gemalto
security to be free

打造更加安全的物联网

金雅拓指南：如何将物联网打造成为安全的连接平台

驾驭第二次数字革命

物联网(IoT)对社会的影响势必会比之前的数字革命都更加强烈。与所有新技术一样，物联网也存在挑战 – 如物联网的安全漏洞及隐私泄密可能会导致重大的损失。因此设备和数据均需得到安全保护。

目录

无限可能源于信任

想象一下未来，我们的周围全是连网设备，帮助我们节省时间、改善福利、提高健康水平并打造更加高效的工作场所。

从阿姆斯特丹到桑给巴尔，连网设备将改变整个世界：提高家庭效率、改善道路安全、鼓励我们培养更加健康积极的生活方式。

物联网依托互联网、移动性及社交媒体技术的广泛部署，旨在推动我们的世界成为更加高效多产、健康、安全的生活场所。消费类电子终端和工业设备制造商、汽车公司、服务企业以及网络和软件开发商都在借助智能连网设备构建大型物联网生态系统。众多行业的制造商都被IoT为关键业务所带来的巨大潜力所吸引，包括：

1. 降低产品的交付或维护成本。例如，通用电气正在使用IoT对喷气发动机进行预防性维护，以便及时发现故障，防止其演变成严重问题。此外，他们还使用跟踪到的飞行数据来降低燃油成本并提高效率。
2. IoT使企业有机会通过增值服务(VAS)和产品即服务(PaaS)等创新型商业模式来创造新收入。例如，劳斯莱斯的“按飞行小时保修合同”(Power-by-the-Hour)支持运营商按飞行小时支付固定费用，而不是一次性全款购买引擎。
3. 改进客户关系，尤其是那些设备一经售出便不再与用户保持联系的制造商。例如，英特尔正在为自动贩售机添加“大脑”，从而支持服务商实施买二送一活动、折扣及忠诚度积分计划来增加销售额。

构建信任

无论目标是降低成本、带来新收入、还是增进对客户的了解，这一商业模式只有在用户与供应商彼此信任时才能发挥作用。

从用户的角度来看，信任取决于连接可靠性及可用性等多个因素。从供应商的角度来看，他们需要相信能够收回对连网设备的投资(收入保证)。

但是，信任最有可能与数据保密性和安全性相关。开发人员在设计连网设备时应考虑信息的整个旅程。

“由Nexus of Forces（云、移动、社交和信息）掀起并由IoT所驱动的数字化革命对许多现有企业造成了威胁。除致力于IoT之外，他们别无选择，就像当年IT消费化一样。”

Jim Tully，Gartner副总裁兼著名分析师 (1)

万物都必须内置安全接口

动态数据将会穿越大量设备和多种网络，最终抵达云中的各个数据中心。

除非用户能够相信他们的连网设备是安全的，相信他们的隐私能够得到保护，否则，IoT将无法充分发挥潜力。因此，不仅设备中的数据需要得到保护，穿越网络的数据以及抵达数据中心之后的数据同样需要得到保护。面对这条传输链中如此众多的连接，您的安全框架必须是互连的、协调一致的，只有这样才能避免数据破坏、窃听、拦截或意外泄露。

