Didier Stevens

Friday 1 January 2016

XOR Known-Plaintext Attack

Filed under: Encryption,My Software — Didier Stevens @ 16:00

To celebrate my Microsoft MVP award 2016, I’m releasing a new XOR-tool. Because you can never have enough XOR-tools in your toolbox 🙂.

When data is XOR-encrypted with a repeating key and you known some of the plaintext, you can perform a simple known-plaintext attack. Because when you XOR the ciphertext with the plaintext, you recover the key-stream.

With “repeating key” I mean the following: let’s assume that the encryption key is “Secret”. Then the first byte of the plaintext is XORed with “S”, the second byte with “e”, the third byte with “c”, …, the sixth byte with “t”. And for the seventh byte, we start again with “S”, then for the eighth byte again with “e”, …

When we know some of the plaintext, for example the beginning of the file, and we XOR this with the ciphertext, we obtain the key-stream: SecretSecretSecretSec It’s simple to extract the repeating key (Secret).

I’ve written a small Python program that automates this process: xor-kpa.py.

As an example, I’ve XORed the notepad.exe program with a key. We know that PE files contain the string “This program cannot be run in DOS mode”, this string is store in text file plaintext.txt. This is how you use xor-kpa:

```
C:\Demo>xor-kpa.py -e 3 plaintext.txt notepad-ciphertext.exe
Key:        Password
Extra:      30
Keystream: rdPasswordPasswordPasswordPasswordPass
```

This result shows that the recovered keystream is “rdPasswordPasswordPasswordPasswordPass”, and that the repeating key is “Password”. Extra (30) is the difference between the keystream length (38) and the key length (8). The higher the value of extra is, the higher the confidence is we recovered the correct key. When Extra is only 1, the confidence is low. To properly recover the key, the known-plaintext must be longer than the key.

With option -e you can filter for the minimum value of Extra.

Since the known-plaintext can often be a a short ASCII string, you can provide it directly as an argument in stead of writing it in a text file. To achieve this, just precede the argument with character #, like in this example (the double quotes are necessary because of the space characters):

```
C:\Demo>xor-kpa.py -e 3 "#This program cannot be run in DOS mode" notepad-ciphertext.exe
Key:        Password
Extra:      30
Keystream: rdPasswordPasswordPasswordPasswordPass
```

xor-kpa_V0_0_1.zip (https)
MD5: 4265BB1AFCD470A98070FFBDFCB1B52A
SHA256: CF41CEDE7281459FA47061B366AA9B4A5F579CC9BA46E73098B52EA8CAB6E816

2 bloggers like this.

Related

Update: XORSearch Version 1.9.2
In "Forensics"

XORSearc
Embedde
In "My Soft

Engineering"

Follow “Didier Stevens”

Get every new post delivered to your Inbox.

Join 359 other followers

Enter your email address

Sign me up

Build a website with WordPress.com

Leave a Comment

Leave a Comment »

No comments yet.

RSS feed for comments on this post. TrackBack URI

Leave a Reply (comments are moderated)

Enter your comment here...

- ## BruCON Spring Training 2016

  2-day Training Analysing Malicious Documents

- ## Didier Stevens Labs

  Visit my company, Didier Stevens Labs

- ## Pages

  - About
  - Didier Stevens Suite
  - Links
  - My Software
  - Professional
  - Programs
    - Ariad
    - Authenticode Tools
    - Binary Tools
    - CASToggle
    - Disitool
    - EICARgen

        - ExtractScripts
        - FileGen
        - HeapLocker
        - Network Appliance Forensic Toolkit
        - Nokia Time Lapse Photography
        - oledump.py
        - OllyStepNSearch
        - PDF Tools
        - Shellcode
        - SpiderMonkey
        - Translate
        - USBVirusScan
        - UserAssist
        - VirusTotal Tools
        - XORSearch & XORStrings
        - YARA Rules
        - ZIPEncryptFTP
    - Public Drafts
        - Cisco Tricks
    - Reverse Engineering Mentoring
    - Screencasts & Videos
- Search

