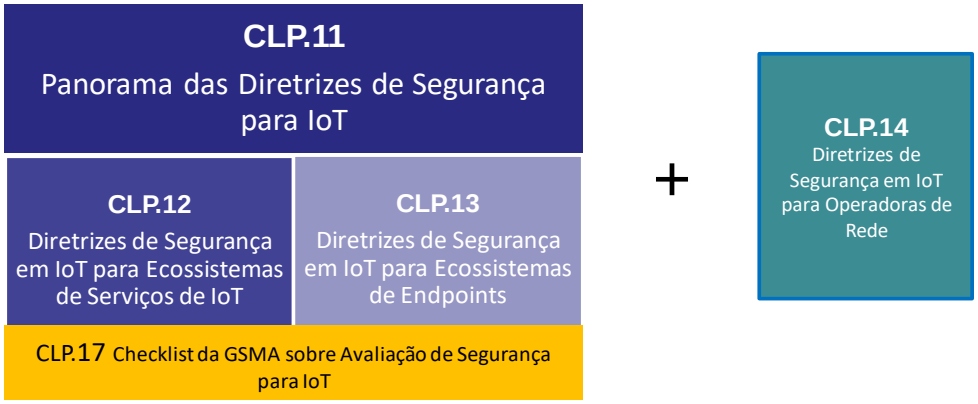

Figura 1 - Estrutura do documento da GSMA “Diretrizes de segurança para IoT”

As operadoras de rede, os provedores de serviços de IoT e outros parceiros no ecossistema de IoT são aconselhados a ler o documento CLP.14 da GSMA "Diretrizes de segurança em IoT para operadoras de rede" [13], que fornece diretrizes de segurança de alto nível para operadoras de rede que pretendem prestar serviços a provedores de serviços de IoT para garantir a segurança do sistema e a privacidade dos dados.

1.2.1 Checklist da GSMA sobre avaliação de segurança para IoT

Um checklist para avaliação é fornecido no documento CLP.17 [16]. Esse documento permite aos fornecedores de produtos, serviços e componentes de IoT autoavaliar a conformidade de seus produtos, serviços e componentes com as Diretrizes da GSMA de segurança para IoT.

Completar um checklist da GSMA para avaliar a segurança em IoT [16] permitirá que uma entidade demonstre as medidas de segurança tomadas para proteger seus produtos, serviços e componentes de possíveis riscos relacionados à segurança cibernética.

Avaliações podem ser emitidas por meio do envio de uma declaração completa à GSMA. Consulte o processo no site da GSMA:

https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/

1.3 Propósito do documento

O objetivo da série de documentos sobre as diretrizes de segurança para a Internet das Coisas é fornecer ao implementador de uma tecnologia ou serviço de IoT um conjunto de orientações para desenvolver um produto seguro. Para alcançar esse objetivo, este documento servirá como um modelo abrangente para interpretar quais aspectos de uma tecnologia ou serviço são relevantes para o implementador. Uma vez que esses aspectos ou componentes forem identificados, o implementador pode avaliar os riscos associados a cada componente e determinar como compensá-los. Cada componente pode ser dividido em subcomponentes, para os quais serão descritos riscos mais granulares. Cada risco deve ser atribuído a uma prioridade para auxiliar o implementador na determinação do custo do ataque, bem como o custo da remediação, e o custo, se houver, de não abordar o risco.

O escopo deste documento está limitado às recomendações relativas ao design e implementação dos serviços de IoT.

Este documento não tem como objetivo estimular a criação de 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.

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

1.4 Público-alvo

Os principais públicos deste documento são:

- Provedores de serviços de IoT - empresas ou organizações que procuram desenvolver produtos e serviços conectados inovadores. Alguns dos muitos setores em que os provedores de serviços de IoT operam são, por exemplo, casas inteligentes, cidades inteligentes, automotivo, transporte, saúde, utilities e eletrônicos de consumo.
- Fabricantes de dispositivos IoT - provedores de dispositivos IoT para provedores de serviços de IoT viabilizarem serviços de IoT.
- Desenvolvedores de IoT que criam serviços de IoT em nome dos provedores de serviços de IoT.
- Operadoras de rede que são prestadores de serviços de IoT ou criam serviços de IoT em nome dos provedores de serviços de IoT.

1.5 Definições

Termo	Descrição
Nome do ponto de acesso	Identificador de um ponto de conexão de rede ao qual um dispositivo endpoint se conecta. Está associado a diferentes tipos de serviços e, em muitos casos, é configurado pela operadora de rede.
Hacker	Definido, para os propósitos deste documento, como agente de ameaças, ator de ameaças, fraudador ou outra fonte de ameaça a um serviço de IoT. Essa ameaça poderia ser oriunda de um criminoso isolado, crime organizado, terrorismo, governos hostis e suas agências, espionagem industrial, grupos de

	hackers, ativistas políticos, hackers por hobby e pesquisadores, bem como de falhas involuntárias de segurança e privacidade.
Nuvem	Uma rede de servidores remotos na internet que hospedam, armazenam, gerenciam e processam aplicativos e seus dados.
Endpoint de Alta Complexidade	Este modelo de endpoint tem uma conexão persistente com um servidor back-end por meio de um link de comunicação de longa distância, como celular, satélite ou uma conexão física (hardwired), como Ethernet. Consulte o documento CLP.13 [4] para obter mais informações.
Componentes	Referem-se aos componentes contidos nos documentos CLP.12 [3] e CLP.13 [4].
Embedded SIM	Um SIM embutido, isto é, que não se destina a ser removido ou substituído no dispositivo e que permite a troca segura de perfis de acordo com a especificação GSMA SGP.01 [2].
Endpoint	Um termo genérico para endpoint de baixa complexidade, endpoint de alta complexidade, gateway ou outro dispositivo conectado. Consulte o documento CLP.13 [4] para obter mais informações.
Ecossistema de Endpoint	Qualquer configuração de dispositivos de baixa complexidade, dispositivos avançados e gateways que conectam o mundo físico ao mundo digital de maneiras inovadoras. Consulte a seção 4.2 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 equipados com recursos de comunicação que lhes permitem enviar e receber dados.
Serviço de IoT	Qualquer programa de computador que aproveite dados gerados por dispositivos de IoT para executar o serviço.
Provedor de Serviço de IoT	Empresas ou organizações que procuram desenvolver produtos e serviços de IoT inovadores.
Operadora de Rede	A operadora é proprietária da rede de comunicação que conecta o dispositivo endpoint de IoT ao ecossistema de serviços de IoT.
Raiz Organizacional de Confiança	Um conjunto de políticas e procedimentos criptográficos que regem o modo como as identidades, aplicações e comunicações podem e devem ser criptograficamente protegidas.
Recomendações	Referem-se às recomendações contidas nos documentos CLP.12 [3] e CLP.13 [4].
Riscos	Referem-se aos riscos contidos nos documentos CLP.12 [3] e CLP.13 [4].
Tarefas de Segurança	Referem-se às tarefas de segurança contidas nos documentos CLP.12 [3] e CLP.13 [4].
Ponto de Acesso ao Serviço	Um ponto de entrada na infraestrutura de back-end do serviço de IoT por meio de uma rede de comunicações.
Ecossistema de Serviços de IoT	O conjunto de serviços, plataformas, protocolos e outras tecnologias necessárias para fornecer recursos e coletar dados dos endpoints implantados em campo. Consulte a seção 3.1 para obter mais informações.

Módulo de Identidade do Assinante (SIM)	O cartão inteligente usado por uma rede móvel para autenticar dispositivos para conexão à rede móvel e acesso a serviços de rede.
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.

1.6 Abreviaturas

Termo	Descrição
3GPP	3rd Generation Project Partnership
API	Interface do Programa de Aplicações
APN	Nome do Ponto de Acesso
CERT	Grupo de Respostas a Incidentes de Segurança em Computadores
CLP	Programa Connected Living da GSMA
CPU	Unidade Central de Processamento
EAP	Protocolo de Autenticação Extensível
EEPROM	Memória Somente para Leitura Programável e Apagável Eletronicamente
GBA	Arquitetura Genérica de Bootstrap
GPS	Sistema de Posicionamento Global
GSMA	GSM Association
GUI	Interface Gráfica do Usuário
HIPAA	Lei de Portabilidade e Prestação de Conta do Seguro de Saúde
IoT	Internet das Coisas
LPWA	Longo Alcance e Baixa Potência
LTE-M	LTE para Máquinas
NB-IoT	Internet das Coisas de Banda Estreita
NIST	Instituto Nacional de Padrões e Tecnologia (EUA)
OBD	Diagnóstico de Bordo
OCTAVE	Avaliação de Ameaça, Habilidade e Vulnerabilidade Operacionalmente Crítica
OMA	Open Mobile Alliance
PIA	Avaliação de Impacto sobre a Privacidade
PII	Informação Pessoal Identificável
RAM	Memória de Acesso Aleatório
SIM	Módulo de Identidade do Assinante

1.7 Referências

Ref	Nº do Documento	Título
[1]	n/a	"Mobile Economy 2017" http://www.gsmamobileeconomy.com/
[2]	SGP.01	"Arquitetura de Provisionamento Remoto do SIM embutido" https://www.gsma.com/iot/embedded-sim/
[3]	CLP.12	Diretrizes de Segurança em IoT para o Ecossistema de Serviços de IoT https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[4]	CLP.13	Diretrizes de Segurança de IoT para o Ecossistema Endpoint de IoT https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[5]	n/a	NIST Estrutura de Gerenciamento de Riscos http://csrc.nist.gov/groups/SMA/fisma/framework.html
[6]	CMU/SEI-2007-TR-012	Introdução do OCTAVE Allegro: Melhorando o Processo de Avaliação de Riscos de Segurança da Informação http://www.cert.org/resilience/products-services/octave/
[7]	Não usado	Não usado
[8]	TS 33.220	Arquitetura de Autenticação Genérica (GAA); Arquitetura Genérica do Bootstrapping (GBA) www.3gpp.org
[9]	RFC 4186	Método de Protocolo de Autenticação Extensível para Módulos de Identidade de Assinante GSM (EAP-SIM) www.ietf.org
[10]	n/a	Realização de um Código de Prática de Avaliação de Impacto de Privacidade https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
[11]	n/a	Aliança Móvel Aberta http://openmobilealliance.org/
[12]	n/a	Especificações OneM2M http://www.onem2m.org/
[13]	CLP.14	Diretrizes de Segurança em IoT para Operadoras de Rede https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[14]	GE.11-13201	Relatório do Relator Especial sobre a promoção e proteção do direito à liberdade de opinião e expressão, Frank La Rue* www.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
[15]	n/a	Direito ao Acesso à Internet https://en.wikipedia.org/wiki/Right_to_Internet_access
[16]	CLP.17	Checklist da GSMA sobre avaliação de segurança para IoT https://www.gsma.com/iot/iot-security-assessment/

2 Desafios criados pela Internet das Coisas

Alguns anos atrás, um relatório especial das Nações Unidas recomendou que a Internet fosse um direito humano básico e que todas as pessoas do mundo deviam ter acesso a serviços de banda larga [14]. Mais recentemente, países como França, Grécia, Espanha e outros [15] têm buscado adotar marcos legais para garantir ampla disponibilidade do acesso à Internet e/ou para impedir que o Estado restrinja injustificadamente o direito do indivíduo de ter acesso à informação e à internet.

Essas declarações são o resultado das rápidas mudanças sociais e tecnológicas decorrentes do crescimento da Internet. Por sua vez, a Internet tem se tornado um estilo de vida, uma das principais fontes de todo tipo de informação e o método mais comum para manter a conectividade com entes queridos e colegas. A Internet não é simplesmente uma tecnologia, tornou-se parte de nós.

Nos últimos anos, junto ao crescente desejo de manter a conectividade, ocorreu uma explosão tecnológica. Enquanto tecnólogos declaravam "A Internet das Coisas está chegando!" por mais de uma década, o interesse em acesso onipresente à informação e o modelo de custo necessário para fazê-lo ainda não haviam sido combinados em um modelo comercial prático até os últimos cinco anos. Neste ponto, os custos dos componentes diminuíram drasticamente, enquanto o acesso a serviços sem fio e a velocidade desses serviços aumentaram consideravelmente. Os protocolos, a vida da bateria e até mesmo os modelos de negócios evoluíram para acomodar nossa demanda cada vez maior por informações e conectividade.

E isso, em essência, define a Internet das Coisas. Não é realmente sobre “coisas”. É sobre Nós. A Internet de Nós. As experiências humanas e digitais já não apenas andam lado a lado; elas são intrinsecamente vinculadas por esse novo modo de vida.

Exatamente porque a experiência física humana está cada vez mais ligada ao mundo digital, deve ser protegida, uma vez que a segurança digital causa, mais do que nunca, impactos diretos no mundo físico. A Internet das Coisas é uma excelente oportunidade para que o mundo avance em conjunto, a fim de criar bases de dados de conhecimento cada vez maiores, experiências compartilhadas e booms de inovação. Mas, para que isso funcione de maneira eficaz, as tecnologias que geram essa conectividade devem ser protegidas para garantir a privacidade, a confiabilidade e a qualidade dos serviços necessários para assegurar que essa grande ferramenta, essa necessidade básica imperativa, continue disponível para todos.

