

工控网络协议模糊测试：用peach对modbus协议进行模糊测试

[blacksunny](#)

2015-12-11



共590376人围观，发现 26 个不明物体

安全管理

工控安全

本文原创作者：blacksunny

0x00 背景

本人第一次在FB发帖，进入工控安全行业时间不算很长，可能对模糊测试见解出现偏差，请见谅。

在接触工控安全这一段时间内，对于挖掘工控设备的漏洞，必须对工控各种协议有一定的了解，然后对工控协议，首先具备的对网络识以及工控行业流程有所熟悉，其次就是对工控协议进行模糊测试。

0x01 模糊测试介绍

下面介绍一下模糊测试概念以及针对网络协议模糊测试的一些框架。

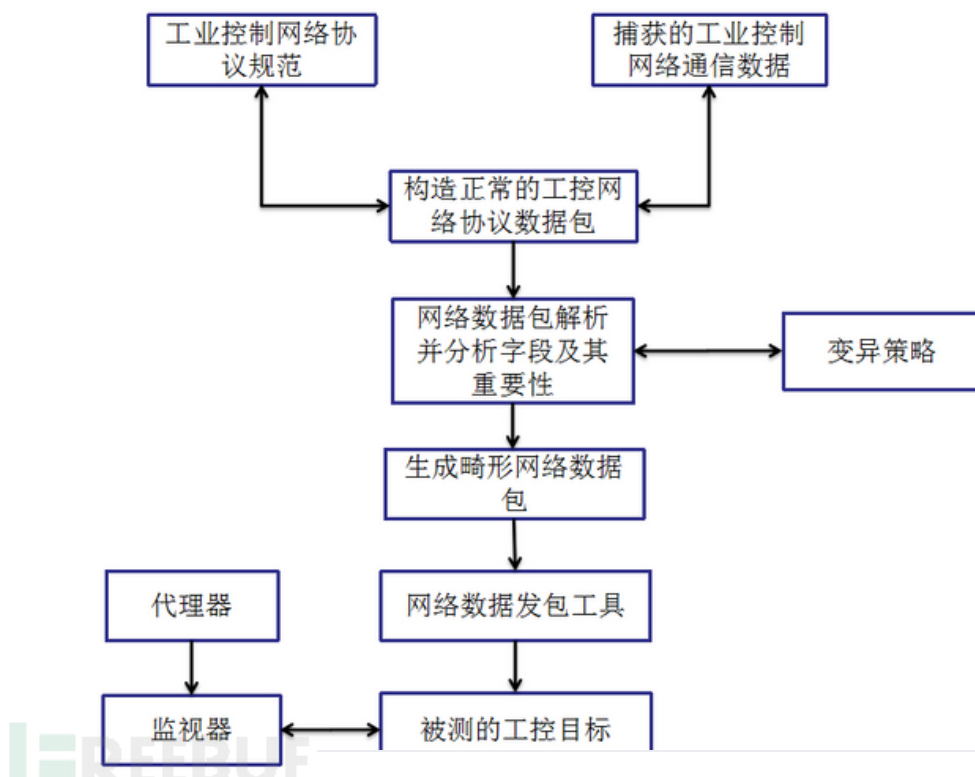
模糊测试就是通过非预期的输入并监视异常结果来发现软件故障的方法。（相对来说比较抽象，个人理解怕有偏差就不在此所描述了）。

针对模糊测试，目前已经开发了一些框架，这些框架统称为模糊器。常见的模糊测试器有sulley(在FB上面已经有人总结了，在此不说明)，Peach，SIPIKE（用在UNIX下）等。

0x02 工控协议安全分析

工业控制网络协议模糊测试的目的是测试工业控制网络协议的实现的健壮性，它是采用构造畸形数据包，将畸形数据包发送给被测工目标，从而测试被测工业控制网络协议的安全性。

下面是具体流程图：



流程图具体工作原理：

- 1、根据协议控制规范或者捕获工业控制网络协议数据流来构造正常的数据包；
- 2、分析正常协议的字段及其重要性；
- 3、根据分析的协议中不同的数据类型，设计有效地变异策略。
- 4、设计并实现工业控制网络协议数据包发包工具；
- 5、设计并实现代理器及监视器；
- 6、采用发包工具，将畸形数据包发送给被测工控目标；
- 7、通过监视器探测被测工控目标异常数据记录。

0x03 peach模糊测试

在研究网络协议模糊测试时，对sulley和peach两大框架都有所研究，依我个人而言，peach相对于sulley有以下几点优势：

- 1、sulley目前已不再维护。
- 2、对sulley模糊测试编写程序，需要有一定的python语言基础。而peach是xml格式的，比较容易理解。
- 3、sulley配置环境相对繁琐，而peach配置环境相对简单（目前我手头有绿色版本，可以直接运行）。
- 4、sulley只能对网络协议进行模糊测试，而peach相对更加多样化。

