Universidade do Minho

Mestrado em Engenharia Informática

Engenharia de segurança

Prática 2 - PA

Grupo 1

Rui Carlos Azevedo Carvalho - PG47633
Daniel Barbosa Miranda - PG47123
Ana Luísa Lira Tomé Carneiro - PG46983

Introdução

Existem vários serviços que utilizam *one-time passwords* (OTP), seja para efetuar autenticação de uma conta, *reset* de *password* ou para permitir algum tipo de transação relacionado com um serviço *online*. Neste método, o serviço *online* envia ao utilizador um SMS com um código temporário (OTP) que será utilizado para autenticar o utilizador no serviço e para que este consiga realizar ações delicadas e privadas, como transações bancárias. [1]

Desta forma, esta tecnologia é um alvo importante para atacantes pois caso se consiga obter estas mensagens OTP torna-se possível obter acesso a contas privadas, efetuar transações bancárias em contas de terceiros, entre outros.

Devido à importância destes ataques, é necessário determinar o potencial de ataque associado ao método de receber OTP através de SMS ou por *push notification*. De modo a se poder analisar este potencial, é necessário verificar e avaliar cenários de ataque e vulnerabilidades que estão a ser exploradas nesses cenários. Para além disso, é também necessário desenvolver uma metodologia que mede, para cada cenário, o tempo gasto para identificar e realizar o ataque, janela de oportunidade, conhecimento do alvo e que tipo de conhecimentos técnicos e programas ou ferramentas é que são necessários para realizar o ataque [2].

Potencial de ataque à tecnologia de OTP

Neste capítulo apresentamos os vários cenários de ataques associados ao método de *one-time password* (OTP) através do envio de um SMS ou *push notification* ao utilizador. Para cada cenário é descrito o seu contexto, as vulnerabilidades associadas ao cenário e a a avaliação da potencialidade do cenário.

SMS

Acesso físico ao dispositivo

Nº 1	Acesso físico ao dispositivo [1]	
Descrição do cenário de ataque	Vulnerabilidade explorada	Potencial de ataque estimado, necessário para efetuar o ataque
Neste primeiro cenário o adverário obtem acesso físico ilegítimo ao disposito da vítima através de um roubo, sendo que, através deste fica a saber o código de acesso ao mesmo o que possibilita o acesso às mensagens que são enviadas por sms para o dispositivo. Posteriormente, este rapidamente tenta aceder às contas da vítima de vários serviços, tais como serviços bancários, redes sociais, entre outros. Como possui acesso ao dispositivo, este consegue realizar o *reset* da *password* de acesso aos serviços que utilizem o método de autenticação OTP por SMS. Desta forma, consegue aceder a informação privada e provocar danos acentuados.	Acesso físico ao dispositivo móvel com acesso ao cartão SIM da vítima. Através deste é capaz de pedir o *reset* da *password* contas que possuam autenticação por OTP e assim obter acesso às contas dos vários serviços utilizados pela vítima.	**Time taken to identify and exploit:** 0 (<= one day) A obtenção do telemóvel da vítima e a exploração das vulnerabilidades associadas ao mesmo pode ser conseguido rápidamente, contudo poderá ser necessário que o atancante dispenda mais tempo a encontrar uma boa altura para conseguir aceder ou roubar o telemóvel da vítima. **Specialist technical expertise required:** 0 (Layman) A obtenção física de um telemóvel não requer nenhum conhecimento técnico especial. **Knowledge of the target's design and operation:** 3 (Restricted) É necessário saber o ćodigo de segurança do dispositivo para poder ter acesso às suas mensagens. **Window of opportunity:** 1 (easy) A execução do furto pode ser feita em poucos minutos e a partir do momento em que possui acesso ao dispositivo o processo de obter acesso às contas da vítima é rápido, apesar deste ataque ser fácilmente detetável. **IT hardware/software or other equipment required for exploitation:** 0 (Standard) Para conseguir explorar a vulnerabilidade basta ter acesso ao telemóvel da vítima, o único dispositivo necessário para que o ataque tenha sucesso. **Total de potencial de ataque estimado: 4 = BASIC**
O segundo cenário vai ao encontro do anterior, sendo que, neste caso quem realiza o ataque não consegue obter acesso aos dados internos do disposito sendo apenas capaz de o destruír, o que impede a vítima de receber códigos OTP.	Através da obtenção do dispositivo e procedendo à sua destruição, o adversário está a provocar um *denial of service*.	**Time taken to identify and exploit:** 0 (<= one day) Como a vulnerabilidade é bastante simples não requer tempo para verificar que ela existe no modo de operação do alvo. Para além disso não é necessário grande esforço para levar a cabo o roubo do dispositivo. **Specialist technical expertise required:** 0 (Layman) A obtenção física de um telemóvel não requer nenhum conhecimento técnico especial. **Knowledge of the target's design and operation:** 0 (Public) Para ter acesso físico ao telemóvel da vítima basta conseguir roubar o dispositivo ao utilizador, não sendo necessário nenhum conhecimento extra em relação à vítima. **Window of opportunity:** 1 (easy) Provocar a destruição do dispositivo é feito em pouco tempo, embora o roubo do mesmo seja facilmente detetado. **IT hardware/software or other equipment required for exploitation:** 0 (Standard) Não é necessário conhecimento ou outro equipamento para destruir o dispositivo. **Total de potencial de ataque estimado: 1 = BASIC**

