准备工具 dnSpy 这个反编译工具(网络上有下载) 电脑要装有 .NET Framework4.0 或以上版本的组件, win10 都带有 4.6 以上的版本 本文中的测试机器是 p8668i 机器 codeplug 版本 11.00.14 cps 版本如图

关于CPS		×
	MOTOTRBO CPS	
HAVN	版本16.0(内部版本823)	
	Copyright © 2018 Motorola Solutions, Inc.	
	保留所有权利。	
🙆 , Motoro	ila Solutions和MOTOTRBO是Motorola Solutions, Inc.的商标	
警告:此程序3 或其中任何都分 定的最大范围起	8 美国和国际版权法保护。未经授权复制或分发本程序 }可能会导致严重的民事和刑事处罚,并且将按法律规 21诉。	确定(<u>O)</u>





将 mototrbocps.exe 和 communication controller.dll 这两个文件拖到 dnSpy 窗口里面

按照下图展开类型引用

🗗 dnSp	у vб.1. <mark>4</mark> (3	2-bit, 管理	员)				
文件(E)	编辑(E)	视图(⊻)	调试(<u>D</u>)	窗口(<u>W</u>)	帮助(<u>H</u>)	G	0
程序集资	源管理器						
▶ 🗇 m	ototrbocp	s (16.0.823	.0)				
🚽 🗇 . co	mmunicat	ioncontrol	ler (16.0.82	3.0)			
1	communi PE	cationcont	troller.dll				
A	■■ 类型引	佣					
4	Þ 🛍 🗛	tion<⊺> @	01000085				ļ
	🕨 🗆 Ar	gumentExc	ception @0	1000036			ļ
1.1	🕨 🗆 Ar	gumentNu	llException	@0100003	8		ļ
100	🕨 🔩 Ar	ray @0100	0052				ļ
	🕨 🔩 Ar	rayList @0	100002B				ļ
	🕨 🔩 As	semblyCo	mpanyAttri	bute @010	00003		ļ
	b 💏 🗛	cambly Cou	oficuration	Attribute @	0100000		
往下拉找	到 Passwo	ordStatus	这个变量	引用"右击	"选择"	分析,	"

P -15	MemoryStream @01000039
* *	MulticastDelegate @01000011
🔁 🕸	NameValueCollection @0100001B
Þ 🔩	NumberFormatInfo @01000063
۵ 🎝	object @0100000E
۵ 🔩	PackedRadioData @01000050
A	PasswordStatus @01000031
Þ 🔩	Path @01000078
۵ 🏤	PbaObject @01000033
÷.	PcrCommunicationRegistry @01000088



在右侧下方窗口找到

CommunicationController.CRadioCodeplugController.ValidateLocalPassword(string) :

PasswordStat	tus 如下图中的方法双击进入,提示正在反编译稍等即可
分析諸	
🔺 🏤 Passwor	dStatus @0200003E
▶ ♀ 实例4	2于
▶ ♪ 扩展7	方法 人名英格兰人姓氏克尔 化乙基乙基乙基乙基乙基乙基乙基乙基乙基乙基乙基乙基乙基乙基乙基乙基乙基乙基乙基
🖌 🔎 被使用	₹
▶ © €	ommunicationController.CRadioCodeplugController.IoControl(string) : T @0600008C
• ● ● ● ℃	ommunicationController.CRadioCodeplugController.ValidateLocalPassword(string): PasswordStatus @06000098
≥ © C	ommunicationController.IRadioCodeplugController.ValidateLocalPassword(string) : PasswordStatus @06000058
Þ 🐾 M	lotorola.Common.Communication.CommonUtil.PCRDeviceInfo. <passwordstatus>k_BackingField : PasswordStatus</passwordstatus>
⊳ <i>≫</i> M	Iotorola.Common.Communication.CommonUtil.PCRDeviceInfo.PasswordStatus : PasswordStatus @17000099
P @ M	${\sf lotorola.Common.Communication.CommunicationManager.MotoDevice.ValidateLocalPassword(string):Password(st$
P @ M	lotorola.Common.Communication.Service.IDeviceOperation.EndValidateLocalPassword(IAsyncResult): PasswordSt
	lotorola.Common.Communication.Service.IDeviceOperation.ValidateLocalPassword(DeviceInfo, string) : PasswordS
	lotorola.Common.Communication.Service.MotorolaDeviceOperation.a(DeviceInto, string) : PasswordStatus @0000
	lotorola.Common.Communication.Service.MotorolaDeviceOperation.ap.d(object, EventArgs) : void @U0000238
	lotorola.common.communication.service.wotorola.evice.peration.cnovalidate.local#assword(IAsynckesuit) : Pai
	lotorola.common.communication.service.viotorolabevice/peration.validateLocalPassword(DeviceInto, string) : Pictorolacommon.com/
Þ 🗘 📩	obotrocps.cchildrame.a(re) bool; void @00000090
	statisborgs (Childrame act), vold goodoodd
▶ @ m	stattbocps. (Childrame b(r, void @0000000
≥ œ m	intertion Characteristic Resource Handler (MainErame usbort string Password Status hool) - hool @060001
Þ 🎯 m	iototrbocps.CDoc.cfint) : bool @060001E6

