OWASP

Open Web Application Security Project

浅谈IoT Top10与物联网安全开发生命周期

任博伦

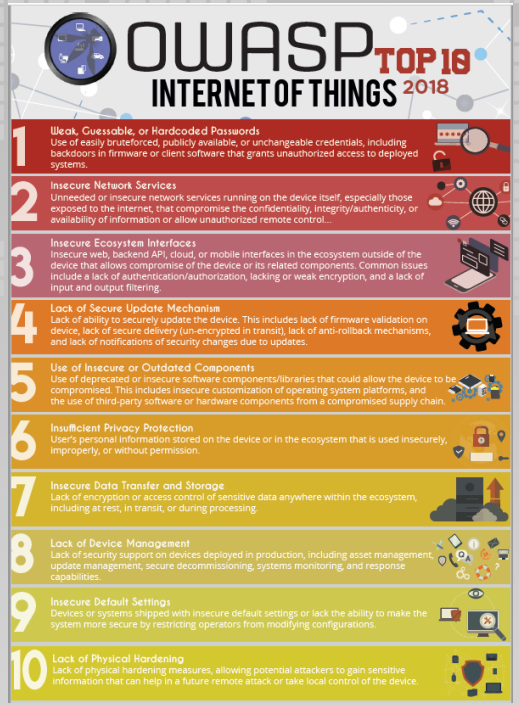
目录

CONTENTS

OWASP IoT Project List

OWASP Internet of Things (IoT) Project
Internet of Things (IoT) Top 10 2018
IoTGoat Project
ByteSweep Project
Firmware Security Testing Methodology
IoT Attack Surface Areas Project
IoT Vulnerabilities Project
Medical Device Testing
Firmware Analysis Project
IoT Logging Events
…

OWASP IoT TOP10



OWASP IoT TOP10

1 Weak, Guessable, or Hardcoded Passwords

Use of easily bruteforced, publicly available, or unchangeable crede
backdoors in firmware or client software that grants unauthorized a
systems.

1 弱密码、可猜测密码或硬编码密码

使用轻易可遭暴力破解的、可公开获取的或无法更改的凭证

户端软件中带有允许对已部署系统进行未经授权访问的后门

A.摄像头弱口令

密码破解是摄像头最常用的攻击方式，一般利用厂家的默认密码。

以下为部分厂家摄像头的最常使用的十大默认用户名/密码：

十大默认用户名/密码	
admin/admin	Admin/1234
admin/1234	admin/123456
admin/<无密码>	admin/password
admin/12345	root/pass
root/<无密码>	root/camera

设备类型	设备名称	CWE	安全影响
	DV摄像机 Mvpower	CWE-521：弱密码以及CWE-284：访问控制不当	几乎任何人都可以访问DVR的设置，因为登录名和密码都是空的。
	DBPOWER U818A WIFI 四轴无人机	CWE-276：不恰当的默认权限	攻击者可以从设备读取文件，如图像和视频文件。
	iSmartAlarm	CWE-287：不恰当的身份验证	攻击者可以向报警装置发送命令，控制报警装置的开/关状态，并激活报警装置的报警功能。
	DblTek GoIP	CWE-598：通过GET请求中的查询字符串泄露信息	攻击者可以通过向GoIP发送命令来修改其配置，比如关闭GoIP。
	Nuuo NVR（网络摄像机）和 Netgear	CWE-259：使用硬编码密码	攻击者可以获得root权限，并使用该设备修改外部摄像机的相关设置来监视用户。
	Sony IPELA Engine网络摄像头	CWE-287：不恰当的身份验证	攻击者可以通过摄像头发送被操纵的图像/视频，让摄像头加入Mirai之类的僵尸网络或仅用于监视用户。
	Western Digital My Cloud	CWE-287：不恰当的身份验证	攻击者可以完全控制设备。
	LG真空吸尘器	CWE-287：不恰当的身份验证	攻击者可以远程激活并访问真空吸尘器的实时视频信息。
	Eminent EM6220相机	CWE-312：以明文形式存储敏感信息	攻击者可以获取相机的root权限并监视相机用户。
	LIXIL Satis卫生间	CWE-259：使用硬编码的密码	攻击者可能会导致设备突然打开/关闭马桶盖，激活坐浴盆或风干功能，引起用户不适或危及人身安全。
	机载娱乐系统	CWE-287：不恰当的身份验证	攻击者可以控制向乘客发送通知的方式，如发送虚假的高度或速度之类的飞行数据。
	燃料型钻孔机	CWE-259：使用硬编码密码	攻击者可以获取root访问权限并修改钻孔机的设置。

OWASP IoT TOP10

2 Insecure Network Services

Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control...