Para que a Internet das Coisas evolua efetivamente, devemos resolver os desafios de segurança inerentes ao seu crescimento, que estão relacionados abaixo:

- Disponibilidade: garantia de conectividade constante entre os dispositivos e seus respectivos serviços
- Identidade: autenticação de dispositivos, serviços e o cliente ou usuário final que operam o endpoint
- Privacidade: redução da possibilidade de dano para indivíduos
- Segurança: garantia de que a integridade do sistema possa ser verificada, rastreada e monitorada

2.1 O desafio da disponibilidade

Para que a Internet das Coisas evolua a um ritmo esperado, os endpoints devem poder comunicar-se constantemente entre si, com usuários finais e serviços de back-end. Para realizar isso, novas tecnologias como NB-IoT e LTE-M estão sendo implantadas para permitir a conectividade ininterrupta para dispositivos de baixa potência. Esse esforço se alinha bem com o desafio de viabilizar o acesso ubíquo à Internet para o mundo moderno. Para que isso tenha sucesso, várias perguntas devem ser respondidas:

- Como as redes LPWA (por exemplo, NB-IoT e LTE-M) podem ser implantadas e operadas com um nível de segurança similar ao dos sistemas móveis tradicionais?
- Como várias operadoras móveis podem sustentar o mesmo nível de segurança de rede enquanto os endpoints IoT migram entre os limites da rede?
- Como a confiança na rede pode ser garantida para os endpoints capilares que dependem de gateways para comunicação?
- Como as restrições de capacidade de endpoints de baixa complexidade podem ser abordadas em ambientes de comunicação seguros?

2.2 O desafio da identidade

Para que um dispositivo funcione dentro de um produto ou serviço do ecossistema de IoT, ele deve ter uma forma de identificação segura para com dispositivos equivalentes e outros serviços. Esse aspecto fundamental da tecnologia da IoT garante que os serviços e os pontos são capazes de assegurar para o que - e para quem - os dados estão sendo entregues. O acesso a informações e serviços não é a única questão diretamente vinculada à identificação. É preciso fazer também as seguintes perguntas:

- O usuário que opera o endpoint pode estar fortemente associado à identidade do dispositivo?
- Como os serviços e dispositivos equivalentes podem verificar a identidade do usuário final ao avaliar a identidade do endpoint ?
- A tecnologia de segurança do endpoint será capaz de autenticar com segurança dispositivos equivalentes e serviços?
- Serviços e dispositivos falsos são capazes de imitar serviços e dispositivos autorizados?
- Como a identidade de um endpoint pode ser protegida contra adulteração ou manipulação?
- Como o endpoint e a rede podem garantir que um serviço de IoT tem permissão para acessar o dispositivo?

2.3 O desafio da privacidade

A privacidade não pode mais ser tida apenas como um complemento em produtos e serviços existentes. Como o mundo físico é diretamente afetado por ações tomadas no mundo digital, a privacidade deve ser projetada nos produtos desde o início, para garantir que cada ação seja autorizada e que cada identidade seja verificada, concomitantemente assegurando que essas ações e os metadados a elas associados não sejam expostos a partes não autorizadas. Isso só pode ser alcançado com a definição da arquitetura apropriada para um produto ou serviço, o que é excepcionalmente difícil e caro de executar retroativamente.

Dispositivos médicos, soluções automotivas, sistemas de controle industrial, automação residencial, sistemas de construção e segurança, entre outros, afetam diretamente a vida das pessoas. É dever dos engenheiros manter esses produtos e serviços no mais alto nível de segurança possível para reduzir a possibilidade de danos físicos, bem como a exposição de dados que possam afetar a privacidade.

Portanto, devemos nos perguntar não só como a privacidade afeta o usuário final, mas como as tecnologias IoT são projetadas:

- A identidade de um endpoint está exposta a usuários não autorizados?
- Os identificadores únicos do endpoint ou serviço de IoT podem permitir que um usuário final ou dispositivo seja fisicamente monitorado ou rastreado?
- Os dados que emanam de um endpoint ou serviço de IoT são indicativos de, ou diretamente associados a atributos físicos relacionados ao usuário final, como localização, ação ou estado (como “adormecido” ou “desperto”)?
- A confidencialidade e a integridade empregadas têm segurança suficiente para garantir que padrões no texto cifrado resultante não possam ser observados?
- Como o produto ou serviço armazena ou manipula as Informações Pessoais Identificáveis (PII, da sigla em inglês *Personally Identifiable Information*) específicas do usuário?
- O usuário final pode controlar o armazenamento ou uso de PII no produto ou serviço de IoT?
- As chaves e os algoritmos de segurança usados para proteger os dados podem ser atualizados?

2.4 O desafio da segurança

Embora a segurança da Internet tenha melhorado drasticamente nas últimas décadas, há várias lacunas significativas na saúde da tecnologia moderna. Essas lacunas têm sido mais evidentes nos sistemas embutidos e nos serviços em nuvem - os dois principais componentes na tecnologia IoT.

Para que a IoT evolua sem expor a riscos grandes grupos de usuários e sistemas físicos, as práticas de segurança da informação devem ser aplicadas tanto nos endpoints quanto nos serviços de IoT.

- As melhores práticas de segurança são incorporadas no produto ou serviço no início do projeto?
- O ciclo de vida de segurança é incorporado nos ciclos de desenvolvimento e vida do software ou produto?
- A solução de segurança está sendo implementada tanto nos serviços quanto nos aplicativos relacionados ao sistema embutido?
- Uma Base de Computação Confiável (do inglês Trusted Computing Base - TCB) é implementada tanto no endpoint quanto no ecossistema de serviço?
- Como a TCB aplica a autoverificação de imagens e serviços de aplicações?
- O endpoint ou o serviço de IoT são capazes de detectar se há uma anomalia em sua configuração ou aplicação?
- Como endpoints são monitorados quanto a anomalias indicativas de comportamento mal-intencionado?

- Como a autenticação e a identidade estão ligadas ao processo de segurança do produto ou serviço?
- Qual plano de resposta a incidentes é definido para responder a anomalias detectadas indicativas de um comprometimento?
- Como serviços e recursos são segmentados para garantir que um comprometimento seja contido de forma rápida e eficaz?
- Como serviços e recursos são restaurados após um comprometimento?
- Um ataque pode ser detectado?
- Um componente comprometido do sistema pode ser detectado?
- Como os clientes podem reportar preocupações relativas à segurança?
- Endpoints podem ser atualizados ou corrigidos para remover vulnerabilidades?

3 A solução móvel

Embora tenham surgido inúmeras tecnologias oferecendo soluções de conectividade para IoT, nenhuma define o futuro da IoT melhor que as redes móveis. As redes móveis ofereceram, há mais de vinte anos, os primeiros serviços sem fio aos consumidores e à indústria. Desde então, têm desenvolvido serviços confiáveis, disponíveis, seguros e custo-eficientes. A indústria móvel tem uma vasta experiência em disponibilidade de rede devido à natureza volátil das redes sem fio gerenciadas para longas distâncias. A identidade de rede tem sido um desafio que gerou inúmeros padrões, tecnologias de dispositivos, protocolos e modelos de análise. A privacidade e a segurança são preocupações constantes da indústria móvel, que trabalha para reduzir a possibilidade de abusos, roubo de identidade e fraude em todas as tecnologias móveis.

A indústria móvel já oferece redes padronizadas e licenciadas que utilizam tecnologias LPWA (do inglês Low-Power Wide-Area), denominadas NB-IoT e LTE-M, para atender às necessidades de aplicativos e serviços de IoT. Essas tecnologias de rede LPWA oferecem conectividade sem fio e área de cobertura equivalente (ou, em muitos casos, até maior) à das redes móveis tradicionais, com uma fração da energia necessária para uma comunicação eficaz. Muitas operadoras de rede estão implantando serviços LPWA de modo que NB-IoT e LTE-M irão se tornar os padrões de fato para LPWA.

Mais informações sobre a implantação das redes NB-IoT e LTE-M no mundo podem ser encontradas no site da GSMA: https://www.gsma.com/iot/mobile-iot-initiative/

3.1 Abordagem do desafio da disponibilidade

Segundo o relatório da GSMA "Mobile Economy 2017" [1]:

No final de 2016, dois terços da população mundial tinham uma assinatura móvel - um total de 4,8 bilhões de assinantes únicos. Até 2020, quase três quartos da população mundial - ou 5,7 bilhões de pessoas - irá adquirir serviços móveis.

A mudança para redes de banda larga móvel e smartphones continua a ganhar impulso. As conexões de banda larga móvel (tecnologias 3G e 4G) representaram 55% das conexões totais em 2016 - um valor que será próximo aos três quartos da base de conexões até 2020. A proporção de conexões 4G, por si só, deve dobrar de 23% para 41% até o final da década.

Mais de 2,3 bilhões de conexões de banda larga móvel estão previstas entre 2016 e 2020, o que vai elevar para 73% a proporção sobre o total. A migração rápida para

4G continuou a ser uma característica chave em 2016, e as conexões 4G aumentaram 55% no ano para 1,7 bilhão. Como resultado, até 2020, 2G não será mais a tecnologia dominante em termos de número de conexões.

O potencial do mercado global para dispositivos LPWA é grande, totalizando cerca de 1,4 bilhão de conexões até 2020, e alguns observadores da indústria estão prevendo 5 bilhões até 2022.

3.2 Abordagem do desafio da identidade

O gerenciamento de identidade tem sido um desafio há décadas e fortaleceu significativamente os padrões e as ofertas de tecnologia da indústria móvel. Embora a indústria móvel esteja normalmente associada ao cartão SIM removível, a GSMA criou uma solução baseada em SIM denominada "Arquitetura de Aprovisionamento Remoto de SIM Embutido" [2], apropriada para uso na IoT, por viabilizar uma integração mais profunda (ao nível de componente) nos endpoints, redução de custos de produção, e gerenciamento de conectividade por meio de plataformas Over-The-Air (OTA) que possibilitam a conectividade dos dispositivos de IoT durante toda a sua vida útil.

Tecnologias de identidade como o Embedded SIM são projetadas como âncoras de confiança que integram a segurança por default. Elas são fabricadas para suportar ataques como:

- Glitching
- Análise de canal lateral
- Intercepção de dados passivos
- Adulteração física
- Roubo de identidade

Um significativo avanço para esta tecnologia, que já tem alto grau de segurança, é que as novas gerações dessas "âncoras de confiança" incorporam uma adição importante ao cenário de IoT: essas tecnologias serão de dupla utilização. Elas não serão usadas exclusivamente para verificar a segurança da rede, mas também serão capazes de proteger as comunicações de aplicativos e a própria aplicação, semelhantes às âncoras de confiança da computação tradicional.

Esta possibilidade de dupla utilização será ainda aumentada pela integração de especificações de segurança da indústria móvel, como as fornecidas pelo 3GPP GBA [8], OMA [11], oneM2M [12] e outros. Essas tecnologias ajudarão, com segurança, a aprovisionar dispositivos que já estão sendo utilizados, habilitar atualizações de firmware over-the-air e gerenciar os recursos e a identidade do dispositivo.

Essas tecnologias, quando usadas em conjunto, irão simplificar os complexos processos de engenharia atuais e combiná-los em um simples componente. Em vez de engenheiros de aplicações criando tecnologias complexas que eles próprios devem gerenciar, a operadora de rede, que já gerencia a identidade da rede, pode executar isso em nome da aplicação. Isso não só reduz a complexidade da engenharia, mas os requisitos diários de gerenciamento por parte da empresa.

3.3 Abordagem do desafio da privacidade e da segurança

Além das capacidades do SIM, a indústria móvel desenvolveu protocolos, processos e sistemas de monitoramento resilientes para permitir a segurança e reduzir a possibilidade de fraude e de outras atividades mal-intencionadas. Por exemplo, as tecnologias 3G e 4G usam autenticação mútua para verificar a identidade do endpoint e da rede. Este processo ajuda a garantir que terceiros não consigam interceptar as comunicações.

Além disso, a tecnologia de rede pode ser protegida por meio do uso do SIM e de tecnologias como GBA [8] ou EAP-SIM [9]. Ao usar essas tecnologias, o SIM pode ser aprovisionado com uma chave de segurança de sessão que pode ser usada em comunicações com redes de aplicativos pareados em protocolos conhecidos. Esse processo pode diminuir a possibilidade de terceiros manipularem o protocolo da aplicação para comprometer os dispositivos ou o serviço. Assim, é possível proteger a rede e a aplicação com este modelo.

4 O modelo de IoT

A figura abaixo mostra que o modelo padrão de IoT usado em todos esses documentos é representado por componentes dos ecossistemas de serviços e endpoints. Cada componente é composto de subcomponentes, que são detalhados em um documento que concentrado exclusivamente no componente principal. Por exemplo, o componente Endpoint, e seus respectivos riscos, são descritos no documento Ecossistemas de Endpoints [3], fornecido neste conjunto de documentos, e os componentes relativos aos Serviços são destacados no documento do Ecossistemas de Serviços [4].

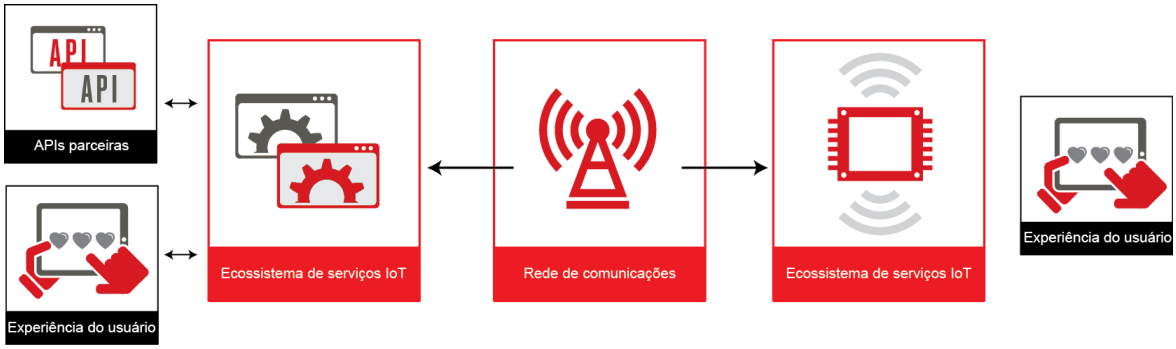

Figura 2 – Exemplo de modelo IoT

Em quase todos os modelos de produtos ou serviços modernos de IoT, este diagrama define os componentes principais necessários ao se utilizar uma tecnologia pronta para implementação.

