Leonardo Schlüter Leite

SEGURANÇA EM COMPUTAÇÃO: TRABALHO INDIVIDUAL 1

Florianópolis

2019

SUMÁRIO

1 PASSE RÁPIDO

O Passe Rápido é o atual sistema de crédito para o Sistema Integrado de Mobilidade(SIM) de Florianópolis. O objetivo do cartão é substituir a venda de crédito através do papel. O primeiro ativo é justamente o valor das passagens pagas pelos usuários, já que são uma parte importante do lucro. Esse ativo é dividido em alguns sistemas diferentes, em resumo: o sistema de recarga; o sistema que mantém o banco de dados dos usuários; o sistema de cobrança(catracas). Existem vários outros ativos, mas por hora vamos descrever melhor os 3 supracitados.

Descrever qual o sistema escolhido

2 ATIVOS

O primeiro sistema, o de recarga, é um sistema complexo e que envolve fatores humanos. Sua complexidade vem da necessidade de atender uma população consideravelmente grande. Para termos uma ideia,o Consórcio Fênix (consórcio de empresas que recebeu a licitação) transporta aproximadamente 5,5 milhões de passageiros(podendo ser repetido) num mês. Outro fator de complexidade do sistema advém dos diferentes tipos de cartão e seus respectivos significados. Por exemplo: o cartão de estudante requer que o usuário apresente o atestado de matrícula para um funcionário, assim comprovando a ocupação do usuário e possibilitando a recarga.

Outro sistema é o que mantém os dados dos cartões dos usuários. Esse sistema mantém informações pessoais dos usuários, ou seja, informações sensíveis que devem ser protegidas. Por exemplo, quando você recebe o cartão de vale transporte da empresa, esse cartão tem um perfil relacionado no banco de dados e esse perfil contém informações como CPF, um identificador da empresa responsável, endereço do usuário e etc. Além disso, esse sistema também contém registros de todas as transações realizadas. Esses registros podem ser alterados de duas formas para beneficiar duas partes diferentes. Por exemplo, um usuário que possa vir ter acesso ao sistema, pode alterar/inserir registros para benefício próprio ou de terceiros.Um segundo exemplo seria que funcionários do próprio consórcio podem apagar transações, dessa forma escondendo dinheiro que entrou no consórcio e podem dessa forma, cometer desvios de dinheiro. Portanto, essa informação é importante pois se tivermos que auditar os gastos e lucros do Consórcio, teremos comos.

Por último, mas não menos importante, temos o sistema de catracas dos ônibus e dos terminais. Esse sistema tem uma sequência bem estabelecida de tarefas: receber um identificador do cartão; se comunicar com o banco de dados e realizar o desconto dos créditos, se houver; receber a resposta do banco e apresentar para o usuário seu novo saldo. Esse sistema é importante para o lucro do Consórcio pois ele que controla quem entra no terminal e tenta garantir que quem entrou, não entrou de graça ou de forma indevida.

3 ADVERSÁRIOS

Mostrando alguns dos ativos, algumas possíveis fraquezas já se apresentam para uma possível exploração. Porém, vamos nos perguntar primeiro quem pode ser um adversário ? Ou seja, quem ganha algo em explorar essas possíveis fraquezas. Basicamente, pessoas que queiram andar gratuitamente utilizando o SIM é o nosso grande adversário. Podemos citar outros possíveis adversários, como: alguém que queira acessar os dados pessoais dos usuários e utilizá-los para benefício próprio ou de terceiros; alguém que queira desviar dinheiro dos lucros da empresa para uma conta própria ou de terceiros.

O adversário com uma boa probabilidade de se tornar um real atacante é aquele que quer utilizar o serviço gratuitamente. A pergunta agora é, qual ativo ele pode atacar para atingir seu objetivo ? Como citado anteriormente, temos um sistema de cobrança das passagens dos cartões, ou seja, as catracas. Uma forma de atacar esse sistema é roubando o cartão de alguém que contenha créditos e usar. Se for um cartão especial ou de estudante(cartões intransferíveis), por exemplo, à empresa sofreria certos danos, como perda de lucro já que a tarifa desses cartões é menor que a padrão. Porém, se for outro tipo de cartão transferível, para o Consórcio não fará diferença, em termos financeiros.