2 不安全的网络服务

设备运行了一些不需要或不安全的网络服务，尤其是那些暴露在互联网上的服务。它会损害信息的保密性、完整性、真实性、可用性，或允许未经授权的远程控制。

设备类型	设备名称	CWE	安全影响
	智能按摩器	CWE-284：访问控制不当	攻击者可以改变按摩器的参数，这会导致相当痛苦的体验甚至引起身体伤害，如引发突然的肌肉条件反射、皮肤烧伤，甚至神经损或导致死亡。
	植入式心脏设备	CWE-284：访问控制不当	攻击者可以修改植入设备的编程命令，从而导致电池耗尽和/或不适当的起搏或电击。
	Hikvision Wi-Fi网络摄像头	CWE-284：访问控制不当	攻击者可以远程利用或禁用摄像头。
	Foscam C1室内高清摄像机	CWE-120：缓冲区复制过程中没有检查输入的大小（经典的缓冲区溢出漏洞）	在摄像机上执行远程代码。该漏洞可能导致用户个人数据泄露。
	玩具Furby	CWE-284：访问控制不当	攻击者可以修改固件并使用Furby来监视儿童。
	玩具My Friend Cayla	CWE-284：访问控制不当	攻击者可以收集用户的信息并实施监控。
	iSmartAlarm	CWE-20：输入验证不当	攻击者可以冻结SmartAlarm，使其停止响应。
	iSPY Camera Tank	CWE-284：访问控制不当	攻击者可以以匿名用户的身份登录设备，并可以访问整个文件系统。

OWASP IoT TOP10

3 Insecure Ecosystem Interfaces

Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.

3 不安全的生态接口

设备外生态系统中不安全的Web、后端API、云或移动接口，导致设备或相关组件遭攻陷。常见的问题包括缺乏认证或授权、缺乏加密或弱加密以及缺乏输入和输出过滤。

设备类型	设备名称	CWE	安全影响
	Heatmiser恒温器	CWE-598：通过GET请求中的查询字符串泄露信息	攻击者可以访问设备的所有设置，进而根据攻击者的意愿来随意更改各种设置，例如时间或温度。
	工业无线接入点Moxa AP	CWE-79：网页生成过程中没有对输入进行严格过滤（跨站脚本漏洞）	攻击者可以获得经过认证的会话，并且该会话永不过期。
	AXIS相机	CWE-20：输入验证不当	攻击者能够以root权限编辑操作系统中的任意文件。
	Belkin智能家居产品	CWE-79：网页生成过程中没有对输入进行严格过滤（跨站脚本漏洞）&CWE-89：没有对SQL命令中的特殊元素进行严格过滤（SQL注入漏洞）	攻击者可以劫持手机，并窃取敏感的个人数据。
	路由器 D-Link DIR-300	CWE-352：跨站请求伪造（CSRF）	攻击者可以修改管理员密码并获得root权限。

	AVTECH网络摄像头、NVR、DVR	CWE-352：跨站请求伪造（CSRF）	攻击者可以通过CSRF修改设备的所有设置，如用户密码。
	AGFEO智能家居ES 5xx/6xx	CWE-79：网页生成过程中没有对输入进行严格过滤（跨站脚本漏洞）	攻击者可以读取存储在操作系统中的所有文件。此外，攻击者还可以修改设备的配置，上传任意更新。
	Loxone智能家居	CWE-79：网页生成过程中没有对输入进行严格过滤（跨站脚本漏洞）	攻击者可以通过基于Web的命令来控制设备的所有功能。
	交换机TP-Link TL-SG108E	CWE-79：网页生成过程中没有对输入进行严格过滤（跨站脚本漏洞）	攻击者可以在设备上植入存储型XSS代码，进而使管理员在浏览器中执行任意JavaScript代码。
	Hanbanggaoke网络摄像头	CWE-650：信任服务器端的HTTP权限方法	攻击者可以修改管理员密码并获得root权限。
	路由器Netgear	CWE-601：URL重定向至不可信站点（Open Redirect漏洞）	互联网上的任何人都可以利用Cockup来控制该路由器，修改其DNS设置，并将浏览器重定向到恶意站点。

OWASP IoT TOP10

4

Lack of Secure Update Mechanism

Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.

