

GPS网络威胁的探测和保护

思博伦干扰探测器如何帮助您了解和对抗影响GPS系统及设备的各类真实威胁？

执行综述

随着越来越多的系统依赖全球定位系统（GPS）来获取位置、导航和计时，民用GPS信号的脆弱性和不受保护的特点已经成为日益严重的风险。

除大气和人为的无线电视频（RF）干扰源外，GPS接收机越来越容易受到干扰机和欺骗设备造成的故意和非故意损伤的影响。GPS依赖系统的制造商、集成商和采购商需要正视这些威胁，并且采取必要的反制措施。

本白皮书简要罗列了GPS所受威胁的规模和演化特质，并且介绍了全新的思博伦解决方案：思博伦干扰探测器。该设备可以探测、捕获并分析特定位置的干扰波型，帮助制造商、集成商和采购商在减轻风险方面做出明智的决策。

简介：GPS的脆弱性

随着越来越多的系统依赖全球定位系统（GPS）来获取位置、导航和计时，民用GPS信号的脆弱性和不受保护的特点已经成为日益严重的风险。

例如，近年来，我们发现那些销售低成本、非法“个人隐私设备”的网站数量急剧增加。这种廉价的干扰设备通常插在汽车的点烟器上，并且可以广播GPS所用频率的无线电波。这种相对较强的发射可以盖过较弱的卫星信号，阻止附近的接收机探测并处理GPS数据。

个人隐私设备（PPD）通常的使用者都是企业公车和卡车司机，其目的是禁用车上安装的遥测装置和其它员工跟踪设备，通常他们都是为了防止其雇主监视自己的活动。另外，有越来越多的证据表明，偷车贼与使用此类设备来封锁高档汽车上安装的防盗跟踪设备。

但许多PPD的能力远远超出了其购买者所知道（或关注）的程度，它们甚至可以将RF噪音广播到车辆500米的范围内。这种干扰会对附近那些依靠GPS才能运行的其它系统造成严重的影响。

最为人所知的例子就是纽瓦克机场。据报道，该机场在2012年的每个工作日都会遭受最多五次GPS扰乱事件。人们认为这些干扰都是由于附近的新泽西收费高速上行驶车辆上的PPD造成的。¹

而在英国，政府资助的SENTINEL项目在2008年至2012年期间对英国数个地点的干扰活动进行了监测，最终在有些地点探测到了每天5至10次此类事件。²

“有些地点每天都能探测到5至10次干扰事件，而有超过50个网站都在销售干扰机，执法部门也缴获了功率更强大，且作用距离和范围更大的干扰机。很明显，这一问题正变得越来越糟。”

— Chronos Technology公司，SENTINEL项目报告，2012年（PDF）

1 Inside GNSS，FCC对影响纽瓦克GBAS的GPS干扰机运营商开出罚单，2013年8月30日

2 Chronos Technology公司，SENTINEL项目报告，2012年（PDF）

GPS网络威胁的探测和保护

GPS受到的威胁并没有远去，其风险只是愈演愈烈

非常干扰机只是GPS信号面临的诸多威胁之一。其它的威胁包括太阳活动和电离层电磁风暴导致的干扰、附近蜂窝发射塔造成的干扰，以及其它的发射器。所有这些威胁都可能对GNSS接收机产生严重的影响，导致它们完全丢失信号，或者计算并报告错误的位置和/或时间。

除人为干扰外，RF干扰和大气干扰在未来的几年中也很可能呈现出增长的趋势，而且有很多黑客都在试验GPS“欺骗”——即广播伪造的卫星信号，欺骗接收机并使之相信自己处在一个不同的地点或时间点。

在过去，如果缺乏高深的导航知识和专业设备，欺骗活动是非常困难的，但在2015年的DEFCON 23大会上，一项演示活动已经证明，即使是非专家也可以很容易地使用廉价元器件和开源软件（见图）执行欺骗干扰。

