物联网安全架构初探*

武传坤

(中国科学院软件研究所信息安全国家重点实验室 北京 100190)

摘要 物联网是信息技术发展到一定阶段的产物,是全球信息产业的又一次科技与经济浪潮,将影响到许多重大技术创新和产业的发展,受到各国政府、企业和科研机构的高度重视。同时,物联网的信息安全问题是关系物联网产业能否安全可持续发展的核心技术之一,必需引起高度重视。因此如何建立合理的物联网安全架构和安全体系将对物联网的安全使用和可持续发展有着重大影响。本文试图从不同层次分析物联网的安全需求,搭建物联网的安全架构体系,希望为物联网可靠的信息安全系统提供理论参考依据。

关键词 物联网,安全架构,信息安全

DOI:10.3969/i.issn.1000-3045.2010.04.007

武传坤研究员

物联网是一种新生事物,在其概念、内涵和外延尚不明确的情况下,各地纷争建立物联网示范工程,这种局面虽有利于推动物联网相关产业的发展,但其间也存在着严重的陷患,目前局部的或小规模的物联网示范工程项目尚不存太多的信息安全问题,因为一方面这些示范工程一般自成体系,很少与其他网络互通,因此受到的攻击来源少;另一方面,由于示范工程使用规模有限,潜在的攻击者也不愿意为此花费太大的投入,因此相对比较安全。但是,一旦这些示范工程将来发展成为真正物联网的一部分,当前看似安全的体系可能在将来会面临重大安全隐患。如何在物联网(包括小型示范工程)建立初期就建立严格规范的信息安全架构,关系到这些系统能否在真正物联网系统下提供良好的安全措施,或能够对安全措施进行升级,以保障系统的可用性。

物联网概念最早是从传感网和射频识别(RFID)发展而来的,其理念是通过网络技术将传感网信息和RFID信息进行远距离识别和处理。2005年,国际电信联盟(ITU)在每年一个专题的年度报告中发布了针对物联网的年度报告"Internet of Things"[1],报告指出RFID和智能计算等技术开启全球物品互连的时代,信息与通信技术的发展已经从任何时间、任何地点连接任何人,发展到连接任何物体的阶段,无所不在的物联网时代

* 本研究得到中科院知识创新工程重要方向项目(YYYJ-1013)资助
收稿日期:2010年5月17日

即将来临。物联网在近年来得到广泛关注，2008年国际上召开了第一届国际物联网学术交流会[2]，同年，Kranenburg出版了关于物联网的专著[3]，Yan等人也编著了一本学术专著[4]。可见物联网目前已成为国际上研究的热点。

在中国，物联网的概念是在温家宝总理去无锡考察后才引起广泛重视的。随着人们对物联网理解的不断深入，物联网的内涵进一步明朗。在2009年的百家讲坛上，中国移动总裁王建宙指出，物联网应具备三个特征：一是全面感知；二是可靠传递；三是智能处理。尽管对物联网概念还有其他一些不同的描述，但内涵基本相同。因此我们在分析物联网的安全性时，也相应地将其分为三个逻辑层，即感知层，传输层和处理层。除此之外，在物联网的综合应用方面还应该有一个应用层，它是对智能处理后的信息的利用。在某些框架中，尽管智能处理应该与应用层可能被作为同一逻辑层进行处理，但从信息安全的角度考虑，将应用层独立出来更容易建立安全架构。本文试图从不同层次分析物联网对信息安全的需求和如何建立安全架构。