Risco 1 - Acesso ao dispositivo

Obter um cartão SIM associado ao número da vítima

<table>
<tr><td>Nº 2</td><td colspan="2">Obter um cartão SIM associado ao número da vítima (SIM Swap) [1]</td></tr>
<tr><td>Descrição do cenário de ataque</td><td>Vulnerabilidade explorada</td><td>Potencial de ataque estimado, necessário para efetuar o ataque</td></tr>
<tr><td rowspan="13">Neste cenário o adversário obtém acesso a dados da vítima através de social engineering (phishing, por exemplo) e através de exploração de informação pública apartir, por exemplo, das redes sociais da vítima. Desta forma, o atacante obtém acesso ao número de telemóvel da vítima e contacta a operadora associada a esse número. Através de social engineering, este é capaz de enganar a empresa, alegando que o cartão SIM associado a este número foi destruído, por exemplo, e esta acaba por lhe fornecer um novo cartão SIM associado ao número da vítima.

Através disto, quem está a realizar o ataque é capaz de obter acesso às mensagens que são geradas pelos serviços da vítima que utilizem autenticação por OTP. Assim, o atacante poderá aceder a diversas contas, como e-mails, redes sociais, PayPal, e especialmente plataformas bancárias. Com estes, poderá descobrir através do email que contas é que a vítima possui, poderá aceder a conversas com outras pessoas e possívelmente adquirir dados pessoais da mesma e, acima de tudo, efetuar alterações a nível bancário.</td><td rowspan="13">Neste cenários de ataque a vulnerabilidade explorada refere-se ao uso de técnicas de social engineering, de forma a obter um novo cartão da vítima. Através do contacto com a operadora móvel é possível convencer a operador a fornecer um novo cartão associado ao mesmo número o que leva a que as mensagens com autenticação OTP sejam enviadas também para este novo cartão.</td><td>Time taken to identify and exploit: 0 (<= one day)</td></tr>
<tr><td>O tempo para adquirir as informações básicas necessárias para realizar o ataque poderá ser bastante baixo dependendo do quão públicas forem as informações da vítima em questão, nas redes sociais.</td></tr>
<tr><td>Specialist technical expertise required: 3 (Proficient)</td></tr>
<tr><td>Requer capacidades de Engenharia Social, de modo a adquirir as informações pessoais da vítima e eventualmente efetuar o pedido de um novo cartão SIM.</td></tr>
<tr><td>Knowledge of the target's design and operation: 0 (Public)</td></tr>
<tr><td>Geralmente o conhecimento sobre a vítima é adquirido através das redes sociais e conversas com a mesma, podendo, em casos mais extremos também ser adquirido através de hacking.</td></tr>
<tr><td>Window of opportunity: 1 (Easy)</td></tr>
<tr><td>Após adquirir os dados necessários e efetuar o processo de troca do cartão SIM, poderá efetuar qualquer operação que requira o dispositivo móvel, como autenticação OTP, num curto intervalo de tempo, até que a vítima repare em alterações em por exemplo passwords, endereços de e-mail, e extratos bancários incomuns e averigue a situação.</td></tr>
<tr><td>IT hardware/software or other equipment required for exploitation: 0 (Standard)</td></tr>
<tr><td>Equipamento básico que permita aceder a redes sociais e um telemóvel que irá receber os dados é suficiente.</td></tr>
<tr><td>Total de potencial de ataque estimado: 4 = BASIC</td></tr>
</table>