- ## Top Posts

    - Howto: Make Your Own Cert With OpenSSL on Windows
    - Howto: Make Your Own Cert With OpenSSL
    - PDF Tools
    - XOR Known-Plaintext Attack
    - Howto: Add a Digital Signature to Executables

- ## Categories

    - .NET
    - 010 Editor
    - Announcement
    - Arduino
    - bpmtk
    - Certification
    - Didier Stevens Labs
    - Eee PC
    - Encryption
    - Entertainment
    - Fellow Bloggers
    - Forensics
    - Hacking
    - Hardware
    - maldoc
    - Malware
    - My Software
    - N800
    - Networking
    - Nonsense
    - nslu2
    - OSX
    - PDF
    - Personal
    - Physical Security
    - Poll
    - Puzzle

-
    - Quickpost
    - Reverse Engineering
    - RFID
    - Shellcode
    - smart card
    - Spam
    - technology
    - UltraEdit
    - Uncategorized
    - Update
    - Vulnerabilities
    - WiFi
    - Windows 7
    - Windows 8
    - Windows Vista
    - Wireshark
- XML

- ## Blog Stats

    - 3,590,224 hits

- ## Twitter @DidierStevens

    - Extracting PE file from .XLS file used in recent Ukrainian news media and electric industry attacks. https://t.co/P7WygE8RrF 11 hours ago
    - RT @virusbtn: At SANS ISC, @DidierStevens explains how to use his emldump tool to analyse MIME files isc.sans.edu/diary/A+Tip+Fo… 12 hours ago
    - New blog post "Update: shellcode2vba.py Version 0.4" blog.didierstevens.com/2016/01/02/upd… 17 hours ago
    - New blog post "XOR Known-Plaintext Attack" blog.didierstevens.com/2016/01/01/xor… 1 day ago
    - RT @__apf__: this is the most amazing YouTube channel... folk dancing to demo sorting algorithms youtube.com/watch?v=XaqR3G… https://t.co/ArEeu… 2 days ago

- ## Archives

    - January 2016
    - December 2015
    - November 2015
    - October 2015
    - September 2015
    - August 2015
    - July 2015
    - June 2015
    - May 2015
    - April 2015
    - March 2015
    - February 2015
    - January 2015
    - December 2014
    - November 2014
    - October 2014
    - September 2014
    - August 2014
    - July 2014
    - June 2014
    - May 2014
    - April 2014

- March 2014
- February 2014
- January 2014
- December 2013
- November 2013
- October 2013
- September 2013
- August 2013
- July 2013
- June 2013
- May 2013
- April 2013
- March 2013
- February 2013
- January 2013
- December 2012
- November 2012
- October 2012
- September 2012
- August 2012
- July 2012
- June 2012
- May 2012
- April 2012
- March 2012
- February 2012
- January 2012
- December 2011
- November 2011
- October 2011
- September 2011
- August 2011
- July 2011
- June 2011
- May 2011
- April 2011
- March 2011
- February 2011
- January 2011
- December 2010
- November 2010
- October 2010
- September 2010
- August 2010
- July 2010
- June 2010
- May 2010
- April 2010
- March 2010
- February 2010
- January 2010
- December 2009
- November 2009
- October 2009
- September 2009
- August 2009
- July 2009
- June 2009
- May 2009
- April 2009
- March 2009
- February 2009
- January 2009

  - December 2008
  - November 2008
  - October 2008
  - September 2008
  - August 2008
  - July 2008
  - June 2008
  - May 2008
  - April 2008
  - March 2008
  - February 2008
  - January 2008
  - December 2007
  - November 2007
  - October 2007
  - September 2007
  - August 2007
  - July 2007
  - June 2007
  - May 2007
  - April 2007
  - March 2007
  - February 2007
  - January 2007
  - December 2006
  - November 2006
  - October 2006
  - September 2006
  - August 2006
  - July 2006
  - June 2006

-

January 2016

M	T	W	T	F	S	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

« Dec

The Rubric Theme. *Blog at WordPress.com.*