

## GRUPO 8

### I/ Potencial de ataque à Chave Móvel Digital

Nº 1	Risco de ataque por <i>brute force</i>	
Descrição do cenário de ataque	Vulnerabilidade explorada	Potencial de ataque estimado, necessário para efetuar o ataque
Um intruso pode, com as ferramentas certas, <b>testar todas as combinações possíveis de 4, 5 ou 6 dígitos representantes do PIN da Chave Móvel Digital associado a determinado número de telemóvel</b> . Para cada combinação, testá-la até uma ser sucedida e dar acesso à fase seguinte de autenticação. Sendo que há um limite de 3 tentativas e, depois desse limite ser atingido, é feito um bloqueio à chave e há um tempo de espera até <b>ser possível realizar próxima tentativa, este tempo é incrementado a cada bloqueio</b> .	Neste ataque é explorado o facto de o PIN para autenticação com a CMD ser composto apenas por um mínimo de 4 e máximo de 6 dígitos, tornando o número de combinações possíveis relativamente pequeno ( $10^4+10^5+10^6$ combinações possíveis).	<p><u><i>Time taken to identify and exploit: 19 (&gt; six months)</i></u><sup>1</sup></p> <p>O serviço de autenticação da CMD conta com uma estratégia de mitigação ou diminuição de risco de ataque para esta vulnerabilidade, que é proceder a um bloqueio da chave após um limite de 3 tentativas. Após 3 tentativas falhadas do PIN, a chave é bloqueada durante 3 minutos, tempo após o qual é possível realizar outra tentativa. No entanto, se esta última for novamente falhada, a chave será bloqueada mais uma vez, mas agora durante 5 minutos. Este tempo de bloqueio/espera para a próxima tentativa é constantemente incrementado a um nível exponencial. O que, com alguns cálculos, nos leva a perceber que serão necessários bem mais que 6 meses para testar todas as combinações possíveis.</p> <p>Assume-se que o tempo necessário para um computador verificar uma combinação será aproximadamente nas grandezas de <math>10^{-3}</math> s. Considerando-se que o PIN pode ter entre 4 e 6 dígitos, o número de combinações possíveis são <math>10^4+10^5+10^6 = 1110000</math>. Contando ainda que depois da 3ª tentativa errada, será sempre necessário esperar um crescente número de tempo, começando em 3 minutos, podemos prever que o tempo total necessário para verificar todas as combinações seria <math>10^{-3} * 1110000</math> somado à soma de todos os tempos de espera para cada uma das tentativas.</p>

<sup>1</sup> Valor e Factor de acordo com tabela 3 do anexo B do *Common Methodology for Information Technology Evaluation, Evaluation Methodology, Version 3.1, Revision 5, CCMB 2017-04-004*

		<p><u>Specialist technical expertise required: 3 (proefficient)<sup>1</sup></u></p> <p>Para efetuar este ataque é necessário ter conhecimento sobre <b>como usar a ferramenta que irá testar todas as combinações</b>. Este conhecimento pode ser adquirido por qualquer pessoa através da internet. É necessário também ter conhecimento sobre o comportamento do sistema de segurança do serviço que pode ser adquirido através de documentação publica e de fácil acesso.</p> <p><u>Knowledge of the target's design and operation: 0 (public)<sup>1</sup></u></p> <p>O conhecimento necessário sobre o alvo é público e pode ser adquirido através da <i>internet</i> na página oficial da plataforma da CMD.</p> <p><u>Window of opportunity: 0 (unnecessary)<sup>1</sup></u></p> <p>Para realizar o ataque apenas é necessário inserir o PIN e ver se este é o correto ou não, não é necessário um acesso ao TOE.</p> <p><u>IT hardware/software or other equipment required for exploitation: 0 (Standard)<sup>1</sup></u></p> <p>Para realizar o ataque, é necessário apenas um computador, ligação à <i>internet</i> e acesso à ferramenta para teste das combinações, algo que é acessível a qualquer pessoa.</p> <p><b><u>Total de potencial de ataque estimado:</u></b></p> <p><b>= 19 + 3 + 0 + 0 + 0 = 22 → High<sup>2</sup></b></p>
--	--	--

---

<sup>2</sup> De acordo com tabela 4 do anexo B do Common Methodology for Information Technology Evaluation, Evaluation Methodology, Version 3.1, Revision 5, CCMB 2017-04-004.



