对物连网引发的安全问题的思考与对策

北京网络安全重点实验室　陆宝华

关键词：物连网　　脆弱性　　传感器　　风险

内容提要：本文通过对物连网脆弱性的分析，提出了物连网的脆弱性可能会导致国家安全和社会公共安全的所引发的巨大风险，并提出了基于网络保护和网络控制方面的防范对策。

物连网是这几年来炒得很热的概念，在中国的无锡还成立了感知中国中心，有许多物连网的项目已经建设或者正在建设当中。但是，一个问题却不能不使人越来越担忧。那就是安全问题，这里说的安全问题，不仅是指物连网本身的安全问题，更重要的是由物连网引发的社会公共安全问题。

物连网将现实社会与现有的网络虚拟社会紧密的结合成为一个整体，互联网与现实社会存在的只是相互的映射（主要的是现实社会在网络上的映射），所以网络安全对于现实社会的直接安全影响还不算大，利用网络实施的犯罪绝大多数都是间接的，从网络战的角度来看，对敌方目标的打击（除了网络目标外）也基本上是间接的。而在物连网环境下，这些情况将发生本质的变化，许多行为均可利用网络来直接实现。

一、物连网本身的脆弱性

物连网可以分为这样几个大的部分，一是基础网络，如目前的互联网；二传感器，是将“物”连接到网络的媒介；三是连接传感器与网络的接入系统；四是 RFID；五是地理度坐标信息。

这五个大部分都存在着严重的脆弱性，有一些脆弱性是无法加固的。对于基础网络的脆弱性已经是不言而喻的了，病毒等恶意代码，黑客攻击等等每天都在发生，每年都会给世界带来极大的损失；传感器是将非电量转换成电量的元件，当然也可以用来逆向转换，用来实施控制，这样就可能带来一系列的安全问题；接入系统可以是有线的，也可以是无线的，对于无线的信息的泄露和插入并不是一件困难的事，即便是光纤由于存在着分光技术（三通）获取对传感器数据篡改和控制也不是不可能的。RFID 是无线的身份识别器，由于是无线方式的，所以窥测是极为容易的，而且如果将 RFID 复制，便可以进行伪造和欺骗。也可以侵入 RFID 数据库，修改 RFID 的属性。

二、对国家安全的影响

网络战是目前全世界许多大国都在抓紧研究和带有战略性的部署，美国已经成立了网络战部队。但是基于计算机网络的网络战，除了对连网的计算机系统目标能够直接打击外，多数情况下对于非连网的其他目标还不能实施直接打击和破坏。在基于物连网环境下，网络战的直接打击目标绝不仅仅是连网的计算机系统目标。各种视在目标也都可能是被打击的对象。美国对伊朗的离心机的破坏和伊朗诱落美国的无人机，都可以看成是网络战直接破坏视在目标的预演。而物连网建成后，这种打击的目标会变得更加广泛，手段也会是五花八门。如制造恐怖事件，破坏基础设施和工业设施，破坏交通运输等等。这些都不是危言耸听，去年的 7.23 涌温线的动车相撞是一起责任事故，这种责任事故会不会变成恐怖事件的翻版呢？

三、对社会公共安全的影响

网络的发展，导致了利用网络进行犯罪，目前形形色色的网络案件频繁发生，但是这些案件绝大多数是将网络作为通信或者媒体工具，除了对网上银行等金融系统可以实施直接的犯罪，而对于其他领域，网络仅仅是犯罪的间接手段。

在物连网环境下，不仅网络遍布到各个角落，而且自动化程度会相当的高，整个社会似乎是在被机器控制和管理着。所以，笔者认为除了性侵害犯罪没有办法利用网络直接实施以外，其他的犯罪几乎都可以利用网络来直接实施。而且，由于是利用网络，使得面对面进行

犯罪的心理障碍没有了，一些犯罪可能就像在玩游戏。

对经济的影响

物连网可能导致的安全事件对经济建设的影响，目前还无法做出科学的预测，但是可以肯定的说，一旦发生了恶性安全事件，对国家经济的打击肯定是巨大的。7·23，甬温线动车相撞事故后，国务院调查报告中给出的数据：“造成 40 人死亡、172 人受伤，中断行车 32 小时 35 分，直接经济损失 19371.65 万元。”

一些机构和个人也做了统计，下面这段文字是采用了网上的一个统计数据：

“事故发生后高铁概念板块整体重挫，高铁指数下跌 5.81%，33 只高铁概念股(剔除停牌个股)总市值蒸发 316 亿元。尽管随后多家上市公司发布澄清公告，撇清与事故的关系，但仍然未能遏制整体颓势。不仅如此，在外媒对中国高铁也是一片"唱衰"，风头正劲的高铁出口前景也黯淡了。至于究竟本次事故会给中国经济发展造成多大的影响，还有待时间的检验。”