GPS欺骗在2015年变得更加容易

在DEFCON 23大会上，中国安全研究员黄琳和杨卿通过展示证明，利用廉价的市售组件和开源代码完全可以制造出低成本GPS信号仿真器。

在不具备专家级GPS知识，而只拥有不到1000美元预算的情况下，他们使用互联网上已公布的研究和代码编写了一个可以充当GPS仿真器的软件定义无线电（SDR）。

黄琳和杨卿使用这些工具搭建起了GPS导航消息的结果，并编写了下载GPS卫星轨道信息（即星历数据）的SDR。

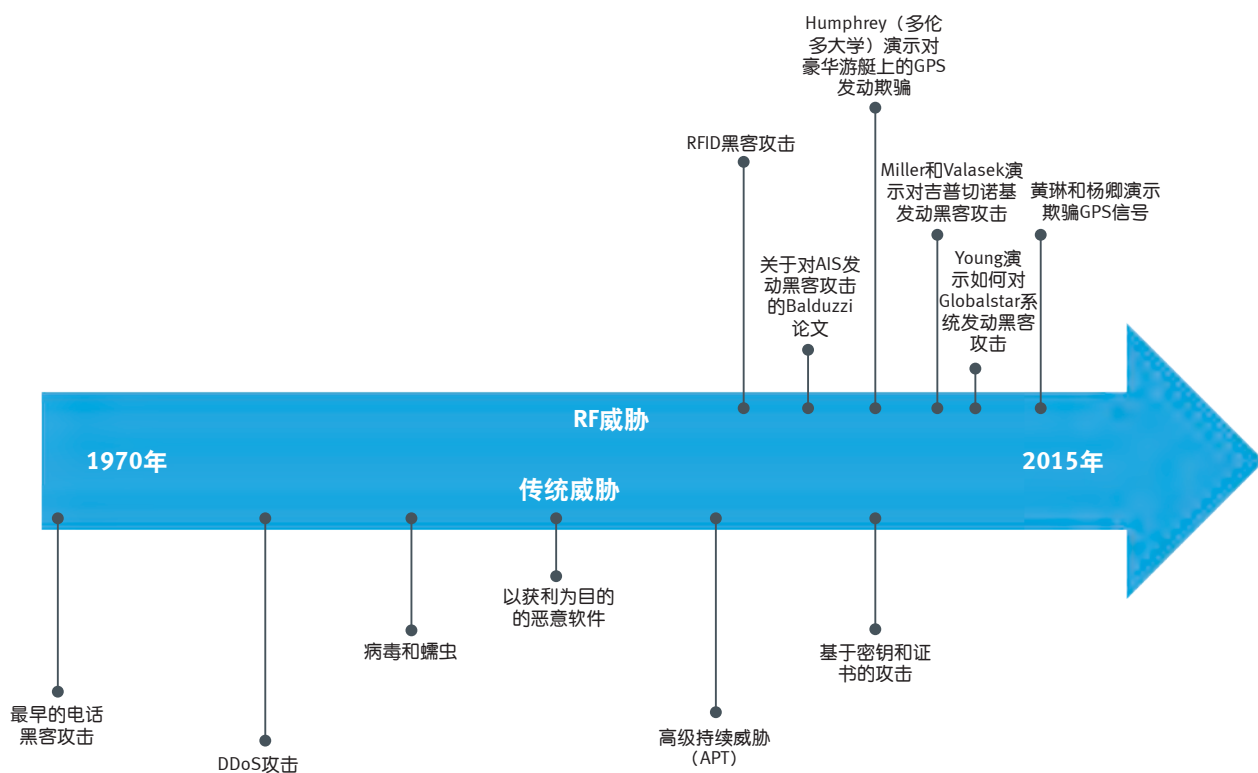
利用这些自制工具，他们证明自己能够控制多种设备的GPS接收机，包括智能电话、无人机和汽车卫星导航系统。