1/5

到2020年，1/5的上路车辆都将配备某种形式的无线网络连接，全球连网车辆将超过

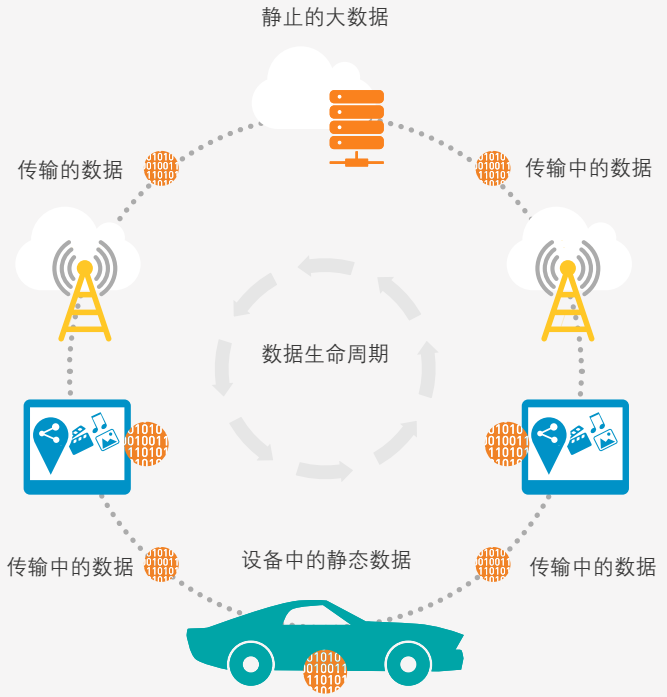
2.5 亿

来源：GARTNER

IoT的主要优势之一在于任何物体 – 无论是汽车、智能电表还是健康监测仪 – 均可在一瞬间成为网络环境中的一份子。某些IoT设备将负责运行我们的关键基础设施，如水、电、公共医疗和交通等，因此也将成为工业间谍、拒绝服务攻击(denial of service- DoS)及其他黑客攻击的对象。保留在网络中的个人数据 – 如财务记录或曾住地等 – 无疑将会成为网络犯罪的主要目标。

必须确保数据在整个移动过程中每一个环节的安全性。以连网汽车为例。连网车辆可通过访问个人日历来规划通往下个会场的最快捷路线。当车辆通过制造商提供的车载导航和娱乐系统发送信息时，必须要使用服务供应商提供的无线连接。信息的下载或发送使用云中的系统。从根本上说，“物体”需要借助互联网和云才能真正建立连接，以便在两个位置之间传输数据。

连网汽车的数据生命周期



IoT生态系统中的数据可能是动态的，也可能是静态的。静态数据是指驻留在设备或云中的数据，动态数据则是指在两个节点之间传输的数据。例如，保存在车载计算机中或通过蜂窝网络发送到云中以便开展油耗分析的驾驶数据属于静态数据。相反，媒体数据可以从云服务器传输至车载数字控制台。

保护我们的隐私

为窃取智能设备收集到大量数据，网络犯罪分子可另辟蹊径入侵我们的生活、家庭和隐私。

您在设计IoT时，绝对不能将隐私、安全性和信任置之脑后。某些情况下，鉴于所有这些设备都在收集严格保密的个人信息，因此，安全性从一开始就必须内置在设备之中，以便管理这些活动信息并控制信息访问。

我们以2015年Foscam婴儿监视器攻击为例。当时正在使用无线Foscam IP婴儿监视器的一户家庭遭受攻击。

> 攻击者控制住并四处移动摄像头，一边同婴儿的母亲对话，一边对其进行跟踪，对她的孩子评头论足。(2)

这个例子彰显出在相互连通的IoT世界中保护消费者隐私的重要性。因为在这个世界，汽车可在发生事故时自动呼叫紧急服务，就连洗碗机也能在一个晾碗架放满时自动找到另一个晾碗架。一直到现在，数据公司保存的与我们有关的大部分数据都是我们明确自愿提供的信息。

但现在，设备所收集和传输的数据日益超出个人识别信息范畴，开始创建我们在日常生活中的具体模式。

以智能电表为例。智能电表能为操控它们的电力公司收集遥测数据，以便电力公司通过分析这些数据来构建电力使用模式图。从消费者的角度来看，这相当于创建了用户在自家活动的活动记录。此类数据如落入不法分子手中，他们将有机会趁家里无人时入室行窃。

双管齐下：隐私保护与身份认证

确保用户身份符实，将设备使用授权作为保护设备安全的关键第一步。

身份认证对连网设备而言至关重要。例如，当我们通过手机打开连网车辆的车锁时，我们希望确定其他任何人都不能为这辆车开锁。

但是，汽车并非一直如您想象得那般安全！澳大利亚安全研究员Silvo Cesare就曾演示过车锁的安全漏洞，这个漏洞使他能够关闭车辆报警系统并成功打开车门，而不会给警察留下任何蛛丝马迹。他只使用简单的软件定义无线电和天线便成功捕获到并传输无线信号，从而顺利开锁。(3)

> “消费者已经开始远离发生过数据泄密事件的企业，他们已经开始意识到与单纯的信用卡认证相比，更耐用的身份凭证将更受欢迎。”
>
> Christian A. Christiansen，IDC安全产品与服务部项目副总裁

企业平均花费

46 天

以及

200万美元

才能从一次网络攻击中恢复过来

(Ponemon Institute 2015年网络犯罪调查)

供应商还必须能够控制远程设备接入权限。电动汽车开发商特斯拉会在软件可以升级和下载时向驾驶员发送通知，从而让驾驶员知晓升级通知是直接由特斯拉提供的，而不是侵入系统的其他人所提供的。(4)