其实，对物联网的几个逻辑层，目前已经有许多针对性的密码技术手段和解决方案。但需要说明的是，物联网作为一个应用整体，各个层独立的安全措施简单相加不足以提供可靠的安全保障。而且，物联网与几个逻辑层所对应的基础设施之间还存在许多本质区别。最基本的区别可以从下述几点看到：(1)已有的对传感网(感知层)、互联网(传输层)、移动网(传输层)、安全多方计算、云计算(处理层)等的一些安全解决方案在物联网环境可能不再适用。首先，物联网所对应的传感网的数量和终端物体的规模是单个传感网所无法相比的；其次，物联网所联接的终端设备或器件的处理能力将有很大差异，它们之间可能需要相互作用；再次，物联网所处理的数据量将比现在的互联网和移动网都大得多。(2)即使分别保证感知层、传输层和处理层的安全，也不能保证物联网的安全。这是因为物联网是融几个层于一体的大系统，许多安全问题来源于系统整合；物联网的数据共享对安全性提出了更高的要求；物联网的应用将对安全提出了新要求，比如隐私保护不属于任一层的安全需求，但却是许多物联网应用的安全需求。

鉴于以上诸原因，对物联网的发展需要重新规划并制定可持续发展的安全架构，使物联网在发展和应用过程中，其安全防护措施能够不断完善。

1 感知层的安全需求和安全框架

在讨论安全问题之前，首先要了解什么是感知层。感知层的任务是全面感知外界信息，或者说是原始信息收集器。该层的典型设备包括RFID装置、各类传感器(如红外、超声、温度、湿度、速度等)、图像捕捉装置(摄像头)、全球定位系统(GPS)、激光扫描仪等。这些设备收集的信息通常具有明确的应用目的，因此传统上这些信息直接被处理并应用，如公路摄像头捕捉的图像信息直接用于交通监控。但是在物联网应用中，多种类型的感知信息可能会同时处理，综合利用，甚至不同感应信息的结果将影响其他控制调节行为，如湿度的感应结果可能会影响到温度或光照控制的调节。同时，物联网应用强调的是信息共享，这是物联网区别于传感网的最大特点之一。比如交通监控录像信息可能还同时被用于公安侦破、城市改造规划设计、城市环境监测等。于是，如何处理这些感知信息将直接影响到信息的有效应用。为了使同样的信息被不同应用领域有效使用，应该有综合处理平台，这就是物联网的智能处理层，因此这些感知信息需要传输到一个处理平台。

在考虑感知信息进入传输层之前，我们把传感网络本身(包括上述各种感知器件构成的网络)看作感知的部分。感知信息要通过一个或多个与外界网连接的传感节点，称之为网关节点(sink 或 gateway)，所有与传感网内部节点的通信都需要经过网关节点与外界联系，因此在物联网的传感层，我们只需要考虑传感网本身的安全性即可。

1.1 感知层的安全挑战和安全需求

感知层可能遇到的安全挑战包括下列情况：

(1)传感网的网关节点被敌手控制——安全性全部丢失；(2) 传感网的普通节点被敌手控制(敌手掌握节点密钥)；(3)传感网的普通节点被敌手捕获(但由于没有得到节点密钥，而没有被控制)；(4)传感网的节点(普通节点或网关节点) 受来自于网络的 DOS 攻击；(5)接入到物联网的超大量传感节点的标识、识别、认证和控制问题。

敌手捕获网关节点不等于控制该节点，一个传感网的网关节点实际被敌手控制的可能性很小，因为需要掌握该节点的密钥(与传感网内部节点通信的密钥或与远程信息处理平台共享的密钥)，而这是很困难的。如果敌手掌握了一个网关节点与传感网内部节点的共享密钥，那么他就可以控制传感网的网关节点，并由此获得通过该网关节点传出的所有信息。但如果敌手不知道该网关节点与远程信息处理平台的共享密钥，那么他不能篡改发送的信息，只能阻止部分或全部信息的发送，但这样容易被远程信息处理平台觉察到。因此，若能识别一个被敌手控制的传感网，便可以降低甚至避免由敌手控制的传感网传来的虚假信息所造成的损失。

