Pensamento de Segurança

Trabalho 1 - Segurança em Computação (INE5429)

Universidade Federal de Santa Catarina

Pensamento de Segurança

Trabalho 1 - Segurança em Computação (INE5429)

Universidade Federal de Santa Catarina

Felipe de Campos Santos

17200441

23/06/2021

# Sistema

Aplicativos de delivery envolvem uma coleta de várias informações pessoais e/ou sigilosas, e quando paramos para análisar que essas informações não são apenas dos usuários-fim (usuários que pedem a comida), mas também dos intermediários (pessoas que fazem a entrega) e dos contratantes (estabelecimentos que “contratam” o serviço do sistema), percebemos que a base de dados coletados é extremamente abrangente - o que torna ainda mais perigoso um ataque, vazamento ou invasão nesse sistema.

Trataremos então de analisar os âmbitos de segurança de maneira destrinchada tocando em cada um dos tipos de usuários do sistema, com base no que foi visto em aula sobre os principais pontos que um profissional de segurança em computação analisa.

Usaremos como base o aplicativo IFood, porém pode ser extendido à outras plataformas, visto que os ativos, agentes e fraquezas são praticamente as mesmas.

# Ativos

Para se tratar dos ativos, é importante antes definir os três tipos de usuários que tem ativos inseridos no sistema:

* Usuário-fim: pessoa que fez o pedido do produto usando o app;
* Intermediário: pessoa responsável pela retirada do produto na contratante e entrega do mesmo para a pessoa usuário-fim (entregador ou entregadora);
* Contratante: estabelecimento que vende o produto

Com as definições acima feitas, podemos analisar mais detalhadamente os males que um ataque aos ativos dos usuários poderiam causar, diferenciando também os ativos que estão presentes no sistema de cada usuário.

Para o usuário-fim, temos a lista de ativos que usaremos como base para análises ao longo do trabalho, já que o número de usuários-fim cadastrados é maior que o numero de contratantes e intermediários.

Estes tem informações pessoais (nome completo e CPF), dados de contato (email e telefone), dados de endereço e dados bancários cadastrados no sistema e vinculados à conta, além do histórico de compras e conversas mantido no aplicativo (podendo mostrar outros endereços que o usuário frequenta, por exemplo) e da ‘carteira’ que a pessoa pode manter também dentro do aplicativo, funcionando como um banco para uso exclusivo de compras no sistema.

