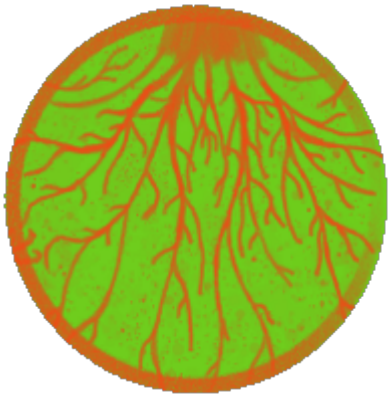
Image not found or type unknown

O que é um telefone? Como as comunicações móveis funcionam? [atividade de aprofundamento]



O objetivo desta atividade é aprofundar o conhecimento de como as comunicações móveis funcionam para apoiar a capacidade do participante de avaliar e planejar os riscos das comunicações móveis. As facilitadoras devem incluí-la em qualquer oficina sobre comunicação móvel ou confirmar que todas as participantes já estão familiarizados com as informações desta atividade. É uma base para poder avaliar os riscos técnicos das comunicações móveis.

Esta atividade tem dois estágios:

- Dissecação mão-na-massa do telefone
- Entrada: dados das comunicações móveis e considerações de risco

Objetivos de aprendizagem aos quais esta atividade responde

- Compreender alguns conceitos básicos de como funcionam as comunicações móveis para nos informarmos sobre os potenciais impactos da utilização das comunicações móveis;

Para quem é esta atividade?

Esta atividade é para qualquer pessoa participando de uma oficina sobre telefonia celular.

Tempo estimado

Esta atividade requer cerca de **45 minutos.**

Recursos necessários para esta atividade

- alguns telefones celulares para abrir e investigar
- um quadro branco, slides ou apresentação

Dinâmica

Mencione ou discuta, dependendo do tempo disponível, que iremos falar sobre comunicações móveis – considerando dispositivos que são facilmente carregados na mão ou bolso e têm capacidades de comunicação desde chamadas de voz e SMS até internet e serviços de dados. Parte dessa sessão se aplica também a *tablets*.

Dentro dos nossos telefones - 5 minutos

Desmonte este telefone. Seu telefone é um pequeno computador. Todas peguem seus celulares e localizem:

- Partes que escutam e projetam sons: microfones, alto-falantes
- Partes que enxergam e mostram imagens: câmeras, telas
- Partes que mandam e recebem informações de outras fontes: GPS, Antena, Wi-fi
- Partes do computador, hardware: bateria, circuitos
- Memória: cartão SD, outra memória embutida no telefone
- *slot(s)* de Cartão SIM

Dispositivo e identidade SIM - 5 minutos

Seu telefone tem todas essas peças e alguns recursos de identificação, além da marca, modelo e sistema operacional, ele tem 2 nomes - um identificador de dispositivo e um identificador de cartão SIM. É importante saber sobre isso porque você pode ser identificado por qualquer um e seu telefone comunica essas informações com frequência, especialmente o IMSI.

- **IMEI** é o nome do seu dispositivo

International Mobile Equipment Identifier (IMEI):
https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity

- **IMSI** é o nome do seu cartão SIM

International Mobile Subscriber Identity (IMSI):
https://pt.wikipedia.org/wiki/International_mobile_subscriber_identity

Nossos telefones se comunicando - 35 minutos

Usamos nossos telefones para nos comunicarmos com as pessoas: SMS, Mensagens, Redes Sociais, Apps, Chamadas. Nossos celulares também comunicam informações sobre nossos telefones e sobre nós mesmas - não apenas nossas mensagens, mas metadados, nossa localização, etc., e isso pode ser vinculado a outras informações sobre nós, como nossas redes sociais, nossas redes de organização, nossos hábitos e locais de trabalho.

É bom estar ciente disso, principalmente para que possamos entender como o uso de nossos telefones celulares pode atuar como um dispositivo de rastreamento no momento e como um

registro histórico de nossas atividades depois que elas acontecem.

1. Seu telefone é tagarela

Seu telefone está chamando diferentes tipos de redes e através de diferentes tipos de comunicação para anunciar que está próximo e para se conectar ou verificar se alguém deseja se conectar.

Operadoras de celular

As operadoras de celular têm torres e antenas com as quais seu telefone se comunica. Cada antena pode cobrir uma área específica. Seu telefone entra em contato com a(s) torre(s) que estiver mais próxima. Ele compartilha **pelo menos seu IMSI** para anunciar qual operadora de celular você está usando e seu número para que você possa receber mensagens, chamadas e comunicações em seu dispositivo. Cada vez que você está perto de uma torre, é como colocar um alfinete em uma linha do tempo mapeada onde você está. Você marca onde está, quando está lá e o que está fazendo naquele local em termos de uso do telefone.

GPS

Se o GPS estiver ativado, o telefone está se comunicando com satélites GPS, fazendo check-in de uma forma parecida, que é marcando com alfinetes em uma linha do tempo mapeada onde você está.

