

看雪.纽盾 KCTF 2019 Q2 | 第七题点评及解题思路

KCTF 看雪学院 7月2日

时光匆匆，不知不觉间已经迈入了七月，我们一路相伴，经过KCTF精彩激烈的比拼，之后又对赛题依次进行了详细的点评和思路分析，不知道看过题目解析的你有没有感到豁然开朗呢？

今天解析的这道题就厉害了，截至比赛结束时无人攻破。废话不多说，下面就让我们来看下第七题，一起斗智斗勇，看看如何去化解部落冲突！

题目简介

题目背景：

经过几天几夜的奋战，双眼已经开始不听使唤，不停的往下掉。终于，世界变成一片黑暗，思想变得虚无。待双眼睁开，白光闪进双眼，只见一个和你相同模样的人正在你的面前仔细端详着你。

“你是谁？”

“我是你”

空气中开始回荡起一阵阴森诡异的笑声.....有一个守护宝石的部落出现在你面前，首领长老叫司看。那个和你长得一样的，是部落里的一位勇士，名叫狂场，勇猛善战。他身后站着一个女巫，斜挎着一个兽皮袋，名叫暴风雪，擅长设置机关和控制天气。

在这个自由的世界里，部落之间经常发生冲突。冲突来临时，他们各有分工。狂场是场上队长，带领着勇士们冲锋陷阵。暴风雪会在开仗之前，先在战场上布下机关，并且在战争过程中通过控制天气来引导狂场正确走位。

如果走位正确，就能毫发无伤；如果走位错误，肯定要被射成刺猬。但是，暴风雪自身很脆弱，一旦被敌人发现就非常危险。所以她通常隐匿在战场的某个角落。而司看的任务就是：监督狂场严格听从天气的指示，禁止狂场回头看暴风雪，以免暴露她隐藏的位置。

狂场已经等了你很久了。能否拿到宝石，就看你的走位了。



本题共有1840人围观，截至比赛结束没有人能攻破此题。是第二赛段难度最高的一道题。

看雪评委crownless点评

“部落冲突”这道题模拟了一个正版软件，假设攻击方花钱购买了这个软件，并获得了一个正确序列号，然后这个攻击者想求出另外一个用户的正确序列号。分析向量表和散列值的叠加结果的随机性，是此题的解题线索。

出题团队简介

本题出题战队 **中娅之戒**：



再拜各位大佬！

本次2019KCTF Q2的中娅之戒由三名队员组成：

Venessa：仍旧被玄学击垮的密码学方向在读研(小)究(姑)生(娘)

loom：我只是一只小猫咪，我不应该为生活发愁.jpg

上海刘一刀：科锐31期4阶段学员，战队里话最多且技术最辣鸡的弟弟，写壳比较像cxk

//这里还有一些奇奇怪怪的资料↓

//<http://www.51asm.com/zuixindongtai/xueyuandongtai/2019/0702/247.html>

设计思路

“部落冲突”是一个模拟实战环境的CM。

模拟场景：攻击者得到了一组授权后，通过观察分析，使用相关技术推算得到另一组授权。

“部落冲突”是“七十二疑冢”的升级作品。

“七十二疑冢”考验的是攻击方的CRC算法能力。它选用了CRC校验作为基本运算，而CRC函数（在多项式意义下）是线性运算的，从而使得“七十二疑冢”能被高效破解。

为了进一步提高难度，“部落冲突”采用了哈希函数作为基本运算，而序列号就是依次序改变哈希函数种子的下标。算法如下：

上一轮种子经过哈希函数生成的散列值（256bit），叠加上由序列号指定的常向量（给定256个向量，每个向量256bit）计算出本轮迭代值，作为下一轮哈希的种子。

按照这样的规则迭代下去，直至穷尽序列号。如果最终计算结果得到全0序列（256bit），即为破解成功。或者说，要想正面攻克部落冲突本质上就是一个寻找弱碰撞的过程，其穷举难度很大。

如果把破解思路安排在hash碰撞上，太没意思，而且也是违规的。

作者安排的正确解法是什么呢？

“部落冲突”模拟了一个正版软件。

假设攻击方花钱购买了这个软件，并获得了一个（以狂场为用户名的）正确序列号，然后这个攻击者想求出另外一个用户（用户名为“你”）的正确序列号。

上述计算过程被包装成一个名为“部落冲突”的游戏。

要求解的序列号就是“你”的走位，只有成功躲开所有射击（中0箭）才能活着走出战阵（破解成功）。

而“你”不是唯一的玩家。游戏中已经有一名称做“狂场”的通关玩家，并且题干中已经显式给出了他的走位（已知一组正确序列号）。

通过分析“狂场”的走位，发现其中暗藏的规律，应当可以得到解题思路。

分析过程如下：

1) 观察狂场的走位，序列号本身并无特殊规律 --> 解题线索蕴藏于走位过程中。

2) 游戏的流程是单向进行的，每一轮迭代值由哈希算法迭代生成，不可逆推或跳过 --> 必须一步一步跟踪迭代结果。

3) 脱壳后最先可以看到256*256bit的向量表，看起来数据随机毫无规律（但作者是有机会在其中精心构造数据的） --> 作为用来叠加到散列值的向量，不太可能单独成为解题线索，所以攻击者不能抛开哈希函数和散列值单独分析向量表。