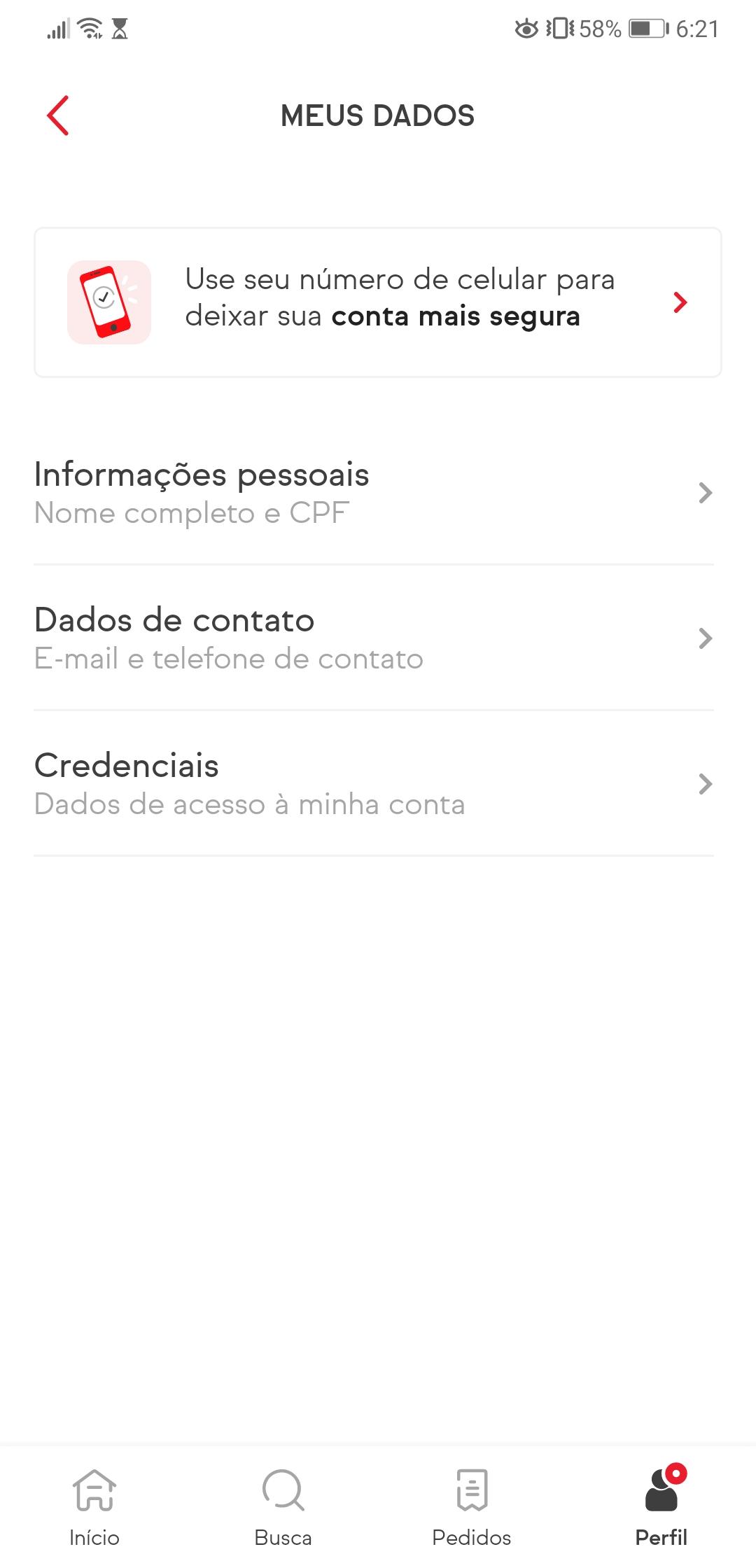


Imagem da página de dados do aplicativo “IFood” (fonte: autor)

Para os próximos dois tipos de usuários, foi necessário conversar com duas pessoas que sabiam me informar melhor sobre os dados: um dono de um estabelecimento que usa o sistema (contratante) e um entregador do sistema (intermediário).

Para o intermediário, temos também os dados pessoais, de contato e dados bancários, além do acesso em tempo real da localização do mesmo e da conta “IFood banking”, por onde o intermediário é pago por suas entregas e pode fazer a retirada (transferência) apenas de 7 em 7 dias, ou seja, existe um período que o dinheiro do intermediário fica no app “congelado”.

Já para o contratante, temos os dados do estabelecimento (endereço, CNPJ), dados dos produtos a venda e a conta “IFood Banking”, funcionando como explicado acima também.

# Adversários

Adversários são aqueles que tem algum interesse em ter acesso ou se apropriar de algum dos ativos citados acima. Para podermos detalhar nossa análise, trataremos de dois grupos de adversários, os ocultos e os expostos.

Os adversários ocultos, em nossa análise, serão os “hackers” (termo escolhido para simplificar o entendimento), pessoas que trabalham para ter acesso ou se apropriarem de informações de maneira online e indevida, sem “se mostrarem” [[1](https://g1.globo.com/economia/tecnologia/noticia/uber-avisa-brasileiros-que-tiveram-dados-roubados-em-ataque-que-vazou-informacoes-de-57-milhoes-no-mundo.ghtml)] [[8](https://olhardigital.com.br/2020/08/07/noticias/dados-de-usuarios-do-uber-eats-vazam-na-dark-web/)]. Esses adversários tem como principal alvo os dados de cartão de crédito, visto que para poder utilizar o cartão no sistema, é necessária a validação do número do cartão junto ao código CCV. O adversário, tendo acesso à esses dados em conjunto com os dados pessoais (nome completo e CPF), poderia utilizar o cartão dentro ou fora do sistema como quisesse, até que a pessoa dona do cartão percebesse e tomasse uma atitude.