Risco 2 - Obtenção de cartão SIM associado ao número da vítima

Intercepção Wireless das mensagens OTP

Nº 3	Intercepção Wireless das mensagens OTP [1] [4] [5]	
Descrição do cenário de ataque	Vulnerabilidade explorada	Potencial de ataque estimado, necessário para efetuar o ataque
Neste cenário, o adversário utiliza *femtocells* dentro de uma rede e começa a capturar tráfego que inclui mensagens SMS. Estas redes como não possuem autenticação entre dispositivos móveis e as estações da rede *wireless* não conseguem verificar que esta é uma estação falsa. Como estas redes utilizam GSM no envio dos SMS, o adversário consegue decifrar as mensagens dado que os algoritmos de segurança são antigos e facilmente decifráveis. De modo a direcionar o ataque para uma vítima em específico, basta então que, este adversário saiba o número da vítima e assim consegue obter todas as suas mensagens OTP e utilizá-las para obter acesso aos serviços e contas da vítima, através do *reset* de *password* nas suas contas ou da confirmação de operações delicadas que utilizem este método OTP.	Neste cenários as vulnerabilidades exploradas estão associadas à rede utilizada pelas operadoras para enviar SMS. De facto, existem diversas vulnerabilidades ao nível da autenticação entre os dispositivos móveis e as estações da rede *wireless* que permitem a instalação de estações falsas que passarão a capturar as mensagens SMS. Para que isto se processe é necessário modificar o *firmware* de *femtocells*, que são dispositivos que podem ser utilizados por utilizadores comuns de modo a aumentar a potência do sinal 3G. Para além disso, existem também vulnerabilidades que são exploradas ao nível dos algoritmos utilizados por estas redes para cifrar as mensagens, tornando-os fáceis de decifrar e assim obter acesso às mensagens OTP.	**Time taken to identify and exploit:** 0 (<= one day) Devido à facilidade de obtenção de tecnologia capaz de efetuar este tipo de ataque não é necessário um intervalo de tempo significativo. **Specialist technical expertise required:** 6 (Expert) Apesar de existirem inúmeros vídeos na internet a explicar como efetuar este tipo de ataques, ainda são necessário alguns conhecimentos a nível protocolar, algorítmico e de segurança para poder operar sobre invidíviduos específicos de forma eficiente. **Knowledge of the target's design and operation:** 0 (Public) Para atacar alguém específico basta saber o idenficador da vítima, neste caso o número telefónico. **Window of opportunity:** 1 (Easy) Ao interceptar as mensagens da vítima o atacante poderá forçar, por exemplo sistemas de recuperação, com recurso a OTP por SMS para adquirir acesso a contas dela e, consequentemente, poder aceder às mesmas e agir como bem quiser. É possível que seja detetado rapidamente, mas o ataque pode ser efetuado de uma forma rápido a partir do momento em que começa a conseguir capturar os SMS com OTPs. **IT hardware/software or other equipment required for exploitation:** 4 (Specialized) É necessário a utilização de *femtocells* que, apesar de serem equipamentos fáceis de obter é necessário modificar o seu *firmware* para poder explorar a captura de mensanges que passem pela rede. **Total de potencial de ataque estimado: 11 = ENHANCED BASIC**
Este tipo de ataque ocorre nas formas de envio de SMS até ao 4G LTE, não inclusive. Nele, o atacante faz-se passar por um SMSC, que trata do armazenamento, redirecionamento, conversão e envio de SMSs, e através disso contacta o HLR, a base de dados que mapeia os clientes ativos a um MSC, adquirindo o identificador do MSC associado à sua vítima na rede. A vítima é identificada por um IMSI que está ligada ao número de telemóvel da vítima. Com esse identificador (IMSI), o atacante age como se fosse um VMSC falso e atualiza o HLR para que passe a receber os SMSs que vão para a vitima. Assim, todos os SMS que seriam enviados para a vítima, agora serão enviadas para esse endereço falso, sobre o qual o adversário possui controlo, ou seja, pode armazenar todas as mensagens que contém códigos OTP e posteriormente reencaminhá-los para a vítima, sendo que, esta não tem como se aperceber que este ataque está a acontecer. Através de serviços de recuperação com recurso a SMSs contendo OTP e, se o atacante tiver conhecimento do numero de telemóvel correspondente ao IMSI que adquiriu, ele poderá dar trigger desses serviços recebendo por fim os OTPs necessários para aceder às contas da vítima, sobre as quais poderá possivelmente efetuar furtos, seja de dados privados ou monetariamente. O identificador da vítima só deixará de estar comprometido quando esta entrar numa nova área, uma vez que o identificador será atualizado pois a vítima conecta-se a outro centro de rede.	As vurnerabilidades exploradas neste cenário dizem respeito à exploração do protocolo SS7 e respetivas vulnerabilidades. O protocolo SS7 possui falhas que permitem com que atacantes alterem o destino das mensagens SMS para si próprios, pois alteram o HLR para que qualquer SMS que esteja destinada para uma determinada vítima, seja enviada primeiro para os atacantes. Desta forma, as mensagens OTP podem ser intercetadas e lidas, e o atacantes pode depois reenviar a mensagem para a vítima.	**Time taken to identify and exploit:** 0 (<= one day) Devido à facilidade de obtenção de tecnologia capaz de efetuar este tipo de ataque não é necessário um intervalo de tempo significativo. **Specialist technical expertise required:** 6 (Expert) É necessário ter conhecimento sobre o protocolo SS7 e alguns conhecimentos sobre comunicação para efetuar este ataque. **Knowledge of the target's design and operation:** 3 (Restricted) Para atacar alguém específico é necessário saber o seu identificador (IMSI). **Window of opportunity:** 1 (Easy) A partir do momento em que inicia o ataque, este pode obter os códigos OTP em pouco tempo. Poderá ser detetado se começar a realizar operações ou *resets* de *password* que alertem a vítima. **IT hardware/software or other equipment required for exploitation:** 0 (Standard) Apenas é necessário o SS7 sdk. [6] **Total de potencial de ataque estimado: 10 = ENHANCED BASIC**

