技术

避免网络世界的“珍珠港事件”

计算机安全专家正努力阻止潜在的毁灭性网络攻击。

撰文 蔡宙（Charles Q. Choi） 翻译 刘敬韬

随着微芯片变得越来越小，功能越来越强大，它们几乎渗透了社会的每一个角落：智能手机，医学设备，以及维持铁路、电网和污水处理设施日常运转的调控系统。但是，计算机安全专家已经发出警告，这些嵌入式计算机非常容易受到攻击，因为它们越来越多地和其他计算机联网工作，却几乎没有任何防护措施来保护其固件（固化在芯片电路中的程序）。

2012年10月，在一场被认为源自伊朗的网络攻击浪潮过后，美国国防部长（Secretary of Defense）里昂·帕内塔（Leon Panetta）发出警示，网络世界的“珍珠港事件”很有可能将在不久后发生。

美国网络影响部（Cyber Consequences Unit，一家非营利机构）主任斯科特·博格（Scott Borg）表示，计算机安全专家通常不太重视固件，因为固件和软件不同，它们的设计初衷就是用来长时间不变地执行指定任务，“不过，实现固件程序的电路一开始就是被设计成可以进行多次读写，所以，它们还是会被网络攻击者入侵并修改”。

现在，工程师在保护微芯片方面已经取得了一些进展。在2012年7月举办的一个计算机安全论坛上，美国哥伦比亚大学的计算机专家崔昂（Ang Cui，音译）和萨尔·斯托夫（Sal Stolfo）报道了他们研发的一款被称为《共生体》（Symbiote）的软件，能够通过随机扫描固件代码来检测是否遭到入侵。该程序可以在不影响计算机运行速度的情况下，对任何类型的固件进行检测。崔昂表示，《共生体》也可以检测到此前人们根本不可能注意到的一些恶意程序，这或许可以阐明“历史上数不清的互联网战争”。崔昂和斯多夫计划在2012年底前，将软件原型提交给美国政府相关部门进行检测。

伯格认为，斯托夫和崔昂研发出的软件“非常有前景”。赛门铁克研究实验室的高级总监马克·达西耶（Marc Dacier）则认为，对于任意一种防护措施而言，它所面临的最主要的障碍在于如何让公司选择并使用。美国国防部正在推进立法，让私营部门与政府部门在网络安全方面加强合作。就像美国国防部长帕内塔在2012年10月的演讲中曾经说过的，如果没有这样的立法，“我们现在，以及将来，在网络世界中都很容易受到攻击”。