为进一步增强认证能力，指纹及虹膜扫描等生物识别数据也已开始越来越普遍用于验明正身。

来源：经济合作与发展组织

威胁不可避免

由于连网设备不断生成大量信息，因此，我们必须将注意力转移到保护有价值的数据上面。

在创建安全框架的过程中，我们首先要辨别威胁类型。以下是某些主要威胁的举例说明：

网络钓鱼

假冒拥有良好信誉的公司发送欺诈性的电子邮件，旨在引诱收件人暴露信用卡号等敏感信息。

应用程序攻击

这是黑客攻击中最容易得手的攻击类型。黑客很容易从市场上获得自动化工具并且许多都是免费工具。不同于集中式Web环境，应用程序存在于不受管制的移动设备生态系统中。移动应用中未得到保护的二进制代码很容易被犯罪分子快速进行修改和利用。二进制代码是指设备为确保应用程序正常工作而必须读取的代码。从根本上来说，就是您在iTunes或Google Play等移动商店访问移动应用时便下载的二进制代码。

DOS攻击

拒绝服务攻击旨在临时或无限期地破坏网络。此类攻击虽然有修复包可用，但就像病毒一样，黑客们总能找到新对策。

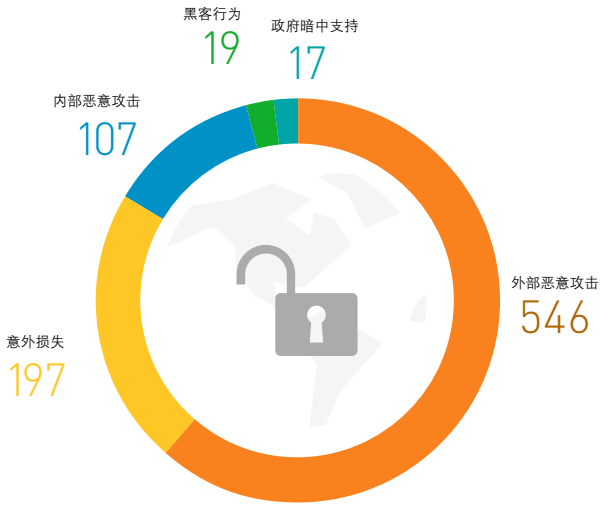
DDoS攻击

分布式拒绝服务攻击旨在通过多个来源的流量将在线服务淹没，使其不可使用。

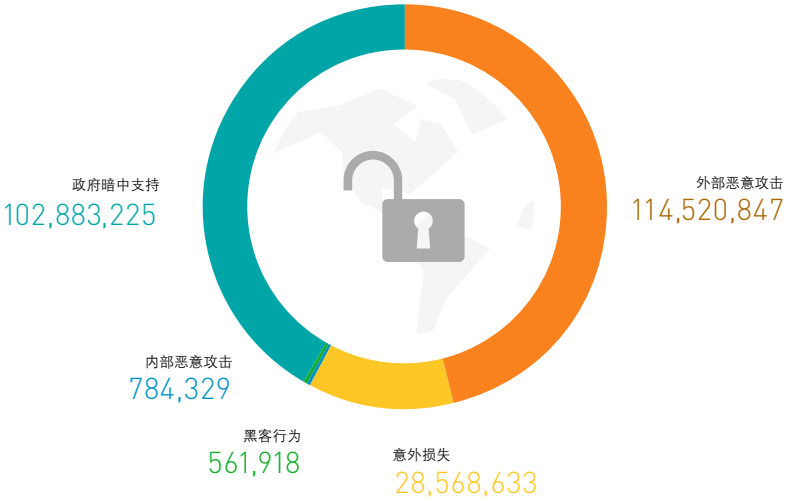
物理入侵

攻击通常都是远程行为。但物理入侵却真正篡改设备及其组件。

2015年的数据泄密事故数量



2015年受到数据泄密事故影响的记录数量



来源：数据泄露水平指数(金雅拓)

您能想到的每个设备都有可能成为攻击目标

网络中的设备数量及切入点越多，网络犯罪分子偷偷潜入网络的机会也就越多。

实际上，从智能电视、健身器及家用安全设备，到打印机、车载系统及网络化灯泡，几乎所有的连网设备都存在可被利用的漏洞。

IoT具备前所未有的容量和规模。如想加速创新并得到认可，面对日益加剧的安全挑战，设备、网络和云间的信息必须尽量确保安全。如将安全机制构建在IoT生态系统中，企业将能为消费者提供简单明了的无阻碍认证体验。