Os componentes da rede de comunicações são inerentes à IoT e, para os propósitos deste modelo, fornecem a conexão entre os dois ecossistemas com cada ponta do link de comunicação discutido no documento do Ecossistema de EndPoint e do Ecossistema de Serviço.

As recomendações específicas das diretrizes de segurança de rede para Operadores de Rede podem ser encontradas no documento da GSMA "Diretrizes de segurança em IoT para Operadoras de Rede" [13].

4.1 Ecossistema de serviços

O ecossistema de serviços representa o conjunto de serviços, plataformas, protocolos e outras tecnologias necessárias para fornecer recursos e coletar dados de endpoints já em funcionamento. Esse ecossistema normalmente reúne dados de endpoints e os armazena no seu ambiente de servidor. Esses dados podem ser renderizados para o usuário ao entregar elegantes compilações dos dados para distintas interfaces de usuário. Estes dados, muitas vezes sob a forma de métricas, parâmetros ou comandos, também podem ser entregues a terceiros autorizados por meio de uma API (por exemplo, oneM2M [12]) originada na infraestrutura de serviços, que geralmente é como os provedores de serviços da IoT rentabilizam o serviço.

As diretrizes de segurança para o Ecossistema de Serviços a serem usadas em conjunto com o processo descrito neste documento de visão geral podem ser encontradas em CLP.12, no documento “Diretrizes de segurança de IoT para o Ecossistema de Serviços de IoT” [4].

4.2 Ecossistema de endpoints

O ecossistema de endpoints [4] consiste em dispositivos de baixa e alta complexidade, e gateways que conectam o mundo físico ao mundo digital por meio de vários tipos de redes com fio e sem fio. Exemplos de endpoints comuns são sensores de movimento, fechaduras de porta digitais, sistemas de telemática automotiva, sistemas de controle industrial orientados por sensor, entre outros. Os endpoints coletam métricas do ambiente físico ao seu redor e enviam esses dados em diferentes formatos por meio de uma rede celular ou capilar para o ecosistema de serviço, muitas vezes recebendo instruções ou ações em resposta. Eles também podem incluir interfaces de usuário avançadas que processam dados obtidos por meio do próprio endpoint ou do ecossistema de serviço.

As diretrizes de segurança para o Ecossistema de Endpoint a serem usadas em conjunto com o processo descrito neste documento de visão geral podem ser encontradas em CLP.13, no documento “Diretrizes de Segurança de IoT para o Ecossistema de Endpoint em IoT”. [13]

5 Avaliações de risco

Embora o conceito de avaliação de risco já seja utilizado há muitas décadas, muitas empresas estão mais familiarizadas com a aplicação do conceito ao risco comercial de modo geral do que à segurança da informação. No entanto, um processo de avaliação de risco de segurança da informação também é imperativo para uma operação segura e para a longevidade do setor tecnológico de uma empresa. Obviamente, na tecnologia da Internet das Coisas, em que a equipe de engenharia é um componente crítico para o sucesso do negócio, o processo de avaliação de risco deve ser o primeiro passo que a organização dá para a construção de uma prática de segurança.

Embora cada organização deva criar uma perspectiva granular de risco tecnológico, há questões de alto nível que servem como pontos de partida para o processo de avaliação de risco:

- Que recursos (digitais ou físicos) precisam ser protegidos?
- Que grupos de pessoas (tangíveis ou intangíveis) são potenciais agentes de ameaças?
- O que se caracteriza como uma ameaça para a organização?
- O que é uma vulnerabilidade?
- Qual seria o resultado se um recurso protegido fosse comprometido?
- Qual a probabilidade de o recurso ser comprometido?
- Qual seria o resultado em um contexto com diferentes grupos de hackers?
- Qual é o valor do recurso para a organização e seus parceiros?
- Qual é a relevância do recurso que está sendo comprometido na segurança?
- O que pode ser feito para remediar ou mitigar a possibilidade de vulnerabilidade?
- Como novas ou emergentes lacunas na segurança podem ser monitoradas?
- Quais riscos não podem ser resolvidos e o que eles significam para a organização?
- Que orçamento deve ser aplicado para a resposta a incidentes, monitoramento e redução de risco?

Esses pontos de partida ajudarão as equipes de engenharia e tecnologia da informação a trabalhar de forma mais eficaz com a organização. O objetivo é garantir que o lado técnico e o lado executivo da empresa estejam de comum acordo quanto a riscos, valores e planos de intervenção. Forçar as equipes a trabalhar em conjunto ajudará a criar uma perspectiva mais realista não só do risco para o negócio, mas também do valor dos recursos. Isso afetará diretamente o orçamento que deve ser aplicado para o fechamento de lacunas na segurança.

Existem alguns riscos que simplesmente não podem ser resolvidos. Alguns desses riscos serão discutidos nessas diretrizes. A organização deve avaliar esses riscos e determinar se eles são aceitáveis. Isso proporcionará aos negócios uma compreensão realista de suas limitações, das limitações da tecnologia e de sua capacidade de reagir a certos tipos de ameaças. Não há nada mais monetariamente comprometedor do que presumir que todas as lacunas na segurança podem ser fechadas de forma econômica.

5.1 Objetivo

O objetivo de uma avaliação de risco é criar (ou atualizar) um conjunto de políticas, procedimentos e controles que corrigem, monitoram e respondem às lacunas na segurança encontradas no setor técnico da organização. O resultado da avaliação de risco deve ajudar o empreendimento a ajustar não apenas sua tecnologia, mas a maneira como a tecnologia é gerenciada, projetada e implantada. Uma vez que o resultado da avaliação de risco tenha mais adequadamente demonstrado o valor das informações e recursos utilizados pela organização, o empreendimento como um todo pode melhorar sua segurança por meio do aprimoramento de seus recursos humanos, processos e políticas.

Os principais benefícios para usar o resultado de uma avaliação de risco são:

- Informar o quadro de funcionários
- Aprimorar processos

- Definir (ou atualizar) políticas
- Executar correções
- Buscar novas lacunas
- Aperfeiçoar o produto ou serviço

Em essência, isso ajuda a organização a implementar uma plataforma que sirva de base para segurança de processos e de pessoal. Esta plataforma, então, deve ser incorporada em um ciclo que constantemente avalia e refina as funções e responsabilidades da organização.

5.2 Referências do modelo de risco

Em vez de tentar definir um processo de avaliação de risco e modelagem de ameaças, revise as seguintes referências para uma ter uma visão mais completa e um passo a passo sobre processo de avaliação de risco:

- Estrutura de gerenciamento de riscos do National Institute of Standards and Technology (NIST) [5]
- Modelo OCTAVE do Computer Emergency Response Team (CERT) [6]

6 Considerações sobre privacidade

Muitos serviços e produtos de IoT serão pensados para criar, coletar ou compartilhar informações. Alguns desses dados podem não ser considerados "dados pessoais" ou afetar a privacidade do consumidor e, portanto, não estão sujeitos a regras de proteção e privacidade de informações. Esses dados podem incluir informações sobre o estado físico de máquinas, dados internos de diagnóstico ou métricas relacionadas ao estado da rede.

No entanto, muitos serviços de IoT envolverão dados sobre ou relacionados a consumidores e estarão sujeitos a leis gerais de proteção de dados e privacidade. Onde as operadoras móveis oferecerem serviços de IoT, elas também estarão sujeitas a regras de segurança e privacidade específicas para o setor de telecomunicações. Os serviços de IoT voltados para o consumidor tendem a envolver a geração, distribuição e uso de informações detalhadas que podem afetar a privacidade do indivíduo, como, por exemplo, fazer inferências sobre sua saúde ou desenvolver perfis com base em seus hábitos e locais de compras. À medida em que os serviços de IoT para consumidor ganham popularidade, mais dados do consumidor serão gerados, analisados em tempo real e compartilhados entre várias partes através das fronteiras nacionais.

Quando os dados estão relacionados a indivíduos específicos, esse ecossistema complexo e conectado pode causar preocupações ao consumidor sobre:

- Quem está coletando, compartilhando e usando os dados dos indivíduos?
- Que dados especificamente estão sendo coletados?
- Onde os dados estão sendo obtidos (por meio de quais tecnologias ou interfaces)?
- Quando os dados estão sendo coletados?
- Por que os dados do usuário são coletados?
- Como é assegurada a privacidade (e não apenas a segurança) das informações dos indivíduos?

- Os indivíduos têm controle sobre como seus dados são compartilhados e como as empresas vão usá-lo?

Todos os provedores de serviços de IoT que dependem de dados do consumidor - assim como as empresas parceiras que capturam ou usam esses dados - têm a obrigação de respeitar a privacidade dos indivíduos e manter seguras as informações pessoalmente identificáveis ou invasivas de privacidade.

Um desafio fundamental para os provedores de serviços de IoT é que existe uma multiplicidade de leis, muitas vezes inconsistentes entre si, que tratam de privacidade e proteção de dados. Diferentes leis podem ser aplicadas em diferentes países, dependendo dos tipos de dados envolvidos, bem como do setor ou indústria e dos serviços oferecidos pelo provedor de serviços. Isso tem implicações para uma série de provedores de serviços de IoT voltados para o consumidor;

Um veículo conectado, por exemplo, pode se mover entre diferentes países, o que significa que as transferências de dados associadas podem ser regidas por várias jurisdições diferentes. Os sensores no carro que rastreiam a localização do veículo (estático ou dinâmico) e seus destinos frequentes podem ser usados para inferir uma série de informações sobre o estilo de vida do motorista, passatempos ou religião - o que o motorista pode considerar informações pessoais. Além disso, informações sobre hábitos de condução por meio de sensores de "diagnóstico on-board" podem ser compartilhados com companhias de seguros que podem usar esses dados para impor um prêmio mais elevado e, assim, discriminar o motorista sem o seu conhecimento.

Os serviços e dispositivos de IoT (incluindo carros conectados) podem ainda se deslocar entre diferentes territórios soberanos e, portanto, diferentes jurisdições. Em muitos casos, os dados pessoais de um indivíduo podem transitar ou residir em jurisdições diferentes do indivíduo. Estas são questões importantes que precisam ser consideradas antes de um serviço de IoT multinacional ser implantado.

Outro desafio é que a maioria das leis de proteção de dados exige que as empresas que coletam dados dos consumidores obtenham consentimento do consumidor (também denominado "titular") antes de processar certas categorias de "dados pessoais" - como dados relacionados à saúde. A maioria das leis define "dados pessoais" como qualquer informação relacionada a uma pessoa natural identificada ou identificável.

Mas, à medida em que mais e mais dispositivos estiverem conectados à internet, mais e mais dados sobre indivíduos serão coletados e analisados, possivelmente afetando sua privacidade, sem que tais dados necessariamente sejam considerados "pessoais" por lei. A combinação de grandes volumes de dados, armazenamento em nuvem e análises preditivas pode fornecer perfis detalhados de usuários. Em particular, anonimizar os dados e informações pessoais que podem ser inferidos de outros tipos de dados pode vir a efetivamente se tornar um desafio.

A necessidade de manter a privacidade de informações sensíveis e de dados relacionados à saúde é bem reconhecida, principalmente devido à possibilidade de abuso comercial de tais registros. Nos Estados Unidos, a Lei de Portabilidade e Responsabilidade de Seguro de Saúde de 1996 (Health Insurance Portability and Accountability Act, HIPAA) inclui requisitos

de privacidade e segurança para mitigar os riscos de divulgação não autorizada de registros de saúde.

HIPAA, a exemplo de muitos outros regulamentos, como os da União Europeia, só se aplica se os dados de saúde forem pessoalmente identificáveis. Os dados armazenados em um dispositivo de monitoramento de sangue (que não identifica o usuário) não seriam cobertos por esses requisitos, enquanto esses mesmos dados em um aplicativo de smartphone ou em um servidor na nuvem provavelmente seriam cobertos por estarem vinculados a um indivíduo (no caso de um smartphone, porque o telefone certamente conterá outros dados que identifiquem o usuário e em um servidor na nuvem, porque ele será associado a uma conta de usuário identificável). Formuladores de políticas em todo o mundo estão percebendo que informações e insights sobre pessoas podem afetar sua privacidade mesmo que não sejam definidas como "pessoalmente identificáveis". Por conseguinte, tem sido cada vez mais comum adotar abordagens baseadas em risco na regulação, além de considerar implicações mais amplas do uso de dados sobre a privacidade em vez de se concentrar em definições legais.

A fim de promover confiança no ecossistema de IoT, os governos devem garantir que a proteção de dados e a legislação de privacidade sejam neutras em termos de tecnologia e que as regras sejam aplicadas consistentemente a todos os envolvidos no ecossistema da internet. Além disso, para que os provedores de serviços de IoT minimizem a necessidade de uma intervenção regulatória formal, recomendamos que sigam as etapas descritas no Anexo A nos estágios iniciais de desenvolvimento de seu serviço ou produto de IoT.