传感网遇到比较普遍的情况是某些普通网络节点被敌手控制而发起的攻击，传感网与这些普通节点交互的所有信息都被敌手获取。敌手的目的可能不仅仅是被动窃听，还通过所控制的网络节点传输一些错误数据。因此，传感网的安全需求应包括对恶意节点行为的判断和对这些节点的阻断，以及在阻断一些恶意节点(假定这些被阻断的节点分布是随机的)后，网络的连通性如何保障。

对传感网络分析(很难说是否为攻击行为，因为有别于主动攻击网络的行为)更为常见的情况是敌手捕获一些网络节点，不需要解析它们的预置密钥或通信密钥(这种解析需要代价和时间)，只需要鉴别节点种类，比如检查节点是用于检测温度、湿度还是噪音等。有时候这种分析对敌手是很有用的。因此安全的传感网络应该有保护其工作类型的安全机制。

既然传感网最终要接入其他外在网络，包括互联网，那么就难免受到来自外在网络的攻击。目前能预期到的主要攻击除了非法访问外，应该是拒绝服务(DOS)攻击了。因为传感网节点的通常资源 (计算和通信能力)有限，所以对抗 DOS 攻击的能力比较脆弱，在互联网环境里不被识别为 DOS 攻击的访问就可能使传感网瘫痪，因此，传感网的安全应该包括节点抗 DOS 攻击的能力。考虑到外部访问可能直接针对传感网内部的某个节点(如远程控制启动或关闭红外装置)，而传感网内部普通节点的资源一般比网关节点更小，因此，网络抗 DOS 攻击的能力应包括网关节点和普通节点两种情况。

传感网接入互联网或其他类型网络所带来的问题不仅仅是传感网如何对抗外来攻击的问题，更重要的是如何与外部设备相互认证的问题，而认证过程又需要特别考虑传感网资源的有限性，因此认证机制需要的计算和通信代价都必须尽可能小。此外，对外部互联网来说，其所连接的不同传感网的数量可能是一个庞大的数字，如何区分这些传感网及其内部节点，有效地识别它们，是

安全机制能够建立的前提。

针对上述的挑战，感知层的安全需求可以总结为如下几点：

(1)机密性：多数传感网内部不需要认证和密钥管理，如统一部署的共享一个密钥的传感网。(2)密钥协商：部分传感网内部节点进行数据传输前需要预先协商会话密钥。(3)节点认证：个别传感网(特别当传感数据共享时)需要节点认证，确保非法节点不能接入。(4)信誉评估：一些重要传感网需要对可能被敌手控制的节点行为进行评估，以降低敌手入侵后的危害(某种程度上相当于入侵检测)。(5)安全路由：几乎所有传感网内部都需要不同的安全路由技术。

1.2 感知层的安全架构

了解了传感网的安全威胁，就容易建立合理的安全架构。在传感网内部，需要有效的密钥管理机制，用于保障传感网内部通信的安全。传感网内部的安全路由、联通性解决方案等都可以相对独立地使用。由于传感网类型的多样性，很难统一要求有哪些安全服务，但机密性和认证性都是必要的。机密性需要在通信时建立一个临时会话密钥，而认证性可以通过对称密码或非对称密码方案解决。使用对称密码的认证方案需要预置节点间的共享密钥[5]，在效率上也比较高，消耗网络节点的资源较少，许多传感网都选用此方案；而使用非对称密码技术的传感网一般具有较好的计算和通信能力，并且对安全性要求更高。在认证的基础上完成密钥协商是建立会话密钥的必要步骤。安全路由和入侵检测等也是传感网应具有的性能。

由于传感网的安全一般不涉及其他网路的安全，因此是相对较独立的问题，有些已有的安全解决方案在物联网环境中也同样适用。但由于物联网环境中传感网遭受外部攻击的机会增大，因此用于独立传感网的传统安全解决方案需要提升安全等级后才能使用，也就是说在安全的要求上更高，这仅仅是量的要求，没有质的变化。相应地，传感网的安全需求所涉及的密码技术包括轻量级密码算法、轻量级密码协议、可设定安全等级的密码技术等。