这次演示可能成为一个时代的开始，证明GPS欺骗已经成为黑客的主流武器——这意味着制造商和用户必须做好准备，应对未受保护接收机面临的欺骗攻击的快速激增。

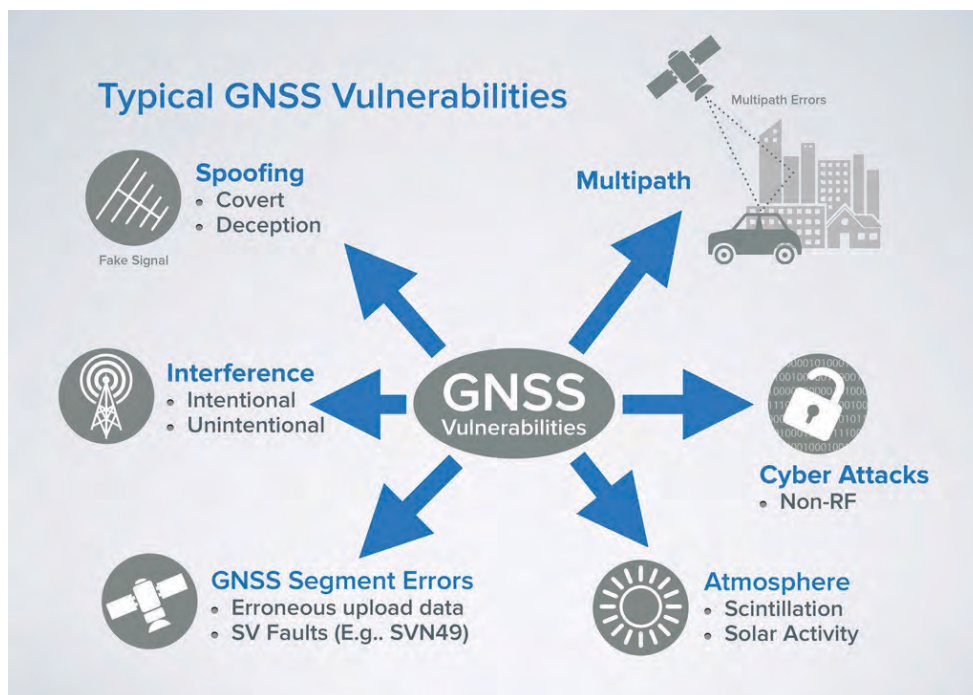
这对GNSS依赖设备的制造商和用户意味着什么

我们可以将这种局面与互联网安全中的“军备竞赛”做一个类比（见图）。这项对比显示，GPS面临的威胁只会增加，尤其是当黑客占据这一全新的攻击阵地之后。如下图所示，IT威胁的演变与当前正在发生的GNSS RF威胁的演变之间存在某种关联。其中一个关键的区别就是，与IT威胁的演变相比，GNSS RF威胁的演进呈现出一种加速的态势。

黑客攻击的演变



GPS网络威胁的探测和保护



因此，GNSS接收机的制造商、集成商和采购商需要了解威胁的规模，并及时跟踪其最新发展。这包括监测、绘制和分析真实的威胁，以便对其盛行程度加以评估，并监视其演化情况，最终的目的就是在易感的GPS依赖系统中构建起适当的对抗措施。

GPS盛行程度的提高充分证明，了解GNSS系统运行、测试或评估过程中的RF环境已经变得非常重要。如果现在还认为真正的GNSS威胁不可能发生，或者一切正常，那么这种想法将是不合理的，也是不安全的。

