UNIVERSIDADE FEDERAL DE PELOTAS

Faculdade de Ciência da Computação

Relatório Trabalho de AED III - Criptografia

Tayssa Jardim de Avila

Pelotas, 2019

1. Introdução

O relatório descreve os passos tomados para decifrar um texto e, no final, minha opinião pessoal sobre ele.

O texto está contido no arquivo cipher_text.enc, que foi criptografado em AES com chave de 256 bits(chave1), e foi codificado em base64. Sabe-se também que o aplicativo OpenSSL foi utilizado.

O arquivo cipher_pass.enc contem a chave1, porém o mesmo foi criptografado utilizando uma chave pública RSA. O arquivo chipher_pub.enc contém essa chave pública RSA, e, por sua vez, foi criptografada usando AES com uma chave(chave2).

O hash da chave2 é "YTEUCxI8/wSjrTpm/EqL7s9aR++fqs2f3JBav3vK5Uk=" e é uma hash SHA256. A senha é apenas números e letras.

Tendo essas informações à disposição, a seguir serão descritos os passos para decodificar o texto.

2. Processo de Decodificação

Para começar é preciso converter a hash da base64 para hexadecimal, utilizando o site Cryptii o resultado da conversão foi 6131140b123cff04a3ad3a66fc4a8beecf5a47ef9faacd9fdc905abf7bcae549, esse valor foi guardado em um arquivo de texto. Após isso foi preciso fazer o download do hashcat, uma ferramenta de recuperação de senha.

O **primeiro passo** é quebrar a hash, para isso utilizou-se a máscara “?l?u?d,?1?1?1?1?1?1?1?1”, e então o comando “hashcat64.exe -w 4 -a 3 -m 1400 hash.txt mask.hcmask -O”, tentando quebrar com 8 caracteres usando hashcat. Assim a senha encontrada na hash foi “SchneiER”.

Cerca de cinco horas foram necessárias para encontrar a senha.

O **segundo passo** é encontrar a chave pública do RSA, para isso abrimos o arquivo que contém a mesma (cipher_pub.enc) com a chave encontrada no primeiro passo, utilizando OpenSSL, que é uma implementação de código aberto que implementa as funções básicas de criptografia.

O comando utilizado é: “openssl enc -d -aes-256-cbc -nosalt -nopad -a -in cipher_pub.enc -out public.txt -k SchneiER”. Com isso chegamos à seguinte chave pública:

“MEwwDQYJKoZIhvcNAQEBBQADOwAwOAIxAL4dl00g/JEIYNa7xH9ItZSweBCmT7hnp8Se/wY9P+lqZyoqpTqjNLEKJScjiKuIzwIDAQAB”.

Agora para o **terceiro passo** devemos encontrar o expoente e módulo da chave pública do RSA. Com o seguinte comando no OpenSSL:” openssl rsa -inform PEM -text -noout -pubin -in public.txt”.

O resultado mostra:

Public-Key: (384 bit)

Modulus:

00:be:1d:97:4d:20:fc:91:08:60:d6:bb:c4:7f:48:
b5:94:b0:78:10:a6:4f:b8:67:a7:c4:9e:ff:06:3d:
3f:e9:6a:67:2a:2a:a5:3a:a3:34:b1:0a:25:27:23: 88:ab:88:cf

Exponent: 65537 (0x10001)

A **quarta parte** é achar o N e E (script "find.py" em python usando pycrypto)

Os resultados são:

N=
292614673915307176454256381648839916922984034877468922880717550624751
4961 737822610290796323654346303091528924263444 7

E= 65537

A **quinta parte** é fatorar o N com cado-nfs, utilizando o comando “./cado-nfs.py”. Os valores primos resultantes da fatoração foram:

P = 54849552419987951213760541173325266932909705839437737791 49

Q = 53348598302996226170475856982949505794854320954688136530 03

Levou cerca de meio dia para obter tais resultados.

O **sexto passo** é achar a chave privada RSA utilizando um script em python "findprivatekey.py.

A chave privada encontrada foi:
“MIHzAgEAAjEAvh2XTSD8kQhg1rvEf0i1lLB4EKZPuGenxJ7/Bj0/6WpnKiqlOqM0sQolJyOIq4jPAgMBAAECMG+Qt+hYMj7+Fq4M1FwJlB1kjaDfqCrEEGnbcHp5eMbVqkpq6KLsP8r0MCXFkmfOKQIZAN+xms6n6IstHvPY5bXSxKcWxzKEjb10zQIZANmSiRZ0YH33umVs9ZOtxdbKFUYvKgWUCwIYEU0+aQ+JqAIka73x/n8/4KCdZaXlBKtdAhkAnyxPUrgtZ7r3CQDf4Py+wlbxnXkf2xjlAhkAvICySx1SKvZtibpoc0gpF69R8YF6GAGR”

O **sétimo passo** foi abrir cipher_pass.enc com a chave privada do RSA encontrada no passo anterior, utilizando o comando: “openssl rsautl -decrypt -in cipher_pass.enc -out password_cipher_pass.txt -inkey privateKey.txt”, resultando na senha dentro do arquivo: 1a6MLmXd42.