7.23 涌温线动车相撞事故，和上海地铁列车追尾事故，已经在给我们报警了；同样，伊朗将美国的无人机诱捕也是基于物连网的战术。

物连网肯定会给人类带来巨大的利益，所以不能因噎废食。但是，如果不能对可能产生的风险及早进行研究并拿出相应的对策，那么后果也将是可怕的。

为了能够及早的进行防范，笔者认为应该从以下几个方面采取相应的措施。

一、提升物连网整体的防范水平，尽可能的减少和消除各要素的脆弱性

防范针对和利用物连网的犯罪，首先就应该有一个本身强壮的物连网络，减少和消除各类脆弱性，对可能存在的威胁源进行屏蔽。

1、提升基础信息网络的防范水平

目前的基础信息网络的防范水平是极其脆弱的。首先基于 IPV4 的互联网协议存在着大量的漏洞，每年由于这些漏洞导致的安全事件不断发生。而且地址资源已经枯竭，无法支持将来物连网的使用。IPV6 在安全性上，相对于 IPV4 已经有了极大的提升，但是仍然还存在着不安全的因素。其次，由于各网络节点服务器上的操作系统和应用程序存在着大量的安全隐患，使得入侵者能够轻而易举的对数据进行窃取和改变。

因此，笔者认为应该对传统的基础信息网络进行大力的改造，提升基础信息网络的防范水平。

（1）在 IPV6 的基础上，进一步提升网络的安全性，如引入可信计算技术，强审计和强认证技术等。

（2）提升各网络节点服务器的操作系统的级别，目前的几乎全部的互联网上的节点服务器所使用的操作系统均是 DoD 标准中的 C2 级水平的。由于对操作系统本身的完整性不具备保护能力，所以入侵者很容易进入系统，并窃取和破坏用户数据。病毒等恶意代码也频繁的破坏系统，而导致大量的安全事件的发生。对于，整个网络上的主机服务器我们不能，也不必要全部提升操作系统的级别，但是对于一些关键节点的服务器（一些重要数据库的服务器），则必须提升操作系统的安全级别，使之达到 B 类操作系统的水平，对操作系统本身的完整性有相应的保护。目前这方面技术在国内已经得到了成功的验证，经过提升的服务器操作系统，病毒、木马等恶意代码无法再对其进行感染。可以这样认为，只要被提升的安全机制没有被破坏，就意味着对恶意代码有免疫作用。

（3）在网络上引入时间戳技术，以防范重放攻击。

2、加强对物连网其他要素的安全性研究，提升防泄露和防篡改的能力。

3、一些关键的、要害的部位，不宜进入公共网络。

二、建立全国性的网络犯罪监控、防范与取证体系。

1、首先建立全国性的网络犯罪监控、防范与取证体系。

这个体系应该是一个全球黑客定位、黑客分类和分级、黑客跟踪、黑客行为分析、取证系统。应致力于跟踪分析全世界范围内的黑客攻击行为及事件，整合成一个集黑客信息、攻击行为、攻击方式、捕获到的 0day 等信息为一体的数据库，并以此为更多产品及服务提供云端数据接口、报表以及参考依据。

反恐对任何一个国家都是一个巨大的挑战，因为一直以来我们都无法知晓恐怖分子带着何种目的从哪里来？何时来？使用什么武器？目标是谁？我们在面对互联网黑客和恐怖分子时也是一片茫然，面临同样的挑战！而在物连网环境下，这种挑战还会更复杂。难度为更高，更需要这种全国性的监控系统。

通过对黑客的行为及行动轨迹分析，我们可以清楚的知道：

- 黑客从哪里来
- 到哪里去
- 做了什么
- 用什么工具和手段
- 攻击结果如何

真正做到全方位跟踪任意黑客的攻击行为，分析其特征及目的。

建立这样体系，就需要在重要的网络节点，国际出口，及重要的接入网络边界安装相应的监控工具，并且建立集中的监控中心。通过对即时的和历史的数据关联，不同地域的同类行为关联等，进行安全事件的预警、防范、和取证。

2、应该加强基于物连网环境的取证技术研究

目前基于互联网环境的取证技术研究，已经取得了一定的成就，通过对审计技术、IDS 技术、报文分析技术、IP 确认技术、路由信息分析、多媒体数据分析、存储介质分析、数据分析等，可以对部分信息安全事件的认定、形成有效的证据链。

在物连网环境下，仅有目前水平的取证技术研究是远远不够的，还需要对物连网的一些特殊环节的取证技术进行研究，如：传感器数据的审计、RFID 与地理坐标信息的轨迹分析技术、传输通道中的异常数据流分析等。

3、电子证据与现实社会中的证据关联技术研究

物连网是将传统社会向网络社会转移，利用物连网实施的犯罪，也必然会有现实社会中的痕迹，在形成证据链时，也不忽略现实社会中的痕迹。应该将现实社会中的行为痕迹与电子证据之间进行关联。