AhnLab

安全月刊

2017.03 Vol. 52

Security 4.0

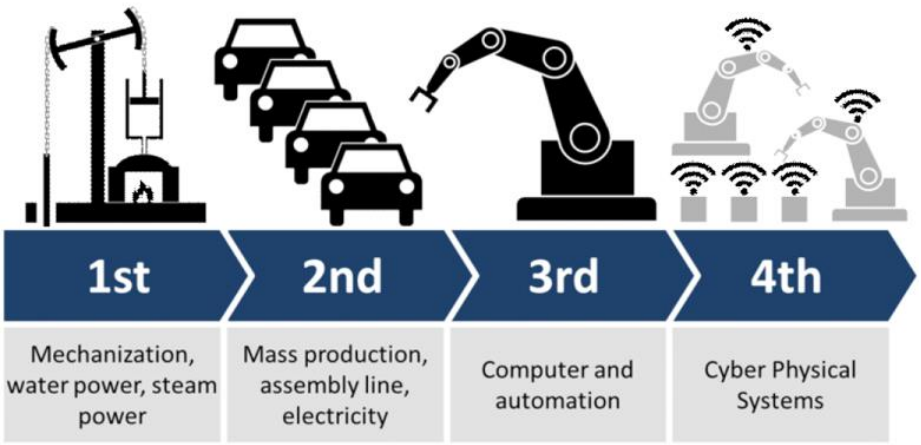
关于第四次工业革命时代安全战略的建议

第四次工业革命变革安全形势

未来十年，世界将如何变化？这是一年前在瑞士达沃斯举行的世界经济论坛(World Economic Forum)上提出的问题。工业4.0(Industry 4.0)，即是这个问题的答案，同时也成为了全球性的话题。说到工业4.0或工业革命4.0，很容易联想到“智能工厂”、“无人机”、“3D打印机”等。然而，这不是一个单一的产品、技术、或特定的工业领域，而这涉及到工业和我们生活整体的变化。那么，第四次工业革命会带来什么样的结果，并且我们的生活将会有什么变化呢？迎来第四次工业革命时代，“网络安全”被重视的理由又是什么呢？

在本文中，首先简单解析即将到来的第四次工业革命概念，然后再来了解与此相关的安全威胁的变化和响应战略。

2016年世界经济论坛描述了未来十年，即到2025年将出现的技术变化和我们的生活变化的前景。世界各地的专家们提及到了如下的几个部分：▲可移植的移动手机的商业化；▲连接到互联网的衣服；▲没有信号灯的城市；▲通过人工智能执行公司会计审计。在这些对未来的未来图像的背景下出现了工业4.0，即第四次工业革命的概念。



【图 1】第四次工业革命（*来源： Christoph Roser, AllAboutLean.com）

如【图 1】所示，第一次工业革命利用蒸汽机实现了机械化；第二次工业革命则构筑了大规模生产系统；随着计算机和数字通信的扩散实现了生产系统的自动化，这即是第三次工业革命。工业革命给人类生活带来了富裕，现在全世界已进入了所谓的“新常态（New Nomal）”时代。

新常态现象，即低增长、低消费、高失业率、高风险状况持续的现象，以美国、日本、德国等发达国家为中心，从2000年初开始出现，并导致长期停滞。为了躲避这种新常态现象，德国推出了工业4.0。西门子、宝马和SAP等德国的全球性公司自2013年以来一直致力于工业4.0平台中心的业务重组。

第四次工业革命或工业4.0的特点是实物和数字领域相结合，实物连接到数字，数字再连接到实物。“网络-物理系统（Cyber-physical System, CPS）”是工业4.0时代背后的驱动力。CPS是基于工业4.0的工业系统，随着计算和网络，传感器和驱动器（Actuator）的发展而数字域和物理域融合和交互的系统。

物联网显示的未来网络威胁预告片

第四次工业革命主要缘于“数字商业（Digital Business）”的扩散。数字商业有必要与传统的“信息化（Information）”分开来理解。“信息化”旨在提高相同产品的“生产力”，而“数字商业”旨在将创新的ICT（Information and Communications Technology）与传统产业相结合，创造一个新的具有竞争力的优势要素。ICT是指近年来广为人知的ICMB，即IoT（Internet of Things）、云（Cloud）、移动（Mobile）、 大数据（Big Data）。基于这些ICT，将出现到目前为止还未曾见到的各种产品。因此，安全也必须迎合新数字商业形式，变化为定制型的安全。为此，必须从对安全的观点开始改变。