Por fim, o **oitavo e último passo**, é abrir o texto, cipher_text.enc, com a senha recém encontrada do cipher_pass.enc, utilizando o comando: “openssl aes-256-cbc -d -md MD5 -a -in cipher_text.enc -out decoded.txt -k 9z7MLmYd22 -nopad –nosalt".

3. Texto Decodificado

Após todos os passos descritos acima, conseguimos decifrar o texto, que está a seguir.

“What Cyber-War Will Look Like
Fonte: https://scholars-stage.blogspot.com/2018/07/what-cyber-war-willlook-like.html

When prompted to think about the way hackers will shape the future of great power war, we are wont to imagine grand catastrophes: F-35s grounded by onboard computer failures, Aegis BMD systems failing to launch seconds before Chinese missiles arrive, looks of shock at Space Command as American surveillance satellites start careening towards the Earth--stuff like that. This is the sort of thing that fills the opening chapters of Peter Singer and August Cole's Ghost Fleet. [1] The catastrophes I always imagine, however, are a bit different than this. The hacking campaigns I envision would be low-key, localized, and fairly low-tech. A cyber-ops campaign does not need to disable key weapon systems to devastate the other side's war effort. It will be enough to increase the fear and friction enemy leaders face to tip the balance of victory and defeat. Singer and company are not wrong to draw inspiration from technological change; nor are they wrong to attempt to imagine operations with few historical precedents. But that isn't my style. When asked to ponder the shape of cyber-war, my impulse is to look first at the kind of thing hackers are doing today and ask how these tactics might be applied in a time of war.

Mark Cancian thinks like I do.

In a report Cancian wrote for the Center for Strategic and International Studies on how great powers adapt to tactical and strategic surprise, Cancian sketched out twelve "vignettes" of potential technological or strategic shocks to make his abstract points a bit more concrete. Here is how Cancian imagines an "asymmetric cyber-attack" launched by the PRC against the United States Military:

The U.S. secretary of defense had wondered this past week when the other shoe would drop. Finally, it had, though the U.S. military would be unable to respond effectively for a while. The scope and detail of the attack, not to mention its sheer audacity, had earned the grudging respect of the secretary. Years of worry about a possible Chinese "Assassin's Mace"-a silver bullet super-weapon capable of disabling key parts of the American military-turned out to be focused on the wrong thing.

The cyber attacks varied. Sailors stationed at the 7th Fleet' s homeport in Japan awoke one day to find their financial accounts, and those of their dependents, empty. Checking, savings, retirement funds: simply gone. The Marines based on Okinawa were under virtual siege by the populace, whose simmering resentment at their presence had boiled over after a YouTube video posted under the account of a Marine stationed there had gone viral. The video featured a dozen Marines drunkenly gangraping two teenaged Okinawan girls. The video was vivid, the girls' cries heart-wrenching the cheers of Marines sickening And all of it fake. The National Security Agency's initial analysis of the video had uncovered digital fingerprints showing that it was a computer-assisted lie, and could prove that the Marine's account under which it had been posted was hacked. But the damage had been done.

There was the commanding officer of Edwards Air Force Base whose Internet browser history had been posted on the squadron's Facebook page. His command turned on him as a pervert; his weak protestations that he had not visited most of the posted links could not counter his admission that he had, in fact, trafficked some of them. Lies mixed with the truth. Soldiers at Fort Sill were at each other's throats thanks to a series of text messages that allegedly unearthed an adultery ring on base. The variations elsewhere were endless. Marines suddenly owed hundreds of thousands of dollars on credit lines they had never opened; sailors received death threats on their Twitter feeds; spouses and female service members had private pictures of themselves plastered across the Internet; older service members received notifications about cancerous conditions discovered in their latest physical.

Leadership was not exempt. Under the hashtag # PACOMMUSTGO a dozen women allegedly described harassment by the commander of Pacific command. Editorial writers demanded that, under the administration's "zero tolerance" policy, he step aside while Congress held hearings. There was not an American service member or dependent whose life had not been digitally turned upside down. In response, the secretary had declared "an operational pause," directing units to stand down until things were sorted out.

Then, China had made its move, flooding the South China Sea with its conventional forces, enforcing a sea and air identification zone there, and blockading Taiwan. But the secretary could only respond weakly with a few air patrols and diversions of ships already at sea. Word was coming in through back channels that the Taiwanese government, suddenly stripped of its most ardent defender, was already considering capitulation.