上面的工业控制网络协议流程图是建立在模糊测试的基础上的，下面针对讲解一些关于peach的模糊测试的知识，对于初学模糊测试必找资源而烦躁了。（目前peach框架的文档相对来说较少，下面讲解的是依据一些英文文档以及相关的博客总结的，如有不足之处，请指出）。

peach概述

Michael Eddington等人开发的peach是一个遵守MIT开源许可证的模糊测试框架，最初采用python编写的发布与2004年，第二版于2007年发布，最新的第三版使用C#重写了整个框架。

peach支持对文件格式、ActiveX、网络协议、API等进行Fuzz测试。

下载和安装

相对比较容易，在Window下使用peach3需要安装.net4和windbg；我用的是绿色版本。

下载地址：<http://pan.baidu.com/s/1eQ6XzyE>

peach基础知识

peach中最重要一部分就是peach Pit配置文件。Peach Pit文件包含以下内容：

- 1、General Configuration(通用配置)
- 2、Data Modeling (数据模型)
- 3、State Modeling (状态模型)
- 4、Agents and Monitors (代理和监视)
- 5、Test Configuration (测试配置)

具体编写步骤如下：

```
<?xml 版本, 编码之类?>
<Peach 创建时间, 地址, 作者等等>
<Include 包含外部文件 />
<DataModel> 类型信息, 关系 (大小, 计数, 偏移)、可嵌套等<\DataMode>
<StateModel>测试逻辑, 状态转换</StateModel>
<Agent>监视被测目标的情况, 崩溃信息等</Agent>
<Test>指定使用哪个StateModel, Agent, Publisher、Strategy、Logger等</Test>
</Peach>
```

这只是编写Peach Pit配置文件的简单步骤，里面涉及的属性很多，下面发出给出一个测试案例：

```
<?xml version="1.0" encoding="utf-8"?>
<Peach xmlns="http://peachfuzzer.com/2012/Peach" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://peachfuzzer.com/2012/Peach ../peach.xsd">
  <DataModel name="HttpRequest">
    <String value="Hello World!" />
  </DataModel>

  <StateModel name="TheStateModel" initialState="TheState">
    <State name="TheState">
      <Action type="output">
        <DataModel ref="HttpRequest" />
      </Action>
    </State>
  </StateModel>

  <!-- Agents that run locally will be started automatically by Peach -->
  <Agent name="RemoteAgent" location="tcp://192.168.1.190:9001">
    <Monitor name="Debugger" class="WindowsDebugger">
      <Param name="CommandLine" value="CrashableServer.exe 192.168.1.190 4242"/>
    </Monitor>

    <Monitor name="Network" class="PcapMonitor">
      <Param name="filter" value="tcp"/>
    </Monitor>
  </Agent>

  <Test name="Default">
    <Agent ref="RemoteAgent" />
    <StateModel ref="TheStateModel"/>

    <Publisher class="TcpClient">
      <Param name="Host" value="192.168.1.190" />
      <Param name="Port" value="4242" />
    </Publisher>

    <Logger class="Filesystem">
      <Param name="Path" value="Logs" />
    </Logger>
  </Test>
</Peach>
```

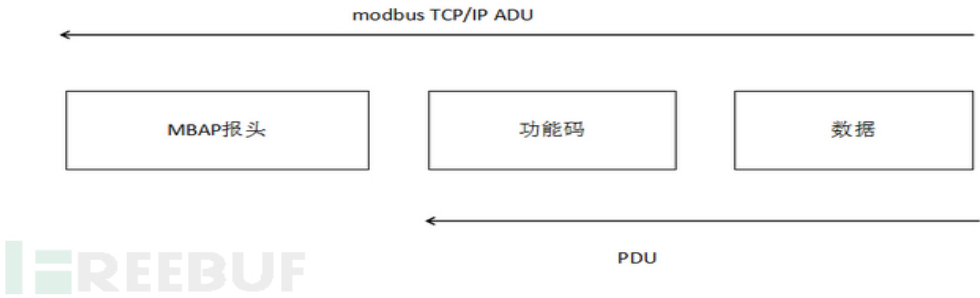
这是关于peach针对http协议模糊测试，具体步骤如图所标。具体属性不做介绍（详情见下面英文文档进行学习）。