为了改变对安全的观点，必须从“保护对象”的定义开始改变。IT系统为中心的当前的环境下，我们要保护的对象是我们创建的系统和数据。然而，在所有事物连接到互联网并且数字和物理领域融合的时代，数字域的安全问题表现为物理威胁。换句话说，数字域和物理域融合并交互的CPS时代，网络空间的安全损害可能转移到现实世界的安全及安保问题。

全球市场研究机构Gartner预测，到2020年，20%的安全威胁将是与物联网相关的威胁。事实上，在2016年10月，与物联网相关的安全威胁中最容易预测到的网络攻击成为了现实。被“Mirai”的恶意软件感染的约有150万个IoT设备对美国最主要DNS服务提供商Dyn发起了大规模DDoS攻击。由于此攻击，导致许多网站如Twitter、纽约时报、Airbnb、PayPal、Netflix、SoundCloud等网站无法访问。

DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

Major cyber attack disrupts internet service across Europe and US

Dyn estimated that the attack had involved '100,000 malicious endpoints', and the company said there had been reports of an extraordinary attack strength of 1.2 terabits (1,200 gigabytes) per second. Photograph: Alamy

The cyber-attack that brought down much of America's internet last week was caused by a new weapon called the Mirai botnet and was likely the largest of its kind in history, experts said.

The victim was the servers of Dyn, a company that controls much of the internet's domain name system (DNS) infrastructure. It was hit on 21 October and remained under sustained assault for most of the day, bringing down sites including Twitter, the Guardian, Netflix, Reddit, CNN and many others in Europe and the US.

The cause of the outage was a distributed denial of service (DDoS) attack, in which a network of computers infected with special malware, known as a "botnet", are coordinated into bombarding a server with traffic until it collapses under the strain.

【图 2】Dyn有关DDoS攻击的报道（*来源：www.theguardian.com）

Mirai恶意软件对物联网设备的DDoS攻击比迄今为止发生的任何DDoS攻击都更具破坏性。在两年前的2015年发生的25Gbps规模的DDoS攻击在当时就成为了社会问题，但Mirai的攻击具有1Tbps的规模或更高的规模。

更重要的是，这种攻击可以说是物联网安全现状的一个简单的例子。一些人将当前的物联网设备分为三个类型。没有确保安全的设备、无法确保安全的设备和不可能确保安全的设备。这意味着现有的所有的物联网设备都具有安全漏洞。Mirai恶意软件的攻击只不过是基于物联网的未来安全威胁的预告而已。随着物联网设备的普及进一步加快，并成为智能生产、物流和服务的重要因素，与此相关的安全威胁也将迅速增加。

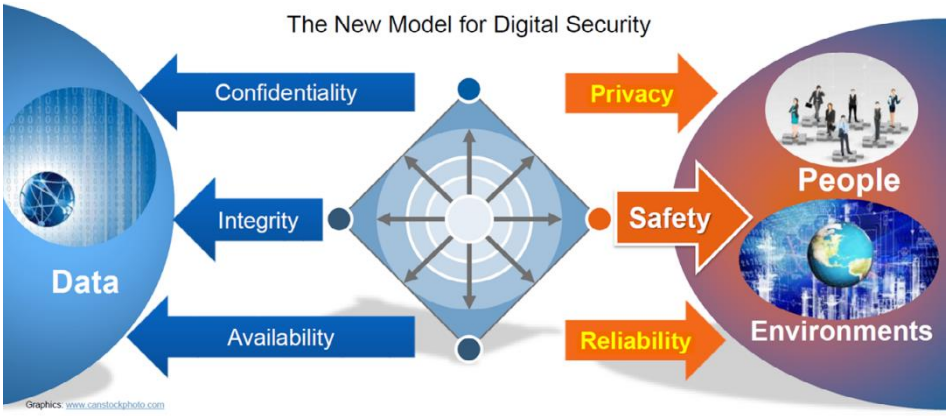
必须从接近安全的观点开始改变

通常，网络威胁和安全的关系被比喻成“矛和盾”。如果出现新的IT技术，将会出现对此的新的威胁，并将研发响应对新的威胁的安全技术。问题是，与IT技术的快速发展相比，安全产品和方法无法跟上新的IT环境的变化。因此，安全威胁和针对此威胁的响应技术和产品之间的差距越来越大。