How is that for a cyber-attack?

A few points should be made about the tactics of this sort of campaign. Consider a tactical option not included in this vignette, but one whose utility has been proven time and again in the real world: swatting. To swat properly, all you would need is a name, an address, and a way to place a phone-call. Swatting is limited in some ways. It is unlikely to kill its targets. Only a few targets living in one jurisdiction could be swatted at one time, as SWAT teams are a limited resource. And you can really only target the same family once; first responders remember places that have been swatted. But there are unique advantages to this sort of thing. Unlike, say, an assassination campaign, swatting could be used to target fairly high-level leadership (say, the NSC lead for Asia, the director of the DIA, or more locally, the commander of a place like Joint-Base Pearl Harbor-Hickham) without putting said leadership in the sort of danger that would call for lethal retaliation in your own capital. On the other hand, if your operational doctrine calls for the assassination of enemy political and military leaders from the outset (as, say, the People Liberation Army's plans for any attack on Taiwan requires), then swatting leaders who are unlikely to be caught up in the first round of attacks would be an efficient way to sow as much chaos as possible. [3]

Sowing chaos is not a goal sought for its own sake. Swatting would be most effective if conducted as part of a broader campaign. If the purpose is to distract the enemy before a surprise invasion, as Cancian's scenario imagines, then it probably would not be wise to go all-out on all fronts a week before zero-hour. That would simply tip the enemy off that an attack is coming. A more subtle and targeted approach would be more

appropriate there. On the other hand, if the goal is to throw a spanner in the enemy OODA loop and throw up as much friction as possible once more traditional military operations have begun, then there would be little reason for restraint. This would be particularly true if participants imagined that the war hinged on a "decisive" campaign fought over a short time period (the PLA's belief that the fight for Taiwan will be won or lost in the first two weeks of fighting is a good candidate here). [4] An alternate rationale for extensive swatting in the lead up to a general attack would be to wear down and overtax the enemy's emergency response systems, who would not enter the coming war or battle in a state of readiness. Finally, a swatting campaign, especially if conducted in tandem with other attacks of a similar nature, could have a demoralizing effect on both the citizenship and the leadership of the enemy. The effect on the leadership is especially interesting to contemplate. Obviously decision making will be hampered if important decision-makers have to spend time in a crisis convincing policemen that there is actually no hostage crisis in their house, finding a way to pay for lunch now that their credit cards don't work, or investigating the rape threats being sent to their teenage daughters' Instagram. Less clear is how psychologically damaging this might be. The political and military leaders of many countries are not used to having their families targeted in times of war. It may very well break their nerve--especially on the short term. In the long term, however, it will likely just embitter enemy leadership and give them a very personal reason to stay committed to the fight.

The good news in all this is that some of these things can be mitigated against. This mode of thinking comes easy to me partly because I follow digital privacy and security blogs and researchers closely. They spread stories of this sort around like 7th grade girls spread rumors. The best of them also share tips on how to protect your family against many of these attacks. My favorites are Michael Bazzell and Justin Carroll, authors of the Privacy and Security Desk Reference vol I and vol II, and hosts of the Privacy and Security Podcast. My hope is that the broader world of federal employees can become familiar with these guys and their tribe. They cannot help with all of scenarios Cancian or I can come up with, but they can help with some of them. For example, if the idea of waking up tomorrow and discovering that PLA hackers have borrowed hundreds of thousands of dollars in your name scares you, Bazzell's guide on how to implement a credit freeze is worth your time.

A final parting thought. It is trivially easy to find an American's address, ruin their credit score, steal their investments, use their social media or email accounts against them, and generally ruin someone's life through digital means. America's two greatest rivals (Russia and China) do not hesitate to harass, beat up, or intimidate American personnel. But stories of this type are very rare. Why is this? It isn't because they lack the capacity. They have it now. If they are not regularly harassing Americans today, it most likely because they do not want Americans to be better prepared for the conflict of tomorrow.”

4. Opinião sobre o texto

Concordo com o texto, quando se pensa em hackers logo se associa a algo extremamente tecnológico, como se um ataque de hackers fosse ser um desastre global cheio de tecnologias desconhecidas, mas na verdade não é nada disso. Um

ataque feito por hackers é algo que poucos podem notar que foi um ataque, a não ser que seja anunciado, como uma notícia falsa se espalhando de uma fonte confiável, alguém acessando arquivos privados, editando arquivos e vídeos, fazendo transações em seu nome.

O nível de ataque hacker vai desde alguém acessando uma foto sua, até o nível de acessar seu cartão de crédito, sua conta no banco. E assim seria uma guerra de hackers, acessando dados privados de seus inimigos para próprio benefício, manipulando sua imagem, roubando seus segredos e cortando seus recursos, mas não seria algo brutal e tecnológico como muitos pensam.