7 Usando este guia corretamente

Embora seja melhor implementar a segurança no início de um projeto de engenharia, este guia também pode ajudar organizações que já projetaram, fabricaram e até lançaram um produto ou serviço de IoT. Independentemente de qual etapa o produto ou serviço do leitor tenha alcançado, há um processo útil que deve ser seguido para obter o máximo de benefícios desse conjunto de documentos:

- Avaliação do modelo técnico
- Revisão do atual Modelo de Segurança do produto ou serviço
- Revisão e avaliação de Recomendações
- Implementação e Revisão
- Ciclo de Vida Contínuo

7.1 Avalie o modelo técnico

O primeiro e mais importante passo no processo é entender o próprio produto ou serviço de IoT da organização. Para realizar uma avaliação de segurança e uma avaliação de risco, a equipe deve estar familiarizada com cada componente usado na solução da organização, como os componentes interagem entre si e como os componentes interagem com seu ambiente. Sem uma compreensão clara de como o produto ou serviço foi (ou será) construído, uma avaliação estará incompleta.

Comece fazendo um documento que descreva cada componente usado no sistema. Identifique como o componente é fornecido, como ele é usado, qual nível de privilégio ele requer e como ele está integrado na solução geral. Mapeie cada componente para as

tecnologias descritas na seção “Modelo” de cada um dos documentos de diretrizes para o ecossistema de endpoint [3] e para o ecossistema de serviço [4]. É aceitável se o documento não corresponder precisamente a um componente, pois se deve mapear a classe geral do componente; simplesmente use a classe de componente, como um microcontrolador, módulo de comunicação ou âncora de confiança como contexto. Considere as seguintes questões:

- Quais componentes são usados para construir o produto ou serviço?
- Quais entradas e saídas são aplicáveis ao componente determinado?
- Quais controles de segurança estão aplicados a essas entradas e saídas?
- Qual nível de privilégio é aplicado ao componente?
- Quem na organização é responsável pela implementação do componente?
- Quem na organização é responsável por monitorar e gerenciar o componente?
- Qual processo está em vigor para corrigir os riscos observados no componente?

Essas perguntas, quando respondidas, vão possibilitar uma compreensão de como os componentes técnicos interagem uns com os outros e como o produto ou serviço de modo geral é afetado por componente.

Este processo corresponde à primeira e segunda fases do modelo de avaliação de risco “CERT OCTAVE” [6], ou à etapa “Frame” da estrutura de gestão de riscos da NIST [5]. Isso auxilia no desenvolvimento de um perfil para cada ativo crítico da empresa e no desenvolvimento de objetivos de segurança, e estabelece uma base de como a empresa irá avaliar, monitorar e responder ao risco.

7.2 Revise o atual modelo de segurança

Em seguida, leia a seção do modelo de segurança do endpoint ou serviço avaliado. Esta seção ajudará o leitor a entender o modelo que um hacker usará para comprometer uma determinada tecnologia. Esse modelo se baseia em anos de experiência na realização de avaliações de segurança, na engenharia reversa e na concepção de sistemas incorporados.

Uma vez que o modelo de segurança tenha sido revisado, o leitor deve ter uma compreensão melhor de quais tecnologias utilizadas no produto ou serviço em desenvolvimento são mais vulneráveis ou mais desejáveis para o hacker. Esta informação deve ser compartilhada com a organização para garantir que tanto os engenheiros quanto a liderança compreendam os riscos e ameaças ao modelo atual.

No entanto, deve-se notar que a organização não deve tomar medidas para ajustar seu modelo de segurança neste momento. É muito cedo para fazer mudanças arquitetônicas.

Novamente, este processo corresponde à primeira e segunda fases do modelo CERT OCTAVE [6], ou à etapa “Frame” da estrutura de gestão de riscos da NIST [5]. A revisão do modelo de segurança ajuda a melhorar o modelo técnico, identificando possíveis lacunas na segurança e destacando os objetivos de segurança que devem ser priorizados.

7.3 Revise a avaliação das recomendações

A seção “Recomendações” deve ser revisada neste momento para avaliar como as Tarefas de Segurança podem ser resolvidas. Esta seção não só fornecerá metodologias para implementar recomendações, mas também fornecerá uma visão dos desafios envolvidos na implementação da recomendação específica.

Para cada recomendação é fornecida uma seção do Método. Esta seção descreverá metodologias que ajudam na remediação ou mitigação de riscos à segurança. Esses métodos, embora sejam de alto nível, abordarão conceitos que, de uma perspectiva holística, ajudam a reduzir o risco, a fim de viabilizar a maximização de ganho a partir de uma carga de esforço razoável e prática.

A seção “Despesas” é fornecida para discutir, quando aplicável, despesas financeiras adicionais que a organização deve prever para implementar uma recomendação específica. Embora a maioria das despesas seja bastante óbvia, como o tempo de engenharia e as matérias-primas, despesas menos evidentes podem alterar as finanças aplicadas a produtos e serviços cujas margens de lucro e limites orçamentários já foram definidos pela liderança empresarial. Apesar de números específicos não serem fornecidos, são especificados tecnologias e serviços que podem resultar em custos adicionais.

A seção “Risco” também é oferecida para que o leitor entenda as lacunas na segurança que podem ocorrer diante da não implementação de uma recomendação específica. Embora o negócio possa aceitar que alguns riscos estão dentro das diretrizes operacionais da empresa, o leitor deve analisar cada seção de risco para garantir que o negócio entenda plenamente os efeitos colaterais de não implementar (ou não implementar corretamente) uma determinada recomendação. Isso pode parecer evidente para recomendações como "Dados encriptados”, mas a sutileza de algumas ameaças, como ataques de repetição contra mensagens que não são criptograficamente únicas, pode ser uma surpresa para o leitor no futuro.

Em alguns casos, são fornecidas referências para uma revisão posterior. Embora este documento não forneça informações detalhadas sobre cada plano de tecnologia, de risco ou de remediação, são oferecidos outros padrões e estratégias testados ao longo do tempo. Este conjunto de documentos fornecerá referências a esses materiais, quando aplicáveis, dentro de cada recomendação.

O resultado da revisão da seção “Recomendações” deve ser diretamente vinculado à seção “Tarefas de Segurança”. As Tarefas de Segurança devem agora ser preenchidas com Recomendações adequadas para garantir a correta implantação das Tarefas de Segurança. Essas Tarefas de Segurança serão vinculadas novamente aos Componentes específicos atribuídos aos membros da organização.

As recomendações de avaliação correspondem ao passo “Aferição” da estrutura de gerenciamento de riscos da NIST [5], e às etapas seis, sete e oito da metodologia CERT OCTAVE [6].

7.4 Implementação e revisão

A esta altura, as Tarefas de Segurança já foram claramente definidas, e as empresas terão uma melhor compreensão de suas vulnerabilidades de segurança, seu valor e seus riscos. A empresa deve agora criar um modelo arquitetônico claro para cada Componente a ser ajustado, e usar o processo escolhido de Avaliação de Risco para desenvolver um modelo de ameaça para cada Componente, incorporando as Recomendações e os Riscos apropriados por Componente e Tarefa de Segurança. Quando o modelo arquitetônico estiver concluído, a organização pode começar a implementar cada Recomendação para cumprir as Tarefas de Segurança.

Quando a implementação estiver concluída, a organização deve analisar os Riscos na subseção “Recomendações” e nas seções sobre Componentes. A organização deve garantir que a implementação atenda aos requisitos estabelecidos por essas seções. A organização deve, então, assegurar que a implementação resolva o desafio de segurança em relação ao contexto no qual o Componente foi projetado no produto ou serviço da organização, pois esses documentos não conseguiriam abordar completamente todos os produtos ou serviços que estão sendo projetados no setor. Se possível, use uma empresa de consultoria terceirizada para avaliar a implementação e garantir que ela realmente esteja adequada às melhores práticas de segurança.

A implementação e a revisão correspondem ao componente “Resposta” da estrutura de gerenciamento de riscos da NIST [5] e ao passo oito do modelo “CERT OCTAVE” [6].

7.5 Ciclo de vida contínuo

O ciclo de vida da segurança não termina aqui. Em vez disso, torna-se parte inerente da engenharia de um processo. Endpoints e serviços de IoT têm um tempo de vida útil, e devem ser atendidos continuamente durante toda essa vida, assim como um organismo vivo.

Os requisitos mudam ao longo do tempo. Os algoritmos criptográficos tornam-se obsoletos ou depreciados. Novos protocolos e tecnologias de rádio devem ser interoperáveis com o produto ou serviço. Esse ecossistema em constante mudança, no qual produtos embutidos são implantados, deve ser constantemente revisado para garantir que a confidencialidade, integridade, disponibilidade e autenticidade sejam mantidas.

A gestão contínua do ciclo de vida da segurança corresponde aos componentes “Monitor” e “Frame” da estrutura de gerenciamento de riscos da NIST [5] e às etapas um, quatro e cinco do modelo “CERT OCTAVE” [6].

8 Exemplo - Monitor de frequência cardíaca vestível

Neste exemplo, um projeto simples de Monitor de Frequência Cardíaca (HRM, do inglês Heart Rate Monitor) será avaliado usando esse conjunto de diretrizes. O endpoint será avaliado usando o documento “Ecossistema Endpoint”, enquanto a parte de serviço do projeto será avaliada usando o documento “Ecossistema de Serviço”.

8.1 Panorama do endpoint

Vamos começar avaliando o projeto de hardware do endpoint.

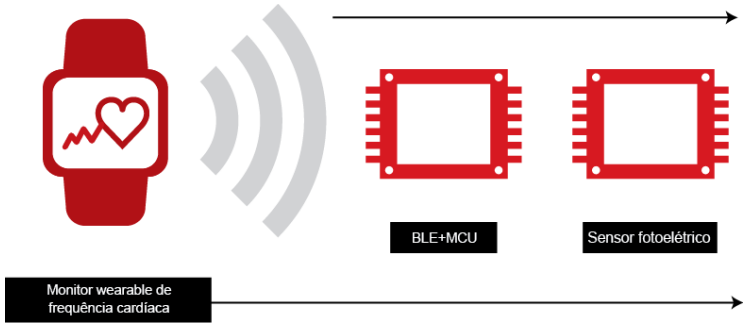

Figura 3 – HRM simples e componentes primários

O HRM é composto de componentes padrão para um dispositivo sem fio e fácil de usar: um sensor fotoelétrico de luz ambiente e um microcontrolador habilitado para transceptor Bluetooth Low Energy (BLE). O sensor é usado para capturar dados de pulsação, enquanto o microcontrolador analisa os dados emitidos pelo sensor e seleciona quais dados enviar pelo transceptor BLE incorporado. Neste exemplo, a pilha BLE usada é a versão 4.2.

Uma bateria formato botão é usada neste exemplo para transmitir dados do HRM a outro dispositivo, como um smartphone ou um tablet. Nenhum outro componente é necessário para que este dispositivo funcione.

De acordo com o documento “Ecossistema do Endpoint”, este dispositivo caberia na classe de dispositivos endpoint de material leve.

8.2 Panorama do serviço

Do ponto de vista do serviço, o aplicativo no smartphone ou tablet leva as métricas do endpoint até um serviço de back-end utilizando qualquer conexão de rede disponível. O serviço de back-end para o aplicativo simplesmente associa o proprietário do dispositivo às métricas capturadas e as armazena em um banco de dados local para o servidor de aplicativos.

A visualização dos dados pode ser obtida por meio do aplicativo móvel ou do site do serviço. Os usuários da tecnologia wearable podem fazer login no site do provedor de serviços para executar mais ações com as métricas capturadas pelo endpoint.

Este é um modelo de serviço muito simples e comum, sem complexidades personalizadas ou desnecessárias.

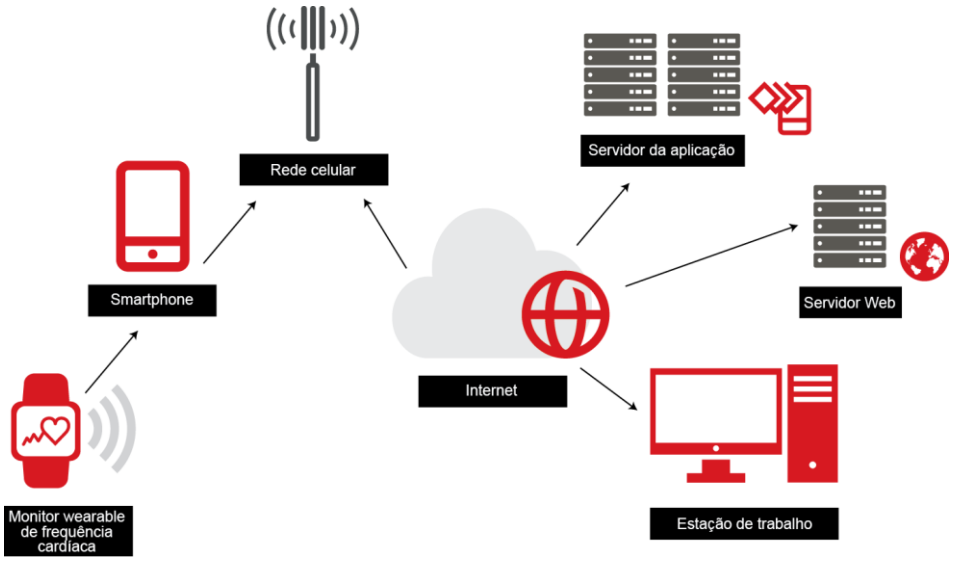

Figura 4 – Fluxo de dados para o serviço de back-end simples

8.3 Caso de uso

O negócio que desenvolve esta tecnologia pretende que o usuário final rastreie dados referentes ao seu pulso ao longo do dia, armazenando-os tanto no aplicativo como no banco de dados de. A intenção é permitir aos usuários rever sua frequência cardíaca ao longo do tempo para acompanhar sua saúde em geral. Os usuários podem acompanhar melhoras ou pioras em sua saúde ao longo do tempo, dependendo do estilo de vida que estejam levando. Isso permite que esses usuários incentivem a si mesmos ao avaliar tendências positivas e negativas nos dados de seu HRM.