在新时代，为了应对新的安全威胁，需要重新规划安全模型。为此，有必要：1. 通过重新解释安全对象和目的的安全模式的变化；2. 安全架构的变化；3. 安全技术的变化等。

首先，让我们探讨安全的对象和目的。作为要保护的对象，首先可以列出多个物联网传感器。大部分的物联网设备具有低功耗，执行简单的功能的传感器级设备，但需要控制和管理，使得防止用在它们初始目的之外的其他目的。另外，保护的对象还有各种智能设备。它们具有一定程度的计算能力，可以自主判断和行为，影响其他事物，甚至可以影响到人。因此，需要进行安全认证和威胁检测等措施。在企业，由于云技术的到来，许多进程和

数据已扩散到组织内部和外部。因此，需要诸如危险诊断、防止数据泄漏、加密等措施。并且还需要配合智能工作时代安全保护数据的措施。即，要保护的对象的范围随着技术和社会的变化急速扩展，网络威胁的影响也明显不同于以前，因此安全模型也应该重新定义。



【图 3】新的安全模式（* 来源：Gartner, 2016）

我们通常将机密性（Confidentiality）、完整性（Integrity）和可用性（Availability）列入“安全的三大原则”。然而，这都是关于如何保护生成和保存的数据的内容。但是未来世界不再是单一的系统上生成统一的数据的时代。此外，在未来网络世界和物理世界将直接连接，因此要保护的数据已再不限于数据。要保护的对象已覆盖到由网络系统运行的社会基础设施和使用或佩戴连接到互联网的设备的人们。即，有必要改变不仅要考虑简单的数据保护（Protection），而且要考虑对任何环境的安全（Safety）的总体的安全模式。

重新设计整体安全架构

迄今为止的基本安全架构被设计为区分内部网络和外部网络，并且在它们之间重重构筑安全解决方案。但是，在将来的数字商业时代，将出现大量的各种终端机（Device），聚集在这个终端收集的信息，平台向各种终端发送命令，最后这些将由企业用户来使用。因此，有必要为每个终端和平台，业务领域制定适当的安全策略。

同时，工业4.0的范围非常广泛，有些专门的组件仅在特定行业或企业使用。因此，比起依赖于当前的安全技术，更重要的是对组件本身内装安全功能，以代替当前的静态边界安全，并强化设备级的细微的边界安全。尤其是，内网和外网的二分法的规定已不再有效，因此必须通过更细分的区分来树立适合每个部分的安全技术和策略。此外，随着工业目的的变化，将出现新的系统，又会出现新的安全威胁，这就需要建立对新的安全威胁的分析和响应方案。在这种多变的环境中，任何组织或安全提供商都难以提供覆盖所有领域的解决方案。这就需要重新设计整体的安全架构，使企业和安全提供商以及安全提供商之间共享威胁信息。

