物联网面临的社会工程学攻击

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Social engineering attacks you might see in the IoT		
原文作者	Tyson Macaulay	**原文发布日期**	2015 年 3 月 4 日
作者简介	Tyson Macaulay 是 Global Telecommunications Strategy（全球电信战略）的副主席兼首席技术官，他负责支持 tier-1 载体安全解决方案的开发，服务供应商和电信设备制造商。https://blogs.mcafee.com/author/tyson-macaulay		
原文发布单位	迈克菲实验室		
原文出处	https://blogs.mcafee.com/business/social-engineering-attacks-might-see-iot		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
免责声明	本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安		

	天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。

物联网面临的社会工程学攻击

Tyson Macaulay

2015 年 3 月 4 日

以下是我们也许会看到的极易出现的两类攻击场景，是对我上次发表关于 IOT（物联网）社会工程学文章的进一步讨论。

攻击场景 1：反射定位并攻击

物联网在处理和存储方面，往往过于局限而不能带来广泛的攻击和操作效应。另外，对于罪犯来说，它们也许并不具有内在价值；然而，它们可作为用于驱动针对家庭或企业内强大的计算平台的高效的社会工程学平台。

设想一下：一个攻击者控制了一个物联生态系统：假设他们要攻击基于云的附带 IoT 产品的服务，如修复和内容管理（智能电视就是这么做的）。假设攻击者控制了云服务，或只是控制了部分允许信息被添加到智能电视与该云服务间的数据流网络元素 。该攻击者会向所有智能电视发送一条当它们下次被打开时就会自动显示的信息：

您的电视机需要软件升级。

为确保安全，其在 60 分钟内将停止工作，直至升级完成。

请登录 www.example.com/smartTV upgrade 下载修复软件，

并在与该电视机属同一网络的任一 Windows 计算机上运行该软件。

想象该主题的变化，通过任一与“云增强”IoT 有关设备（多数是它们）的控制面板显示。这相当于“IoT-钓鱼攻击”。大多数人（当然并非所有人）懂得要忽略并删除包含这类

指令的钓鱼邮件。若该类指令来自智能 IoT 设备又当如何？多数人没有经历过智能设备作为攻击平台而使用，故没有理由去怀疑。并且，他们热爱电视：“我的业余舞蹈表演还有 45 分钟就开始了！”。

与这类攻击相伴而生的额外要素是，这类攻击可以规避传统的安全系统，如桌面邮件保护与反病毒、发恶意软件和 URL（统一资源定位器）声誉阻断。这是为何？因为此类攻击并没有将邮件作为社会工程学的平台使用，而是包括了相当于带外的传输通道，与我们在安全方面的投资所在有关。好消息是：即使它们无法处理初始的社会工程学攻击，传统的安全系统也或许可以提供针对将恶意软件下载到桌面系统的保护。但在此类攻击的传播初期，它们或许无法做到。

攻击场景 2: IoT 余额攻击

世界上已有多种储值系统，这些系统的流行已逐步发展到将其视作“影子银行”的地步。Apple 和 Starbucks 这类的供应商接受并采用预付保证金方式来简化后续购买，省去了登录（或结算）信用卡数据的麻烦。同样的企业效益将会被制造商采用-转向创造生态系统和余额账户来锁定消费者及他们的钱财。

例如：你的（未来的）智能咖啡机。为了不仅可以控制咖啡机加工咖啡方法，还可以让它从其它特殊的咖啡机那里买到更多咖啡，在其中嵌入小型触摸屏。该系统当然通过互联网与基于云的门户相链接。该门户不一定安全，因此，与之相链接的智能咖啡机设备或许也一点不安全。假设，要么是此云服务，要么是此智能咖啡机被攻击了。该设备可能是被起源于家庭网络内部的台式机、笔记本电脑或移动应用程序（为了专门鉴别并攻击热门机器而研发的应用程序）的本地攻击所攻击。

一旦咖啡机被攻击就会显示：“咖啡机降价 50%出售，仅此一天” “请输入您的咖啡机帐户 PIN（个人身份编码）来进行购买”。像往常下订单一样将 PIN 输入机器，会打开本地存储并发布帐户数据。很不幸，此时您的帐户数据已被俘获，或订单在云门户已从购买转变为“礼物”。 接着，背后黑手利用该门户“发送礼物”这一特征将帐户的余额转移，转到一个“朋友”（幕后黑手）的帐户。或许，您只是收到您已发送的礼物作为设备界面被攻击的结果。现在，您的帐户已没有余额。如果您之前启动了某类自动充值功能，那么您也许会在帐户余额被转移几十次之后才会发现问题！

与此同时，新“朋友”一直收到礼物，并在其它店面将礼物转化为商品（昂贵的新咖啡机或其它商品），或将其发送给促使被盗商品前行的运送“接力者”（这是互联网内众所周知的技术）。一旦得手，一次盗取 25 美金，十万次就是 250 万美金，零头大概是 50 万或更多？厉害。

说句题外话，英格兰银行于 2015 年 2 月 3 日发布了一篇关于为了支持本国货币，中央银行可能使用加密货币（如：比特币）的调查论文。该论文涵盖于他们所称的“主题五：中央银行对基础的技术、制度、社会和环境方面的改变的回应”之中。