

第4课 ▽ 智能穿戴安全策略 ——物联网隐私与安全

智能穿戴设备因其小巧便捷、可随身携带、简单实用的特点，正逐渐受到人们的喜爱和广泛的应用，但随着互联网和物联网技术的不断发展，人们也逐渐发现其存在的安全隐患。如何让互联网和物联网健康持续地发展，让智能穿戴设备更好地为人们所用，都是人们在不断思考的问题。



思考

同学们，想一想，在使用智能穿戴设备的时候有没有遇到什么问题？你觉得它给你带来的安全隐患有哪些呢？



知识大讲堂

一、智能穿戴设备的安全问题

由于与互联网相连,智能穿戴设备等物联网设备也不可避免地会出现许多网络安全隐患,智能穿戴设备的安全问题实际上也是互联网和物联网目前存在的问题,主要体现在设备安全、网络安全、数据安全和应用安全等方面。

设备安全

在物联网系统中,感知控制层是最基础的部分,它一般是指连接网络的各种设备或传感器。由于这些设备或传感器往往是通过 Wi-Fi 或蓝牙来传输数据,因此容易受到黑客的攻击和威胁。例如,在某马拉松比赛现场,就有人携带蓝牙嗅探设备,记录了多个不同智能穿戴设备终端的信息,轻易地获得了设备名称及佩戴者的健康等信息,如图 1.4.1 所示;在医疗领域,假如不法分子对智能穿戴医疗设备发出攻击,那么将会给人们乃至社会带来巨大的影响。



图 1.4.1 智能穿戴设备的安全问题

课堂活动

物联网应用中的无人快递投送车需要使用不少感知设备,请同学们结合无人快递投送车的应用,想一想,感知控制层中有哪些安全问题?记录在表 1.4.1 中。

表 1.4.1 物联网应用及安全问题

应用名称	使用的感知设备	安全问题
无人快递投送车	1. 摄像头 2.	1. 不法分子通过恶意攻击使摄像头分辨错误。 2.

网络安全

在物联网应用中，互联网是连接各大设备的基础，起到了桥梁作用。智能穿戴设备对互联网的依赖性高，接入的网络类型也很多。但同时，互联网本身也存在许多风险，会带来许多安全问题，主要有以下体现。

➤ 恶意程序。如图 1.4.2 所示，恶意程序会阻碍设备的正常运转。恶意程序种类繁多，对网络安全构成较大威胁的主要有计算机病毒、蠕虫、木马、流氓软件、后门入侵等。在智能穿戴设备中，系统和应用软件也经常被爆出存在系统漏洞，这些漏洞有可能被恶意利用，埋下隐患。