监测威胁的RF环境已经成为风险评估和数据采集中一项高度重要的技术，而且应当是确保GNSS依赖系统安全性过程中的首要步骤。

思博伦干扰探测器隆重推出

为帮助各类机构监测、分析和理解GNSS干扰的威胁，思博伦及其伙伴NSL已共同开发了一种独特的解决方案：[思博伦干扰探测器](#)。

工作原理

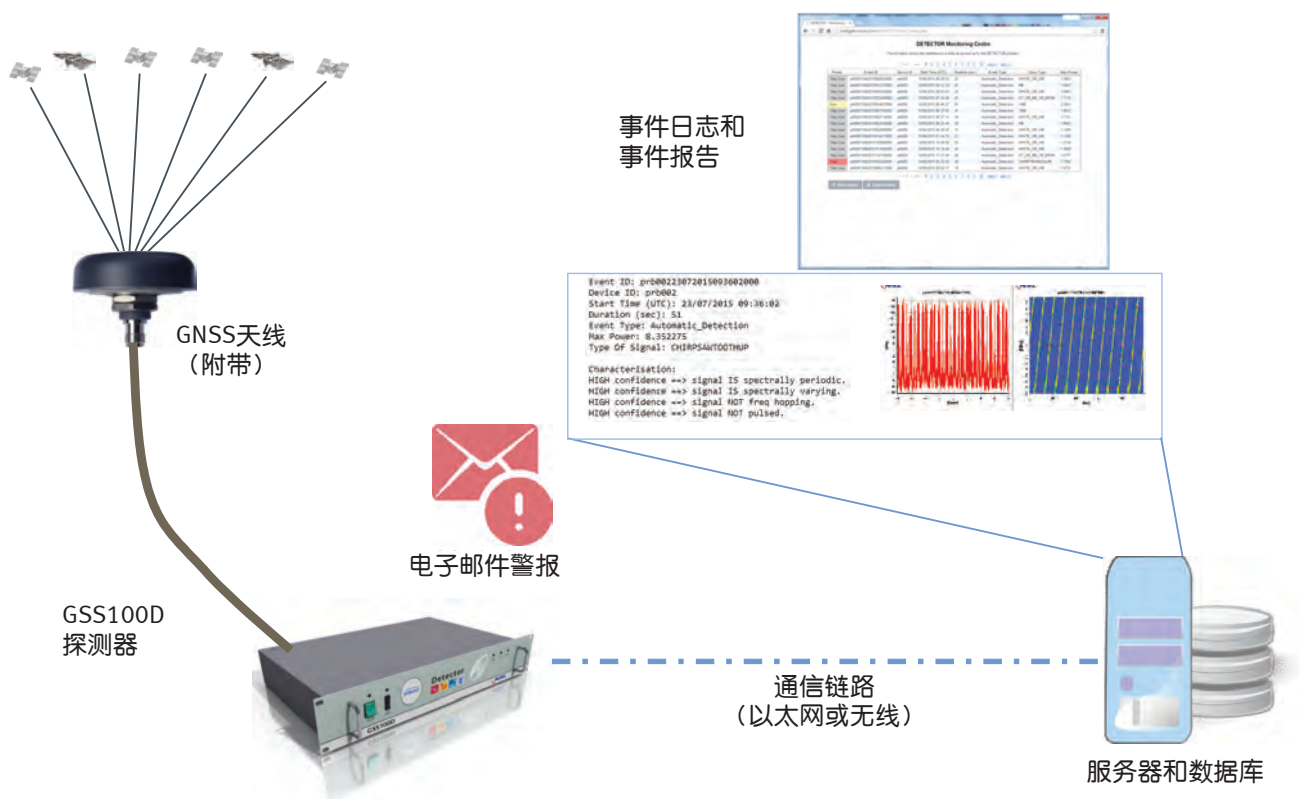
思博伦干扰探测器是一种固定侦听设备，可以在约500米的范围内监测GPS波段中的RF环境，探测对GPS信号产生干扰的潜在来源。