2 传输层的安全需求和安全框架

物联网的传输层主要用于把感知层收集到的信息安全可靠地传输到信息处理层，然后根据不同的应用需求进行信息处理，即传输层主要是网络基础设施，包括互联网、移动网和一些专业网（如国家电力专用网、广播电视网）等。在信息传输过程中，可能经过一个或多个不同架构的网络进行信息交接。例如，普通电话座机与手机之间的通话就是一个典型的跨网络架构的信息传输实例。在信息传输过程中跨网络传输是很正常的，在物联网环境中这一现象更突出，而且很可能在正常而普通的事件中产生信息安全隐患。

2.1 传输层的安全挑战和安全需求

网络环境目前遇到前所未有的安全挑战，而物联网传输层所处的网络环境也存在安全挑战，甚至是更高的挑战。同时，由于不同架构的网络需要相互连通，因此在跨网络架构的安全认证等方面会面临更大挑战。初步分析认为，物联网传输层将会遇到下列安全挑战。

(1)DOS 攻击、DDOS 攻击；(2)假冒攻击、中间人攻击等；(3)跨异构网络的网络攻击。

在物联网发展过程中，目前的互联网或者下一代互联网将是物联网传输层的核心载体，多数信息要经过互联网传输。互联网遇到的 DOS 和分布式拒绝服务攻击(DDOS)仍然存在，因此需要有更好的防范措施和灾难恢复机制。考虑到物联网所连接的终端设备性能和对网络需求的巨大差异，对网络攻击的防护能力也会有很大差别，因

此很难设计通用的安全方案，而应针对不同网络性能和网络需求有不同的防范措施。

在传输层，异构网络的信息交换将成为安全性的脆弱点，特别在网络认证方面，难免存在中间人攻击和其他类型的攻击（如异步攻击、合谋攻击等）。这些攻击都需要有更高的安全防护措施。

如果仅考虑互联网和移动网以及其他一些专用网络，则物联网传输层对安全的需求可以概括为以下几点：

（1）数据机密性：需要保证数据在传输过程中不泄露其内容；（2）数据完整性：需要保证数据在传输过程中不被非法篡改，或非法篡改的数据容易被检测出；（3）数据流机密性：某些应用场景需要对数据流量信息进行保密，目前只能提供有限的数据流机密性；（4）DDOS 攻击的检测与预防：DDOS 攻击是网络中最常见的攻击现象，在物联网中将会更突出。物联网中需要解决的问题还包括如何对脆弱节点的 DDOS 攻击进行防护；（5）移动网中认证与密钥协商（AKA）机制的一致性或兼容性、跨域认证和跨网络认证（基于 IMSI）：不同无线网络所使用的不同 AKA 机制对跨网认证带来不利。这一问题亟待解决。

2.2 传输层的安全架构

传输层的安全机制可分为端到端机密性和节点到节点机密性。对于端到端机密性，需要建立如下安全机制：端到端认证机制、端到端密钥协商机制、密钥管理机制和机密性算法选取机制等。在这些安全机制中，根据需要可以增加数据完整性服务。对于节点到节点机密性，需要节点间的认证和密钥协商协议，这类协议要重点考虑效率因素。机密性算法的选取和数据完整性服务则可以根据需求选取或省略。考虑到跨网络架构的安全需求，需要建立不同网络环境的认证衔接机制。另外，根据应用层的不同需求，网络传输模式可能区分为单播通信、组播通信和广播通信，针对不同类型的通信模式也应该有相应的认证机制和机密性保护机制。简言之，传输层的安全架构主要包括如下几个方面：

（1）节点认证、数据机密性、完整性、数据流机密性、DDOS 攻击的检测与预防；（2）移动网中 AKA 机制的一致性或兼容性、跨域认证和跨网络认证（基于 IMSI）；（3）相应密码技术。密钥管理（密钥基础设施 PKI 和密钥协商）、端对端加密和节点对节点加密、密码算法和协议等；（4）组播和广播通信的认证性、机密性和完整性安全机制。

