第一章
了解威胁模型

如果你来自软件渗透测试世界，你可能已经熟悉攻击面。对于我们其余的人，攻击面是指所有可能的攻击目标的方法，从个别组件的脆弱性，影响到整个车辆。在讨论攻击面时，我们不考虑如何利用目标；我们只关心进入点。你可能会想到攻击面像目标的表面积与体积相对。两个物体可以有相同的体积，但完全不同的表面积。表面积越大，暴露风险越高。如果你考虑一个对象的体积的值，我们在硬化安全的目标是创造低风险价值比率。

发现攻击面

当评估车辆的攻击面，假设你自己是一个邪恶的试图对坏事的间谍。为了找出车辆安全性的弱点，评估车辆的边界，并记录车辆的环境。一定要考虑数据可能进入车辆的所有的方法，这是车辆与外界沟通的所有的方法。

当你检查车辆的外观，问自己这些问题：

- 收到什么信号？无线电波？钥匙？距离传感器？
- 是否有物理键盘访问？
- 有触摸或运动传感器吗？
- 如果车辆是电动的，它如何充电？

当您检查内部时，考虑以下内容：

- 音频输入选项是什么：CD？USB？蓝牙？
- 是否有诊断端口？
- 仪表板的功能是什么？有GPS？蓝牙？互联网？

正如你所看到的，有很多数据可以进入车辆的方法。如果这些数据是畸形的或有意地预谋的，会发生什么？这就是威胁模型的由来。

威胁模型

整本书都写了关于威胁模型，但我要给你一个快速的旅途，所以你可以建立自己的威胁模型。（如果你有进一步的问题，或如果这部分让你兴奋，通过各种手段，抓住另外一本关于这个主题的书）

当构建威胁建模汽车时，你收集有关于你的目标的结构的信息，并创建一个图来说明汽车的部件如何通信。然后，您使用这些地图，以确定更高的风险投入，并保留一个检查表进行审计；这将有助于您优先处理入口点，可以产生最大的回报。

威胁模型通常是在产品开发和设计过程。如果生产特定产品的公司有一个良好的开发生命周期，它会在产品开发开始时产生威胁模型，并随着产品生命周期的不断更新而不断更新模型。威胁模型是随着目标的变化而变化的真实文档，随着你对目标的了解越来越多，所以你应该经常更新你的威胁模型。

你的威胁模型可以包含不同的层次；如果你的模型中的过程是复杂的，你应该考虑在你的图表中添加更多的层次来进一步分解它。然而，等级2是关于你能去的地方。我们将在以下几节讨论各种级别，从威胁级别0开始。

Level 0:鸟瞰

在这个等级上，当考虑攻击面的时候，我们使用我们建立的检查表。思考数据如何进入车辆。在中心画辆车，然后标记外部和内部空间。图1-1显示了一个可能的0级图。

矩形框是输入端，在中心的圆代表整个车辆。在他们到达车辆的路上，输入端穿过两条的虚线代表外部和内部威胁。

车辆循环并不代表一个输入端，而是一个复杂的进程，即一系列可以进一步分解的任务。进程是编号的，正如你所看到的，这一个是数字1.0。如果在你的威胁模型中有多个复杂的部分，你将会接连地为它们编号。例如，您将标记第二个进程2.0；第三个进程，3.0；等等。当你了解你的车辆的功能，你更新这张图。如果你依旧不认识所有图中的首字母缩略词没关系；你将很快认识。

