万物互联下的物联网安全问题浅析

李鸿培

2015.12

随着移动互联网、物联网技术的快速发展，智能家居电器、智能汽车以及各式各样的穿戴式装置，这些智能装置都可以连接至网络，能够轻易地从中获得资讯，为人们的日常生活带来前所未见的便利。同时，云计算、大数据、物联网等新技术也在更快地融入到传统的产业中，物联网（IoT）有望激发下一代的工业革命，实现制造业、零售业、交通运输业和家用设备的自动化。这将是一个万物互联的时代，依据 Gartner 最新报告，预计在 2020 年将会有超过 250 亿个连接互联网的智能装置，而物联网更会为全球带来规模巨大的经济效益。而“万物互联”及“物联网平台”则被视为 2016 年的十大战略科技趋势。

李克强总理在 2015 年的政府工作报告中提出“制定‘互联网+’行动计划，就是要利用互联网、物联网以及信息技术，融合传统行业在内的各行各业，在新的领域创造一种新的生态。而这种新的产业生态的健康发展离不开城市基础设施及其职能服务的信息化、智能化显然，当前国内“智慧城市”（智慧医疗、智能交通、智能电网、智慧水利、智慧社区、智慧政务、智能制造、智慧物流、城市智能监控等）及试点建设以及“中国制造 2025”战略规划也将极大地促进物联网在城市关键基础设施以及企业自动化生产系统中得到更为广泛的应用发展。

万物互联虽然为我们工作和生活带来了诸多便利，但这种广泛的互联性也为黑客的攻击提供了便利。针对个人来说，当相关可穿戴智能装置到处印刻着健康指数、行为习惯、生活偏好和工作履历痕迹的时候，个人隐私泄露的危险大大增加。万物互联时代，大量智能设备/系统必然存在的脆弱性以及因其互联而产生的海量高附加值数据，必将为安全研究者与黑客提供广阔的攻防研究空间，也必将掀起一个新的攻防研究热潮。近年来，陆续报道的特斯拉汽车安全破解、海康威视摄像头安全门以及 GeekPwn、Pwn2Own、DEFCON 等黑客大会上频繁出现的覆盖智能家居、智能穿戴、智能终端、智能交通、智能娱乐等多方面的智能设备的安全破解竞赛，表明物联网安全已成为当前安全行业的热点。

至于能源、交通、水、燃气、医疗以及关键制造业等涉及国计民生的关键基础设施的工业控制系统，因其重要性，自从 2010 年震网事件以来，这些系统更是黑客们研究和攻击的重点，不仅这几年安全事件频发，而且一些用于控制工控系统的恶意软件也被陆续曝光，诸如，BlackEnergy、Stuxnet、Shamoon 以及 Dragonfly/Havex 等。工控系统因其早期开发时多

重视功能实现，忽视安全问题，而造成安全脆弱性普遍存在的现实也加重了工控系统所面临的安全风险；即使被广泛用于物联网嵌入式设备及工业控制领域的 VxWork，也有多个安全漏洞被发现。根据 CNCERT 的漏洞库 CNVD 的统计数据，近年来工控系统相关的漏洞累计已有近千条，并且多为高风险级别的漏洞。而且这些工控设备因种种原因不能及时实现系统更新/或打补丁，多数情况下只能“带病”运行。

随着“互联网+”战略的推进，各种联网和智能化、自动化传感装置的应用，预计 2016 年工业控制系统所面临的安全风险态势将会更加严峻。RSA 总裁 Amit Yoran 在回顾 2015 年网络安全行业，预测 2016 年的行业趋势中就指出：ICS（industrial Control System，工业控制系统）将成为攻击突破口。

针对工业控制系统所面临的安全风险，国内外的安全业内都给予了极大的关注，陆续出台一系列的研究报告、标准规范（NIST 的 ICS 安全指南、IEC-62443 等），国内也诞生了一些专注于做工控安全的企业（比如，威努特、力控华康、海天炜业、匡恩等），同时传统安全厂商的网御神州、绿盟科技、启明星辰、中科网威以及工控系统厂商西门子、施耐德、和利时等也都基于自身的优势推出了各自特色的安全产品或解决方案。而知道创宇的“钟馗之眼（ZoomEye）”则是通过提供网络空间中工控/物联网/网络设备的发现与系统信息检索能力，帮助系统安全人员审查所管辖工控/物联网设备是否暴漏在互联网上，进而可调整相应的安全防护策略，降低系统遭受黑客直接攻击的风险（当然黑客也可用其快速定位攻击目标，这是一个双刃剑）。由于工控系统安全属于一个跨界的、快速增长的新兴市场，需要工控系统厂商、信息安全厂商、IT 系统厂商、系统使用方（用户）以及政府监管方等多方协同，发挥各自专长，构建一个合作共赢的生态环境。