8000人

一个匿名团伙侵入欧洲航天局把盗取的姓名、电子邮箱、和密码信息泄露发布在JUSTPASTE.IT上面的三个数据转储平台中。约有8000人受到波及。

中佛罗里达大学的研究人员演示了当黑客对设备进行物理攻击时，如何能够轻而易举地盗取Nest Learning恒温器。攻击者不到15秒便将Nest从支架上拆除、插入微型USB线缆并从后门偷偷运走，而不被房主察觉。然后，黑客可利用被盗取的Nest开展不法活动，如暗中监视房主的活动、攻击网络中的其他设备或盗取无线网络证书等。(5)

赛门铁克曾使用定制的Rasberry Pi计算机来吸引黑客注意到健身追踪器中显眼的安全漏洞。安全专家发现某些设备的地理位置很容易被跟踪到。(6)

安全专家Proofpoint发现联网电冰箱在2014年节假日曾帮助黑客发送了超过7.5万封垃圾邮件及网络钓鱼电子邮件。(7)

FBI调查局在2015年4月申请的逮捕令中指出，来自美国丹佛One World Labs的电脑黑客兼安全专家Chris Roberts曾侵入一架飞机的机载娱乐系统，导致飞机暂时性偏离航道。(8)

David Stupples教授告诉BBC，如用于控制全英国所有列车的高科技信令系统遭遇黑客攻击，将会引发严重事故。负责测试欧洲铁路流量管理系统的Network Rail公司也承认这的确是潜在威胁。(9)

车内连接持续增长但是如果车辆遭遇黑客攻击将会出现什么状况。Wired记者Andy Greenberg发现当他驾驶着Jeep Cherokee在美国圣路易斯高速路上以70mph的速度行驶时，车辆已被黑客“接管”。(10)

这些安全研究员还指出只要攻击者知道目标车辆的IP地址，便可从全世界的任何地方对47.1万辆连网汽车发动攻击。

为设备提供终生安全保护

为了增强并保持用户信任，为互联网基础提供支持的生态系统必须通过协作式伞形方法来确保物联网安全。

没有任何一种控制方法有能力阻断攻击。因此，您必须在设备开启之际便对其使用多层保护方法。简言之，您必须在从设计到运行的整个生命周期中始终确保设备安全性。

此外，为IoT提供各级保护同样至关重要，其中包括设备本身、设备与网络间的连接以及设备在云中的连接。

"连网厨房能在食品供应链及零售食品服务链的各个层面创造数字化商机。借助传感器收集的与厨房食材相关的实时库存数据，可自动生成购物单并下单，从而创建简单高效的存货清单并优化供应链管理。"

Satish R.M，Gartner首席分析师

安全保护：随时随地按您所选方式提供安全保护

要想围绕着IoT构建保护墙，您需要攻克多个相关挑战，包括：

> 连接技术的多样性：连接方式多种多样。移动网络、蓝牙及WiFi都是迄今为止的主要连接方法，但是，LoRa、UNB、PL-C、shortrange BTLe、Weightless、LTE-M及ZigBee等新兴网络技术也在其他地方找到了用武之地。每项新兴网络技术都伴随有新威胁。

> 行业多样性：IoT覆盖了从大型工业系统(如风电场)到可穿戴设备的所有领域，并且每个领域都有自己的生态系统。虽然它们的安全模式可能不同，但它们却有一个共同点，即收集大量数据。某个信息越详细，则该信息越敏感。

每个阶段的每条连接都会向这条价值链中添加一个单元。在这条价值链中的任何一点，安全解决方案都必须能够彼此协作。从用户的角度来看，保护物联网安全需要依赖安全的设备，网络，以及具备可信服务管理、数据管理及合规能力的生态系统。

适用于物联网保护的四种最佳实践方法：

评估风险 – 开发人员需了解所有的潜在安全漏洞，需对隐私、安全性、欺诈、网络攻击及IP盗用等事项进行评估。由于网络犯罪分子不断发起新威胁，因此，评估风险并不是件容易的事情。现阶段，安全专家还没有给我们推荐什么万能的通用方法。

安全始于设计 – 设备安全性是应该在开发阶段便开始考虑的重要事项，包括端点间安全保护和对策，如防篡改硬件及软件。

保护数据安全 – 您应将严格的认证和加密机制及妥善管理的加密秘钥结合在安全产品中，以便同时保护存储在设备中的静止信息及活动信息。

生命周期管理 – 安全保护不是设置后不管的一次性工作。您必须在整个生命周期中始终保护物联网设备的安全，无论是独立的产品还是集成在汽车中的产品。

到2020年，连网厨房至少能够帮助食品和饮料行业节省15%的成本。

实现全面连接世界的优势

消费者将日益被物联网的便利性所吸引，相信它是安全的。而这种信任也将推动物联网陆续履行其他承诺，如提高各行各业的工作效率、帮助医疗卫生部门节省成本以及帮助我们的城市节能减排等等。