O negócio pretende usar esses dados para fazer parcerias com fabricantes de dispositivos médicos, planos de saúde e outras organizações que podem usar essas métricas para identificar se um consumidor é mais ou menos susceptível de incorrer em um evento relacionado à saúde, como um ataque cardíaco ou um acidente vascular cerebral.

8.4 O modelo de segurança

A equipe de engenharia neste exemplo de negócio aproveitou as seções de “Perguntas Frequentes” dos documentos sobre endpoint e sobre serviço para determinar quais problemas são mais relevantes para seus produtos e serviços.

Da perspectiva do endpoint, a equipe aprendeu que os seguintes problemas são preocupantes:

- Clonagem
- Adulteração de endpoint
- Adulteração de serviço
- Proteção à privacidade

Do ponto de vista do serviço, a equipe decidiu que as seguintes questões são preocupantes:

- Clonagem
- Serviços hackeados
- Identificação de comportamento anômalo de endpoint
- Limitação de compromisso
- Redução de perda de dados
- Redução de exploração
- Gerenciamento da privacidade do usuário
- Melhoria da disponibilidade

A equipe analisou as recomendações para cada uma das questões acima, conforme sugerido para cada seção de Perguntas Frequentes. A equipe então optou por implementar recomendações que eram melhorias econômicas e garantiam a maior segurança.

Neste exemplo de modelo, o endpoint não exigiria uma alteração substancial. Como o endpoint possui pouca funcionalidade, pode-se empregar uma segurança mínima no endpoint tanto para aplicações de segurança quanto de comunicação. Uma vez que o aplicativo do endpoint é ativado em um único dispositivo, desde que o firmware do dispositivo esteja bloqueado, não há ameaça real de ataque contra o endpoint dentro do caso de uso determinado.

No entanto, uma vez que a privacidade é um desafio, a organização deve empregar pelo menos uma versão PSK Personalizada de uma Base de Computação Confiável (TCB, do inglês Trusted Computing Base). Isso garantiria que os tokens de criptografia fossem exclusivos para cada endpoint, de modo que um endpoint comprometido não comprometesse todos os outros. Se as chaves personalizadas (únicas) fossem codificadas no microcontrolador bloqueado, seria razoável acreditar que este caso de uso estaria adequadamente protegido contra desafios como clonagem, falsificação e riscos à privacidade. Reveja os documentos de Serviços de IoT [3] e Endpoint [4] para uma discussão mais completa sobre o que é uma Base de Computação Confiável dentro do contexto de cada ecossistema.

A infraestrutura do servidor, no entanto, requer um volume significativo de mudanças. Os engenheiros percebem que, de acordo com as recomendações, estão em grave risco de abuso. Os seguintes problemas são reconhecidos:

- Não há segurança front-end diminuindo os efeitos de um ataque de Negação de Serviço (DoS)
- Não há controles de entrada ou saída limitando o fluxo de tráfego de ou para serviços
- Não há separação de tarefas entre níveis de serviço
- Não existe um banco de dados seguro separado que contenha tokens PSK Personalizados
- Nenhuma medida de segurança adequada foi implementada no sistema operacional do serviço
- Não há métricas adotadas para avaliar comportamentos anômalos do endpoint

8.5 O resultado

Após a implementação das recomendações, a organização possui uma arquitetura de serviço back-end muito mais bem definida que aborda adequadamente os riscos identificados por meio das diretrizes.

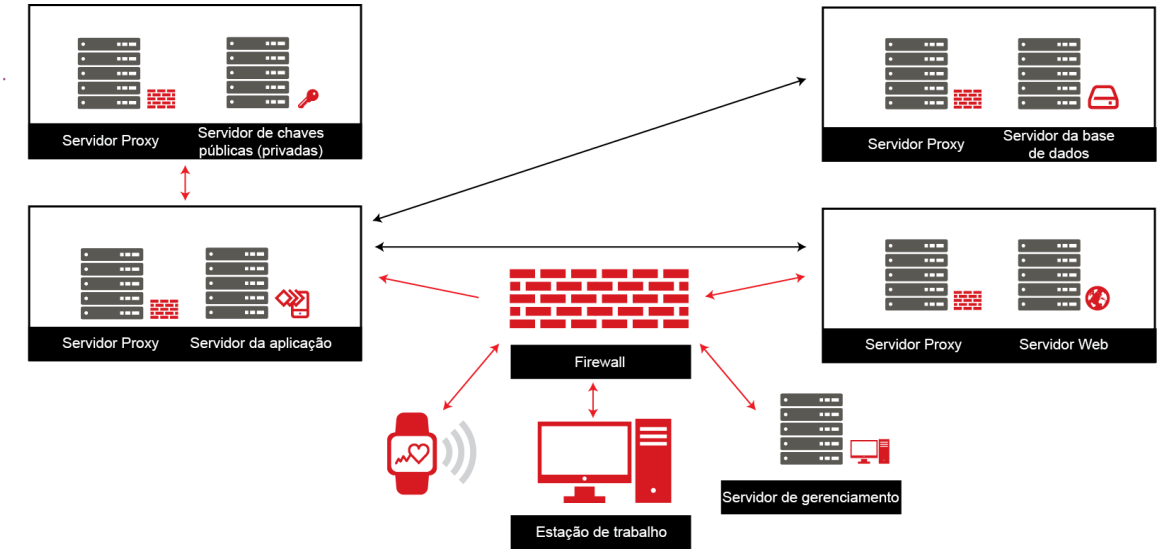

Figura 5 – Ecossistema de serviço resultante

Na figura acima, as mudanças no ecossistema de serviço são facilmente observáveis. Cada classe de serviço foi dividida em camadas separadas para ajudar a proteger e dimensionar facilmente a tecnologia no caso de picos de demanda. Foram somados dois níveis adicionais, uma camada de banco de dados e um nível de autenticação para separar sistemas críticos de serviços que interagem diretamente com o mundo externo. Um front-end de segurança foi implementado para ajudar a proteger a rede interna de vários tipos de ataques, incluindo ataques DoS e DDoS, que reduzem a disponibilidade do sistema. Finalmente, um modelo administrativo foi definido para permitir o acesso seguro de gerenciamento ao ambiente de produção. Um componente não representado no diagrama acima é a presença de um modelo analítico que observa quando o comportamento do endpoint pode ser indicativo de um compromisso ou uma falha no design do firmware ou do hardware.

8.6 Resumo

De modo geral, essa tecnologia simples poderia ter sido facilmente comprometida se tivesse sido implantada como estava. No entanto, com algumas mudanças rápidas, simples e econômicas feitas no endpoint, garante-se que a tecnologia tenha anos de vida em uso sem alterações em sua arquitetura.

Diante de um ecossistema de serviços reforçado, há muito menos ameaça tanto para os usuários quanto para os negócios. Clonagem e falsificação não são mais uma ameaça. A privacidade é garantida pela atribuição de tokens criptográficos exclusivos para cada endpoint. Os sistemas que contêm informações críticas são separados e protegidos de

sistemas voltados ao público, que são mais passíveis de abuso. Este modelo, embora um pouco mais complexo, reduz o risco global do ambiente de produção.

9 Exemplo – drone pessoal

Neste exemplo, um pequeno dispositivo de drone pessoal será avaliado usando este conjunto de diretrizes. O endpoint será avaliado usando o documento “Ecossistema do Endpoint”, enquanto a parte de serviço do projeto será avaliada usando o documento “Ecossistema de Serviço”.

9.1 Panorama do endpoint

Vamos começar avaliando o design do hardware do endpoint.

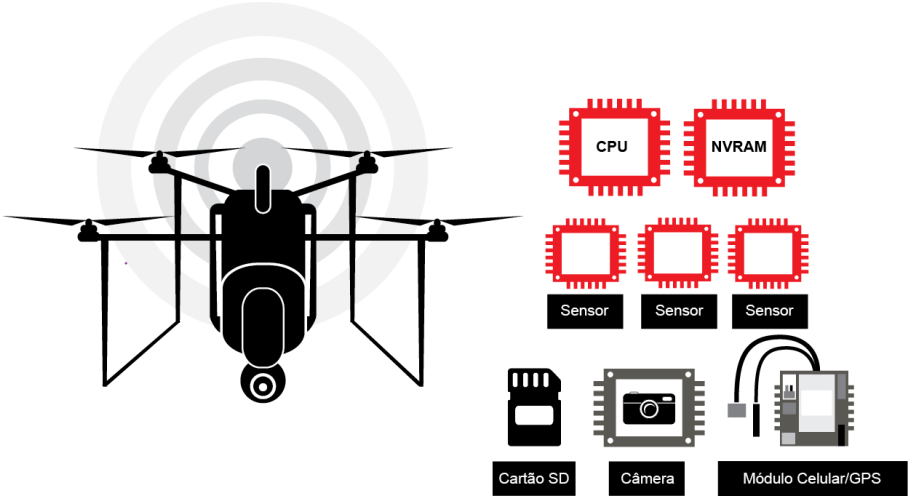

Figura 6 – Um drone e seus componentes primários

Este drone pessoal é composto por um conjunto robusto de componentes. As capacidades de processamento do drone são de alto desempenho devido aos múltiplos motores, sensores e outros equipamentos que devem funcionar de forma eficiente em paralelo. Este modelo usa uma CPU ARM Cortex-A8 com o sistema operacional primário (Linux) armazenado em NVRAM em um chip separado. É necessária uma série de vários sensores para detectar movimento, luz, velocidade, entre outros. Um cartão SD / MMC é usado para armazenar vídeo, métricas de sensores e metadados. Uma câmera é usada para permitir que o operador veja do ponto de vista do drone. Um módulo contendo capacidade celular e GPS é usado para garantir que o drone possa manter a conectividade com seu operador, mesmo quando está fora do alcance de um protocolo proprietário. O GPS também é usado para orientação e para uma automação mínima.

Uma bateria de Polímero de Lítio (LiPo) é usada para pilotar o drone. Quando todas as funções estão ativas simultaneamente, seu tempo de voo é de aproximadamente duas horas antes de uma nova carga ser necessária.

De acordo com o documento “Ecossistema de Endpoint”, este dispositivo caberia na classe de endpoint de alta complexidade. Embora contenha um módulo celular, ele não é considerado um gateway, pois não roteia mensagens para ou de outros endpoints.

9.2 Panorama do serviço

Do ponto de vista do serviço, o back-end é usado apenas para a conectividade do operador quando a perda é detectada na interface de rádio proprietária durante o voo. Se o drone estiver em voo e a conexão celular puder ser habilitada, ele tentará aguardar a conexão do seu operador por meio da rede LTE. Se, no entanto, o drone for incapaz de ser controlado por meio de rede LTE, ele tentará uma aterrissagem automática do último local em que ele decolou.

No entanto, como o drone tem alguns recursos simples de automação, é possível dar coordenadas e um caminho a percorrer enquanto ele tira fotos ou faz vídeos curtos. Esses arquivos de mídia podem ser carregados em tempo real por meio da rede LTE para o serviço de back-end para mostrar ao operador seu curso e ponto de vista durante a execução automática.

Assim, é necessário um serviço de back-end robusto para garantir um alto grau de disponibilidade de serviço para cada drone que possa se conectar ao sistema. A disponibilidade também é necessária para atender aos picos de tráfego da rede decorrentes da transmissão de vídeos e imagens de alta resolução por meio de um link celular. Também deve haver uma interface web que permita ao operador visualizar os uploads de mídia a partir de um navegador web.

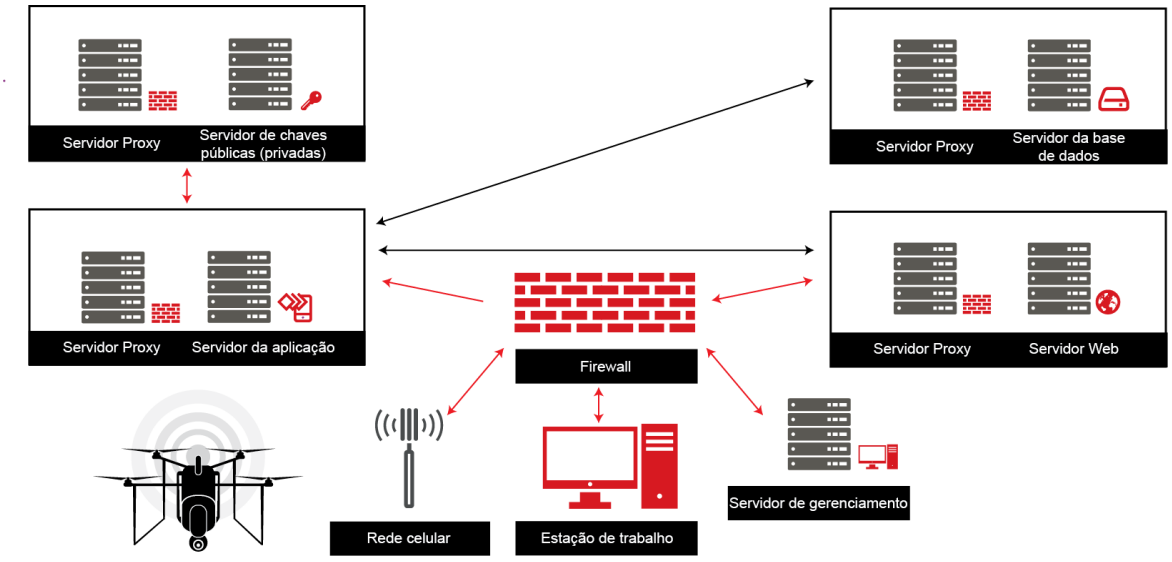

Figura 7 – Fluxo de dados para serviços de back-end

9.3 Caso de uso

A intenção do desenvolvimento dos negócios em torno dessa tecnologia é que o usuário use o drone para filmagens na natureza. No entanto, alguns de seus clientes já usaram o drone para cenas de filmagem no cinema, uma vez que a câmera e as capacidades de estabilização do drone são excepcionais para a faixa de preço. Como resultado, o drone será usado em caros projetos de filmagem em que a propriedade intelectual e a privacidade são grandes preocupações.