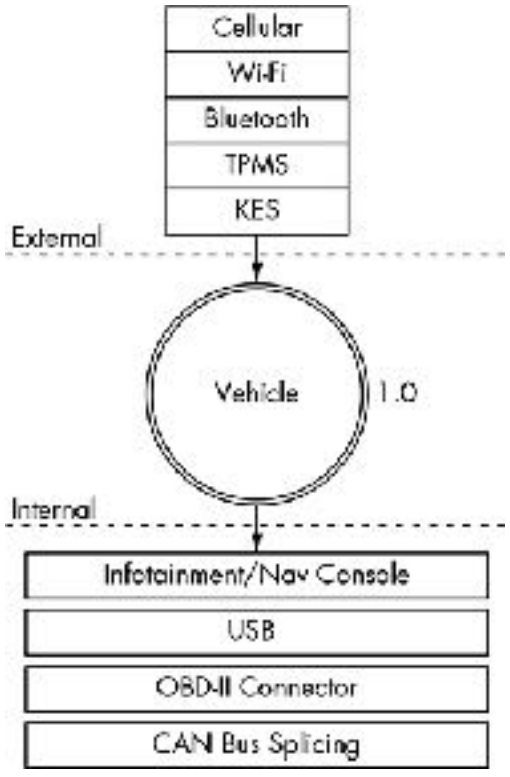

图1-1：等级0输入端

Level 1: 接收器

为了移动到等级一的图表，选择一个进程来探索。因为在我们的图中，我们只有一个进程，让我们深入到车辆的进程并注意每一个输入端交流些什么。图1-2所示的1级图几乎与0级图相同。唯一不同的是，在这里，我们指定的车辆连接点接收0级输入。我们现在还没有深入地研究接收器，我们只看输入端的基本设备或区域。

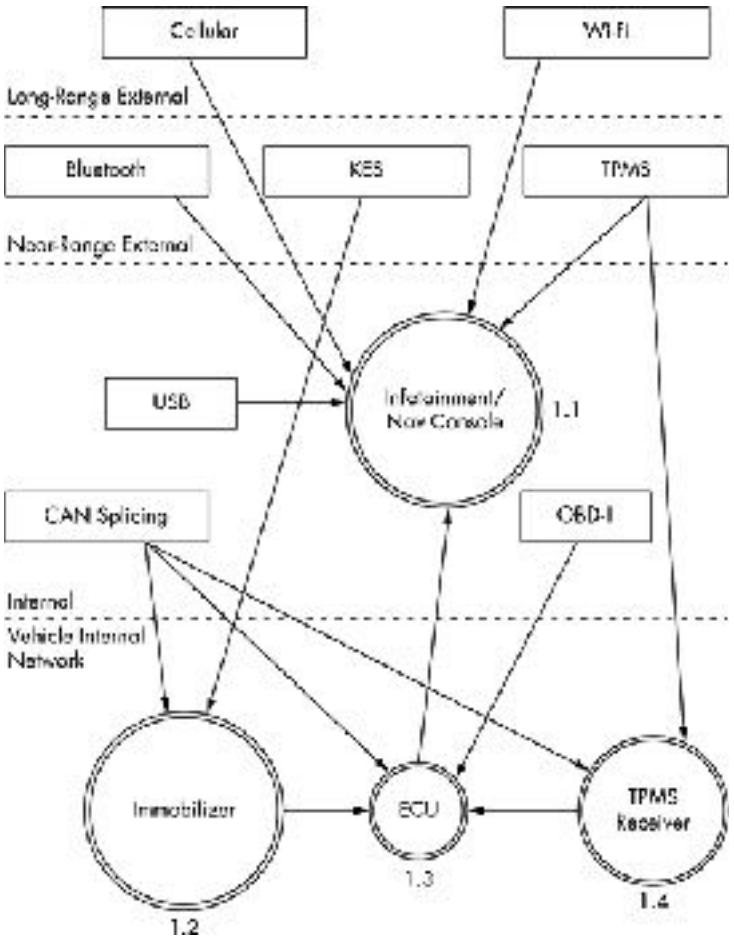

图1-2：等级1输入和车辆连接图

在图1-2中注意到我们给每个接收器编号。第一个数字代表进程标签来自图1-1的0级图，第二个数字是接收器的编号。第二个数字是接收器的数量。因为该信息单元是一个复杂的进程和输入端，我们给了它一个进程

循环。我们现在有三个过程：防盗器、ECU和TPMS接收器。

1级图中映射的虚线代表了信任边界之间的划分。图中顶部的输入是最不可信的，而底部的输入是最受信任的。通信信道越信任边界越大，信道越有风险。

Level 2: 接收器分解

在等级2中，我们检查车辆内部发生的通信。我们的样品图（图1-3）的重点是基于Linux的信息控制台，接收机1.1。这是一个更复杂的接收器，它往往直接连接到车辆的内部网络。

