Hack.lu 2005 - The Crypto Challenge

Claus R. F. Overbeck - RedTeam Pentesting
claus.overbeck@redteam-pentesting.de
http://www.redteam-pentesting.de

20th October 2006
Introduction

- Crypto challenge as part of last years *Capture The Flag (CTF)* contest
- Based on a cipher by Peter Thoemmes (thank you for the nice challenge!)
  - weakened for the contest (so don’t blame him!)
- Uses 4 byte symmetric key
The Task

What you have:

- You have the plain text  "***This is the ..."
- You have the cipher text  "F8 72 C2 51 AA 05 82 21 ..."
- You have the software (encrypt/decrypt) and its source

What you want:

- Find the key! (So you can decrypt other protected material)
First Attempt: Brute Force I

Idea: Write a perl script that tries all keys:

```perl
#!/usr/bin/perl
for ($i=1 ; $i<4294967295 ; $i++){
    $key=printf("%.8x",$i);  # change to hex
    if (!`./pitcrypt -k $key -d in.crypt | diff - plain.txt -q`) {
        print "We found the key!: ", $key;
    }
    print "Tried another key. Just tried key $key.\n"
}
```
How long will this run?

47.5 sec for 500 keys.
$2^{32}$ possible keys = 4, 294, 967, 296
⇒ $\approx 408021893$ seconds
⇒ $\approx 6800364$ minutes
⇒ $\approx 113339$ hours
⇒ $\approx 4722$ days
⇒ $\approx 12.9$ years
⇒ $\approx$ too long for a CTF!
Wow, only 13 years, ain’t that fast?

To give you an idea: I will be 40 by then :-)

Photo: Nico van Geldere, Apeldoorn, Holland, wikipedia.org - GNU-FDL.
Second Attempt: Analyse the cipher

Byte-wise XOR

plaintext . . . . .

\text{XOR}

key \rightarrow \text{key stream} . . . . . .

= 

\text{ciphertext} . . . . . .

⇒ 

- Plain text, cipher text and key stream always have the same length.
- We can get the keystream by XORing plain and cipher text.
- We can encrypt and decrypt documents up to the length of the key stream. ⇒ We don't need the key!
Second Attempt: Analyse the cipher

Byte-wise XOR

\[
\begin{align*}
\text{PLAINTEXT} & \quad . \quad . \quad . \quad . \quad . \\
\text{XOR} & \\
\text{CIPHERTEXT} & \quad . \quad . \quad . \quad . \quad . \\
\Rightarrow & \\
\text{Key} & \quad \rightarrow \quad \text{KEY STREAM} & \quad . \quad . \quad . \quad . \quad . \\
\Rightarrow & \\
\quad & \quad \text{Plain text, cipher text and key stream always have the same length.} \\
\quad & \quad \text{We can get the keystream by XORing plain and cipher text.} \\
\quad & \quad \text{We can encrypt and decrypt documents up to the length of the key stream.} \quad \Rightarrow \quad \text{We don't need the key!}
\end{align*}
\]
Second Attempt: Analyse the cipher

Byte-wise XOR

\[
\begin{align*}
\text{PLAINTEXT} & \cdot \cdot \cdot \\
\text{XOR} & \cdot \\
\text{CIPHERTEXT} & \cdot \cdot \cdot \\
\Rightarrow & \\
\text{Key} \rightarrow & \text{KEYSTREAM} \cdot \cdot \cdot \\
\Rightarrow & \\
\end{align*}
\]

- Plain text, cipher text and key stream always have the same length.
- We can get the keystream by XORing plain and cipher text.
- We can encrypt and decrypt documents up to the length of the key stream. \(\Rightarrow\) We don’t need the key!
Second Attempt: Analyse the cipher

How is the keystream calculated? (Read the source)

- Every byte of the keystream is calculated from the last four bytes.
- \[ \Rightarrow \] We only need the first four bytes of the stream.
- We get those with: plain text XOR cipher text
- We can encrypt and decrypt documents with any length
Now, what about the real key???

Idea: Do it the C++ way:

- Use the source and change it to try keys (Rewrite main() function)
- Do not write to disk.
- Only encrypt/decrypt 4 bytes and compare
How long will this run?

50 sec for 10,000,000 keys.
$2^{32}$ possible keys = 4, 294, 967, 296
⇒≈ 21.474 seconds
⇒≈ 358 minutes
⇒≈ 5, 9 hours

Key is: 99343628 (Maybe it is just a collision?)
Conclusion

What we learned:

- You don’t need to be a math genius to crack a cipher.
- There might be several approaches.
- If you want to do some math you could also try to reverse the key stream function. (Left for you as an exercise ;-)

Claus R. F. Overbeck RedTeam Pentesting

Hack.lu 2005 - The Crypto Challenge
Questions?

(If there is still time left...)