9.4 O modelo de segurança

A equipe de engenharia neste exemplo de negócio utilizou as seções sobre Perguntas Frequentes dos documentos sobre o endpoint e sobre o serviço para determinar quais questões são mais relevantes para seus produtos e serviços.

Do ponto de vista do endpoint, a equipe aprendeu que os seguintes desafios merecem atenção:

- Identidade do endpoint
- Adulteração do endpoint
- Ataques às âncoras de confiança
- Manipulação de software e firmware
- Gerenciamento remoto seguro
- Detecção de endpoints comprometidos
- Adulteração de serviço
- Proteção à privacidade

Do ponto de vista do serviço, a equipe decidiu que as seguintes questões merecem atenção:

- Gerenciamento da privacidade do usuário
- Melhora da disponibilidade

A equipe analisou as recomendações para cada um dos problemas acima, conforme sugerido em cada seção das perguntas frequentes. A equipe escolheu implementar recomendações de melhorias custo-eficientes que garantiram maior segurança.

Neste exemplo, a infraestrutura do serviço não requer uma mudança substancial. Isso ocorre porque essa infraestrutura já foi construída para acomodar os picos de tráfego necessários para a manutenção do serviço no endpoint. A arquitetura já exigia uma arquitetura bem planejada e segura simplesmente para poder escalar de forma efetiva e manter a disponibilidade de recursos, mesmo quando alguns serviços demonstrassem falhas temporárias. Porém, a organização optou por investir mais na privacidade do usuário, já que isso se tornou um ponto importante de atenção em razão do uso do produto em nichos de negócio inesperados.

A infraestrutura do endpoint, no entanto, requer um número significativo de mudanças. Os engenheiros percebem que, de acordo com as recomendações, elas estão em grave risco de abuso. Os seguintes desafios são identificados:

- O carregador de inicialização não está validando adequadamente o aplicativo antes de executar o kernel do sistema operacional, levando a um risco de adulteração
- Não é usada TCB para gerenciar a segurança do aplicativo ou das comunicações
- Como não existe um TCB devidamente implementado ou uma âncora de confiança, existe o problema de clonagem do endpoint, o que pode levar ao vazamento de dados
- Sem uma TCB bem implementada, o endpoint não pode autenticar os serviços adequadamente
- Sem uma TCB bem implementada, o endpoint não pode autenticar adequadamente o operador sobre a interface de rádio proprietária

- Os engenheiros confiaram na segurança do LTE para garantir que o canal de comunicação não seja comprometido, mas não consideraram a ameaça de falsificação de endpoints ou a reutilização da Femtocell, sendo que ambos são capazes de atravessar a segurança do LTE e comprometer a baixa segurança do serviço

9.5 O resultado

Depois de implementar as recomendações para as questões citadas acima, a organização conseguiu uma arquitetura de endpoint mais bem definida, que aborda adequadamente os riscos identificados por meio dos documentos de orientação.

Para o sistema de drone em uso, a equipe de engenharia emite uma atualização de firmware que implementa um modelo de segurança Pubkey Personalizado. A atualização do firmware melhora o carregador de inicialização também para garantir a segurança na arquitetura central. Uma vez que um modelo de Pubkey Personalizado foi usado, qualquer pessoa que tente se aproveitar da falta inicial de segurança no endpoint para tentar falsificar o endpoint de outro usuário falharia, pois os engenheiros utilizaram seu banco de dados de mapeamento de usuário-para-endpoint para criar chaves personalizadas por usuário. Desta forma, nenhum usuário sem as credenciais de Web apropriadas pode baixar e instalar a atualização de Pubkey Personalizada de outro usuário. Embora este processo tenha sido complexo e demorado para ser implementado, valerá o esforço.

Futuras versões da tecnologia do drone implementarão uma âncora de confiança de CPU interna. Esta âncora de confiança estará vinculada a uma TCB Pubkey Personalizado para garantir que cada endpoint seja instalado de forma exclusiva, com segurança excepcional desde o início.

A implantação de uma criptografia com esse nível de segurança é imperativa, pois também anula a possibilidade de outros tipos de ataques que a empresa tenha identificado como uma preocupação. Ao alavancar o benefício de uma criptografia forte e uma TCB para verificação e autenticação, a equipe de engenharia pode identificar facilmente se os serviços não autorizados estão sendo disponibilizados para o drone. O drone, ao detectar serviços não autorizados, pode pousar de volta no local de decolagem original.

Qualquer serviço que detecte um drone indevidamente protegido também pode gerar alertas internamente. A equipe de administração poderá então determinar como lidar com o drone potencialmente comprometido. Isso fornece um alto nível de agilidade em relação aos eventos de segurança, e fornece à organização um meio de avaliar se há problemas de software ou hardware que estão causando um comportamento anormal no endpoint.

9.6 Resumo

Embora a equipe de engenharia obviamente tenha gasto uma quantidade excepcional de tempo criando uma arquitetura resiliente a partir de uma perspectiva de engenharia mecânica e serviços de back-end, um trabalho substancial precisava ser feito para criar uma tecnologia de endpoint segura. Embora este cenário não tenha representado uma ameaça crítica para o negócio como um todo, foi possível encontrar uma solução que funcionasse suficientemente bem para as necessidades de seus clientes. Se essa tivesse

sido uma tecnologia mais crítica para a segurança, até mesmo a solução implantada aqui poderia não ter sido suficiente.

Para obter mais informações sobre as variantes de TBC, tais como o Pubkey Personalizado TCB ou o TCB PSK Personalizado, reveja os documentos “Ecossistema de Serviço de IoT” [3] e “Endpoint” [4].

10 Exemplo – rede de sensores de veículo

Neste exemplo, uma rede de sensores de veículo implantada em uma nova classe de automóveis será avaliada usando este conjunto de diretrizes. O endpoint será avaliado usando o documento “Ecossistema de Endpoint”, enquanto a parte de serviço do projeto será avaliada usando o documento “Ecossistema de Serviço”.

10.1 Panorama do endpoint

Vamos começar avaliando o design do hardware do endpoint.

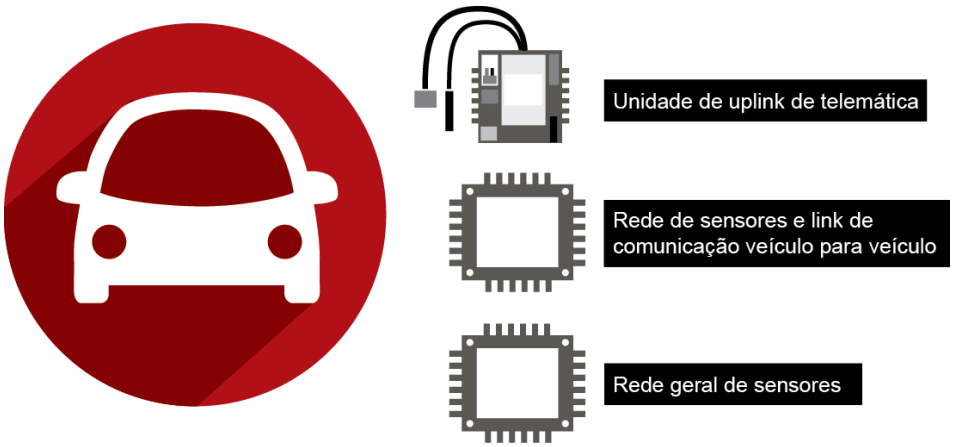

Figura 8 – Rede completa de sensores de veículo e sistemas de comunicações

Embora o modelo acima seja muito complexo para ser representado adequadamente em um diagrama simples, os três componentes de alto nível envolvidos são:

- Uma unidade de uplink de telemática que gerencia a rede de sensores, toma decisões complexas em nome do motorista e mantém uma conexão com o sistema de back-end
- Um sistema veículo-para-veículo (V2V) que detecta e reage a eventos V2V
- Uma rede de sensores que fornece métricas para a unidade de uplink de telemática

Nos sistemas automotivos modernos, a unidade telemática faz parte da rede de computadores do automóvel e toma decisões com base em dados de sensores e comunicações de back-end. Esta unidade irá tomar decisões com ou em nome do condutor do veículo. A unidade garante que o veículo está funcionando corretamente, tenta tomar decisões inteligentes durante emergências e realiza comandos da rede back-end.

A rede de sensores V2V identifica veículos nas proximidades e toma decisões com base em métricas coletadas pelos sensores. Enquanto a unidade telemática toma decisões

principalmente com base no estado dos componentes (como freios ou monitores de pressão dos pneus), o sistema V2V toma decisões com base na presença de outros veículos ou envia alertas para veículos próximos no caso de um evento crítico.

A rede de sensores é uma série de componentes que fornecem dados para a unidade telemática e, às vezes, à unidade V2V. Essas unidades usam as informações coletadas pela rede de sensores para tomar decisões precisas durante eventos críticos.

De acordo com o documento “Ecossistema de Endpoint”, este sistema possui componentes que se encaixam em todas as categorias de endpoint de IoT. A unidade de uplink de telemática atua como um gateway. A unidade V2V atua como um endpoint complexo. Os sensores são endpoints de baixa complexidade.

10.2 Panorama de serviço

Do ponto de vista do serviço, a rede de sensores do veículo fornecerá métricas ao ambiente de back-end. Estes dados podem ou não ser fornecidos ao consumidor. Em vez disso, os dados podem ser armazenados pelo fabricante para observar ou identificar possíveis problemas com os componentes. Isso pode desencadear alertas de serviço emitidos para o consumidor.

O sistema também pode ser ampliado para fornecer ao consumidor serviços úteis como "desbloquear remotamente a porta", "ligar o motor" e recursos semelhantes. No futuro próximo, esses sistemas poderão permitir que os veículos sejam conduzidos remotamente por meio de sistemas de orientação automatizados.

Embora a maior parte das decisões críticas seja tomada nas unidades de processamento do próprio veículo, é razoável conjecturar que algumas decisões serão feitas na nuvem, em que mais machine learning (ML) e inteligência artificial (IA), juntamente com modelos comportamentais ou estatísticos, podem ser utilizados para tomar decisões mais complexas.

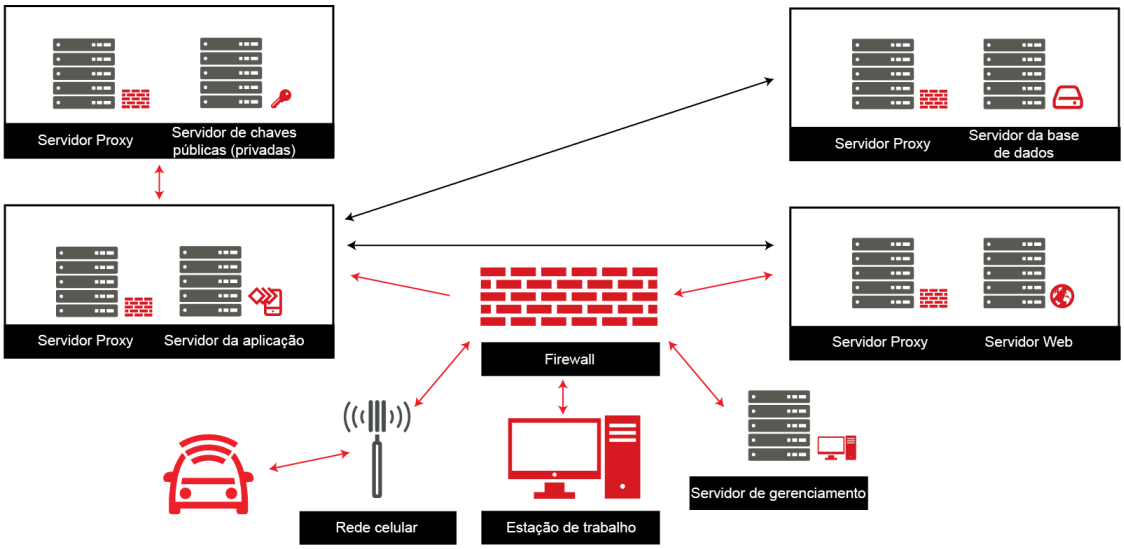

Figura 9 – Fluxo de dados para serviços de back-end

10.3 O caso de uso

O caso de uso desta tecnologia é óbvio: construir veículos inteligentes que possam tomar decisões complexas em cenários críticos de segurança. O objetivo é aproveitar a inteligência de todos os sensores possíveis para tomar decisões críticas em curto período de tempo. Freio automático, alertas de esvaziamento de pneus e outros cenários críticos podem ser resolvidos por meio do uso de sensores e sistemas de computadores bem projetados.