这是peach框架模糊测试的英文文档下载地址：链接: <http://pan.baidu.com/s/1gdGyJZL> 密码: ibnc

0x04 peach模糊测试modbus工控协议

modbus是全球一个真正用于工业现场的总线协议，是公开的协议，协议报文格式比较简单。下面以modbus协议为例来讲解关于pea在工业控制协议方面的模糊测试。

modbus在TCP/IP通信数据报格式



MBAP报头字段如下：

modbus中1号功能码请求的报头格式：

由上面的报文格式可以组包为：00 01 00 00 00 06 01 01 00 00 00 01

对modbus协议可以组包之后通过peach框架编写Peach Pit配置文件：

在上图所示中，简单的描述了编写网络协议模糊测试的Pit文件。里面没有涉及到代理和监听还有调试功能（主要是工控设备目前不支持，仅我个人理解），在这里不是很懂的话，请详细了解peach的英文文档多加了解。其中的日志路径实际包含运行名字和时间戳。]到检测到一个故障信息，这些记录才会记录到磁盘空间。

下面是对01号功能码进行安全性测试过程，如图所示：

针对执行过程，通过wireshark抓包可以获取通信数据流量，如图所示：

上面的例子只是简单的运用peach框架对工控中modbus的一个使用。

0x05 总结

模糊测试技术是发现工业控制网络协议未知漏洞和隐患的重要技术。针对工业控制网络协议，在这里介绍了相关的工业控制协议模糊测试挖掘漏洞的流程图，以及对peach框架简单的介绍，还有对modbus协议如何组包以及如何编写peach pit文件对工业控制协议进行模糊测试实例。第一次发帖，可能讲的不是很好，如有新手想学习，可以给我留言，大神勿喷。

***原创作者：blacksunny，本文属FreeBuf原创奖励计划，未经许可禁止转载**

更多精彩

fuzz

工控安全

网络协议

上一篇：[霍尼韦尔Midas气体检测器被曝严重漏洞，再为工控安全敲响警钟](#)

下一篇：[2016企业安全9大技术趋势](#)

这些评论亮了



[mcgrady](#) (1级)

去年用sully对modbus协议做过fuzz测试，peach3和2也都玩过，作者有兴趣可以交流一下经验

回复

亮了(20)



LR

用啥做monitor

回复

亮了(12)



[blacksunny](#) (3级) 追求理想化

@ ameng929 我知道你，你是工控安全的前辈啊，求指教，能发私信吗

回复

亮了(17)



[ppmorning](#) (1级)

前面讲的都很清楚，最后有些不明白的地方，请问Peach是怎么进行模糊测试的呢？我看你是对NUM进行fuzz，你构造的NUM不就是00 01 吗，但是最后结果却是好多，他自+1迭代？你在CMD中输入的什么指令？

回复

亮了(10)



[blacksunny](#) (3级) 追求理想化

@ mcgrady 可以啊

回复

亮了(8)

已有 26 条评论

太君！不要	2015-12-11	1楼	回
您这里提到的是对安全协议的分析，有没有关于工控在实际安全测试时的一些技巧呢？在现实中工控安全出现疏漏和安全隐患的都集中在那些点上呢？求指教		亮了 (1)	
blacksunny_  (3级) 追求理想化	2015-12-11		1
@ 太君！不要			
这些其实说起来挺多的，我有时间了我整理一下关于这方面的资料，到时候发布一下吧		亮了	
LR	2015-12-11	2楼	回
用啥做monitor		亮了 (1)	
ameng929	2015-12-12	3楼	回
方便留个联系方式么		亮了 (1)	
blacksunny_  (3级) 追求理想化	2015-12-12		1
@ ameng929 我知道你，你是工控安全的前辈啊，求指教，能发私信吗		亮了	
败类_ (1级)	2017-08-30		1
@ ameng929 能给个联系方式吗		亮了	
mcgrady_ (1级)	2015-12-12	4楼	回
去年用sulley对modbus协议做过fuzz测试，peach3和2也都玩过，作者有兴趣可以交流一下经验		亮了 (2)	
blacksunny_  (3级) 追求理想化	2015-12-12		1
@ mcgrady 可以啊		亮了	
ppmorning_ (1级)	2015-12-15	5楼	回
前面讲的都很清楚，最后有些不明白的地方，请问Peach是怎么进行模糊测试的呢？我看你是对NUM进行fuzz，你构造的NUM不就是00 01 吗，但是最后结果却是好多他自+1迭代？你在CMD中输入的什么指令？		亮了 (1)	
芋儿骚 (1级)	2016-01-14	6楼	回
求指教阿。我们现在正在老师的项目里做modbus/tcp的fuzzing测试，卡住有一段时间了。能不能私信请教几个问题呢？		亮了 (1)	
flypuma_ (1级)	2016-09-20	7楼	回
异常监控是怎么做的？		亮了 (1)	