安全技术将如何变化？

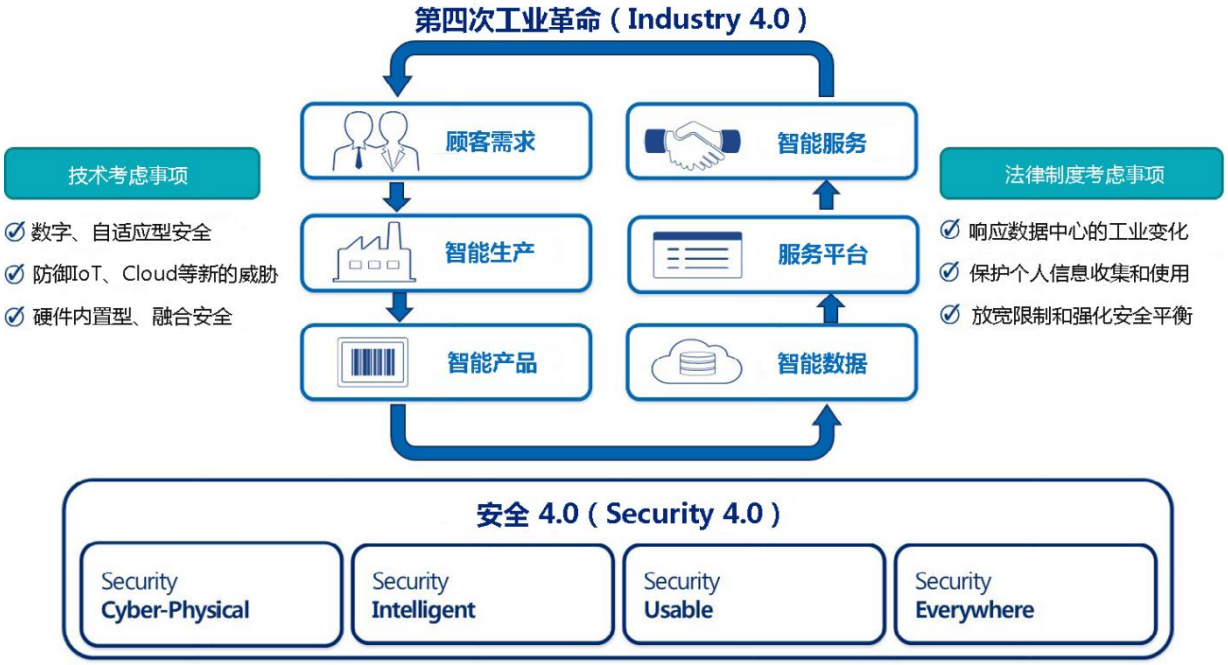
当安全对象和安全模式，架构等发生变化，安全技术也需要变化。诸如认证、加密、大数据分析、威胁评估、检测等技术类别是目前仍然存在的技术，但详细的技术随着对象将迅速变化。此外，基于人工智能的安全技术围绕主要安全提供商（包括AhnLab）将具体实施。

首先，安全技术的研发将伴随硬件或软件产品的设计起点，而不是以前的先制造硬件后研发相应的安全技术。将转变为反映包括设备的设计、开发、运营整个过程的安全技术和进程的，而不是现有的简单的安全系统的构筑和

运营管理。在企业引进解决方案时，构筑适合于该行业的系统时，从产品的设计阶段到运营阶段，安全将一起应用。为此，若以前采用的是在系统准备以后才构筑安全解决方案并运营的方式，那么以后将转变为在初期开始进行安全构筑事业。

安全4.0（Security 4.0）的时代

到目前为止，我们一起来了解了第四次工业革命时代的安全威胁前景和安全技术的变化。如工业革命类似，安全也可以按时代进行区分。在大型机军用计算机在1970年左右投入实际使用的时代，对独立型（Stand-alone）计算的安全技术是核心。在20世纪80年代，以太网被开发，企业内的计算机被连接，形成了服务器-端点的结构，这个时期被称为安全的第二代。进入2000年，互联网开始传播，全世界的系统开始连接，此时期被称为安全的第三代。在2010年中期以后到现在是以物联网、云、大数据、移动为主力的时代，我们可以称为安全的第四代（Security 4.0）。



【图 4】Security 4.0

在前面解释说，第四次工业革命是整个工业平台的改变而不是特定技术或产品的改变。在这种情况下，为了避免安全风险，需要能够快速应用于环境变化的自适应安全（Adaptive Security）技术。特别是，需要融合硬件和软件的安全技术来防御在物联网和云环境下出现的新的威胁。此外，有必要通过自动收集和分析客户需求来确保针对新的安全威胁的情报。为此，需要制定政策来减轻或补充和加强各种规章与第四次工业革命之间存在的隔阂。

由于第四次工业革命正在进行中，并处于动态发展的阶段。因此，特定第四次工业革命时代的安全技术和安全解决方案还为时尚早。近年来，AhnLab通过数多年的积累和研究，一直致力于持续新技术的开发，主要以四个领域为中心。首先是，在所有事物都连接的时代，将最小化不适，这个不适是安全的代价。第二是，通过收集有关新威胁的信息，建立分析的情报，基于人工智能积极响应新的威胁。终极目标是利用物联网、云、大数据来构筑整体威胁响应体系，同时为网络区域和物理区域连接点建立安全措施，不仅是设备和系统的安全，还要实现对人的安全。

AhnLab

安全月刊

http:// cn.ahnlab.com
http://global.ahnlab.com
http://www.ahnlab.com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，
确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。
我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、
移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。
AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ahnlab.com