Nº 2	Risco de ataque de <i>phishing</i>	
Descrição do cenário de ataque	Vulnerabilidade explorada	Potencial de ataque estimado, necessário para efetuar o ataque
<p>Um atacante, através de um meio externo de comunicação, como mensagem telefónica ou através de um e-mail, requisita os dados pessoais de um utilizador do sistema CMD, fazendo-se passar pela página oficial deste serviço. O utente insere os seus dados no website de <i>phishing</i> acabando por fornecer as suas credenciais ao atacante.</p>	<p>Neste ataque é explorada a ignorância do utilizador do serviço. Usando ferramentas de software o atacante envia mensagens eletrónicas em massa, para o maior número de pessoas possível, quer sejam utilitárias da CMD ou não. Utilizando linguagem cuidada, termos oficiais e inventando algum tipo de problema técnico que necessite da intervenção do usuário, o atacante procura remeter o utilizador que recebeu o e-mail até um website idêntico ao que representa a CMD. A partir daqui consegue obter os dados de diferentes utilizadores.</p>	<p><u><i>Time taken to identify and exploit: 1 (&lt;= one week)</i></u><sup>1</sup></p> <p>A grande maioria das pessoas que vai ser afetada por este ataque faz parte das pessoas que utilizam regularmente serviços de correio eletrónico.</p> <p>Por estes motivos, a maior proporção dos utilizadores que serão prejudicadas por um e-mail (por exemplo) será afetada nos primeiros dias após o envio do e-mail, isto tendo em conta que o processo de ceder os seus dados é bastante rápido e muitas vezes aparentemente inofensivo, ficando assim o atacante com uma quantidade absurda de dados relativos a diferentes utilizadores em muito pouco tempo.</p> <p><u><i>Specialist technical expertise required: 3 (proeficient)</i></u><sup>1</sup></p> <p>Há 2 pontos fulcrais nesta abordagem, o envio das mensagens e o desenvolvimento do site clone da entidade oficial. Para ambos é necessário ter algumas capacidades técnicas de maneira que a ferramenta não esteja obviamente associada ao atacante, mas também para que esta envie as mensagens para um determinado "público-alvo"- seria bastante improvável ser bem-sucedido se se enviasse mensagens <i>phishing</i> relativas à chave móvel digital para pessoas que não sejam de nacionalidade portuguesa.</p> <p>Relativamente ao website em si, apesar de ser bastante fácil replicar a aparência deste, é preciso saber como aglomerar e armazenar os dados que a partir dele são obtidos, e para este aspeto em particular é necessário ter algum conhecimento especializado.</p> <p><u><i>Knowledge of the target's design and operation: 0 (public)</i></u><sup>1</sup></p> <p>O conhecimento necessário sobre o alvo é público, podendo-se ter acesso à página de login do CMD a qualquer altura, visto que o endereço é público, e facilmente se simula o seu comportamento.</p>

		<p><u>Window of opportunity: 0 (unnecessary)<sup>1</sup></u></p> <p>Este ataque pode ser feito a qualquer altura, não havendo qualquer momento em específico que possa ser tido como mais ou menos oportuno.</p> <p><u>IT hardware/software or other equipment required for exploitation: 0 (Standard)<sup>1</sup></u></p> <p>Este ataque pode ser feito por qualquer pessoa, sendo que o único acréscimo seria ter um servidor para dar <i>host</i> ao website e ter (ou desenvolver) uma ferramenta de software que possa enviar os emails em massa.</p> <p><b><u>Total de potencial de ataque estimado:</u></b></p> <p><b>= 1 + 3 + 0 + 0 + 0 = 4 → Basic<sup>3</sup></b></p>
--	--	--

---

<sup>3</sup> De acordo com tabela 4 do anexo B do Common Methodology for Information Technology Evaluation, Evaluation Methodology, Version 3.1, Revision 5, CCMB 2017-04-004.

