Misc 总结 ----隐写术之图片隐写(三)

M1n3 / 2017-12-26 09:19:43 / 浏览数 11109 安全技术 CTF 顶(0) 踩(0)

实验简介

隐写术是关于信息隐藏,即不让计划的接收者之外的任何人知道信息的传递事件(而不只是信息的内容)的一门技巧与科学。英文写作Steganography,而本套教程内容将

实验内容

本次图片隐写实验包括四大部分

- 一、附加式的图片隐写
- 二、基于文件结构的图片隐写
- 三、基于LSB原理的图片隐写
- 四、基于DCT域的JPG图片隐写
- 五、数字水印的隐写
- 六、图片容差的隐写

第三部分 基于LSB原理的图片隐写

实验环境

- 操作机: Windows XP
 - 实验工具:
 - Stegsolve
 - Python
 - Java环境 ## 背景知识 什么是LSB隐写?

LSB, 最低有效位, 英文是Least Significant Bit

。我们知道图像像素一般是由RGB三原色(即红绿蓝)组成的,每一种颜色占用8位,0x00~0xFF,即一共有256种颜色,一共包含了256的3次方的颜色,颜色太多,而人的 Stegosolve介绍

CTF中,最常用来检测LSB隐写痕迹的工具是Stegsolve,这是一款可以对图片进行多种操作的工具,包括对图片进行xor,sub等操作,对图片不同通道进行查看等功能。

简单的LSB隐写

实验

- **IIIIIII**chal.png
- -----
- Stegsolve
- **BESSELLE SELLE**flag
- ■■■flag■flag:key{forensics_is_fun}

用Stegsolve打开图片,并在不同的通道中切换,

flag是flag:key{forensics_is_fun}

思考

- 1. 我们如何实现这种LSB隐写的?是否可以通过photoshop这样的工具实现?
- 2. 查阅更多关于LSB隐写的资料。

有一点难度的LSB隐写

我们从第一个部分可以知道,最简单的隐写我们只需要通过工具Stegsolve切换到不通通道,我们就可以直接看到隐写内容了,那么更复杂一点就不是这么直接了,而是只能

- **IIIIIII**LSB.bmp
- ----

- Stegsolve
- ----
- -----
- **IIIIIIIIIIIIIIIIIIIII**flag

首先:从Stegsolve中打开图片

首先点击上方的FIle菜单,选择open,在题目文件夹中找到这次所需要用的图片whereswaldo.bmp

其次:切换到不同通道,通过痕迹来判断是否是LSB隐写

分析是否有可能是LSB隐写,我们开始点击下面的按钮,切换到不同通道,我们逐渐对比不同通道我们所看到的图片是怎么样子的。 我们发现在Red plane0和Greee plane 0以及B略 plane 0出现了相同的异常情况,我们这里基本可以断定就是LSB隐写了

编写代码提取信息

因为是LSB隐写,我们只按位提取RGB的最低位即可,代码如下:

```
from PIL import Image
im = Image.open("extracted.bmp")
pix = im.load()
width, height = im.size
extracted_bits = []
for y in range(height):
   for x in range(width):
      r, g, b = pix[(x,y)]
       extracted_bits.append(r & 1)
       extracted_bits.append(g & 1)
       extracted_bits.append(b & 1)
extracted_byte_bits = [extracted_bits[i:i+8] for i in range(0, len(extracted_bits), 8)]
with open("extracted2.bmp", "wb") as out:
   for byte_bits in extracted_byte_bits:
              byte_str = ''.join(str(x) for x in byte_bits)
       byte = chr(int(byte_str, 2))
       out.write(byte)
```

打开我们需要提取信息的的图片,y,x代表的是图片的高以及宽度,进行一个循环提取。运行代码,extracted.py,打开图片即可。

思考

- 1. 我们这里用的LSB隐均对R,G,B,三种颜色都加以修改是否可以只修改一个颜色?
- 2. 参考2016 HCTF的官方Writeup学习如何实现将一个文件以LSB的形式加以隐写。

归档.zip (0.624 MB) <u>下载附件</u>

点击收藏 | 0 关注 | 0

上一篇:关于禅道9.1.2最新版免登陆SQ... 下一篇: PHP安全新闻早八点-高级持续渗透...

1. 14 条回复



wooyun 2017-12-26 10:17:58



hades 2017-12-26 10:34:41

动动手指,沙发就是你的了

0 回复Ta



wahaha_a 2017-12-26 14:54:26

学习学习!

0 回复Ta



<u>老锥</u> 2018-01-23 16:31:15

支持



<u>1815837370479554</u> 2018-05-29 13:57:33

学习 学习

0 回复Ta



wuq****@126.com 2018-07-21 08:31:10

很好

0 回复Ta



<u>Oaspir1ng0</u> 2018-07-22 21:22:08

非常想详细啊,一下子看懂了Isb怎么检测



1997CN 2019-03-20 09:54:54

支持一下子,很详细了,最近在总结,学习一下~

0 回复Ta



tulne**** 2019-05-06 22:27:20

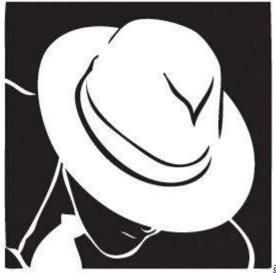
很详细的介绍

0 回复Ta



<u>朱元璋好帅</u> 2019-07-10 20:28:14

正在以这四部曲为基础学习misc隐写



azure**** 2019-09-01 00:33:33

感谢分享

0 回复Ta



<u>川上日111</u> 2019-09-26 10:25:08

新人求教:那个extracted.py我也复制出来了,然后执行图片也打开了,但是并没有找到flag啊?

0 回复Ta



t_1505312495641_ 2019-10-08 16:42:25

感谢大佬



shutdown r 2019-11-18 06:14:43

我这边图片不显示了

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS <u>关于社区</u> 友情链接 社区小黑板