36%

2020年，连网智能电视

到2020年，智能电视机将占到连网电视机总量的36%，达到3.2亿台(其中美国占到5600万台，中国6400万台)。

(来源：数字化电视调研报告，连网电视预测报告)

安全可信的IoT系统能为企业带来以下优势：

降低业务运营成本

例如，ThyssenKrupp Elevator在全世界负责维护超过120万部电梯。通过借助Microsoft IoT技术对电梯主动实施预防性维修保养，公司可确保延长电梯使用寿命，并且公司接听到的求助电话数量也已开始减少。(11)

减少因数据泄密而生成的法律诉讼及相关成本

IBM及Ponemon Institute开展的联合调查显示，企业因数据泄密而需要支付的平均总成本高达379万美元。提高安全性可降低风险。

为合作伙伴带来更多机遇

IoT能为合作伙伴开辟更多市场并提供更多机遇。例如，Google一直在研发能帮汽车制造商制造出无人驾驶汽车的软件。

业务连续性

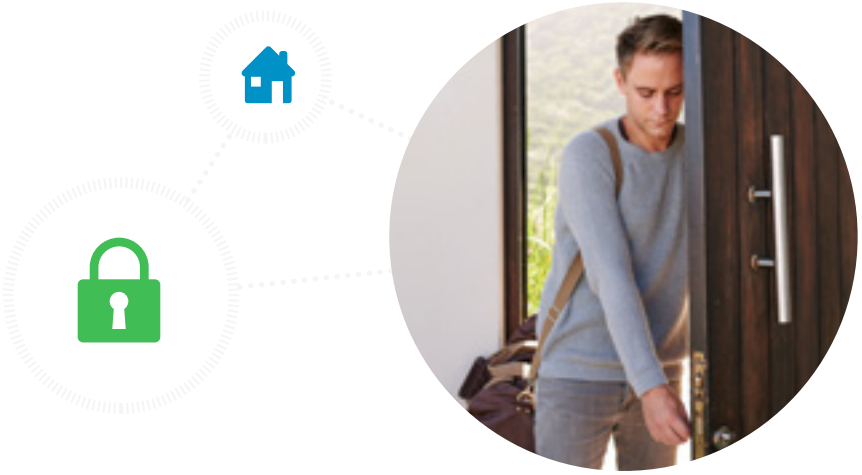
鉴于IoT生态系统中包含如此众多的参与者(设备制造商、连接供应商、云服务供应商及ISV等)，因此，这个生态系统中的所有组件和步骤都必须得到适当保护以确保不间断运行，这一点无比重要。强大的安全机制可确保企业能与客户连续开展业务，以便从中受益。

数字化世界始终都在迅速发展演进，安全的生态系统能为物联网打造更加可信的未来。

由内至外的全面安全

设备、网络和云级安全性乃是确保物联网安全高效运行的关键，可同时保护静止和传输中的数据。此外，您还必须利用支持设备在物联网生态系统中执行任务的智能性来助力设备识别并抵御恶意威胁。金雅拓始终致力于提供强大的安全解决方案，帮助这个由数十亿个连网“物体”创建的日益复杂的世界变得更加美好。

今天的创新仅仅是个开始。IoT将在我们未来的工作和生活中无处不在。但是，消费者的信任乃是这些联网“物体”充分发挥潜能的唯一方式。金雅拓能为您部署物联网提供万无一失的通道，确保您始终安全，享受真正连通的世界带来的优势。



金雅拓用于保护物联网的核心产品

- 软件激活与许可
- 动态密钥管理（适用于认证和加密）
- 密钥证书及令牌的安全配置

- 大数据加密
- 服务器保护
- 云应用安全性
- 安全的设备接入
- 敏感数据安全性
- 通信加密
- 保护软件完整性

如需了解更多信息，请访问**gemalto.com/iot**
或发送电邮至**iot.query@gemalto.com**

来源：

(1) Gartner Symposium/ITExpo 2014

(2) Foscam baby monitor hack

(3) Silvo Cesare car lock hack

(4) Telsa firmware updates

(5) Hacking the Nest Thermostat

(6) Symantec security flaws in fitness trackers/wearables

(7) Fridges sending spam

(8) Aeroplane hack

(9) Train hack

(10) Jeep hack

(11) ThyssenKrupp elevators reduced downtime with IoT

gemalto
security to be free