Nº 3	Risco de intercepção do segundo fator de autenticação	
Descrição do cenário de ataque	Vulnerabilidade explorada	Potencial de ataque estimado, necessário para efetuar o ataque
<p>Neste cenário de ataque assume-se que a vítima usa o segundo fator de autenticação por mensagem direta na rede social Twitter. Ou seja, depois de inserir o seu PIN de acesso à CMD, a vítima recebe na sua conta do Twitter uma mensagem privada com o código temporário que deve inserir para proceder com a autenticação. Então, será claramente possível ganhar acesso à conta do Twitter da vítima e conseguir ver o código; ou até usar um ataque MITM para espionar (<i>sniffer</i>) a rede (se o atacante estiver na mesma rede que a vítima) e conseguir ter acesso ao conteúdo da mensagem com o código. Este cenário juntado ao do risco de ataque por <i>brute force</i> permite um ganho de acesso total à CMD da vítima, permitindo um roubo de identidade por parte do atacante.</p>	<p>A vulnerabilidade aqui explorada é o facto de a autenticação por 2 fatores da CMD poder ser feita através de uma rede social, que, usualmente, têm pouca segurança e são facilmente atacadas. No caso do <i>Twitter</i>, a password de uma conta específica poderia ser descoberta com um ataque por <i>brute force</i>, fazendo uso de <i>passwords</i> comuns para agilizar o processo, visto que o processo de autenticação na rede social em questão não conta com nenhum tipo de bloqueio ou restrição na presença de várias tentativas de autenticação com a <i>password</i> incorreta.</p>	<p><u><i>Time taken to identify and exploit:</i> 0 (&lt;= <b>one day</b>)<sup>1</sup></u></p> <p>Assume-se, neste cenário, que a vítima terá na sua conta de <i>Twitter</i>, uma <i>password</i> com um número de caracteres comum (8 caracteres), usando letras maiúsculas e minúsculas e números. De acordo com uma tabela<sup>4</sup> que relaciona a quantidade de caracteres com o tipo de caracteres presentes na <i>password</i> e determina o tempo que um hacker levaria a descobrir a <i>password</i> por <i>brute force</i>, seria necessária apenas 1 hora para descobrir a sua <i>password</i> e ter acesso à conta do <i>Twitter</i> e, consequentemente, à mensagem com o código de segurança para a autenticação na CMD.</p> <p><u><i>Specialist technical expertise required:</i> 3 (<b>proefficient</b>)<sup>1</sup></u></p> <p>O conhecimento que é necessário ter é sobre como usar uma ferramenta que irá testar todas as combinações de <i>passwords</i> possíveis. Este conhecimento pode ser adquirido por qualquer pessoa através da <i>internet</i>.</p> <p><u><i>Knowledge of the target's design and operation:</i> 0 (<b>public</b>)<sup>1</sup></u></p> <p>Para testar as <i>passwords</i> possíveis numa rede social, não é necessário ter qualquer conhecimento sobre o alvo. No entanto, saber quais as restrições mínimas que a rede social tem para as <i>passwords</i> pode ajudar a reduzir o número de <i>passwords</i> a testar, reduzindo, consequentemente, o tempo necessário para o teste. Este conhecimento, no entanto, pode ser adquirido facilmente na <i>internet</i>.</p> <p><u><i>Window of opportunity:</i> 0 (<b>unnecessary</b>)<sup>1</sup></u></p> <p>Não é necessário haver um acesso ao TOE, visto que se trata apenas de uma</p>