Risco 3 - Interseção das mensagens OTP enviadas por SMS através da rede (tabela A)

<table>
<tr><td>Nº 3</td><td colspan="2">Intercepção Wireless das mensagens OTP [4] [5]</td></tr>
<tr><td>Descrição do cenário de ataque</td><td>Vulnerabilidade explorada</td><td>Potencial de ataque estimado, necessário para efetuar o ataque</td></tr>
<tr><td rowspan="11">Este tipo de ataque é baseado no protocolo sucessor ao SS7, o Diameter, utilizado nas redes posterior às 4G LTE. Nele, o atacante faz-se passar por uma rede desconhecida, apresentando-se como um SMSC e, de modo a adquirir o identificador da vítima (IMSI), contacta o HSS, a base de dados de utilizadores e afirma necessitar do identificador da vítima para poder enviar-lhe um SMS. Como este é um pedido normal e não existe autenticação a base de dados fornece-lhe o identificador sem qualquer problema. Com o identificador, o atacante age como se fosse um MME, um nodo em que normalmente se efetua registo quando se está num serviço de roaming noutro país, e de seguida a sua localização é atualizada, fazendo com que os SMS sejam enviados para si. Assim, todos os SMS que seriam enviados para a vítima, agora serão enviadas para esse endereço falso, sobre o qual o adversário possui controlo, ou seja, pode armazenar todas as mensagens que contém códigos OTP e posteriormente reencaminhá-los para a vítima, sendo que, esta não tem como se aperceber de que está a ser alvo de um ataque. Através de serviços de recuperação com recurso a SMSs contendo OTP e, se o atacante tiver conhecimento do numero de telemóvel correspondente ao IMSI que adquiriu, ele poderá dar trigger desses serviços recebendo por fim os OTPs necessários para aceder às contas da vítima, sobre as quais poderá possivelmente efetuar furtos, seja de dados privados ou monetariamente.
O identificador da vítima só deixará de estar comprometido quando esta entrar numa nova área, uma vez que o identificador será atualizado pois a vítima conecta-se a outro centro de rede.</td><td rowspan="11">Interceção de mensagens OTP através da exploração do protocolo Diameter e as suas vulnerabilidades.