Já os adversários expostos são aqueles que realizam seu “golpe” no mundo real, como por exemplo os casos relatados de “golpedo entregador”, onde o adversário é tambem um *intermediário* do sistema. O golpe consiste em o intermediário realizar a cobrança de uma “taxa” indevida do usuário-fim [[2](https://www.cnnbrasil.com.br/business/2021/06/24/golpe-do-delivery-cresceu-186-neste-ano-veja-como-se-proteger)], assim roubando ele, ou então casos onde o intermediário ameaça o usuário-fim na hora da entrega e cobra uma transferência externa de valores monetários [[3](https://g1.globo.com/economia/tecnologia/noticia/2020/04/25/usuario-diz-que-sofreu-golpe-de-r-6-mil-de-entregador-de-comida-procon-notifica-empresas.ghtml)]. Também há a possibilidade de uma pessoa externa ao sistema se passar por intermediário para poder assaltar o usuário-fim [[4](https://www1.folha.uol.com.br/cotidiano/2019/03/motoqueiros-se-passam-por-entregadores-de-aplicativos-para-assaltar.shtml)].

# Gerenciamento de risco

Lendo as notícias (que inclusive são recentes) percebemos que existem diversas fraquezas no sistema. O que é preocupante é que a maioria delas não é uma fraqueza à ataques, ou seja, não depende de pessoas externas explorarem ela, pois a própria empresa dona da plataforma “causa” os problemas, como por exemplo no caso da IFood que, por um erro no aplicativo, expôs os dados de milhares de usuários à outros usuários da plataforma [[5](https://www.uol.com.br/tilt/noticias/redacao/2020/06/19/usuarios-do-ifood-relatam-surgimento-de-dados-de-outras-contas.htm)] - só esperando alguem se aproveitar da situação - o que nos indica uma coisa muito importante: se os dados podem ser expostos assim por um simples erro vindo de dentro da plataforma, quão seguros eles realmente estão? A que nível poderia chegar uma ameaça vinda de um atacante externo?

Como já foi abordado, a plataforma guarda uma informação que qualquer pessoa tem medo que “vaze”, que são os dados do cartão de crédito. Nos casos que foram documentados, os usuários não podiam - ou não falaram se conseguiram - usar os dados do cartão exposto para fazer compras indevidas dentro da plataforma. Mas será que numa próxima também vai ser assim? Ou será que na próxima, a plataforma vai ter sucesso em esconder o vazamento? [[6](https://www.istoedinheiro.com.br/uber-pagara-us-148-milhoes-por-vazamento-de-dados/)]

Tais ataques podem ter custos altissimos para a empresa, vindos desde custos de prevenção para ataques futuros, custo de reforço da segurança que, teoricamente, já existe, ou até o custo de processos advindos dos vazamentos [[7](https://tecnoblog.net/429320/ifood-e-condenado-a-indenizar-em-12-mil-por-golpe-de-entregador/)], e cada vez mais e mais - com o aumento dos usuários das plataformas e, consequentemente, aumento do volume de dados - o valor montante desses dados aumenta.

E como comentado acima, o maior problema pode nem ser ataques externos aos ativos, e sim falhas internas do aplicativo. Considerando que tais falhas tem tanto potêncial de desastre quanto ataques, a probabilidade de um ‘ataque’ bem sucedido é alta, porque pessoas mal intencionadas podem apenas se aproveitar das falhas ao invés de realmente atacar a plataforma. Até porque se a própria empresa “deixou esses dados a disposição” de qualquer usuário, utilizar eles de maneira indevida poderia ser considerado um ataque?

# Contra medidas

Depois dessa rajadade notícias ruins, aqui temos um ponto positivo: existem formas secundárias de se reforçar a segurança dessas plataformas, principalmente com maneiras não-técnicas.

Recentemente tenho visto diversos “avisos” dentro dos apps dessas plataformas, que reforçam ao usuário que parte da segurança dela também é responsabilidade dele, como por exemplo “lembre-se de checar a placa do entregador” e detalhes sobre o veículo que ele está usando (modelo, cor, etc), ou até mesmo sobre confirmação do nome da pessoa intermediária quando ela chega para entregar. Essas maneiras podem ser consideradas de custo-zero para a plataforma, pois são apenas algumas linhas de texto e *push notifications* inseridas.

