

新型攻击方式可通过硬盘灯突破物理隔离

● 杨碧瑶 / 国家保密科技测评中心

近年来,随着国内外窃密斗争形势的日益复杂,物理隔离网络逐渐成为重要攻击目标,出现了许多突破物理隔离的方式(如表1所示)。近日,以色列本古里安大学网络安全研究中心公布了一种突破

物理隔离的新方法,主要利用的是当前大多数计算机和服务服务器上都有硬盘灯(HDD LED)。该攻击方式通过一台感染了恶意软件的计算机上的硬盘灯来发送机器内敏感数据,然后通过摄像机、光传感

器等接收信息。

攻击过程

该攻击过程主要分为恶意软件植入、数据发送、数据接收三个阶段。一是恶意软件

表1 现有突破物理隔离的方法及特点

方式	实例	最大速率 (比特/秒)	有效传输距离 (米)
电磁	AirHopper	480	约5—10
	GSMem	1—1000	
	USBee	4800	
	Funthenna	<100	
声学	Fansmitter (利用风扇噪声)	0.25	约15
	DiskFiltration (利用硬盘噪声)	2.8	
光学	键盘LED	150	可视范围内
	屏幕LED	20	
	植入红外LED	15	
	硬盘灯(文中新方法)	4000	可视范围内(一般大于30米)

植入。主要通过供应链攻击(在目标设备运输过程中安装恶意软件)、社会工程学攻击(通过心理操纵来诱导攻击目标实施某种行为,如在公共社

交网站上获得某涉密人员信任,而后诱使其在所在物理隔离网络中安装恶意软件)等,使目标计算机、服务器等感染相应的恶意软件。恶意软

件随后便可在目标计算机中收集敏感信息(如涉密文档等)。二是数据发送。由于技术限制,恶意软件不能通过主板芯片组直接打开硬盘灯,而

是通过调用特定的读（写）命令、间接打开硬盘灯，从而利用硬盘灯的打开、关闭状态来分别表示“1”“0”，将窃取到的文件数据等以二进制形式发送出去。三是数据接收。主要通过内部隐蔽摄像头、恶意入侵人员随身携带的摄像机、涉密场所遭入侵的监控摄像头等内部接收装置，以及高分辨率远程摄像机、无人机载摄像机、光学传感器等远程接收装置进行数据接收。接收距离主要受接收者位置、环境亮度、硬盘灯光波长等影响，一般大于30米，事实上，只要接收者在硬盘灯发送光信号的可视范围内，辅以光学变焦透镜等装置，接收距离甚至可以更远。

主要特点

该攻击方式主要具有以下三大特点。一是隐蔽性。对于其他使用光学方式（如键盘灯和屏幕电源灯）突破物理隔离的方法，由于其异常情况可轻易被观察到，因此并不隐蔽。在该攻击方式中，由于硬盘灯在正常工作状态（读/写文件）下就频繁闪动，因此闪动时间和速度的受控变化可能不会引起特别关注。此外在高速传输情况下，硬盘灯的闪烁对于人眼来说是不可见的，这使得该窃密通道更加隐蔽。二是便利性。该攻击方式无需其

他任何特殊硬件，只需一个带有硬盘灯的机器，而硬盘灯在当今大多数桌面计算机、笔记本电脑和服务器的上都普遍存在。此外，激活硬盘灯通过普通的用户级代码（恶意软件）即可实现，并不需要改动操作系统内核。三是高速性。在该攻击方式中，信息传输速率最高时可达每秒4000比特，比其他利用光学方式突破物理隔离技术的速度至少快10倍，因此可以更快地传送数据。例如，对于4096比特的加密密钥传送，一般可在数十秒内完成。

应对措施

针对上述攻击方面，建议从以下三个方面加强防范。一是防止恶意软件植入。强化计算机所在环境的防护，加强

内部网络设备供应链的安全保密管理，同时开展相应突破物理隔离恶意软件的检测技术研究。二是防止敏感数据通过光信号发送。适时断开硬盘灯与计算机的连接，或用黑色磁带覆盖硬盘灯。此外，还可引入对硬盘的随机读写操作，使得光信号与随机噪声混合，通过干扰降低攻击的有效性。三是防止外部光接收设备窃取信息。在计算机所在环境内禁用所有摄像装置，并采用遮蔽窗户方式防止外部光探测器窃取涉密信息。定期检查场所内的监控摄像头，防止其被用作接收信息的工具。END（根据LED-it-GO: Leaking a lot of Data from Air-Gapped Computers via the small Hard Drive LED，原载于cyber.bgu.ac.il的《通过小小硬盘灯泄露物理隔离计算机上大量信息》等编译）