Através do facto de não haver autenticação entre algumas entidades que fazem parte da rede que utiliza este protocolo é possível obter o identificador da vítima e alterar o destino das mensagens OTP para que sejam recebidas por quem está realizar o ataque. De facto, para alterar o destino destas é também explorada uma vulnerabilidade que permite ao adversário fingir que é um MME (nodo da rede que recebe SMS quando o utilizador utiliza o serviço de roaming) e provoca um update da da localização do dispositivo da vítima junto da base de dados que mapeia os identificadores às entidades que lhes podem redirecionar as mensagens SMS, para que estas sejam redirecionadas para o adversário. Desta forma, pode provocar o envio de mensagens OTP de serviços que a vítima use, sendos as mensagens recebidas primeiro por quem realiza o ataque.</td><td>Time taken to identify and exploit: 1 (<= one week)</td></tr>
<tr><td>Apesar de as vulnerabilidades estarem explícitas em vários meios de informação, é necessário desenvolver o software em questão o que pode levar algum tempo. A realização do ataque em sí é um processo rápido.</td></tr>
<tr><td>Specialist technical expertise required: 6 (Expert)</td></tr>
<tr><td>É necessário ter conhecimento sobre o protocolo Diameter e alguns conhecimentos sobre comunicação para efetuar este ataque.</td></tr>
<tr><td>Knowledge of the target's design and operation: 3 (Restricted)</td></tr>
<tr><td>Para atacar alguém específico é necessário saber o seu identificador (IMSI).</td></tr>
<tr><td>Window of opportunity: 1 (Easy)</td></tr>
<tr><td>A partir do momento em que inicia o ataque, este pode obter os códigos OTP em pouco tempo. Poderá ser detetado se começar a realizar operações ou resets de password que alertem a vítima.</td></tr>
<tr><td>IT hardware/software or other equipment required for exploitation: 7 (Bespoke)</td></tr>
<tr><td>É necessário desenvolver o software necessário que permita ao atacante apresentar-se como um SMSC, efetuar pedidos ao HSS para adquirir o IMSI da vítima.
Esse software também tem de permitir que este faça-se passar por um MME e utilize o IMSI que adquiriu de modo a registar-se como se estivesse serviço de roaming noutro país e a que o HSS atualize a sua localização, sendo por fim os SMS pertencentes à vítima encaminhados para si.</td></tr>
<tr><td>Total de potencial de ataque estimado: 18 = Moderate</td></tr>
</table>

Risco 3 - Interseção das mensagens OTP enviadas por SMS através da rede (tabela B)