在图1-3中，我们将通信信道分组到带有虚线的框中，以再次表示信任边界。现在，在信息控制台里的一种新的信任边界称为内核空间。系统直接与内核交流比与系统应用程序交流的风险更高因为他们可以绕过对信息单元的任何访问控制机制。蜂窝信道比Wi-Fi信道的风险更高是因为它跨信任边界到内核空间。Wi-Fi信道，另一方面，在用户空间与WPA Supplicant进程通信。

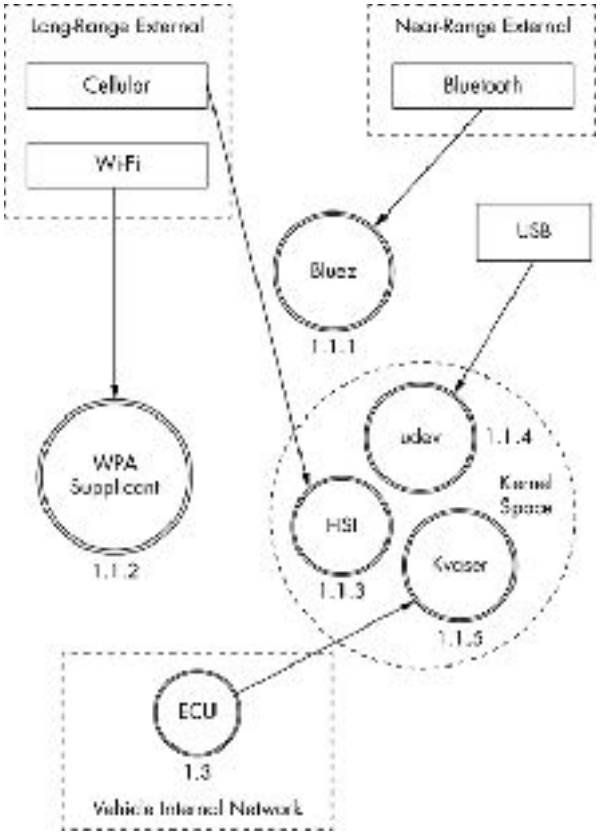

图1-3:等级2信息娱乐控制台图

本系统是一个基于Linux的车载信息（IVI）系统，它使用部分与Linux相同的环境。在内核空间，你会看到从我们的威胁模型接收输入的内核模块udev，HSI和Kvaser。udev模块加载USB设备，HSI是一个处理蜂窝通信的串行驱动程序，Kvaser是车辆的网络驱动程序。

等级2的编号模式是x.x.x,并且识别系统和以前是一样的。在等级0中，我们采取的车辆进程是1.0并且纯洁的深入其中。

注意

理想情况下，在这个阶段，你会绘制出哪些过程处理哪些输入，但我们现在不得不猜测。在现实世界中，你需要逆向信息系统来找到这样的信息。

当建立或设计一个汽车系统时，你应该继续尽可能多地研究复杂的进程。引入开发团队，并开始讨论每个应用程序使用的方法和库，以便你将它们集成到自己的威胁图中。您可能会发现应用层上

的信任边界通常在应用程序和内核之间、应用程序和库之间、应用程序和其他应用程序之间，甚至在函数之间。当探索这些连接，马克方法有更高的特权或处理更敏感的信息。当探索这些连接，标记方法有更高的特权或处理更敏感的信息。

威胁识别

现在，我们已经深入到我们的威胁建模地图的两个层次，我们可以开始识别潜在的威胁。威胁识别往往与一群人和一块白板做更有趣，不过你可以把它当作你自己的一个思想练习。

让我们一起试试这个练习。开始于等级0-鸟瞰-并考虑潜在的高层次的问题，输入端，接收器和威胁边界。现在让我们列出所有潜在的威胁与我们的威胁模型。

Level 0: 鸟瞰（Bird's-Eye View）

当确定在等级0中的潜在威胁，尽量保持高等级。这些威胁中的一些似乎不现实，因为你知道额外的障碍或保护，但重要的是包括在列表中的所有可能的威胁，即使有些已经被解决。这里的要点是集中每一个过程和输入的所有风险。