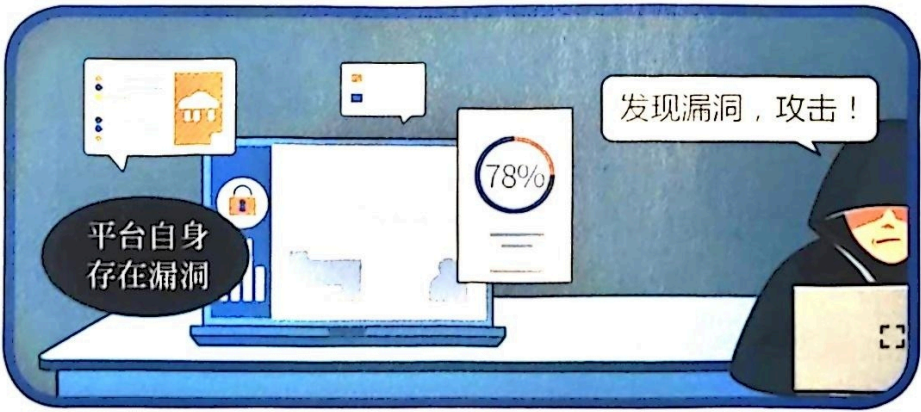


图 1.4.2 恶意程序阻碍设备正常运转

➤ Wi-Fi 热点安全。无线网络连接技术是智能穿戴设备应用的关键所在，但是在许多公共场所，Wi-Fi 热点的传输通道是没有经过加密的，如果智能穿

戴设备用户接入 Wi-Fi，并没有对自己传输的信息进行加密，就会增加信息泄露和被黑客攻击的风险。

➤ 云服务安全。如今，许多设备都使用云存储来实现服务，它可以将大量的数据放在云存储空间供用户存取和利用。但是云存储空间也容易遭受恶意攻击，这么庞大的数据信息一旦泄露，将会带来不可预料的后果，如图 1.4.3 所示。

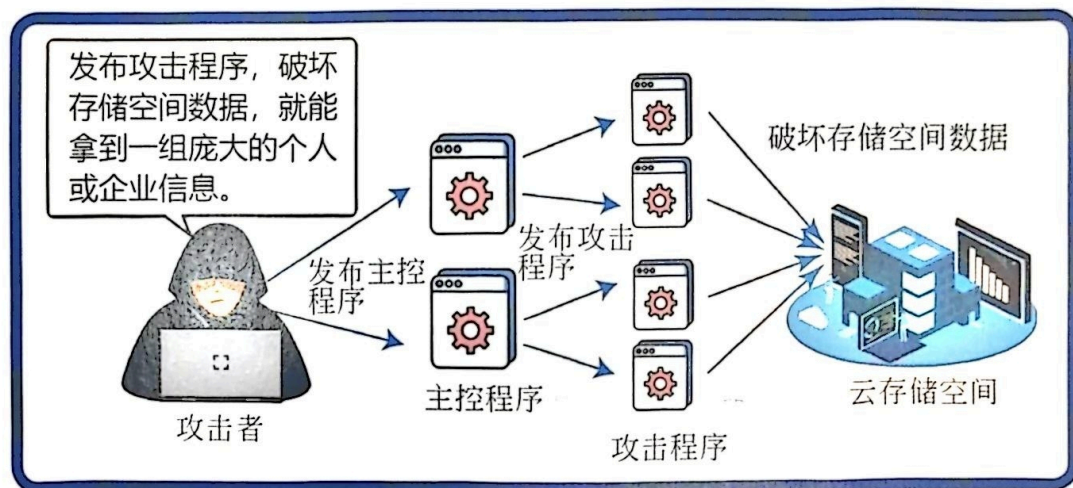


图 1.4.3 恶意攻击给云服务带来的安全隐患

课堂活动

互联网自诞生以来，受到的攻击层出不穷，物联网各应用中无一不用到互联网基础服务，如智能交通、公共基础设施等。请同学们思考，在不同应用中，使用网络传输数据时会出现什么问题？请记录在表 1.4.2 中。

表 1.4.2 不同的物联网应用场景及出现的问题

应用场景	出现的问题
智能交通	网络传输速度不够快，还无法安全自动化
公共基础设施	光纤缆线等年久失修或被损伤，造成网络中断

数据安全

智能穿戴设备通过各种传感器、摄像头等对人或周围的事物进行感知，无时无刻不在记录用户的行为动作、位置信息及环境信息等，因此产生了大量的数据。这些数据常面临一定的安全风险，主要集中在个人隐私泄露和核心数据被窃取这两个方面。

➤ 个人隐私泄露。如图 1.4.4 所示，智能穿戴设备可以收集用户的活动轨迹、生活方式、健康状况等各个方面的详细信息。无论是在设备中，还是在数据的传输和存储过程中，这些信息都有泄露个人隐私的风险，有时甚至会在用户不知情的情况下出现泄露。