3 处理层的安全需求和安全框架

处理层是信息到达智能处理平台的处理过程，包括如何从网络中接收信息。在从网络中接收信息的过程中，需要判断哪些信息是真正有用的信息，哪些是垃圾信息甚至是恶意信息。在来自于网络的信息中，有些属于一般性数据，用于某些应用过程的输入，而有些可能是操作指令。在这些操作指令中，又有一些可能是多种原因造成的错误指令（如指令发出者的操作失误、网络传输错误、得到恶意修改等），或者是攻击者的恶意指令。如何通过密码技术等手段甄别出真正有用的信息，又如何识别并有效防范恶意信息和指令带来的威胁是物联网处理层的重大安全挑战。

3.1 处理层的安全挑战和安全需求

物联网处理层的重要特征是智能，智能的技术实现少不了自动处理技术，其目的是使处理过程方便迅速，而非智能的处理手段可能无法应对海量数据。但自动过程对恶意数据特别是恶意指令信息的判断能力是有限的，而智能也仅限于按照一定规则进行过滤和判断，攻击者很容易避开这些规则，正如垃圾邮件过滤一样，这么多年来一直是一个棘手的问题。因此处理层的安全挑战包括

如下几个方面：

(1)来自于超大量终端的海量数据的识别和处理；(2)智能变为低能；(3)自动变为失控(可控性是信息安全的重要指标之一)；(4)灾难控制和恢复；(5)非法人为干预(内部攻击)；(6)设备(特别是移动设备)的丢失。

物联网时代需要处理的信息是海量的，需要处理的平台也是分布式的。当不同性质的数据通过一个处理平台处理时，该平台需要多个功能各异的处理平台协同处理。但首先应该知道将哪些数据分配到哪个处理平台，因此数据类别分类是必须的。同时，安全的要求使得许多信息都是以加密形式存在的，因此如何快速有效地处理海量加密数据是智能处理阶段遇到的一个重大挑战。

计算技术的智能处理过程较人类的智力来说还是有本质的区别，但计算机的智能判断在速度上是人类智力判断所无法比拟的，由此，期望物联网环境的智能处理在智能水平上不断提高，而且不能用人的智力去代替。也就是说，只要智能处理过程存在，就可能让攻击者有机会躲过智能处理过程的识别和过滤，从而达到攻击目的。在这种情况下，智能与低能相当。因此，物联网的传输层需要高智能的处理机制。

如果智能水平很高，那么可以有效识别并自动处理恶意数据和指令。但再好的智能也存在失误的情况，特别在物联网环境中，即使失误概率非常小，因为自动处理过程的数据量非常庞大，因此失误的情况还是很多。在处理发生失误而使攻击者攻击成功后，如何将攻击所造成的损失降低到最小程度，并尽快从灾难中恢复到正常工作状态，是物联网智能处理层的另一重要问题，也是一个重大挑战，因为在技术上没有最好，只有更好。

智能处理层虽然使用智能的自动处理手段，但还是允许人为干预，而且是必须的。人为干预可能发生在智能处理过程无法做出正确判断的时候，也可能发生在智能处理过程有关键中间结果或最终结果的时候，还可能发生在其他任何原因而需要人为干预的时候。人为干预的目的是为了处理层更好地工作，但也有例外，那就是实施人为干预的人试图实施恶意行为时。来自于人的恶意行为具有很大的不可预测性，防范措施除了技术辅助手段外，更多地需要依靠管理手段。因此，物联网处理层的信息保障还需要科学管理手段。

智能处理平台的大小不同，大的可以是高性能工作站，小的可以是移动设备，如手机等。工作站的威胁是内部人员恶意操作，而移动设备的一个重大威胁是丢失。由于移动设备不仅是信息处理平台，而且其本身通常携带大量重要机密信息，因此，如何降低作为处理平台的移动设备丢失所造成的损失是重要的安全挑战之一。

