Breaking Your Own Encryption

Felix Herrmann

July 23, 2017
What happened?

- Let me tell you a story
What happened?

- Let me tell you a story
- My whole disk is encrypted
What happened?

- Let me tell you a story
- My whole disk is encrypted
- And I forgot my password
What happened?

- Let me tell you a story
- My whole disk is encrypted
- And I forgot my password
- But I had backups!
What happened?

- Let me tell you a story
- My whole disk is encrypted
- And I forgot my password
- But I had backups!
- Encrypted...with the same password
What happened?

- Let me tell you a story
- My whole disk is encrypted
- And I forgot my password
- But I had backups!
- Encrypted...with the same password
- This is what I forgot: f9tg#7f=<Ihe$1S-kK*1
Linux and files, devices, partitions

- A lot of things behave like files
Linux and files, devices, partitions

- A lot of things behave like files
- A disk is a file. /dev/sdX
Linux and files, devices, partitions

- A lot of things behave like files
- A disk is a file. /dev/sdX
- A partition is a file. /dev/sdX1, /dev/sdX2, ...
A lot of things behave like files
A disk is a file. /dev/sdX
A partition is a file. /dev/sdX1, /dev/sdX2, ...
To get the data, mount /dev/sdX1 to some folder
A lot of things behave like files
A disk is a file. /dev/sdX
A partition is a file. /dev/sdX1, /dev/sdX2, ...
To get the data, mount /dev/sdX1 to some folder
Example: `mount /dev/sdc1 /home/felher`
My Encryption

EFI-Boot Partition

LUKS Header

Encrypted Data

/dev/sdc

/dev/sdc1

/dev/sdc2

/devmapper/crypted
The LUKS Header (kinda)

<table>
<thead>
<tr>
<th>Cipher</th>
<th>VHash</th>
<th>ItCountV</th>
<th>SaltV</th>
</tr>
</thead>
<tbody>
<tr>
<td>SaltK</td>
<td>ItCountK</td>
<td>Key Offset</td>
<td></td>
</tr>
</tbody>
</table>

Encrypted Master Key

- Use SaltK + ItCountK + Password to derive KeyKey
- Use KeyKey to decrypt the master key
- Use ItCountV + SaltV + master Key to derive VHash
- Check if Equal
Let’s Crack

1. generate possible passwords
2. let `hashcat` try them agains LUKS
Possible passwords

```scala
def gen(str: Str, Δ: Int): List[Str] = 
  if (Δ == 0) List(str)
else str match {
  case Nil => List()
  case x::Nil =>
    if (Δ == 1) chars.map(c => List(c)) else List()
  case x1::x2::xs => {
    val rt = gen(x2::xs, Δ - 1)
    rt ++
    gen(x2::xs, Δ).map(l => x1::l) ++
    gen(x1::xs, Δ - 1).map(l => x2 :: l) ++
    chars.flatMap(c => rt.map(l => c :: l)) ++
    chars.flatMap(c => rt.map(l => c :: x1 :: l))
  }
}
```
Running HashCat

```
hashcat -m 14600 enc.luks_schenker/tmp/list \
    --gpu-temp-disable -w 3
```
And after 5 hours

\[ f_{9tg#7f} = <Ihe$lS-kK*1 \]