在第0级的高级威胁的攻击者可以是：

- 远程接管车辆
- 关闭车辆
- 监视驾乘人员
- 解锁车辆
- 偷车
- 跟踪车辆
- 阻止安全系统
- 在车辆上安装恶意软件

起初，这可能很难想出一堆攻击方案。这通常是好的，有不是工程师的人员也在参与这个阶段，因为作为一个开发人员或工程师，你往往牵扯于内在的运作以至于很自然的拒绝相信甚至毫无意义的主意。

要有创造力，尽量想出最多的你可以想到詹姆斯·邦德-罪犯攻击。也许想想其他的攻击场景，以及它们是否也可以适用于车辆。例如，考虑勒索，一个恶意软件，可以加密或锁定你的电脑或手机直到你付钱给别人远程控制软件。这可以用在车辆上吗？答案是肯定的。记下勒索。

Level 1: 接收器（Receivers）

在等级1的威胁识别中更侧重于连接的每一部分，而不是连接本身，这可能是一个直接的输入端。这些脆弱性是指我们假设在这个水平有什么影响连接到车辆的设备脆弱性。

蜂窝（Cellular）

攻击者可以利用车辆的蜂窝连接到：

- 从任何地方访问内部车辆网络
- 利用在信息娱乐单元的应用处理来电
- 通过信息娱乐单元访问用户身份识别模块（SIM）
- 使用蜂窝网络连接到远程诊断系统（OnStar）
- 窃听手机通讯
- 干扰紧急电话
- 跟踪车辆的运动
- 建立移动通信全球系统（GSM）伪基站

Wi-Fi

攻击者可以利用Wi-Fi连接：

•从300码远或更多访问车辆网络
•发现一个软件的漏洞处理传入连接
•安装信息娱乐单元安装恶意代码
•破解Wi-Fi密码
•设立一个假冒的经销商访问点欺骗车辆认为它正在服务
•截获通过Wi-Fi网络的通信
•追踪车辆

Key Fob
攻击者可以利用钥匙连接：
•发送畸形的钥匙要求把车辆的防盗器置于未知状态。（防盗应该保持车辆锁定，所以无法而言。我们需要确保它保持适当的功能。）
•积极探测防盗器使车用蓄电池耗尽。
•锁定一把钥匙
•捕获在握手过程中从防盗器泄漏的密码信息
•暴力破解钥匙的算法
•克隆钥匙
•干扰钥匙信号
•耗尽钥匙的力量

轮胎压力监测传感器(Tire Pressure Monitor Sensor)
攻击者可以利用TPMS连接：
•发送一个不可能的条件下发动机控制单元（ECU），造成故障，然后被可以利用
•为了欺骗道路状况欺骗ECU为过度矫正。
•把TPMS接收器或ECU设为不可恢复的状态，这可能会导致司机靠边停车检查据报告的平面或甚至关闭车辆
•基于TPMS的唯一ID追踪车辆
•欺骗TPMS信号引起内部警报

信息娱乐控制台(Infotainment Console)
攻击者可以利用信息娱乐控制台连接：
•将控制台设置为调试模式
•改变诊断设置
•找到一个输入错误可以导致意想不到的结果
•安装恶意软件到控制台
•使用恶意应用程序访问内部CAN总线网络
•使用恶意应用程序来窃听的驾乘人员的动作
•使用恶意应用程序来欺骗数据显示给用户，如车辆定位

USB
攻击者可以使用USB端口连接：
•在信息娱乐单元安装恶意软件
•利用在信息娱乐单元的USB栈的一个缺陷
•用特制文件附加一个恶意的USB设备被用于破坏进口商的信息娱乐单元，如地址簿和MP3解码器
•在车辆上安装修改更新软件

•使USB端口短路，从而损害了信息娱乐系统

蓝牙(Bluetooth)
攻击者可以使用蓝牙连接到：
•在信息娱乐单元执行单元
•利用在信息娱乐单元的蓝牙栈的一个缺陷
•上传格式畸形的信息，如损坏的地址簿被用于执行代码
•近距离访问车辆（小于300英尺）
•干扰蓝牙设备