Uma característica interessante desta tecnologia é que ela pode ser inteiramente transparente para o usuário. O usuário não precisaria configurar esses computadores para atuarem de certa forma. Em vez disso, eles devem ser capazes de navegar cenários por meio do uso de métricas derivadas de sensores. Isso permitirá que os computadores se comportem corretamente, independentemente do ambiente.

10.4 O modelo de segurança

A equipe de engenharia neste exemplo utilizou as seções de Perguntas Frequentes dos documentos “Endpoint” e “Serviço” para determinar quais questões são mais relevantes para seus produtos e serviços.

Do ponto de vista do endpoint, a equipe determinou que os seguintes desafios são pertinentes:

- Falsificação de endpoint
- Falsificação do serviço ou dos pares
- Ataques de canal lateral
- Detecção de endpoints comprometidos
- Garantia de proteção

Do ponto de vista do serviço, a equipe decidiu que os seguintes desafios são pertinentes:

- Identificação de comportamento anômalo de endpoint
- Gerenciamento da privacidade do usuário

O maior risco para este ambiente que não foi discutido em exemplos anteriores é o risco de falsificação em relação aos pares. Uma preocupação que os engenheiros têm neste tipo de ambiente é o risco de um computador tomar decisões críticas usando dados que não sejam devidamente autenticados.

Como os dados de sensores em cenários críticos necessitam de tempos de processamento excepcionalmente rápidos, convencionou-se que nem sempre é possível implementar criptografia assimétrica ou comunicações baseadas em PKI. No entanto, essa pode não ser uma afirmação precisa. Em vez disso, um modelo de segurança preciso deveria antecipadamente considerar cenários críticos em termos de tempo e armazenar no cache chaves de sessão para os endpoints próximos. Por exemplo, se dois objetos estiverem se aproximando a uma velocidade conhecida, aplicações de segurança no ecossistema de serviço podem preparar chaves de sessão específicas para esses dois endpoints antes que eles atinjam uma distância a partir da qual pode haver colisão. Isso garantiria que a comunicação segura entre os endpoints e seus sensores ainda poderia ser usada no caso

de não haver tempo para renegociar uma sessão segura instantânea quando a possibilidade de um cenário crítico (como um acidente iminente) fosse detectada.

Assim, é necessária uma ampliação na implementação da TCB. Uma solução interessante é o GBA, em que o UICC usado na unidade de uplink de telemática pode distribuir as chaves de forma segura aos endpoints em todo o sistema. Este protocolo permitirá que mesmo endpoints rudimentares recebam chaves de sessão seguras que podem ser usadas em vários cenários críticos. Desta forma, o ambiente sempre pode ser propagado a partir de uma raiz de confiança, mesmo se endpoints de menor complexidade não sejam capazes de realizar cálculos críticos críticas para a inicialização da sessão de chave pública.

Outra questão crítica nesses ambientes é a detecção de endpoints comprometidos. Por exemplo, como o ambiente pode reconhecer se um sensor simples, como um Monitor de Pressão de Pneus (TPM), foi comprometido? Se o computador tomar uma decisão crítica com base no alerta do TPM de que um pneu teria esvaziado, pode surgir um problema de segurança. Como resultado, o comportamento de dispositivos e sua confiabilidade devem ser reavaliados em cada fase de inicialização. Todos os dispositivos devem ser resistentes à adulteração e devem poder notificar a rede se forem comprometidos. Inversamente, deve haver uma maneira de outros dispositivos na rede de sensores poderem avaliar a confiabilidade de seus pares na rede.

10.5 O resultado

Depois de implementar as recomendações, a rede de sensores do veículo está bem protegida contra os ataques à rede de comunicações do veículo. O GBA é usado para distribuir chaves para todos os endpoints no sistema, e faz isso em cada inicialização, garantindo que chaves antigas não sejam reutilizadas. Isso, juntamente com a resistência à adulteração, uma TCB forte em todos os endpoints e uma raiz organizacional de confiança, permite que o ambiente funcione com muito menos risco.

No entanto, independentemente dessas mudanças, a segurança física ainda é um fator crítico. A equipe de engenharia e os líderes da organização, juntamente com a equipe jurídica da empresa e seguradoras, devem avaliar a tecnologia crítica de segurança física e determinar se a segurança cibernética pode ser implementada sem arriscar a segurança física dos usuários. Embora a segurança cibernética possa ser implementada mesmo em cenários críticos, com alguns ajustes na arquitetura, há momentos em que a segurança física deve vir antes de todas as outras preocupações.

10.6 Resumo

Sistemas como este muitas vezes são bem projetados e não são vulneráveis a ataques triviais. No entanto, falhas sutis na arquitetura de comunicação podem levar a um ambiente comprometido. Em áreas controladas, como algumas redes CANbus, um único endpoint defeituoso pode fazer com que todo o sistema se torne vulnerável. Isso, em ambientes críticos, é inaceitável.

Anexo A Considerações e recomendações sobre privacidade para provedores de serviços de IoT

Para criar confiança no ecossistema IoT e minimizar a necessidade de uma intervenção regulatória formal, a GSMA propõe as seguintes etapas de alto nível como um guia para minimizar riscos de privacidade. Recomendamos que os prestadores de serviços de IoT sigam estes passos e considerem estas questões nos estágios iniciais de desenvolvimento do seu serviço ou produto de IoT.

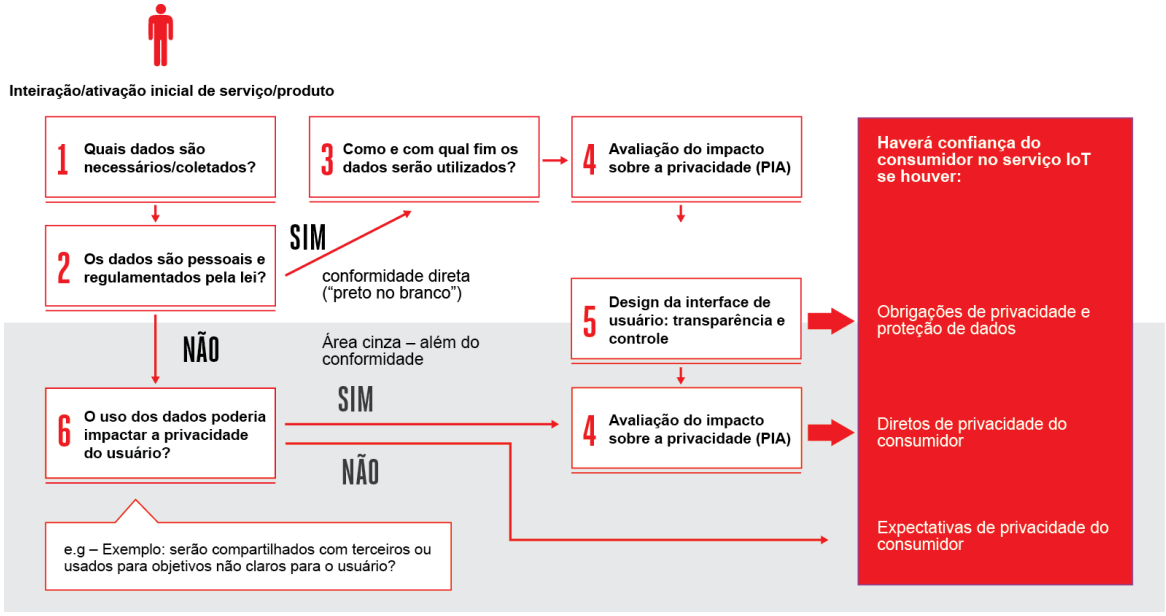

Figura 10 – Árvore de decisão da GSMA sobre privacidade by design

Passos	Consideração
Passo 1	**Quais dados você precisa coletar do/sobre o usuário para que seu serviço ou produto IoT possa funcionar corretamente?** Uma das primeiras etapas em qualquer modelo de negócio que depende de dados é identificar quais informações são realmente necessárias do ou sobre o consumidor para que o serviço ou produto funcione corretamente. Os tipos de dados que um serviço requer podem ser categorizados como estáticos - como o nome do consumidor ou o endereço residencial - e dinâmicos, como a localização em tempo real. Então, se você está oferecendo, por exemplo, uma pulseira fitness que rastreie os passos de alguém e as calorias queimadas, você precisaria saber o peso, a idade, o sexo, a distância percorrida e a frequência cardíaca do indivíduo que está usando a pulseira, mas você provavelmente não precisa da localização real do indivíduo. Ao avaliar os tipos de dados necessários, também é importante decidir se o consentimento dos indivíduos é necessário para usar esses dados e como você obteria esse consentimento, ou alternativamente se ofereceria aos usuários opções para controlar suas preferências de privacidade. Um smartphone pode atuar como um meio para oferecer as opções de privacidade do usuário (por exemplo, aplicativo móvel ou painel de controle online) quando o produto em si não possuir tela.

Passo 2	**Os dados são "pessoais" e regulados por lei?** O próximo passo deve ser identificar os requisitos de proteção de dados e privacidade que a lei impõe. Perguntas a considerar incluem: ● Qual é a definição de dados "pessoais" no país/mercado em questão? ● Os dados coletados são "pessoais" e regulamentados por lei? Em caso afirmativo, você identificou a base jurídica que lhe permite processar esses dados? ● Você está sujeito a quaisquer condições de licença relacionadas à privacidade (por exemplo, como um provedor de telecomunicações) ● Existem leis federais, estaduais, locais ou específicas do setor que se aplicam em relação ao modelo de coleta de dados proposto, além das leis gerais de proteção de dados? por exemplo: o Serviços financeiros / bancários, regulamentações de saúde o Restrições potenciais sobre transferências transfronteiriças de dados
Passo 3	**Como e para que os dados serão utilizados?** Uma vez que você estabeleceu quais são seus requisitos de conformidade legal, o próximo passo é mapear como os dados que você coleta serão usados - e com quem eles precisam ser compartilhados - para alcançar os resultados pretendidos como parte de sua oferta de serviços. As seguintes perguntas devem ajudá-lo a abordar questões de segurança e privacidade em relação ao tratamento dos dados: ● Os dados são mantidos seguros quando são armazenados ou transmitidos? ● Você definiu claramente os fluxos de dados? Isto é, identificar de que forma os dados serão usados e compartilhados em toda a cadeia de valor e para quais fins ● Você pode justificar por que cada tipo de dado coletado é necessário no contexto específico de oferta do serviço pretendido? ● Você definiu termos para seus parceiros relativos às responsabilidades de privacidade (e o design do seu produto reflete essas responsabilidades?) ● Existem acordos contratuais adequados com as empresas com as quais você compartilha os dados dos consumidores? (Por exemplo, limitando o uso de dados por provedores de análise para seus próprios fins comerciais). Tais acordos ou restrições podem ser bilaterais ou você pode estabelecer um código de conduta ou diretrizes e pedir aos seus parceiros que se comprometam com eles, com consequências e responsabilidades definidas caso o descumpram.

Passo 4	**Realize uma avaliação de impacto de privacidade** Realizar uma avaliação de impacto de privacidade (PIA, do inglês Privacy Impact Assessment) trata de: ● Identificar se, e como seu produto ou serviço gera algum risco de privacidade para o usuário ● Reduzir o risco de danos ao usuário que possam resultar do possível mau uso de suas informações pessoais ● Projetar um processo mais eficiente e efetivo para lidar com dados sobre indivíduos Os requisitos da PIA tornam-se cada vez mais comuns nas leis de proteção de dados e privacidade. Existem vários guias sobre como conduzir uma PIA, incluindo os publicados pelo Comitê do Comissário da Informação do Reino Unido [10] e aqueles feitos pela Associação Internacional de Profissionais de Privacidade. Perguntas típicas a serem abordadas na realização de uma PIA incluem: ● O projeto resultará em que você/seus parceiros tomem decisões ou tomem medidas contra indivíduos de maneira que possam ter um impacto significativo sobre eles? ● As informações sobre indivíduos são de um tipo particularmente susceptível de gerar maior preocupação ou expectativa de privacidade? Por exemplo, registros de saúde, registros criminais ou outras informações que as pessoas considerariam privadas? ● O projeto exigirá que você entre em contato com indivíduos de uma forma que eles possam achar intrusiva?
Passo 5	**Incluir privacidade na interface do usuário** Depois de avaliar os riscos de privacidade para os consumidores, você deve considerar como aumentar o nível de informação desses consumidores sobre tais riscos e sobre como mitigá-los, além de oferecer opções para expressar suas preferências de privacidade. Em última instância, esta etapa é sobre garantir que você ofereça um serviço que atenda suas obrigações legais e as necessidades e expectativas dos consumidores de forma amigável. E é sobre construir confiança, assegurando aos usuários que eles têm mais controle sobre sua privacidade. Perguntas a considerar incluem: ● Como os consumidores podem ser informados de quaisquer riscos para sua privacidade e como eles podem fazer escolhas informadas? ● Você obteve consentimento (quando legalmente exigido)? Os principais elementos de consentimento incluem: divulgação, compreensão, voluntariedade, competência e concordância) ● Os dados são protegidos em trânsito e em repouso? ● Existe um período definido para o qual você precisa manter os dados do consumidor (e por quê)? ● A jornada do consumidor ajuda a ganhar confiança? Por exemplo: ○ Eles entendem quais dados eles estão compartilhando em troca de usar o serviço? ○ Os consumidores podem expressar suas preferências de privacidade em etapas simples, por exemplo, por meio de um "painel de controle de permissões" baseado na web, notificações "just-in-time", um call center, um aplicativo móvel, um comando ativado por voz etc.