Malware no dispositivo móvel

Nº 4	Malware no dispositivo móvel [1]	
Descrição do cenário de ataque	Vulnerabilidade explorada	Potencial de ataque estimado, necessário para efetuar o ataque
Neste cenário o atacante cria um software atrativo que possui caracteristicas que lhe permitem reenviar mensagens SMS que foram recebidas pelo dispositivo onde está instalada, como por exemplo um trojan. O atacante envia um link através de um email de phishing que permite à vítima descarregar a aplicação, sendo que para isso faz-se passar por uma entidade credível para enganar a vítima. Esta descarrega a aplicação e numa primeira análise parece-lhe um software normal mas que consegue ter acesso às mensagens que recebe, reenviando-as para quem está a realizar o ataque. Assim sendo, quem realiza este ataque consegue interceptar as mensagens associadas ao dispositivo em questão e provocar a receção de OTPs que permitem adquirir acesso total às contas da vítima.	Utilização de técnicas de *social engineering (phishing)* para levar a vítima a instalar uma aplicação que é na verdade um *malware* (trojan, por exemplo), sendo capaz de obter acesso aos SMS que são recebidos pela vítima e por isso provocar o *reset* de contas que utilizem o sistema OTP ou autenticar-se perante operações ou serviços associados à vítima que utilizem este método.	**Time taken to identify and exploit:** 4 (<= one month) O tempo necessário irá depender maioritariamente do tempo que a vítima demora a instalar o *software* e o tempo dispendido em criá-lo. O tempo que demora a identificar esta vulnerabilidade é bastante baixa, já que é algo bastante comum de ser realizado. **Specialist technical expertise required:** 6 (Expert) Para criar o *malware* é indispensável conhecimentos protocolares, algorítmicos e de segurança além de capacidades em Engenharia Social, que façam com que as vítimas instalem o *software*. **Knowledge of the target's design and operation:** 3 (Restricted) É necessário saber que tipo de dispositivo é que a vítima utiliza (*android*, por exemplo) para poder desenvolver um software compatível com o mesmo. **Window of opportunity:** 1 (Easy) Ao interceptar as mensagens da vítima o atacante poderá forçar, por exemplo sistemas de recuperação, com recurso a OTP por SMS para adquirir acesso a contas dela e, consequentemente, poder aceder às mesmas e agir como bem quiser. É possível que seja detetado rapidamente, mas o ataque pode ser efetuado de uma forma rápido a partir do momento em que consegue capturar os SMS com OTPs. **IT hardware/software or other equipment required for exploitation:** 4 (Specialised) É necessário desenvolver o *malware*. **Total de potencial de ataque estimado: 18 = MODERATE**

Risco 4 - Obtenção das mensagens OTP através de um malware instalado no dispositivo da vítima

Ataques PRMitM

<table>
<tr><td>Nº 5</td><td colspan="2">Ataques PRMitM (password reset man in the middle) [3]</td></tr>
<tr><td>Descrição do cenário de ataque</td><td>Vulnerabilidade explorada</td><td>Potencial de ataque estimado, necessário para efetuar o ataque</td></tr>