控制器区域网络(Controller Area Network)
攻击者可以利用CAN总线连接：
•安装恶意诊断设备将数据包发送到CAN总线
•直接插入CAN总线，试图启动没有钥匙的车辆
•直接插入到一个CAN总线上传恶意软件
•安装恶意诊断设备跟踪车辆
•安装恶意诊断设备，使远程通信直接到CAN总线，使一个正常的内部攻击变成现在外部的威胁

等级2:接收器故障(Receiver Breakdown)
在等级2中，我们可以谈论更多关于识别特定的威胁。当我们查看哪个应用程序处理哪个连接时，我们可以开始基于可能的威胁进行验证。
我们将威胁分为五组：BlueZ（蓝牙守护进程），该wpa_supplicant（Wi-Fi守护进程），HSI（高速同步接口细胞内核模块），udev（核设备管理器），和Kvaser的司机（CAN收发器驱动）。在下面的列表中，我指定了每个程序的威胁。

BlueZ
旧的或未打补丁的版本的开放进程：
•可能被利用
•无法配置来确保适当的加密
•无法配置来处理安全的握手
•可以使用默认的密钥

wpa_supplicant
•旧版本可能被利用
•不能执行适当的WPA2无线加密方式
•可能连接到恶意接入点
•可能通过BSSID泄漏关于驾驶员的信息（网络接口）

HSI
•旧版本可能被利用
•可被注射串行通信（中间人攻击，攻击者插入串行命令到数据流）

udev
•旧版本，未打补丁的版本可能会受到攻击
•可能设备没有保持白名单，允许攻击者加载额外的驱动器或USB设备进行试验或使用
•可能允许攻击者加载外来的设备，如键盘访问信息娱乐系统

Kvaser Driver

•旧版本，未打补丁的版本可能被利用
•可能允许攻击者上传恶意固件到Kvaser设备
这些潜在漏洞的清单绝不是详尽无遗的，但它们应该让你知道这个头脑风暴会议是如何工作的。如果你去一个等级3的地图的潜在威胁到你的车，你会选择其中的一个过程，像HSI，开始查看它的内核源来识别敏感的方法和依赖关系，这些可能容易受到攻击。

威胁评估系统
我们已经记录了许多我们的威胁，现在可以用风险等级来评估它们。常见的评级系统包括DREAD、ASIL，和mil-std-882e。DREAD是常用的Web测试，而汽车行业和政府共同使用ISO 26262 ASIL和MIL-STD-882E，分别为威胁等级。不幸的是，ISO 26262 ASIL和MIL-STD-882E专注于安全的失败和不足以处理恶意威胁。对这些标准的更多细节，可以参考
http://opengarages.org/index.php/Policies_and_Guidelines.

DREAD评估系统
DREAD代表以下：
伤害潜在的伤害有多大?
重现性如何容易复制?
它是多容易被利用攻击的?
受影响的用户中有多少用户受到影响?
它是有多容易的发现找出脆弱性?
表1-1为每个评估分类列出了从1至3的风险等级。

评估分类	高(3)	中(2)	低(1)
D 潜在的破坏	可以破坏安全系统并获得充分信任，最终接管系统	可以泄漏敏感信息	可以泄露无价值的信息
R 复现性	总是可以复现的	只能在特定的条件或时间窗口中进行复现	很难重现，甚至给出了具体的漏洞信息
E 可利用性	允许新手攻击者可利用	允许一个熟练的攻击者创建一个可以被重复使用的攻击	只允许一个拥有丰富经验的熟练的攻击者来执行攻击
A 受影响的用户	影响所有用户，包括默认设置用户和主要用户	影响某些用户或特定设置	影响一小部分用户；通常影响有隐蔽特征的
D 可发现性	可以很容易的发现被公布说明的攻击	影响一个很少使用的部分意思是攻击者需要非常灵活地为它发现恶意的使用点	模糊的，这意味着它不太可能会被攻击者找到一种方法来利用