Passo 6	**O uso de dados pode afetar a privacidade do indivíduo?** Seu produto ou serviço pode coletar dados que não são necessariamente classificados como "pessoais" na lei, mas ainda podem ter implicações de privacidade para o consumidor e, portanto, devem ser considerados no início. Para verificar se os dados relevantes podem ser usados com impacto na privacidade de um consumidor, considere o seguinte: • Os dados (não pessoais) do seu serviço/produto podem ser combinados com outros dados de diferentes fontes para fazer inferências sobre a vida pessoal de um consumidor? Por exemplo, inferências sobre seu estilo de vida, hábitos ou religião que: o Afetem a sua capacidade de obter seguro de saúde? o Sejam usados por terceiros (varejistas, seguradoras) para discriminar o preço contra um consumidor em particular? • Se seu produto ou serviço provavelmente mudará em qualquer ponto no futuro, quais são as possíveis implicações de privacidade de qualquer mudança para o consumidor. Por exemplo: o A mudança envolve a coleta de novos dados sobre o consumidor (como dados de localização)? o Os dados do consumidor, existentes ou novos, são compartilhados ou vendidos para terceiros (por exemplo, anunciantes) que começarão a usar dados do consumidor para fins diferentes dos originalmente obtidos? • Se ocorrerem tais alterações, você deve: o Verificar o possível impacto em sua empresa se novas leis forem invocadas como resultado da mudança o Estabelecer processos para informar os consumidores e obter o seu consentimento quando necessário o Fornecer os meios para que os consumidores alterem suas preferências de privacidade • Algumas considerações adicionais que recomendamos aos prestadores de serviços de IoT são: o Certifique-se de ter acordos contratuais apropriados que definam as responsabilidades de cada parceiro na cadeia de valor o Tenha um claro processo de reparação para que os consumidores saibam para quem recorrer se as coisas derem errado ou se sofrerem uma violação de privacidade

O diagrama a seguir apresenta uma opção de como as etapas propostas acima podem ser ilustradas:

Anexo B Exemplo baseado em sistema de rastreamento automotivo

Neste exemplo, um sistema de rastreamento automotivo será avaliado a partir da perspectiva das Diretrizes de Segurança para a IoT. O processo será derivado da seção seis deste documento de visão geral - "Usando este guia corretamente".

B.1 Avalie o modelo técnico

No primeiro passo, "Avaliando o modelo técnico", a equipe de engenharia avalia como o dispositivo funciona com base na arquitetura de seus produtos. A equipe de engenharia cria um documento que detalha as tecnologias usadas na solução para organizar o quadro de funcionários, atribuir Tarefas de Segurança e acompanhar o progresso.

Por uma questão de simplicidade, nosso sistema de rastreamento automotivo terá as seguintes capacidades:

- **Ecossistema do endpoint:**
  - Uma simples Interface Gráfica de Usuário (GUI, do inglês Graphic User Interface) que permite ao usuário:
  - Fazer login com um nome de usuário e senha
  - Desativar rastreamento
  - Ativar rastreamento
  - Identificar e visualizar a localização atual
  - Um módulo celular para conexão a serviços de back-end
  - Um cartão SIM para o módulo celular
  - Uma bateria de polímero de lítio para energia de reserva
  - Uma Unidade Central de Processamento (CPU)
  - Um aplicativo incorporado na RAM não volátil
  - RAM
  - EEPROM

- **Ecossistema de serviços:**
  - Conectividade de dados celulares
  - APN privada e segura
  - Ponto de acesso ao serviço
  - Serviço de gerenciamento OTA de modem celular
  - Serviço de gerenciamento OTA do cartão SIM

Depois de marcar as informações relevantes para cada tecnologia, a equipe revisa a seção “Modelo” de cada documento das Diretrizes e identifica o modelo tecnológico apropriado. Este endpoint é considerado de alta complexidade. O modelo de Serviço e Rede é um serviço IoT habilitado para dispositivos móveis padrão.

B.2 Revise o modelo de segurança

Com um modelo técnico delineado, a organização deve estar pronta para avançar com a revisão do modelo de segurança. No modelo de segurança, a equipe vai avaliar como um hacker provavelmente atacaria a solução.

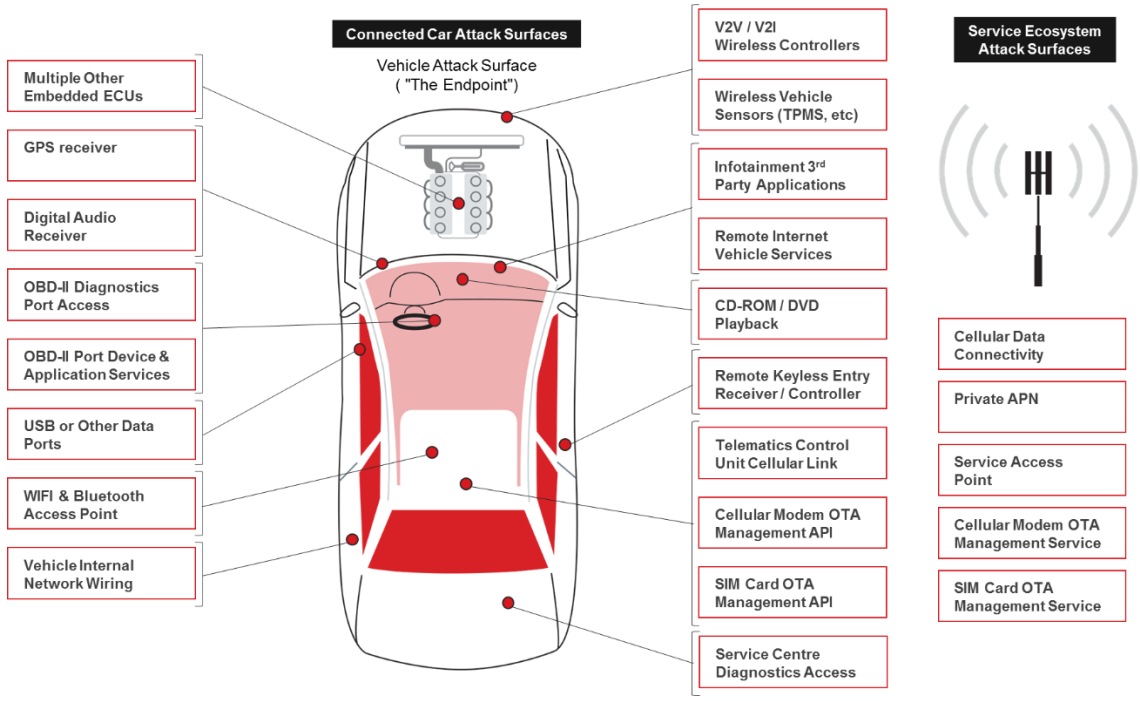

Figura 11 – Avenidas de ataque em um carro conectado

Na nossa solução de exemplo, existem apenas duas avenidas de ameaça que são relevantes para um ataque:

- A rede celular
- Um ataque localizado no veículo

Uma vez que não existe uma conexão de rede local, apenas uma conexão de rede móvel, um hacker teria que comprometer a conexão de rede celular, entrar no canal de comunicação da APN privada ou entrar por meio do Ponto de Acesso ao Serviço, do servidor de gerenciamento OTA do modem celular ou do Servidor de Gerenciamento de cartão SIM OTA.

Os ataques físicos são a única maneira de comprometer o dispositivo, que possui múltiplos pontos de entrada, como mostrado no diagrama acima, então, no caso desse serviço de IoT, o endpoint deve ser um importante foco.

B.3 Revise e atribua tarefas de segurança

Com o modelo de segurança avaliado, agora é mais fácil atribuir Tarefas de Segurança. Cada equipe deve designar uma pessoa específica para cada Componente da solução que precisa ser avaliado. Isso deve ser avaliado não apenas a partir da perspectiva de alto nível (endpoint, rede e serviço), mas a partir da perspectiva do subcomponente. Isso significa designar uma pessoa para a CPU, outra para o sistema operacional, outra para o serviço de rede e assim por diante.

Uma vez que cada Componente é atribuído a um responsável, o processo pode começar. Isso significa que, nesta fase, a equipe entende:

- Como a tecnologia é composta
- Quais tecnologias afetam a segurança
- Quais partes interessadas da engenharia possuem a tecnologia fornecida

B.4 Revise as recomendações

Na fase de revisão da recomendação, cada membro da equipe deve ler e entender o maior número possível de recomendações. Isto é feito by design. Em vez de se concentrar unicamente nas recomendações afixadas em um Componente específico, os engenheiros devem empregar seu tempo para entender quantas recomendações forem capazes, mesmo que apenas por alto, para obter uma visão melhor de como seu Componente afeta a segurança geral do produto ou serviço. Desta forma, o grupo pode se envolver em uma valiosa discussão sobre quais estratégias de remediação ou mitigação terão o maior equilíbrio de uma perspectiva de custo-benefício, longevidade e gerenciamento.

Uma vez que as recomendações estejam revisadas, os responsáveis por cada Componente podem determinar se uma recomendação já foi aplicada ou indicar uma recomendação pendente. Isso permitirá que o grupo tenha uma discussão sobre a aplicabilidade de uma recomendação antes da sua implantação. Esta é uma estratégia melhor a seguir, já que algumas recomendações podem ter efeitos colaterais que afetam o cumprimento de outras recomendações ou controles existentes.

Neste exemplo, a equipe teria determinado que:

- Uma base de confiança de aplicativo deve ser usada
- Uma Raiz Organizacional de Confiança deve ser definida
- A personalização do dispositivo deve ser implementada
- Case resistente à adulteração deve ser implementado
- Gerenciamento de senha do endpoint deve ser implementado
- A segurança das comunicações do endpoint deve ser aplicada
- Imagens assinadas criptograficamente devem ser implementadas
- Gerenciamento de privacidade deve ser implementado
- Alertas de energia do dispositivo devem ser integrados

B.5 Revise o risco do componente

Em seguida, a seção “Componentes” deve ser avaliada para identificar os vários riscos envolvidos na implementação ou integração de um Componente específico no produto ou serviço. Esta seção geralmente pode ser revisada apenas pelo responsável pelo Componente para minimizar o trabalho. No entanto, é sempre benéfico ler o máximo possível.

Após revisar as Recomendações e a seção de risco de Componente, foram identificadas as seguintes lacunas na segurança:

- Os segredos foram armazenados sem proteção na EEPROM
- Os segredos não foram processados na RAM interna
- A interface do usuário deve proteger as senhas
- A privacidade do usuário deve ser descrita para o usuário

B.6 Implementação e revisão

Agora, a equipe pode ajustar a solução para aderir aos requisitos de segurança previamente acordados. A equipe implementa novamente os componentes, onde necessário, e adiciona controles de segurança, onde necessário.

Nessa instância particular, a equipe identificou que eles estão trabalhando com um membro da GSMA que é capaz de fornecer um cartão SIM com tecnologia de âncora de confiança capaz de usar aplicativos. Eles resolverão sua necessidade de uma âncora de confiança usando o cartão SIM existente. Isso também resolve a personalização, pois cada SIM pode ser personalizado no campo usando a tecnologia GSMA padrão.

A tecnologia SIM também pode ajudar a fornecer chaves de segurança de comunicação over the air, resolvendo a necessidade de implementar autenticação e privacidade de comunicações.

A zona de SIM de determinada empresa pode ser programada com uma base de raiz confiável que permite à empresa autenticar pares usando uma cadeia de certificados. Isso resolve os requisitos da raiz organizacional de confiança e de autenticação de pares.

A embalagem do produto é atualizada com uma embalagem apropriada resistente à adulteração.

A EEPROM é codificada com dados criptografados com chaves de segurança armazenadas na âncora de confiança do SIM.

O carregador de inicialização é alterado para usar a âncora de confiança para a autenticação da imagem da aplicação.

O endpoint é reprogramado para suportar a entrada de senha segura do usuário ao bloquear os caracteres da senha à medida em que eles são digitados.

Uma GUI de gerenciamento de privacidade é adicionada para que o usuário possa visualizar e controlar quais informações estão sendo coletadas pelo negócio.

Os segredos são processados apenas na memória interna do mesmo chip.

Uma vez que essas implementações são definidas, a equipe reavalia todas as Recomendações e Riscos de segurança e analisa o Modelo de Segurança para identificar se as mudanças resolvem suas preocupações.

B.7 Ciclo de vida contínuo

Agora que a equipe conquistou uma configuração aprovada, está pronta para implantar sua tecnologia. No entanto, a segurança não para aqui. A equipe deve negociar uma metodologia para monitorar anomalias de segurança em endpoints e uma metodologia para identificar se a tecnologia usada contém lacunas na segurança recentemente descobertas.

A equipe deve planejar como cada incidente ou lacuna será identificado, resolvido e recuperado. Isso garantirá que, ao longo do tempo, a evolução do panorama tecnológico e de segurança não pegará a organização de surpresa.

Anexo C Gerenciamento de documento

C.1 Histórico do documento

Versão	Data	Breve Descrição da Mudança	Responsável pela aprovação	Editor / Empresa
1.0	08-Fev-2016	Novo PRD CLP.11	PSMC	Ian Smith GSMA & Don A. Bailey Lab Mouse Security
1.1	07-Nov-2016	Adicionadas referências ao esquema de avaliação de segurança em IoT da GSMA. Correções editoriais menores.	PSMC	Ian Smith GSMA
2.0	28-Set-2017	Adicionadas informações sobre rede LPWA ao documento e outras atualizações menores.	Grupo de Segurança em IoT	Rob Childs GSMA

C.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 erros ou omissões, entre em contato conosco com seus comentários. Você pode nos notificar em prd@gsma.com

Seus comentários, sugestões e perguntas são sempre bem-vindos.