

从互联网的核心梳理网络安全防线

编者按：互联网、移动互联网的发展，一方面给人类生活带来极大的便利，另一方面新的安全隐患也随之而来。近年来，随着工业发展，我们进入了一个万物互联的物联网时代。连接所带来的边界消失，信息壁垒瓦解，一方面加速了工业信息化的发展，另一方面安全更是成为不容忽视的重要一环。如何构筑一条网络安全防线，为工业互联网的发展提供安全保障？在中国信息协会信息安全专业委员会 2018 年会暨第八期网络安全创新发展高端论坛上国家网络信息安全技术研究所第三研究室、网络安全应急技术国家工程实验室副主任何跃鹰从互联网的本质出发，梳理网络安全的防护思路，本刊撷取部分内容，以飨读者。

从互联网到移动互联网再到物联网，IT 技术一直是其核心。追溯过去，互联网出现前有通信网、工业网，但他们都不是互联网，而是一个孤立的网络，有各自的标准，在各自领域发挥作用。从互联网到移动互联网到物联网，抽象来讲，计算机构建的核心是 0 和 1，任何复杂的东西追溯到最后都是 0 和 1，网络安全是攻和防，网络构成是一个端点和一个线，不管多么复杂的网络最后都归结为一个端点、一个线。所以无论是互联网、移动互联网，还是物联网从本质看是没有区别的。

物联网之所以会引起关注，是因为物联网与我们每个人息息相关。我们除了生活在一个真实的世界，还生活在网络空间中。在物联网安全中，从网络攻击方面来看，物联网时代，我们的人可能也会遭受攻击，例如：心脏起搏器受到控制，互联网冰箱有可能遭受攻击，甚至是工厂、城市。

移动互联网发展到下半场有一个非常简单的应用平台，即：云管端。移动互联网时代的端是手机，物联网时代的端是各种各样的物件。网络的发展会越来越复杂，每个人在网中，会发现真实世界和物理世界完美地结合在一起。

首先，从端的角度来看，在物联网时代，硬件和软件会呈现一个碎片化的特征。无论是工业互联网还是工控系统都是一个笼统的概念，烟草、石化、电网等不同行业都有各自的标准、平台，所以从安全角度来看，会呈现出一个碎片化的特征，从端的角度来说，这是一个挑战。

其次，从网络角度来看，互联网是固定的网络连接，包括计算机网、工业网，但是到移动互联网时代是移动网络连接，到物联网时代其实是一个泛在的互联。这其中最大的本质改变是随着物联网的发展引进不存在内网、外网了，很难做到内网、外网分开。

最后，从云的角度看，通用云到物联网云最大的区别是，通用云联网的机器是程序在跑，随着物联网的发展要加上控制功能。例如，在联网电梯实验中，电梯是非常传统的设备，但是在云平台里，可以使电梯起停。所以在物联网安全中，最大的威胁之一是在云平台上可以实现远程操控。所以物联网终端的防护会是一个难点。

物联网安全与通信网络安全会交织在一起，会相互影响。不仅仅是从互联网端发起攻击去攻击物联网，同时反过来还可以通过物联网调来攻击通信网络，这是第二个挑战。

在云平台上，除了业务平台安全，包括云架构的安全，更重要的是数据安全。在互联网中大部分是用户信息，而在工业互联网中有很多重要的工业数据，所以对于数据安全的防护则显得更加重要。

随着物联网的发展，越来越多的设备联网，首先从端的角度，传统设备要做最基本的网络安全检测，设置一个安全门槛。其次在云平台上，对其进行安全监测。总体而言，安全要回归到构成的网，要认识这个网、了解其结构、特点。