<tr><td rowspan="11">Neste tipo de ataques, o atacante cria um website malicioso (B), onde o utilizador introduz os seus dados para criar uma nova conta (email, número de telemóvel, etc...). De seguida, o website B aciona o processo de reset de password de uma conta da vítima num outro website (A), sendo enviado um SMS para o utilizador com um código OTP para finalizar o processo de reset. O utilizador ao receber este SMS pensa, erradamente, tratar-se de uma SMS de autenticação OTP para finalizar o registo no website B e por isso introduz o código que recebeu. Assim, é possivel que o atacante consiga terminar o processo de reset da conta redirecionando o código OTP que a vítima introduziu para o website A, alterando a password e, portanto, ficando com acesso total à sua conta privada no website A.</td><td rowspan="11">A vulnerabilidade explorada é a utilização de técnicas de social engineering, através da criação de um website malicioso, de modo a enganar a vítima fazendo-a pensar que esta está num processo de autenticação num site legítimo, sendo que, na verdade, está permitir ao atacante que realize um reset duma conta que associada à vítima num outro website, ou seja, é realizado um ataque man in the middle. Desta forma, a pessoa perde total acesso à sua conta na plataforma, sem se aperceber do processo que foi efetuado.</td><td>Time taken to identify and exploit: 4 (<= one month)</td></tr>
<tr><td>Para realizar o ataque é necessário desenvolver um site man-in-the-middle que vai fazer de intermediário entre o utilizador e o site onde a vitima tem uma conta. Para desenvolver o método de ataque, ou seja o site intermediário, é necessário algum tempo. Também pode ser necessário algum tempo até que a vítima decida registar-se neste website.</td></tr>
<tr><td>Specialist technical expertise required: 6 (Expert)</td></tr>
<tr><td>Para que o site B a ser desenvolvido pelo o atacante consiga comunicar com o site A é necessário ter um conhecimento especial em relção aos protocolos usados na comunicação entre o site A e o utilizador, para assim o site B fazer intermediário nesta comunicação. Para que o ataque tenha sucesso é também necessário ter conhecimentos de engenharia social para conseguir iludir o utilizador a registar-se no site B e acreditar que a mensagem SMS que recebe é de autenticação no website B e não de reset de password no website A.</td></tr>
<tr><td>Knowledge of the target's design and operation: 0 (Public)</td></tr>
<tr><td>É necessário ter conhecimentos em relação ao utilizador, como sites ou aplicações onde possui contas, que pode ser facilmente obtido através de rede sociais ou internet.</td></tr>
<tr><td>Window of opportunity: 1 (Easy)</td></tr>
<tr><td>Este tipo de ataques dá oportunidade ao atacante de conseguir entrar em contas de diversos utilizadores sendo dificilmente detetada a relação entre o registo no site B e o reset de password no site A. Desta forma, o atancante consegue desenvolver um ataque de larga escala, com pouca probabilidade de ser detetado.</td></tr>
<tr><td>IT hardware/software or other equipment required for exploitation: 4 (Specialised)</td></tr>
<tr><td>Para desenvolver um site man-in-the-middle que esteja disponível para todos os utilizadores será necessário o uso de servidores e outros dispositivos para que o site consiga correr livermente na internet e que consiga ser acedido por vários utilizadores em várias localizações.</td></tr>
<tr><td>Total de potencial de ataque estimado: 15 = MODERATE</td></tr>
</table>