通过过去几年的市场培育和研究的深入，国内部分企业的解决方案和产品已经逐渐成熟，并且已有部分项目得到落实，工控系统安全的市场正在被逐步扩大。根据 Gartner 的预测：基于日益严重的 ICS 系统所面临的安全威胁及可能的存在严重破坏后果，来自政府合规性的推动也越来越明显，预期 2016 年，工控系统安全市场会加速成长。

工控系统厂商因其在工控系统的技术、渠道与品牌方面具有极大的优势，也许这些厂商更愿意把相关安全工具/机制整合到工控系统建设方案中。从这个角度来看，解决其安全技术能力不足的方法，要么是找一个合适安全厂商合作，要么就是兼并收购一个专注于工控系统安全的团队。 在工控系统安全市场快速增长的时候，兼并收购预期应该会增加。但就国内情况来看，这种并购的机会其实并不多（因为国内专注于做工控安全的团队本就不多），也许国内各方进行项目、技术或方案层面的多层次战略合作会更切实。

回到技术层面，NIST 的 ICS 安全指南中对 ICS 所面临的安全问题进行了归类总结：①阻断或延迟 ICS 网络中的信息流，干扰 ICS 的操作；②非授权修改 ICS 设备的控制命令或报警阈值，造成 ICS 设备功能失效、关机或受到损毁，甚至危及人员生命安全；③向系统操作者发送错误信息，导致错误的操作行为；④篡改 ICS 软件的配置项；⑤ICS 软件受到恶意软件的感染，干扰系统运行或窃取敏感数据；⑥干扰或破坏 ICS 的功能安全系统，等等。针对这些安全问题，可以从不同的系统层面结合适当的安全防护技术、开发相应的安全产品综合考虑来应对：

- **工控系统的脆弱性评估工具与服务**：虽然工控系统中存在的漏洞很多情况下难以通过系统升级或打补丁的方式消除风险，但通过工控系统漏扫和配置审查工具，可以帮助了解系统存在的安全脆弱点以及不适当的安全配置，这也将是工控系统安全防护战略的重要部分，可以在“知己”的基础上优化安全防护策略，是系统面临的安全风险最小化。许多 ICS 安全服务提供商都会将系统脆弱性评估作为其安全解决方案的重要组成部分。
- **终端管控**：在终端系统上可以加强对端口的管控、禁止或限制 U 盘等移动设备的接入，这可有效避免恶意软件的传播；同时采用应用程序白名单方式确保只有通过认证的可信应用程序才能够执行，可有效降低恶意应用程序产生的风险。
- **身份与访问管理**：针对 ICS 的非授权操作问题，首先身份和访问管理（IAM）机制是进行合法用户的身份认证以、访问授权以及规范系统操作的行为，进而可通过操作行为的合规性审查/审计机制发现和阻止对 ICS 的非授权操作（或误操作）。
- **网络层安全管控**：ICS 安全产品仍将侧重工作在网络层，首先在网络层可方便实现网络隔离、数据安全以及访问控制；其次因为种种原因难以为工控系统设备提供内置的安全性、升级或打补丁，网络层面的入侵检测、行为监管以及阻断防护（FW、IPS）就成了必然的选择；第三，网络层协议具有相对的通用性，可提高安全产品的通用性和可扩展性；第四，一些专业的 ICS 安全厂商在进入 ICS 安全市场时，因顾及工控系统的业务连续性，前期也多从网络攻击检测、审计类产品开始着手。
- **安全监测预警与威胁情报服务**：物联网系统复杂，互联的智能设备品种繁多，所面临的安全问题也各种各样；同时 ICS 系统因其重要性，也可能会遭受类似于 APT 之类的定向攻击。为保证其安全，在了解系统自身安全状况（脆弱性及防护资源）的前提下，尽可能了解相关的各种安全威胁信息（安全行业内称其为“威胁情报”，诸如：大规模网络攻击信息、安全态势报告、攻击方法及防护实践、漏洞信息、可

机读的安全规则等），将有助于用户及时调整策略，建立对潜在的可能攻击进行监测、预警与及时响应的能力。这对于系统漏洞无法及时进行加固的工控系统来说，能够及时的发现针对漏洞的攻击行为，通过有预案的应急响应或快速处理来减损或止损的方案将更为有效。因此，在万物互联时代，针对物联网/工控系统的安全，应建立基于“威胁情报”的全新安全监测与防护体系，加强与国家公共部门及第三方的威胁情报合作，及时获取、交换、分析、整合系统相关的威胁情报信息；进而通过提供“基于威胁情报感知的防护手段”，提升纵深防御体系中各安全机制间的协同与综合防护能力。

随着“互联网+”国家战略的快速推进，物联网和工控系统的安全也日益受到重视，安全机制间的快速协同与智能控制将为可用于物联网/工控系统安全的安全威胁情报分享提出更为迫切的需求。据 Gartner 的预测：“到 2017 年，30％的威胁情报服务将会提供物联网相关的威胁情报。”