Outra forma que esse mesmo adversário pode atacar é utilizar alguma fraqueza da tecnologia empregada, os smart-cards(CC). Os CCs são cartões de plástico com um circuito integrado embutido. Este cartão utiliza a tecnologia NFC para se comunicar com um dispositivo à fim de realizar o serviço de acesso da catraca. Desta forma, o cartão serve de RFID tag. Uma das forças dessa tecnologia é que seu alcance de comunicação é de apenas 20 centímetros. Isso restringe os possíveis tipos de ataque, porém ainda é possível realizar alguns tipos de ataques, como: observar a comunicação entre o "reader"e o cartão; fazer a modificação de dados enviados; podemos atacar fraquezas conhecidas dos protocolos de comunicação.

4 GERENCIAMENTO DE RISCO

Desta forma parece que o sistema é muito vulnerável, mesmo explorando poucos aspectos. Porém, antes de sairmos atirando para todos os lados, temos que verificar qual a probabilidade ou qual os reais ganhos de um atacante. Por exemplo, no caso de um atacante roubar algum cartão intransferível. Este atacante precisa assaltar alguma pessoa que possua tal cartão, precisa conseguir lidar com as consequências e sair ileso para só depois utilizar o cartão. E ainda assim, o prejuízo para a empresa não seria comparável às possíveis perdas do atacante.

Agora, vamos analisar o risco de termos o sistema de catracas atacado por uma fraqueza tecnológica. Vamos supor que um atacante possa ter conhecimento técnico, dinheiro e tempo para desenvolver um sistema móvel que seja capaz de atacar o "reader"do RFID tag. Em primeiro lugar, a probabilidade de tal suposição já é baixa por si só, o que já diminui a prioridade de nos defendermos contra tal ataque. Porém, caso aconteça, para uma rede de 5 milhões de passagens consumidas em um mês, esse prejuízo não é muito grande. Podemos visualizar isso se pensarmos que tenham 10 atacantes que utilizam o transporte coletivo três vezes ao dia, isso gera uma perda de 900 passagens no mês. Portanto, esse tipo de ataque, ainda que seja um grande desafio tecnológico para defendermos, é de uma certa forma de baixa prioridade.

Outro possível ponto a ser explorado pelo atacante, é o sistema de recargas. Com uma breve reflexão podemos pensar em duas fraquezas: uma física e outra tecnológica. A fraqueza física é referente aos funcionários. Eles podem recarregar cartões sem cobrar o total de créditos que está sendo depositado no cartão, ou eles podem recarregar cartões com tarifas diferenciadas sem cobrar os devidos documentos necessários. Dessa forma, a perda de lucro pode ser considerável. E a probabilidade de isso acontecer, dependendo da segurança do sistema, pode ser consideravelmente grande. A Segunda fraqueza, que é de natureza tecnológica, é o sistema e seu funcionamento. Mas esse tipo de fraqueza cai no mesmo enredo da fraqueza tecnológica dos cartões. Porém, o grande diferencial é, se um atacante conseguir burlar o sistema e criar créditos em cartões como queira, esse atacante pode vender os créditos de forma mais barata gerando lucro para si. Dependendo do tamanho do ataque, o prejuízo da empresa pode ser considerável, ou até mesmo desastroso. Portanto, é vantajoso para a empresa mitigar esse risco.

5 CONTRA-MEDIDAS

Como vimos, apesar de várias fraquezas, nem todas são recompensadoras para o atacante. Porém, mesmo as que não são de grande impacto, deveriam ser resolvidas. Vamos primeiro falar do que a empresa parece fazer para se defender, isto da perspectiva de fora. O primeiro exemplo é o risco de alguém desenvolver algum tipo de dispositivo que ao se aproximar do leitor do RFID tag libera a catraca. Primeira contra medida contra ataques ao leitor é o fato da presença do cobrador, que pode e deve ser instruído a observar movimentos suspeitos e negar a passagem do suspeito pela catraca.