<sup>4</sup> <https://www.komando.com/security-privacy/check-your-password-strength/783192/>

		<p>constante verificação de <i>passwords</i>.</p> <p><u><i>IT hardware/software or other equipment required for exploitation: 0 (Standard)</i></u><sup>1</sup></p> <p>Para realizar o ataque, é necessário apenas um computador, ligação à <i>internet</i> e acesso à ferramenta para teste das combinações, algo que é acessível a qualquer pessoa.</p> <p><b><u>Total de potencial de ataque estimado:</u></b></p> <p><b>= 0 + 3 + 0 + 0 + 0 = 3 → Basic</b> <sup>5</sup></p>
--	--	---

---

<sup>5</sup> De acordo com tabela 4 do anexo B do Common Methodology for Information Technology Evaluation, Evaluation Methodology, Version 3.1, Revision 5, CCMB 2017-04-004.

Nº 4	Risco de intercepção do <b>segundo fator de autenticação</b>	
Descrição do cenário de ataque	Vulnerabilidade explorada	Potencial de ataque estimado, necessário para efetuar o ataque
<p>Os ataques SS7 exploram a capacidade de autenticação dos protocolos de comunicação executados sobre o protocolo SS7 para espiar comunicações de voz e texto.</p> <p>Uma vez ligado a uma rede SS7, o atacante pode direcionar os utilizadores da rede enquanto engana a rede fazendo-a pensar que o dispositivo do atacante é na verdade um nó MSC/VLR.</p>	<p>Semelhante a um ataque Man In the Middle, os ataques SS7 têm como alvo as comunicações de telemóveis, em vez de comunicações wi-fi.</p> <p>Uma precaução de segurança comum usada por muitos é um dos alvos dos ataques SS7. A autenticação de dois fatores (também conhecida como 2FA) via SMS usando SS7 é inerentemente falível, pois essas mensagens SMS não são criptografadas e os atacantes sabem como intercetá-las.</p>	<p><u><i>Time taken to identify and exploit:</i></u> 0 (&lt;= <b>one day</b>)<sup>1</sup></p> <p><b>Basta instalar o SDK SS7 e ligar à rede – assumindo uma boa velocidade de internet, o tempo é bastante reduzido.</b></p> <p><u><i>Specialist technical expertise required:</i></u> <b>3 (proficient)</b><sup>1</sup></p> <p>É necessário ter estudado a arquitetura protocolar em causa, cuja documentação pode ser encontrada na <i>internet</i>.</p> <p>Também é necessário conhecimento do Unix e Linux, o que é facilmente encontrado na internet.</p> <p><u><i>Knowledge of the target's design and operation:</i></u> <b>0 (public)</b><sup>1</sup></p> <p>É necessário ter estudado a arquitetura protocolar em causa, cuja documentação pode ser encontrada na <i>internet</i>.</p> <p><u><i>Window of opportunity:</i></u> <b>0 (unnecessary)</b><sup>1</sup></p> <p>Não há risco de ser detetado pelo serviço da cmd nem pelo protocolo ss7.</p> <p><u><i>IT hardware/software or other equipment required for exploitation:</i></u> <b>0 (Standard)</b><sup>1</sup></p> <p>Para realizar o ataque, é necessário apenas um computador, ligação à <i>internet</i> com o SO Linux e o <b>SDK SS7</b> – ambos gratuitos na Internet.</p>



		<p>Qualquer pessoa tem acesso a este tipo de equipamento.</p> <p><b><u>Total de potencial de ataque estimado:</u></b></p> <p><b><math>= 0 + 3 + 0 + 0 + 0 = 3 \rightarrow \text{Basic}^6</math></b></p>
--	--	---

---

<sup>6</sup> De acordo com tabela 4 do anexo B do Common Methodology for Information Technology Evaluation, Evaluation Methodology, Version 3.1, Revision 5, CCMB 2017-04-004.