Risco 5 - Ataques *man in the middle* com a finalidade de realizar reset a *passwords* das contas da vítima

Push Notification

Ataque PRMitM

Nº 6	Ataques PRMitM (password reset man in the middle) [3]	
Descrição do cenário de ataque	Vulnerabilidade explorada	Potencial de ataque estimado, necessário para efetuar o ataque
Neste tipo de ataques, o atacante cria um *website* malicioso (B), onde o utilizador introduz os seus dados para criar uma nova conta (email, número de telemóvel, etc...). De seguida, o *website* B aciona o processo de *reset* de *password* de uma conta da vítima num outro *website* (A), sendo enviado um SMS para o utilizador com um código OTP para finalizar o processo de *reset*. Neste SMS, o OTP encontra-se indicado no início da mensagem enquanto que a sua finalidade (*reset* da *password*) encontra-se apenas no fim. O utilizador ao receber este SMS pensa, erradamente, tratar-se de uma SMS de autenticação OTP para finalizar o registo no website B, pois verifica apenas a notificação no ecrã com o código OTP mas não a finalidade e por isso introduz o código que recebeu no *website* B. Assim, é possivel que o atacante consiga terminar o processo de *reset* da conta redirecionando o código OTP que a vítima introduziu para o *website* A, alterando a *password* e, portanto, ficando com acesso total à sua conta privada no *website* A.	Com este ataque é possível explorar vulnerabilidades associadas à autenticação OTP via SMS, especialmente devido a uma funcionalidade introduzida pelos *smartphones*, as notificações *push*. Nesta funcionalidade os SMS recebidos nos *smartphones* são apresentados ao utilizador através de notificação no ecrã com as primeiras linhas da mensagem, só sendo apresentado todo o SMS quando o utilizador clica na notificação. Desta forma, estes ataques, exploram o facto de nas notificações *push* o utilizador só vê as primeiras linhas com o código OTP, não sendo por vezes possível ao utilizador verificar o propósito desse código. Assim, o utilizador é engando, pois pensa que o código tem uma finalidade quando na verdade é utilizado para outra. Estes ataques só conseguem explorar efetivamente esta vulnerabilidade, quando os SMS de autenticação OTP não têm indicação da entidade ou da funcionalidade do código no início da mensagem. Caso contrário é possível que nas primeiras linhas da notificação *push* tenha a informação completa para que o utilizador consiga validar o SMS que recebeu.	**Time taken to identify and exploit:** 4 (<= one month) Para realizar o ataque é necessário desenvolver um site *man-in-the-middle* que vai fazer de intermediário entre o utilizador e o site onde a vitima tem uma conta. Para desenvolver o método de ataque, ou seja o site intermediário, é necessário algum tempo. Também pode ser necessário algum tempo até que a vítima decida registar-se neste *website* **Specialist technical expertise required:** 6 (Expert) Para que o site B a ser desenvolvido pelo o atacante consiga comunicar com o site A é necessário ter um conhecimento especial em relação aos protocolos usados na comunicação entre o site A e o utilizador, para assim o site B fazer intermediário nesta comunicação. Para que o ataque tenha sucesso é também necessário ter conhecimentos de engenharia social para conseguir iludir o utilizador a registar-se no site B e acreditar que a mensagem SMS que recebe é de autenticação no *website* B e não de *reset* de *password* no *website* A. **Knowledge of the target's design and operation:** 0 (Public) De forma a explorar a vulnerabilidade associadada às OTP via notificação *push*, basta aceder a informação pública que se encontra na internet. É também necessário ter conhecimentos em relação ao utilizador, como sites ou aplicações onde possui contas, que pode ser facilmente obtido através de rede sociais ou internet. É também necessário saber se o conteúdo da mensagem SMS do *website* alvo pode enganar o utilizador através da *push notification*, ou seja, tem se tem a finalidade do código no inicio ou no fim da mensagem. **Window of opportunity:** 1 (Easy) Este tipo de ataques dá oportunidade ao atacante de conseguir entrar em contas de diversos utilizadores sendo dificilmente detetada a relação entre o registo no site B e o *reset* de *password* no site A. Desta forma, o atancante consegue desenvolver um ataque de larga escala, com pouca probabilidade de ser detetado. **IT hardware/software or other equipment required for exploitation:** 4 (Specialised) Para desenvolver um site *man-in-the-middle* que esteja disponível para todos os utilizadores será necessário o uso de servidores e outros dispositivos para que o site consiga correr livermente na internet e que consiga ser acedido por vários utilizadores em várias localizações. **Total de potencial de ataque estimado: 15 = MODERATE**

Risco 6 - Ataques *man in the middle* com o auxilio das *push notifications* geradas ao receber os códigos OTP

Conclusão

A tecnologia OTP demonstra ser passível de ser atacada de diversas formas. De facto, apenas se verificou um ataque que, à luz da metodologia seguida, demonstra ser um ataque moderado, possuindo os restantes uma classificação inferior (*basic* e *enhanced basic*).

Existem várias formas de realizar ataques contra este método, utilizando tanto *software* e como *hardware* específico ou simplesmente o uso de engenharia social, havendo uma grande probabilidade de as vítimas serem enganadas de uma forma bastante fácil.

Assim, esta tecnologia não revela ser segura, especialmente, quando é utilizada através do uso de SMS, que por si só operam em redes com protocolos que revelam algumas vulnerabilidades que tornam a sua interceção e leitura possíveis.

Bibliography

[1] Mulliner C. Borgaonkar R. Seifert J. 2014. SMS-based One-Time Passwords: Attacks and Defense.

[2] Common Methodology for Information Technology Evaluation, Evaluation Methodology, Version 3.1, Revision 5, CCMB 2017-04-004.

[3] Shibayama R. Kikuchi H. 2021. Vulnerability Exploiting SMS Push Notifications.

[4] Ullah K. Rashid I. Afzal H. Iqbal M. Bangash Y. Abbas H. SS7 Vulnerabilities—A Survey and Implementation of Machine Learning vs Rule Based Filtering for Detection of SS7 Network Attacks.

[5] Oliver I. Holtemanns S. 2017. SMS and One-Time-Password Interception in LTE Networks.

[6] "A Step by Step Guide to SS7 Attacks". [online]. https://www.firstpoint-mg.com/blog/ss7-attack-guide/ [Acedido em março 2022]