每当该探测器探测到高于某一特定阈值并可能对GPS产生干扰的波形，它就会采取两项行动：

1. 触发警报，通知用户已探测到干扰事件。
2. 捕获干扰波形，对其进行分析，并对其性质做出一些判断。

捕获的波形和相关判断将被记录在数据库中，并在经过一定时间后构建起干扰器约500米半径内所有干扰活动的完整图景。

捕获的波形可以再次合成，并引入测试条件下的GNSS接收机，从而更好地对接收机在真实干扰状况下的行为加以了解和定性。



GPS网络威胁的探测和保护

使用思博伦干扰探测器的两种方式

思博伦干扰探测器有两种类型的主要设计用途：

1. 监测和分析特定位置发生的干扰事件及干扰类型。
2. 验证特定位置的GPS信号环境是否“干净”并且无干扰。

监测和分析干扰事件

在第一个场景中，GNSS依赖设备的用户可以使用探测器来了解系统周围GPS信号的威胁。例如：

- 移动网络运营商或金融机构需要依赖GPS获得精确的计时，它们可以使用该探测器来侦测主时钟天线附近的信号干扰。
- 集装箱港口运营商可以使用港口周边的一台或多台探测器，查明可能影响GPS自动化吊车正常运行的干扰来源。
- 机场当局可以使用它来监测机场的环境，找出GPS着陆辅助系统可能面临的干扰源。
- GPS公路收费公司可以使用它来监测为逃避自动支付而使用干扰机的情况。

RF干扰器上所得的数据可用于为风险管理方法提供信息。它可以说明反复发生的来源存在哪些明显的模式，从而将干扰事件报告给相当主管部门。它可显示哪些地点存在不可移动的干扰源，例如蜂窝发射塔或其它发射器，因此原本就不适于安置GPS设备。它还可以用于对某特定位置上系统遭遇干扰和欺骗威胁的风险加以量化。

这些数据将显示特定位置上GPS依赖设备面临的威胁程度，使用户能够做出明智的决策，通过替换或修改设备的方式来提高其抗干扰能力。

在探测到干扰后，如果用户决定替换、修改或升级其GPS设备，则可以在实施前实验室环境中使用GPS信号模拟器，将已捕获的干扰波型回放给新的设备，确保其在面对已知威胁事件时的弹性。

确保干净的真实天空测试环境

在第二个场景中，测试团队要使用“真实天空”测试来评价接收机、设备或系统在真实世界中的性能，但他们也可以使用该探测器来完成任务。该探测器将验证真实的卫星信号未受到干扰的污染，并且会在周围环境受到染污时发出警报。

它还可以对探测到的任何干扰事件添加时戳，使测试团队可以找出干扰的时间点，既可以用于在测试中避开这些时间，也可以用于调查意外的测试结果。

通过使用探测器来确保未受污染的天空，能够在测试时间和成本方面产生巨大的利益。首先，过去某些测试会因干扰的存在而被丢弃和重复进行测试，而使用干扰器后可以避免此类麻烦和对时间的浪费。它还意味着您可以找出具体的干扰，确保测试时拥有“干净”的天空，一旦设备的运行出现异常，也可以排除因干扰造成的误报误警。

关于思博伦通信公司

思博伦通信公司正在为众多高技术设备制造商和服务商提供众多软件解决方案，用于简化和加快设备及系统测试进程。开发者和测试人员可以创建并共享自动化的测试，对来自多个设备、流量生成器和应用的结果加以控制和分析，同时还可利用通过/未通过标准进行，将每一项测试详尽记录在案。利用思博伦的解决方案，企业可以在迈向自动化的同时加快质量保障（QA）周期，缩短入市时间，并且提高已发布产品的质量。通信、航空航天及国防、消费电子、汽车、工业和医疗设备等行业都从思博伦的产品中受益匪浅。

结论

随着GPS依赖系统面临的威胁变得越来越普遍且越来越复杂，制造商、集成商和采购商都需要了解威胁的环境，并且构建起适当的反制措施。

思博伦干扰探测器是一种系统性的可靠手段，能够监测、捕获和分析特定位置的GPS干扰，了解在该位置影响GPS设备的那些威胁所具有的规模、性质和演化情况。

定价和上市情况

目前，客户可以从思博伦通信公司购买或租用干扰探测器。如果客户需要，思博伦还可提供实施咨询和使用培训服务。如欲了解更多信息，或者您有任何疑问，敬请接洽：www.hoyateq.com。

联系我们

网址：www.hoyateq.com

电话：010-82897220

传真：010-82897320

北京市海淀区上地信息路11号彩虹大厦北楼东407室

HOYATEQ

北京浩宇巡天科技有限公司