现在我们可以从表1-1将每个DREAD类别，一个被从本章前面的得分确定的威胁分为由低到高的威胁(1–3)。例如，我们将在第10页的等级2的HSI威胁论述为“等级2:接收器故障”，我们可以拿出如表1-2所示的危险等级。

表1-2：HSI威胁为等级2的DREAD分数

HSI 威胁	DREAD总数
一个古老的，未打补丁版本的可以被利用的HSI	3 3 2 3 3 1 4
一个可能可以受到串行通信注射的HSI	2 2 2 3 3 1 2

你可以通过使用总列数中的值来确定综合评估，如表1-3所示。

表1-3：DREAD风险评分表

总数	风险等级
5-7	低
8-11	中
12-15	高

在进行风险评估时，将评分结果可视化是很好的做法，这能使阅读结果的人能够更好地理解风险。就HSI威胁来说，我们将高风险归属到每个威胁，如表1-4所示。、

表1-4:等级2的HSI威胁的DREAD风险级别的应用。

HSI威胁	DREAD总数	风险
一个古老的，未打补丁版本的可以被利用的HSI	3 3 2 3 3 1 4	高
一个可能可以受到串行通信注射的HSI	2 2 2 3 3 1 2	高

尽管风险都被标记为高，我们可以注意到老版本带来的风险要比受到串行通信注射攻击的风险要高，因此，我们可以优先处理这一风险。为什么串行通信注射的风险较低，严重损坏较少并且利用难度比HSI老版本更难复现。

CVSS：另一种DREAD

如果你担心DREAD对于你来说不够详细，考虑更详细的风险方法称为通用漏洞评分系统(CVSS)。CVSS在三组中提供比DREAD更多的类别和细节：基数，时间和环境。每个组又划分子区域-6个基础区，3个时间区和5个环境区-总共14个评分区！(关于CVSS如何运转的详细信息，请看http://www.first.org/cvss/cvss-guide。)

注意

当评估风险的时候，我们可以使用ISO 26262 ASIL 或者 MIL-STD-882E，我们想要更多的细节而不仅仅是风险=概率X严重度。如果你不得不选择从这两个系统之间进行安全审查，使用由国防部(DoD)发布的MIL-STD-882E。汽车安全完整性等级（ASIL）系统经常会有陷入QM排名的风险，这基本上就是“meh”。美国国防部的系统往往会导致更高的排名，这就等同于一个高成本的生活价。同时，MIL-STD-882E被设计用于整个系统的身=生命周期，包括处置，这是一个非常适合的安全开发生命周期。

使用威胁模型结果

在这一点上，对于车辆，我们设计了许多潜在危险，并且我们将它们进行风险排名。现在干什么？那取决于你在哪个队，使用军事术语，攻击方是“红队”，防守方是“蓝队”，如果你在红队，你的下一步是开始攻击有可能获得成功的最佳机会的最高风险领域。如果你在蓝队，回到你的风险图表并且修改每个威胁的对策。

例如，如果我们在第11页的“DREAD评级系统”中承担两个风险，我们可以为每个风险添加一个对策部分。表1-5包括HSI代码执行风险的对策，表1-6包括HSI拦截的风险对策。

Table 1-5: HSI 代码执行风险

风险	在内核空间执行代码
风险	高
攻击技术	利用旧版本HSI的漏洞
对策	内核和内核模块应该更新到最新的版本

Table 1-6: 拦截 HSI 命令

风险	高
攻击技术	拦截HSI的串行通信
对策	所有的命令都是经过加密的签名被发送到蜂窝

现在你有一个高风险漏洞解决方案的文档列表。根据不执行该解决方案的方案，您可以优先考虑当前未执行的任何解决方案。

总结

在本章中，你了解了会用威胁模型来识和记录你的安全态势的重要性。并获得技术和非技术的人头脑风暴可能的情景。然后，我们钻入这些场景来识别所有潜在的风险。使用评分系统，我们为每一个潜在的风险进行排名和分类。这种方式评估威胁后，我们以一个定义了我们当前产品的安全态势的文档来结束，当前的任何对策，以及仍然需要被解决的高优先级项目的任务列表。