Outra contra medida, executada também pelo cobrador, é que existe um botão ao alcance apenas do cobrador que precisa ser pressionado para que o leitor aceite uma nova requisição. Então caso o cobrador veja um dispositivo estranho ou algo diferente do cartão sendo aproximado do leitor, basta o cobrador não apertar este botão e manter a catraca travada. Uma terceira contra medida é da natureza tecnológica, esta provavelmente não é implementada pela empresa. É possível modificar o tempo que o leitor aguarda a resposta do cartão. Por exemplo, se o tempo atual for grande o suficiente para que algum dispositivo execute seu algoritmo quebrando o leitor, podemos diminuir a janela de tempo e dessa forma mitigando o risco por pura falta de processamento do dispositivo do atacante. Sobre as fraquezas do sistema de recargas, temos algumas medidas já tomadas e observáveis. A respeito da fraqueza física, o sistema quando termina de fazer a recarga, imprime um comprovante. Neste comprovante existe um identificador de quem recebeu e de quem executou a recarga. Por isso, podemos deduzir que o sistema guarda informação do funcionário logado no sistema na hora da recarga. Porém, podemos supor que um funcionário deixe seu perfil logado no sistema durante a troca de turnos. Desta forma um segundo funcionário poderia usar o perfil do primeiro para efetuar recargas ilícitas e que, teoricamente, não seriam ligadas ao segundo funcionário. Contudo, em todos os guichê de recargas existe um sistema de Closed-Circuit Television (CCTV), desta forma permitindo que o correto culpado seja identificado.

6 CUSTO/BENEFÍCIO

Sobre custo/benefício das contramedidas comentadas temos um baixo custo e um resultado satisfatório. No caso da fraqueza tecnológica das catracas, o maior custo será treinar os cobradores para identificar possíveis dispositivos maléficos ao leitor dos cartões. Porém, a empresa já contém cobradores e já é implementado o sistema de bloqueio de catracas. Mesmo com esse único custo, é difícil dizer se vale a pena, pois a probabilidade de termos esta fraqueza tecnológica explorada é consideravelmente baixa e o prejuízo seria baixo. Entretanto, existe a possibilidade desse dispositivo do atacante ser replicado em grande quantidade e vendido à outros usuários do sistema, se caso isso acontecer. O custo da contramedida seria baixo perto do prejuízo, assim valendo a pena ministrar um curso aos cobradores.

Agora sobre a contramedida tecnológica da fraqueza tecnológica do sistema de catraca, podemos deduzir e supor algumas coisas. A primeira dedução é que o custo de realizar a alteração da janela de tempo dos leitores seria um tanto quanto cara, pois existem "450 veículos no transporte convencional e 80 no Executivo"(Consórcio Fênix). Essa contramedida só valeria a pena para a empresa se, como suposto antes, o atacante reproduzisse o seu dispositivo, vendesse ilegalmente para vários passageiros diários e esse dispositivo não pudesse ser identificado facilmente apenas com o curso oferecido aos cobradores. Portanto, podemos dizer que o custo benefício dessa contramedida, nos estados atuais, não compensa.

Por último, outra contra medida comentada é referente a fraqueza física comentada do sistema de recarga. Esta contra medida é sem custo, visto que os terminais já são instalados com CCTV e que o sistema mantém o perfil do funcionário ligado à transação. Desta forma, basta manter algum funcionário, ou setor da empresa, para analisar os dados para verificar uma possível fraude periodicamente. Assim, o custo da solução é barato se pensarmos em toda a estrutura já posta e o possível prejuízo(que depende das intenções do funcionário fraudulento.)

7 REFERÊNCIAS

https://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/#gref

http://www.consorciofenix.com.br/