

第6章 物联网安全技术

1. 总结和梳理一下物联网安全的主要特点。

答：设备种类繁多：涵盖低功耗传感器、工业控制器、智能终端等，安全需求差异大。

大规模部署：设备数量庞大且分布广泛，增加监控和管理难度，攻击面扩大。

资源受限：多数设备计算、存储能力有限，难以运行复杂加密协议。

异构网络环境：采用多种通信协议，跨协议安全协作困难。

长期使用与更新困难：设备生命周期长，固件更新不便，易遗留漏洞。

隐私保护问题：敏感数据易被窃取或滥用。

攻击面广：硬件漏洞、软件缺陷、协议漏洞均可被利用。

低成本设计牺牲安全性：为降低功耗/成本，常省略加密模块。

安全性与可用性冲突：加密认证降低实时性。缺乏标准化：厂商协议差异大，统一安全标准缺失。

2. 物联网安全主要包含了哪些部分？各部分的主要内涵是什么？

答：物联网安全主要包含感知层安全、网络层安全、数据层安全和应用层安全四个部分，各部分内涵如下：

感知层安全：主要针对物联网终端设备（如传感器、RFID 标签、智能终端等）的安全防护，包括物理安全（防止设备篡改、盗窃）、数据采集安全（确保感知数据不被窃取、伪造）以及节点身份认证（避免恶意节点接入网络）。例如，通过轻量级加密算法保护 RFID 标签通信，或采用硬件防护技术防止传感器节点被物理破坏。

网络层安全：聚焦于数据传输过程的安全性，涵盖网络协议安全（如防止协议漏洞被利用）、传输加密（确保数据在有线或无线网络中不被窃听）、入侵检测与防御（抵御 DDoS 攻击、伪基站诈骗等网络攻击），以及异构网络（如有线、无线、移动网络）互联时的安全协作。

数据层安全：关注数据全生命周期的安全，包括数据存储加密（防止云端或本地存储数据泄露）、数据隔离（多用户共享存储时的访问控制）、数据完整性审计（验证数据未被篡改）以及隐私保护（如用户敏感信息匿名化处理）。

应用层安全：针对物联网业务应用的安全防护，涉及应用程序漏洞修复（如防止 SQL 注入、跨站脚本攻击）、用户身份认证与权限管理（避免越权操作）、服务可用性保障（防止恶意请求导致服务瘫痪），例如智能家居控制指令的加密与校验。

3. 如何实现复杂环境下的物联网安全？

答：采用“乐高积木式”安全组件，按云、边、端分层设计安全模块，适配多通信协议、多系统环境和多硬件架构，灵活组合以覆盖不同场景需求。构建云—边—端全覆盖的智能化安全体系，即智能化的物联网安全体系。终端上称为安全知觉系统，连接时称为安全神经系统，所有的物联网连接时采用密码学技术保障双向身份认证，实现安全性。最后汇聚到云端的安全智能分析系统/智能决策系统，把所有的威胁特征和安全情况汇集起来后运行实时动态的决策机制，实现整个物联网闭环的安全体系。

4. 请结合土木工程学科的专业背景，调研 1~2 个有关物联网安全的案例。

答：言之成理即可。

5. 物联网感知层的特点是多源异构、资源受限、设备类型复杂等，传统的计算、存储和通信开销较大的安全协议无法满足物联网感知层的需求，因此需要研究开发什么类型的安全协议？

答：需研发轻量级安全协议，满足以下要求：

低计算开销：采用哈希锁(如 MetalD 验证)替代复杂公钥加密。

抗跟踪能力：随机哈希锁引入随机数，防止位置追踪。

前向安全性：哈希链协议(使用 G/H 函数)确保历史记录不可追溯。

资源适配性：适用于存储受限的 RFID 标签或传感器节点。