Wi-fi

Se o seu wi-fi estiver ligado, conforme você passa pelas redes wi-fi, seu dispositivo pode tentar se conectar a essas redes, deixando um registro com a rede wi-fi, e também gravar o nome da rede no seu telefone.

Bluetooth / NFC

Se estiverem ativados, outros dispositivos que usam Bluetooth e NFC podem se comunicar com seu dispositivo, tentar se conectar e compartilhar arquivos, etc.

Facilite a discussão: Quais coisas você precisa que estejam ligadas em quais momentos? Os registros de onde você está são um risco para você ou não?

2. Você é tagarela

Nós usamos nossos telefones para nos comunicarmos. Diferentes tipos de comunicação se mostram de forma diferente durante a comunicação e depois que as mensagens foram enviadas.

SMS

Mensagens de texto e metadados - na comunicação, uma vez armazenados no dispositivo e nas operadoras, são enviados em texto não criptografado. Uma analogia útil é que um SMS é como um cartão postal. Se alguém o interceptar, pode ler todo o conteúdo, bem como metadados (ex.: remetente, destinatário, hora, data).

MMS

Mensagens de mídia e metadados - na comunicação, podem ou não serem criptografadas, portanto, se alguém estiver tentando interceptar suas comunicações, varia se será possível vê-las. Depois de enviadas, você e os provedores e dispositivos móveis do seu destinatário têm um registro da mensagem e, portanto, a investigação sobre qualquer um deles pode revelar metadados (ex.: remetente, destinatário, hora, data) e conteúdo.

Chamadas

Conteúdo e metadados da chamada - da mesma forma - as chamadas devem ser criptografadas conforme estão em andamento, mas o seu provedor e o provedor do destinatário armazenam metadados sobre a chamada (por exemplo, remetente, destinatário, hora, data) e se o seu oponente tem acesso aos seus provedores, eles podem ter acesso para ouvir chamadas ou gravá-las.

> Para obter mais informações sobre aplicativos e aplicativos de mensagens, consulte: Discussão, interações + mão-na-massa: Escolhendo aplicativos móveis

Uma observação sobre a vigilância de Estado: de país para país, a vigilância de Estado varia. Em alguns lugares, os governos terão acesso a todos e quaisquer dados que as operadoras tenham - então, com eles, você deve considerar que todos os seus metadados e conteúdos de serviços não criptografados são acessíveis aos governos em tempo real e após o fato, se houver um investigação para esses registros.
Sua melhor defesa contra a vigilância é a criptografia de ponta-a-ponta.

3. Um telefone é um pequeno computador

Bug de software - um telefone é um computador e pode ser infectado com malware, assim como um desktop ou laptop. Indivíduos e governos usam software para bugar os dispositivos móveis de outras pessoas. Este tipo de software geralmente usa partes do telefone para funcionar como um bug ou um dispositivo de rastreamento, ouvindo com o microfone ou enviando dados de localização.

4. A nuvem é um gabinete de arquivos

Alguns dados que meu telefone acessa não estão localizados no meu telefone, estão na nuvem. A "nuvem" é apenas um termo que significa "a internet" - dados que estão armazenados fisicamente em algum lugar com um dispositivo conectado à internet. Seus aplicativos podem estar acessando dados que estão na nuvem e não realmente em seu dispositivo.
Considerações: os meus dados estão criptografados no trânsito entre mim e o serviço? São criptografados quando armazenados pelo serviço? Sei de alguma ocasião em que oponentes tenham conseguido obter acesso a essas informações - quando, como?
Nota para a facilitadora: Enquanto você fala, os participantes podem fazer perguntas sobre partes dos telefones ou riscos associados aos métodos de comunicação mencionados. Tome o tempo para responder às perguntas. Se puder, mantenha uma lista contínua de questões e tópicos sobre os quais as pessoas pedem informações adicionais - uma lista contínua em um quadro branco bastará. Além disso, mantenha uma lista contínua de questões e tópicos que você não abordou nesta oficina específica, para que possa aborda-los mais tarde na oficina ou sugerir um acompanhamento após a oficina.

Recursos adicionais

- 7 maneiras de encontrar o número IMEI ou MEID do seu telefone (em inglês): http://www.wikihow.com/Find-the-IMEI-or-MEID-Number-on-a-Mobile-Phone
- International Mobile Equipment Identifier (IMEI) (em inglês): https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity
- International Mobile Subscriber Identity (IMSI)(em inglês): https://en.wikipedia.org/wiki/International_mobile_subscriber_identity

O site My Shadow do Tactical Tech tem várias guias de treinamento excelentes para facilitar o aprendizado sobre tecnologia móvel.

- My Shadow downloadable materials: https://myshadow.org/materials (em inglês)
- My Shadow website: https://myshadow.org/pt



Revision #5

Created 26 April 2023 01:40:24 by Kira

Updated 28 July 2023 15:05:17 by Kira