3.2 处理层的安全架构

为了满足物联网智能处理层的基本安全需求，需要如下的安全机制。

(1)可靠的认证机制和密钥管理方案；(2)高强度数据机密性和完整性服务；(3)可靠的密钥管理机制，包括 PKI 和对称密钥的有机结合机制；(4)可靠的高智能处理手段；(5)入侵检测和病毒检测；(6)恶意指令分析和预防，访问控制及灾难恢复机制；(7)保密日志跟踪和行为分析，恶意行为模型的建立；(8)密文查询、秘密数据挖掘、安全多方计算、安全云计算技术等；(9)移动设备文件(包括秘密文件)的可备份和恢复；(10)移动设备识别、定位和追踪机制。

4 应用层的安全需求和安全框架

应用层设计的是综合的或有个体特性的具体应用业务，它所涉及的某些安全问题通过前面几个逻辑层的安全解决方案可能

仍然无法解决。在这些问题中，隐私保护就是典型的一种。无论感知层、传输层还是处理层，都不涉及隐私保护的问题，但它却是一些特殊应用场景的实际需求，即应用层的特殊安全需求。物联网的数据共享有多种情况，涉及到不同权限的数据访问。此外，在应用层还将涉及到知识产权保护、计算机取证、计算机数据销毁等安全需求和相应技术。

4.1 应用层的安全挑战和安全需求

应用层的安全挑战和安全需求主要来自于下述几个方面：

(1)如何根据不同访问权限对同一数据库内容进行筛选；(2) 如何提供用户隐私信息保护，同时又能正确认证；(3)如何解决信息泄露追踪问题；(4)如何进行计算机取证；(5)如何销毁计算机数据；(6)如何保护电子产品和软件的知识产权。

由于物联网需要根据不同应用需求对共享数据分配不同的访问权限，而且不同权限访问同一数据可能得到不同的结果。例如，道路交通监控视频数据在用于城市规划时只需要很低的分辨率即可，因为城市规划需要的是交通堵塞的大概情况；当用于交通管制时就需要清晰一些，因为需要知道交通实际情况，以便能及时发现哪里发生了交通事故，以及交通事故的基本情况等；当用于公安侦查时可能需要更清晰的图像，以便能准确识别汽车牌照等信息。因此如何以安全方式处理信息是应用中的一项挑战。

随着个人和商业信息的网络化，越来越多的信息被认为是用户隐私信息。需要隐私保护的应用至少包括如下几种：

(1)移动用户既需要知道(或被合法知道)其位置信息，又不愿意非法用户获取该信息；(2) 用户既需要证明自己合法使用某种业务，又不想让他人知道自己在使用某种业务，如在线游戏；(3)病人急救时需要及时获得该病人的电子病历信息，但又要保护该病历信息不被非法获取，包括病历数据管理员。事实上，电子病历数据库的管理人员可能有机会获得电子病历的内容，但隐私保护采用某种管理和技术手段使病历内容与病人身份信息在电子病历数据库中无关联；(4)许多业务需要匿名性，如网络投票。很多情况下，用户信息是认证过程的必须信息，如何对这些信息提供隐私保护，是一个具有挑战性的问题，但又是必须要解决的问题。例如，医疗病历的管理系统需要病人的相关信息来获取正确的病历数据，但又要避免该病历数据跟病人的身份信息相关联。在应用过程中，主治医生知道病人的病历数据，这种情况下对隐私信息的保护具有一定困难性，但可以通过密码技术手段掌握医生泄露病人病历信息的证据。