找到这句 result = this.b. ValidateLocalPassword(this.a, **password**);

在最前面位置点击一下,会出现一个红点,意思是在此处下断点,输入密码点确认后程序运行 到这里会在这里断下来



接下来在 dnSpy 窗口按下 F5 键. 会以调试模式打开 CPS



下图直接点确认

调试程序		×
调试引擎(<u>D</u>) .	NET Framework	
可执行程序(<u>X</u>)	C:\Program Files (x86)\Motorola\MOTOTRBO CPS\mototrbocc	
参数(<u>R</u>)		
工作目录(<u>W</u>)	C:\Program Files (x86)\Motorola\MOTOTRBO CPS	
中断于(B)	不要中断	
	确定 (<u>O</u>) 取消((2

连接好对讲机,点击读取,随意输入一个密码然后点击确认

	输入Codepl	ug密码
	•••••	•
5 <u>-</u>		
	确定(0)	取消(C)

然后回到 dnSpy 窗口会发现红点里面有个箭头

2000	LLY
3861	
3862	num = 1113;
3863	int num2 = num;
3864	num = 1113;
3865	switch (num2 == num)
3866	
3867	
3868	mum = 1;
3869	if $(num != 0)$
3870	
3871	
3872	num = 0;
- 3873	if $(num != 0)$
3874	
3875	3
3876	result = this.b.ValidateLocalPassword(this.a, password);
3877	
3878	catch (Exception ex)
3879	
3880	CommonExpToCustomExpHelper.ConvertCommonExceptionAndThrow(ex)
3881	throw CommunicationController.CCustomExceptionHandler.Createl

按一下 F10

程序会运行到 num=0;处停下来

在下方窗口找到 result 这个变量,点击前面的三角展开



展开后找到 IsPasswordValidationSuccess

同部分	之里	
名称		值
۵	Motorola.Common.Communication.Service.IDeviceOperati	Motorola.Common.Communication.CommonUtil.Pa
₽ 🤗	this	CommunicationController.CRadioCodeplugControll
•	password	"00000001DC1544D905C10DC5893CFA378E977FF25
4 🥥	result	Motorola.Common.Communication.CommonUtil.Pa
	🔑 AlgorithmID	0x0000000
	🔑 ConfigurationLocked	0x00
	🏓 IsPasswordValidationSuccess	false
	🌶 Policy	None
	🔑 RemainingAttempts	0xFF
_	₽ Salt	
۵ 🏈	ex	
9	num	0x0000000
	num2	

把这个 IsPasswordValidationSuccess

后面的参数值改成 true

passworu	0000001001344030301000363
🔺 🤗 result	(Motorola.Common.Communication
🏓 AlgorithmID	0x0000000
🔑 ConfigurationLocked	0x00
IsPasswordValidationSuccess	true
🏓 Policy	None
🄑 RemainingAttempts	0xFF
🔑 Salt	null
Þ 🥥 ex	null
num	0x0000000
8 num2	

然后按下 F5 继续



至此你会发现 CPS 里面进度条在走.听到声音后就能看到读取成功了,找到常规设置,再在右侧 找 codeplug 密码 点击小眼睛就能看到了

XiR	P8668i		4 .	
SET -	常规设置	Cadaalua常知	44000044	
-	附件	Codeping#ras	11223344	_
	按钮	检查密码	只读	-
🖂	短信	家口具名当话为新始本	-	