Lucas Fonseca 221150154

https://drive.google.com/file/d/1JKCxz9wUpHUOw\_v\_DLcyKds2B4-xC2RP/view?usp=sharing

O EMV Preplay Attack se define pela estratégia de reenviar dados de uma transação já realizada e gravada de um cartão alvo. Esses dados ficam gravados em um cartão falso que simula um cartão EMV que consegue enganar o detector de fraude dos caixas eletrônicos e dos pontos de venda, e é através desse cartão que os ataques são posteriormente simulados, os transgressor podem também realizar esse ataque sem o uso de cartão, através da inserção dos dados via PIN e utilizando um cartão magnético. Este ataque pode ocorrer de diversas formas, se aproveitando dos RNGs (random number generator) fracos para falsificar ou adulterar transações, utilizar um dispositivo man-in-the-middle para interceptar a comunicação entre os caixa eletrônico (ATM)/maquininhas de cartões (POS) e o banco, algum desses terminais infectados por um malware ou até mesmo através de vendedores mal-intencionados com esse tipo de ataques.

**RNGs fraco**

Quando um ATM ou POS possui um RNGs fraco, tornando-o previsível, além desta falha uma especificação do EMV requer que apenas quatro números aleatórios (UNs) consecutivos sejam únicos, fazendo com que o quinto número gerado possa ser idêntico ao primeiro número. Por conta dessas vulnerabilidades invasores podem se aproveitar para realizar o preplay attack. Para começar o ataque o transgressor escolhe uma ATM que irá realizar o ataque e coleta uma lista de UNs gerados pelo terminal, depois ele utiliza um POS ou uma ATM para enviar essa lista gerada para o cartão da vítima, a fim de receber os ARQC (chave de autorização criptografada enviada pelo cartão para cada transação) do cartão para aqueles UNs. Agora com essa lista de ARQCs, o infrator volta para o ATM de onde extraiu os UNs e simula transações até que o caixa envie um UN para o qual ele tenha o ARQC, quando isso ocorre ele envia o ARQC da vítima e consegue realizar a transação que desejar.

**Vendedores mal-intencionados**

Os vendedores podem modificar suas POS para que elas sejam vulneráveis ou para que injetem dados de outros cartões no sistema de autorização. Com isso eles conseguem clonar o cartão das vítimas ou executar um preplay attack, com os dados roubados pela máquina.

**Ataque com malware**

Os ataques com malware ocorrem quando um infrator utiliza um cartão falso, como descrito anteriormente, para contaminar com um malware caixas eletrônicos e pontos de vendas, e dependendo da arquitetura interna do dispositivo esse malware consegue interferir com a geração dos números aleatórios, tornando eles previsíveis ou até mesmo permitindo que o transgressor saiba qual número será gerado.

**Man-in-the-middle**

Outra forma de realizar o ataque é com um dispositivo man-in-the-middle, entre ATM ou o POS e o banco. Para isso o transgressor escolhe um UN de forma arbitrária, e envia esse UNs para o cartão da vítima através de um ATM ou POS adulterado, assim conseguindo o ARQC do cartão para aquele UN. Em seguida ele iniciará uma transação em um ATM normalmente e enviará o ARQC coletado da vítima, e quando o terminal enviar os dados para o banco, o transgressor irá interromper a comunicação e substituir o UN gerado pelo terminal pelo UN escolhido por ele. Assim a transação passará como válida.

**Formas de se proteger**

Uma das formas de se proteger deste ataque é possuir um RNG que gere números criptografados seguros, e a outra forma de se proteger é verificando o certificado da transação, que é uma autenticação que é emitida pelo cartão para o terminal quando a transação é finalizada com sucesso, pois embora um preplay attack possa possuir um certificado de transação, os dados de aplicativo do emissor irá mostrar que a autenticação do emissor não foi concluída.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| # | Ameaça | STRIDE | Damage potencial | Reproducibility | Exploitability | Affected users | Discoverbility | Risco |
| 1 | Vendedores mal-intencionados | STI | 9 | 8 | 4 | 9 | 10 | 8,2 |
| 2 | Usar o gerador de RNG fraco para autenticar transações falsas | SI | 8 | 3 | 4 | 5 | 10 | 6 |
| 3 | interceptar a comunicação do ATM/POS com o banco através de um man-in-the-middle | STI | 10 | 8 | 9 | 10 | 10 | 9,4 |