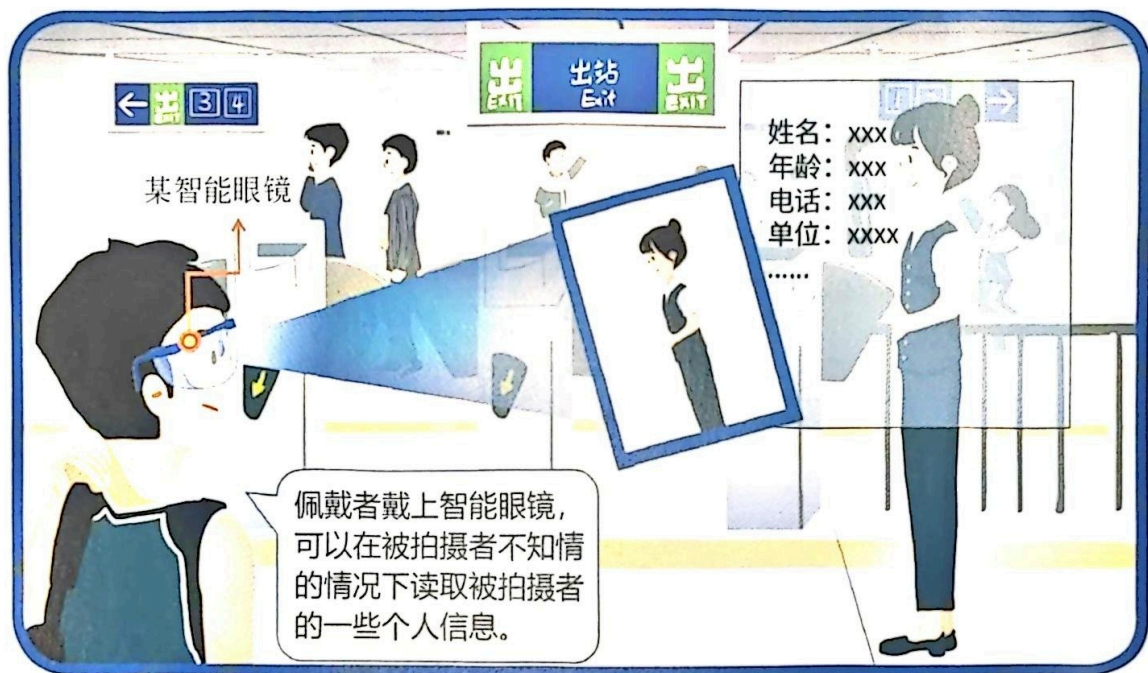


图 1.4.4 智能穿戴设备给个人隐私安全带来的隐患

➤ 核心数据被窃取。随着互联网向智能化转型，智能穿戴设备将会被更广泛地应用在社会各个领域。当智能穿戴设备被带入政府、企业、医院等工作场所，接入这些场所的局域网后，一方面，智能穿戴设备的使用者可能获取该局域网内的数据信息，造成关键信息被窃取；另一方面，黑客有可能利用智能穿戴设备窃取信息，并对这些场所的局域网进行攻击，影响国家和社会的安全。

应用安全

智能穿戴设备不只有自带的各种功能，还可以与各种应用提供商进行合作，安装各种应用软件，从而提供更多功能。但是应用软件种类繁多，鱼龙混杂，容易在安装时出现恶意软件的安装和广告的推广。同时，不法分子还会在设备网络或应用软件中潜藏恶意代码，诱使用户执行病毒程序，可能造成用户信息的丢失，甚至使系统崩溃，损坏设备，如图 1.4.5 所示。