在使用互联网的商业活动中，特别是在物联网环境的商业活动中，无论采取了什么技术措施，都难免恶意行为的发生。如果能根据恶意行为所造成后果的严重程度给予相应的惩罚，那么就可以减少恶意行为的发生。技术上，这需要搜集相关证据。因此，计算机取证就显得非常重要，当然这有一定的技术难度，主要是因为计算机平台种类太多，包括多种计算机操作系统、虚拟操作系统、移动设备操作系统等。与计算机取证相对应的是数据销毁。数据销毁的目的是销毁那些在密码算法或密码协议实施过程中所产生的临时中间变量，一旦密码算法或密码协议实施完毕，这些中间变量将不再有用。但这些中间变量如果落入攻击者手里，可能为攻击者提供重要的参数，从而增大成功攻击的可能性。因此，这些临时中间变量需要及时安全地从计算机内存和存储单元中删除。计算机数据销毁技术不可避免地会被计算机犯罪提供证据销毁工具，从而增大计算机取证的难度。因此如何处理好计算机取证

和计算机数据销毁这对矛盾是一项具有挑战性的技术难题，也是物联网应用中需要解决的问题。

物联网的主要市场将是商业应用，在商业应用中存在大量需要保护的知识产权产品，包括电子产品和软件等。在物联网的应用中，对电子产品的知识产权保护将会提高到一个新的高度，对应的技术要求也是一项新的挑战。

4.2 应用层的安全架构

基于物联网综合应用层的安全挑战和安全需求，需要如下的安全机制：

(1)有效的数据库访问控制和内容筛选机制；(2) 不同场景的隐私信息保护技术；(3)叛逆追踪和其他信息泄露追踪机制；(4)有效的计算机取证技术；(5)安全的计算机数据销毁技术；(6) 安全的电子产品和软件的知识产权保护技术。

针对这些安全架构，需要发展相关的密码技术，包括访问控制、匿名签名、匿名认证、密文验证(包括同态加密)、门限密码、叛逆追踪、数字水印和指纹技术等。

5 影响信息安全的非技术因素

物联网的信息安全问题将不仅仅是技术问题，还会涉及到许多非技术因素。下述几方面的因素很难通过技术手段来实现。

(1)教育。让用户意识到信息安全的重要性和如何正确使用物联网服务以减少机密信息的泄露机会；(2)管理。严谨的科学管理方法将使信息安全隐患降低到最小，特别应注意信息安全管理；(3)信息安全管理。找到信息系统安全方面最薄弱环节并进行加强，以提高系统的整体安全程度，包括资源管理、物理安全管理、人力安全管理等；(4)口令管理。许多系统的安全隐患来自于账户口令的管理。

因此在物联网的设计和使用过程中，除了需要加强技术手段提高信息安全的保护力度外，还应注重对信息安全有影响的非技术因素，从整体上降低信息被非法获取和使用的几率。

6 存在的问题

物联网的发展，特别是物联网中的信息安全保护技术，需要学术界和企业界协同合作来完成。许多学术界的理论成果看似很完美，但可能不很实用，而企业界设计的在实际应用中满足一些约束指标的方案又可能存在可怕的安全漏洞。信息安全的保护方案和措施需要周密考虑和论证后才能实施，设计者对设计的信息安全保护方案不能抱有任何侥幸心理，而实践也证明攻击者往往比设计者想象得更聪明。

然而，现实情况是学术界与企业界几乎是独立的两种发展模式，其中交叉甚少，甚至双方互相鄙视：学术界认为企业界的设计没有新颖性，而企业界看学术界的设计是乌托邦，很难在实际系统中使用。这种现象的根源是学术机构与企业界的合作较少，即使有合作，也是目标导向很强的短期项目，学术研究人员大多不能深入理解企业需求，企业的研究人员在理论深度有所欠缺，而在信息安全系统的设计中则需要很强的理论基础。

再者，信息安全常常被理解为政府和军事等重要机构专有的东西。随着信息化时代的发展，特别是电子商务平台的使用，人们已经意识到信息安全更大的应用在商业市场。尽管一些密码技术，特别是密码算法的选取，在流程上受到国家有关政策的管控，但作为信息安全技术，包括密码算法技术本身，则是纯学术的东西，需要公开研究才能提升密码强度和信息安全的保护力度。