4) 哈希函数得到怎样的散列值，对于出题者来说也是难以控制（预测或构造）的，同时哈希函数因其特性可以作为伪随机数生成器（或伪随机数生成器的一部分） --> 散列值应当依概率满足伪随机序列的特点，因此也不能作为作者预埋解题线索的地方。

5) 结合3) 4) 分析，尽管向量表和散列值都看似随机，但根据计算流程，二者的叠加结果才是真正值得分析的，作者预留的解题线索只能在这个地方。

6) 如果此题的计算过程真的都是随机的，那么作者也难设计有效解法 --> 作者预埋的解题线索必然是“不随机”的。

所以，分析向量表和散列值的叠加结果的随机性，是此题的解题线索。

据此分析“狂场”的走位，使用经典的随机性检测方法*分别对迭代值进行随机性检测，会发现：每3步会出现一个“游程分布*”严重不随机的迭代值。

本题的随机性检测方法，基于 国家密码管理局发布的《GM/T 0005-2012 随机性检测规范》。

具体算法如下：

4.4.7 游程分布检测

a) 计算 $e_i = (n - i + 3) / 2^{i+2}$, $1 \leq i \leq n$, 并求出满足 $e_i \geq 5$ 的最大整数 k 。

5

GM/T 0005—2012

b) 统计待检序列 ε 中每一个游程的长度。变量 b_i, g_i 分别记录一个二元序列中长度为 i 的 1 游程和 0 游程的数目。

c) 计算 $V = \sum_{i=1}^k \frac{(b_i - e_i)^2}{e_i} + \sum_{i=1}^k \frac{(g_i - e_i)^2}{e_i}$ 。

d) 计算 $P\text{-value} = \text{igamc}(k-1, V/2)$ 。

e) 如果 $P\text{-value} \geq \alpha$, 则认为待检序列通过游程分布检测。

其中:

n 为待检测序列长度 (此题中 $n=256$)

igamc 为不完全伽马函数 (Incomplete Gamma Function)


本题中“狂场”的走位先后经过的迭代值及其游程分布检测 $P\text{-value}$ 值如下:

000:	BF F1 B3 A1 00	0.0000000000000000
001:	B1 A9 97 CC D0 8C F2 21 DF 70 4F 2E 93 0C 95 4A AE A5 46 05 59 57 5F 73 21 06 7F C8 3F 97 4C 25	0.1218268595980383
002:	8B 51 0C 4C 3B D2 72 0A 8B 41 08 03 C2 4C 3B D0 72 0F 41 FF C1 48 83 C1 28 45 3B CB 72 E2 33 C0	0.0227953575762776
003:	AA D2 6B 41 6E 1D 54 9F AB 7D E9 7A 95 6B 4D D5 55 28 DD DF 95 06 AF 6A AB AA AA D5 C0 A6 D9 8D	0.0000000000005602
004:	5F 12 B2 14 DB AE ED 7A A2 AB 42 DD 99 AA DB 8A 66 07 B9 52 27 B9 04 8E B7 E7 9F 60 40 29 00 3B	0.3886191346953774
005:	48 63 22 3C 47 03 C8 33 C0 81 39 50 45 75 0C BA 0B 02 00 66 39 51 18 0F 94 C0 45 33 C9 33 C0 C3	0.0131779319325869
006:	55 A6 E8 AD 42 CA FA AF AC 34 32 AA 0D 5F 6C 92 95 DD 6A FD A7 DA AB 4A BB 6B 68 FD AA B5 A1 7A	0.0000000000002456
007:	3F A5 86 99 6C 3B A5 D7 26 F6 FA 80 69 AE 90 CD 1A 9C 86 A7 1C A4 04 E9 5B 13 73 AA 2C A5 EE EB	0.0568732265771914
008:	48 83 EC 20 8B D9 33 C9 74 28 48 8B C8 E8 87 65 43 48 85 C0 74 1B B9 02 00 00 00 66 39 48 5C C3	0.0936249125865450
009:	57 2E B6 D5 35 A2 B5 1F 8A AA EA 15 5F 50 24 2B 57 F5 5A AF FD 45 55 DB 35 FF 6E 25 A8 95 AA A5	0.0000000000000025
010:	B1 A1 F3 7B 47 29 5F 1B 03 66 99 DF 9D 20 0D D7 F9 7E DC EF 63 6C D1 14 23 E0 98 98 52 62 2A D8	0.2618064777702203
011:	48 89 5C 24 08 48 89 6C 24 10 48 89 74 24 18 57 41 54 41 55 41 56 41 48 83 EC 20 33 FF 4C 63 E9	0.0004036533597940
012:	AA D5 67 DA 92 CC B4 24 A1 51 6A 36 4A 15 35 54 A1 B5 2B EB 25 F7 AE A6 D5 5F 29 3A A2 AE AA 22	0.0000000000005478
013:	8C 1C 26 4D B9 BE 01 B3 DD 8F 1F EA C3 76 D5 C1 91 5A 83 ED B3 42 B7 67 15 BB 19 7B 95 7B 5C 71	0.0224037205836325
014:	76 3F 74 65 22 2F 21 71 75 32 79 61 75 6F 36 2B 28 23 64 7C 2B 7C 77 22 60 6B 31 66 7C 38 7B C3	0.6777511045704474
015:	2A D0 A5 56 49 94 42 5E 52 12 AB 81 15 20 B2 56 50 2F 5A EA 95 CE BC AA 92 15 52 55 A0 4E 75 4A	0.0000000000003175
016:	AD 9B 0A 47 67 2D 57 97 83 52 EF 64 2C 0D B0 21 2F 90 BD 7A EA 53 DB 2A F7 16 1B 13 83 DE BA 8D	0.1491027395997713
017:	3D 2E 3F 24 62 33 77 6A 30 3F 7E 37 3C 7F 26 78 25 7A 61 20 63 2A 63 68 2E 78 29 35 3E 64 7B 31	0.0621546015447141
018:	52 AB A0 8D 54 AA A2 BA 16 88 90 67 12 89 3A 8B FA AA A9 55 15 11 6E 8E 2B A0 D9 51 71 52 2B C0	0.0000000000005624
019:	00 00	0.0000000000000000