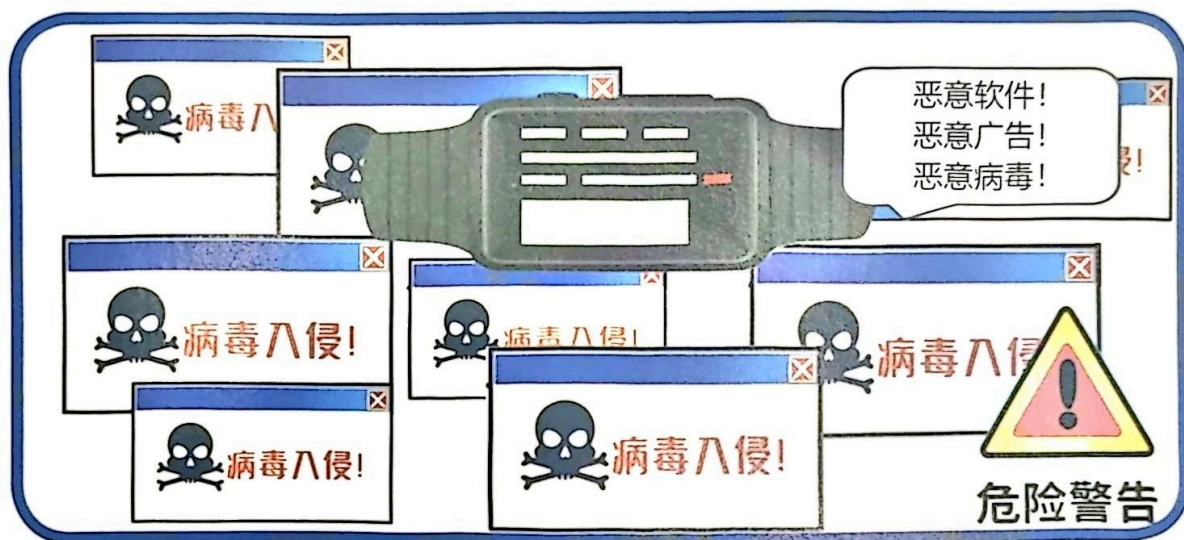


图 1.4.5 应用软件安全问题

二、智能穿戴设备安全问题的应对策略

互联网和物联网技术目前还处于不断发展的阶段，智能穿戴设备要不断为人们提供更加优质的服务，因此加强对其安全风险的防范尤为重要。

加强数据加密技术

要解决数据丢失、信息被窃取、隐私被暴露等安全问题，数据加密是首要的措施。通过加密软件对上传的数据进行加密，可以避免被黑客窃取和使用，从源头上应对安全风险的出现。

优化设备自身系统及应用

智能穿戴设备的许多安全问题都是由设备本身存在的某些缺陷造成的，因

此设备的开发者、应用的提供者都应重视其安全问题，提高设备的防护能力，同时要避免系统或应用存在漏洞，避免被不法分子利用。

增强用户信息安全意识

作为智能穿戴设备的直接使用者，每个用户都应该提高自我保护意识，重视对信息安全的保护。如图 1.4.6 所示，首先，用户应该明确设备的使用环境，了解设备可能出现的安全隐患；其次，要注意智能穿戴设备无线通信的安全性，避免使用免费公共 Wi-Fi 等不安全的通道；最后，用户应该加强对信息的防护，安装相关的防护软件，避免病毒程序的执行等，同时，对相关数据要进行备份和加密处理，防止信息的泄露。



图 1.4.6 常见的保护用户信息安全的方法

实 践

在了解了互联网和物联网安全问题的相关知识之后，不如来个对抗赛吧！结合前面所学知识，请同学们自主查找资料并回答问题：针对智能穿戴设备存在的主要安全问题及防范策略，人们正在研发或使用的安全技术都有哪些呢？看看在一定时间内，谁收集到的资料又多又好！



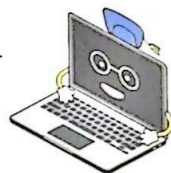
拓展阅读

同态加密技术



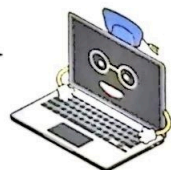
智能穿戴设备在使用过程中，保护隐私至关重要，现在的物联网应用中是否已有比较有力的加密技术呢？

一般的加密方案关注的都是数据存储安全，即把数据加密后再进行存储或者传输。加密技术有很多，而在物联网中，大量应用使用到了云计算，同态加密技术是配合云计算较为有效的加密方法。