7 发展建议

借鉴国外一些成功的经验，鼓励科研机构的研究人员与企业界的研究人员多进行技术沟通，共同完成某些研究项目。这一点

国家已经做了大量努力，特别一些面向企事业单位合作的国家重大研究专项提供了很好的企事业合作平台，这一政策需要继续贯彻下去并不断加强。

在对科学研究的资助方面，需要一种更好的管理方式，减免“跑经费”的时间，使得科研人员，特别是一些有能力的科研人员，能够安心科研工作，做出更大的科技创新。

主要参考文献

1 International Telecommunication Union. ITU Internet Reports 2005: The Internet of Things, 2005.

2 Floerkemeier C. Langheinrich M, Fleisch E, Mattern F. The Internet of Things: Lecture Notes in Computer Science. Springer, 2008, 49-52.

3 Van Kranenburg R. The Internet of Things. Amsterdam: Waag Society, 2008.

4 Yan L, Zhang Y, Yang L T. The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems. Auerbach Publications, 2008.

5 Chakrabarti D, Maitra S, Roy B. A Key Pre-distribution Scheme for Wireless Sensor Networks: Merging Blocks in Combinatorial Design. Journal of Information Security, 2006, 5(2): 105-114.

A Preliminary Investigation on the Security Architecture of the Internet of things

Wu Chuankun

(State Key Laboratory of Information Security, CAS 100190 Beijing)

Abstract Internet of Things (IOT) is the outcome of the development of information technology to a certain stage, and is a new scientific, technological, and economical wave of global information technology industry, and it will have big impact on many important scientific and technological innovations as well as industry development, and has attracted high attention from governments, enterprises, and research organizations in various countries. However, the information security of the IOT is one of the core technologies that will influence the security and sustainable development of the IOT. High attention should be paid to that. Therefore, a well-defined security architecture and security system for the IOT will have great impact on the save application and sustainable development of the IOT. This paper tends to analyze the security requirements in different layers of the IOT, and hence establish a security architecture system for the IOT, expecting to offer a theoretical reference for the establishment of reliable security systems of information for the IOT in the future.

Keywords internet of things, security architecture, information security

武传坤 中科院软件所信息安全国家重点实验室研究员，博士生导师。1994 年获西安电子科技大学工学博士学位。曾任教于西安电子科技大学，1991 年度获机械电子工业部“优秀科技青年”称号。1995 年 9 月在澳大利亚昆士兰科技大学进行博士后工作研究，1997 年 7 月在澳大利亚西悉尼大学被聘为研究员，2000 年 5 月在澳大利亚国立大学计算机系任讲师，2003 年入选中科院“百人计划”。目前已承担和参与多项科研资助项目，包括国家自然科学基金项目、国家“863”项目和国家“973”项目等。研究领域：密码学、无线网络安全、安全协议、物联网安全、Femtocell 安全、三网融合安全研究等。E-mail:ckwu@is.iscas.ac.cn

物联网安全架构初探

作者： 武传坤， Wu Chuankun
作者单位： 中国科学院软件研究所信息安全国家重点实验室,北京,100190
刊名： 中国科学院院刊
英文刊名： BULLETIN OF THE CHINESE ACADEMY OF SCIENCES
年，卷(期)： 2010,25(4)

参考文献(5条)

1. Chakrabarti D;Maitra S;Roy B A Key Predistribution Scheme for Wireless Sensor Networks:Merging Blocks in Combinatorial Design 2006(02)

2. Yan L;Zhang Y;Yang L T The Intemet of Things:From RFID to the Next.Generation Pervasive Networked Systems 2008

3. Van Kranenburg R The Intemet of Things 2008

4. Floerkemeier C;Langheinrich M;Heisch E;Mattern F The Internet of Things:Lecture Notes in Computer Science 2008

5. International Telecommunication Union ITU Internet Reports 2005:The Internet of Things 2005