第0步, 初始种子, 若以 %s 输出为“狂场”的汉字, 即玩家用户名;

第19步, 迭代值为全0序列 (中0箭, 中箭支数其实就是256bit序列中有多少个1), 为此题目标;

第3、6、9、12、15、18步 (即每隔3步) 所处迭代值及其游程分布检测 $P\text{-value}$ 值如下:

*向右滑动, 查看更多 

{ 0xAA, 0xD2, 0x6B, 0x41, 0x6E, 0x1D, 0x54, 0x9F, 0xAB, 0x7D, 0xE9, 0x7A, 0x95, 0x6B,

{ 0x55, 0xA6, 0xE8, 0xAD, 0x42, 0xCA, 0xFA, 0xAF, 0xAC, 0x34, 0x32, 0xAA, 0x0D, 0x5F,

{ 0x57, 0x2E, 0xB6, 0xD5, 0x35, 0xA2, 0xB5, 0x1F, 0x8A, 0xAA, 0xEA, 0x15, 0x5F, 0x50,

◀ [REDACTED] ▶

在得知了“游程分布不随机”这个线索之后，可以求解本题：

- 附“你”的正确走位各步迭代值的P-value:



1、随机性检测方法：

2、游程分布检测 (runs distribution test) :

END

- <https://mp.weixin.qq.com/s?biz=MjM5NTc2MDYxMw==&mid=2458297601&idx=1&sn=eff6731ed460967e5566e18269072893&chksm=b1819...> 8/10

- 3、看雪.纽盾 KCTF 2019 Q2 | 第二题点评及解题思路
- 4、看雪.纽盾 KCTF 2019 Q2 | 第三题点评及解题思路
- 5、看雪.纽盾 KCTF 2019 Q2 | 第四题点评及解题思路
- 6、看雪.纽盾 KCTF 2019 Q2 | 第五题点评及解题思路
- 7、看雪.纽盾 KCTF 2019 Q2 | 第六题点评及解题思路

主办方

看雪学院 (www.kanxue.com) 是一个专注于PC、移动、智能设备安全研究及逆向工程的开发者社区！创建于2000年，历经19年的发展，受到业内的广泛认同，在行业中树立了令人尊敬的专业形象。平台为会员提供安全知识的在线课程教学，同时为企业提供智能设备安全相关产品和服务。

合作伙伴

上海纽盾科技股份有限公司 (www.newdon.net) 成立于2009年，是一家以“网络安全”为主轴，以“科技源自生活，纽盾服务社会”为核心经营理念，以网络安全产品的研发、生产、销售、售后服务与相关安全服务为一体的专业安全公司，致力于为数字化时代背景下的用户提供安全产品、安全服务以及等级保护等安全解决方案。



[10大议题正式公布！第三届看雪安全开发者峰会重磅来袭！](#)



👉 小手一戳，了解更多



公众号ID: ikanxue

官方微博: 看雪安全

商务合作: wsc@kanxue.com

戳原文，查看更多精彩writeup!

阅读原文