什么是同态加密技术呢？

它的直观定义是一种不需要访问数据本身就可以加工数据的方法。经同态加密后的数据，其他人不能直接获取原数据，但可以对其进行加工处理，拥有密钥的人解密后，就能获取处理过的数据结果。我们一起来看看同态加密技术与普通加密技术（见图 1.4.7）有哪些不同吧！



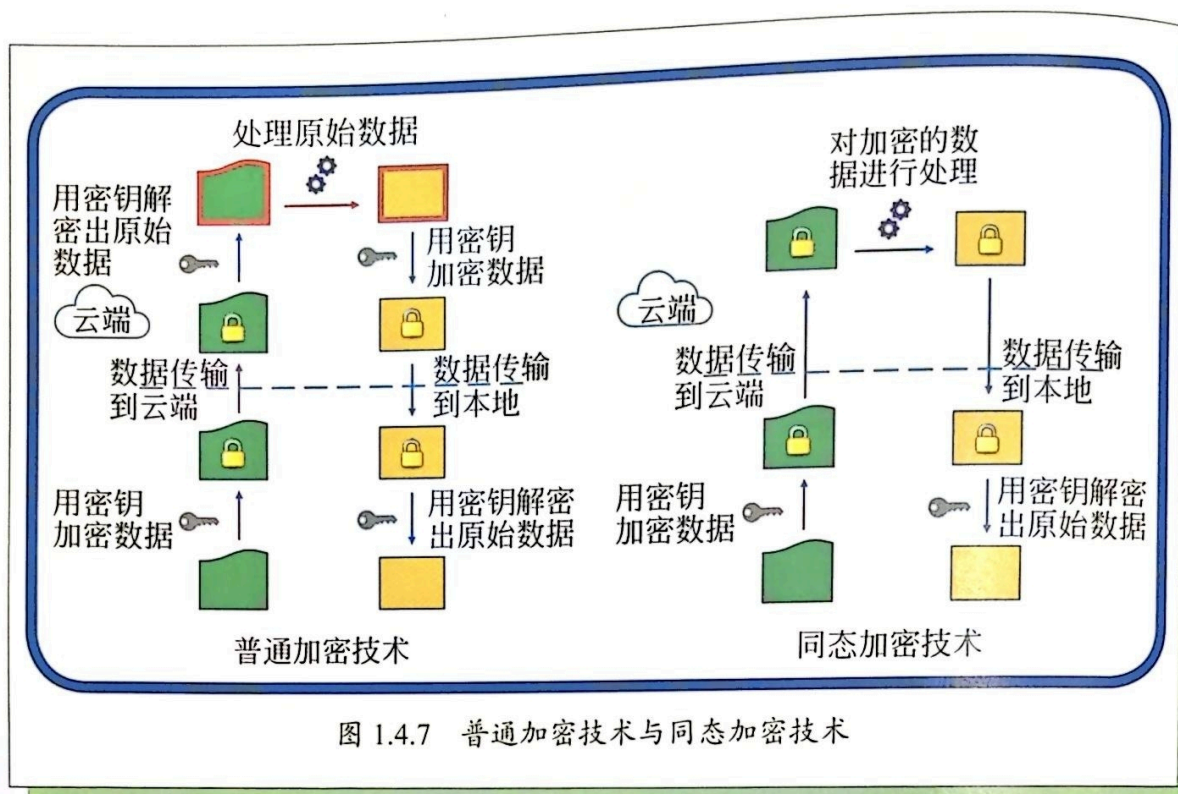


图 1.4.7 普通加密技术与同态加密技术

项目日志

项目日志		班级:	姓名:
项目名称			
项目环节	1□ 2□ 3□ 4□ (在对应环节画 □)		
项目完成内容			
项目完成度	□□□□□□□□□□ (100%)		
项目小结	问题与反思: _____		
	改进的方法: _____		