葱头的洋葱梦 (1级) 我发现我只要不换头像,我就变成了一个白帽子~ 2016-11-01	8楼 回
刚开始接触工控这个,文章中的绿色版的链接取消了,可以私信吗?	
还有关于配置文件的话,英文的文档还没看,所以配置文件的那个部分我没看懂,当然了,可能不是讲的不好,是我没有理解,不好意思.	亮了
PoseidonTrident (1级) 2016-11-08	9楼 回
最近也尝试了文中的方法,我遇到情况时精简Linux系统中不知道怎么放peach的agent,试了文中的方法,由于没有涉及到代理和监听还有调试功能,所以能够触发崩溃,但是对于崩溃点的分析,我看了peach生成的日志信息,我觉得对下一步的定位作用不大。	
所以我觉得重点还是放在如何在精简linux上运行agent,因为peach3系统基于C#,如果是linux系统运行peach3,则需要安装mono,对于完整版linux系统是可行的,但对于精简linux很难实现。	
大家有哪些好的思路可以聊聊。	亮了 (
PoseidonTrident (1级) 2016-11-08	10楼 回
@ LR 文中的说法是“里面没有涉及到代理和监听还有调试功能”,所以文中就没有做monitor,实际情况是,对于部分系统部署agent很困难,大家可以交流下。	亮了 (
rye_ (1级) 研究生方向: 工控安全。希望多交流,多学习 2017-05-02	11楼 回
前辈,能交流学习吗	亮了
小面 (1级) 2017-06-23	12楼 回
@ mcgrady 你好,请问我在电脑上用modbus SIM 和modbus scan 通信,用defensics等模糊测试工具能测吗? 希望得到回答	亮了
wuyong391 (1级) 2017-07-19	亮了
@ 小面 我们公司一直用Achilles测试的, defensics没用过	亮了
wuyong391 (1级) 2017-07-19	13楼 回
测试Modbus协议,完全可以使用成熟产品Achilles,测试用例Achilles都定义好了的	亮了 (
败类 (1级) 2017-08-30	14楼 回
工具链接取消了 绿色版本 还能从哪下载?	亮了 (
大海2288 (1级) 2017-11-17	15楼 回
加拿大Achilles工控测试平台 /Achilles认证 中国区代理商 达信通成科技有限公司 销售联系人: 田宝钢 联系电话: 13120102288	亮了 (
alwynhuang_ (1级) student, study on safety of i... 2018-01-12	16楼 回
前辈,能给个联系方式交流下吗,我这边想要使用peach针对车载网络进行一个模糊测试的研究。目前对peach那一块如何自定义monitor和publisher还不太了解。	亮了 (
blacksunny Z (3级) 追求理想化 2018-01-13	亮了
@ alwynhuang 私聊吧	亮了

- [lizhihui](#) (1级)

HI, 志在安全!

2018-01-27

17楼 [回](#)
- 前辈, 我想模糊测试一下工控协议, 怎么模拟通讯环境. 请指教一下。

亮了 (
- [一诺0000](#) (1级)

2018-03-24

18楼 [回](#)
- 里边的网盘链接不能用了, 可以私信发一下么?

亮了 (
- [canodon](#) (1级)

2019-04-10

19楼 [回](#)
- 怎么做异常监测的?

亮了
- [chenhao894471780](#) (1级)

2019-11-05

20楼 [回](#)
- @ mcgrady 联系方式 一起交流

亮了 (

选择文件

未选择任何文件

欢迎 [TideSec](#) 再次光临! [退出 >](#)


表情

插图

提交评论(Ctrl+Enter)

[取消](#)

☒ 有人回复时邮件通知我



[blacksunny](#)^z

追求理想化

3

文章数

42

评论数

最近文章

[MySQL绕过WAF实战技巧](#)

2017.12.04

[WiFi-Pumpkin无线渗透测试框架实战教程](#)

2017.06.29

[工控网络协议模糊测试：用peach对modbus协议进行模糊测试](#)

2015.12.11

浏览更多

- FINS协议格式及功能码简介
- beSTORM之网络协议Fuzz入门教程
- 2013黑帽大会：失控 — 针对工业SCA...
- 西门子集中修复了工控设备中的安全...
- 工控安全现场实施经验谈之工控系统...

推荐关注

FreeBuf+微信小程序

FreeBuf官方微信小程序，把安全装进口袋



扫码添加小程序

FreeBuf微信订阅号

国内领先的互联网安全新媒体，同时也是爱好者们交流与分享安全技术的社区



10月

公开课双十一活动

已结束

9月 上海

CIS 2019官网上线，早鸟票同步开售

已结束

9月 上海

CIS 2019「议题征集」启动

已结束


聚焦热点企业安全话题与策略方案，
助推企业安全建设发展



扫码关注公众号



Copyright © 2019 WWW.FREEBUF.COM All Rights Reserved [沪ICP备13033796号](#)

 阿里云 提供计算与安全服务



[新浪微博](#)

[PreviousNext](#)