Ou então maneiras técnicas, como a requisição de um código aleatório gerado no celular do usuário-fim, que o intermediário tem que digitar no dispositivo dele para poder finalizar a entrega, garantindo assim que o usuário realmente é quem comprou e o intermediário - ao pedir o código - também confirma para o usuário que ele é de fato a pessoa responsável pela entrega.

# Custo x Benefício

Para se tratar do custo x benefício das ações preventivas citadas acima, é preciso ressaltar que a receita de tais plataformas advém quase que inteiramente dos usuários-fim, seja de forma direta, com eles comprando produtos dentro da plataforma, ou indireta, já que sem usuários-fim as contratantes saem da plataforma e deixam de pagar taxas.

Então nossa análise pode ser resumida a: até que ponto o aumento da segurança, e consequentemente da complexidade, faria os usuários se sentirem mais seguros e ainda assim usarem a plataforma?

Como já abordado, existem alternativas sendo implementadas que tem custo-zero e conseguem aumentar a segurança, porém essas alternativas dependem quase que exclusivamente da colaboração e atenção do usuário, são passivas,e podem ser consideradas alternativas paliativas e fracas.

Outras alternativas técnicas são a inserção do pedido do código aleatório gerado no dispositivo do usuário-fim, com o intuito também de prevenir que uma pessoa pegue um produto que não é dela.

Mas se tratando da segurança dos ativos dentro do sistema (informações), e considerando os custos que as empresas tem quando acontecem vazamentos de dados [[6](https://www.istoedinheiro.com.br/uber-pagara-us-148-milhoes-por-vazamento-de-dados/)]o benefício de se ter uma plataforma mais segura com certeza pagaria o valor necessário para se aumentar essa segurança. Não apenas o dinheiro “economizado” em processos, mas também porque o volume de usuários e de uso da plataforma seria maior que o de uma outra plataforma menos segura, inclusive acredito que muitos usuários pagariam um valor ligeiramente mais alto se tivessem uma confirmação de segurança maior.

# Referências

[1] G1. **Uber avisa brasileiros que tiveram dados roubados em ataque que atingiu 57 milhões no mundo**. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/uber-avisa-brasileiros-que-tiveram-dados-roubados-em-ataque-que-vazou-informacoes-de-57-milhoes-no-mundo.ghtml>

[2] WESLEY SANTANA. **'Golpe do delivery' cresceu 186% neste ano; veja como se proteger**. Disponível em: <https://www.cnnbrasil.com.br/business/2021/06/24/golpe-do-delivery-cresceu-186-neste-ano-veja-como-se-proteger>

[3] **Golpe da falsa taxa extra em app de comida dá prejuízo de R$ 6 mil a cliente; Procon notifica empresas**. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2020/04/25/usuario-diz-que-sofreu-golpe-de-r-6-mil-de-entregador-de-comida-procon-notifica-empresas.ghtml>

[4] FOLHA. **Bandidos de moto se passam por entregadores de aplicativos para assaltar**. Disponível em: <https://www1.folha.uol.com.br/cotidiano/2019/03/motoqueiros-se-passam-por-entregadores-de-aplicativos-para-assaltar.shtml>

[5] UOL. **Falha de segurança do iFood bagunça pedidos e expõe dados; entenda**. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/06/19/usuarios-do-ifood-relatam-surgimento-de-dados-de-outras-contas.htm>

[6] REDAÇÃO, D. **Uber pagará US$ 148 milhões por vazamento de dados**. Disponível em: <https://www.istoedinheiro.com.br/uber-pagara-us-148-milhoes-por-vazamento-de-dados/>

[7] SILVA, V. H. et al. **iFood é condenado a indenizar em R$ 12 mil por golpe de entregador**. Disponível em: <https://tecnoblog.net/429320/ifood-e-condenado-a-indenizar-em-12-mil-por-golpe-de-entregador/>

[8] OLHAR DIGITAL. **Dados de usuários do Uber Eats vazam na dark web**. Disponível em: <https://olhardigital.com.br/2020/08/07/noticias/dados-de-usuarios-do-uber-eats-vazam-na-dark-web/>