4

缺乏安全的更新机制

缺乏安全更新设备的能力，包括：缺乏对设备固件的验证、缺乏安全交付（未加密的传输）、缺乏防回滚机制以及缺乏对更新的安全变更的通知。

OWASP IoT TOP10

5 Use of Insecure or Outdated Components

Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.

5 使用不安全或已遭弃用的组件

使用已遭弃用的或不安全的软件组件/库，将导致设备遭攻陷。组件包括操作系统平台的不安全定制以及使用来自受损供应链的第三方软件或硬件组件。

设备类型	设备名称	CWE	安全影响
	路由器D-Link DIR8xx	CWE-295：证书验证不当	攻击者可以更新路由器的固件，使设备变成僵尸网络的一部分。
	GeoVision公司的设备	CWE-295：证书验证不	攻击者可以更新固件并完全接管设备。
	ikettle智能咖啡机	CWE-15：允许外部人员控制系统或进行相关配置	攻击者可以完全控制设备，例如，打开设备并使其长期工作，这可能会引发火灾。
	Billion路由器 7700NR4	CWE-798：使用硬编码的证书	攻击者可以完全控制设备。
	iSmartAlarm	CWE-295：证书验证不当	攻击者可以获取用户的密码或个人数据。
	路由器Dlink 850L	CWE-798：使用硬编码的证书	攻击者可以完全控制设备。

OWASP IoT TOP10

6 Insufficient Privacy Protection

User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.

6 隐私保护不充分

存储在设备或生态系统中的用户个人信息被不安全的、不当的、或未经授权的使用。

设备类型	设备名称	CWE	安全影响
	Gator 2 smartwatch	CWE-359：泄露隐私信息（侵犯隐私）	攻击者可以访问包含软件版本、IMEI、时间、定位方法（GPS与Wi-Fi）、位置坐标、电池电量等信息。
	路由器D-Link DIR-600和DIR-300	CWE-200：信息泄露	攻击者可以读取设备的敏感信息，或便其成为僵尸网络的一部分。
	三星智能电视	CWE-200：信息泄露	攻击者可以找到用于录音的二进制文件。
	家庭安全摄像头	CWE-359：泄露隐私信息（侵犯隐私）	用户的私人照片可能被攻击者盗取并公布到互联网上。
	智能成人玩具We-Vibe	CWE-359：泄露隐私信息（侵犯隐私）	攻击者可以获取设备温度和振动强度等信息。
	iBaby M6婴儿监视器	CWE-359：泄露隐私信息（侵犯隐私）	攻击者可以查看用户的信息，包括视频录像等。

OWASP IoT TOP10

7 Insecure Data Transfer and Storage

Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.

7 不安全的数据传输和存储

缺乏对生态系统中任何位置的敏感数据进行加密或访问控制，包括：未使用时、传输过程中或处理过程中的敏感数据。

设备类型	设备名称	CWE	安全影响
	Owlet Wi-Fi婴儿心脏监护仪	CWE-201：通过发送数据泄露信息	攻击者可以监视婴儿及其父母。
	三星冰箱	CWE-300：通过非端点访问通信信道（中间人攻击漏洞）	攻击者可以窃取用户的Google凭据。
	大众汽车	CWE CATEGORY：加密问题	攻击者可以克隆遥控器并获得未经授权的汽车访问权限。
	HS-110智能插座	CWE-201：通过发送数据泄露信息	攻击者可以控制插头的状态，如关闭其LED。
	Loxone智能家居	CWE-201：通过发送数据泄露信息	攻击者可以控制智能家庭系统中的每台设备并窃取用户的凭证。

	三星智能电视	CWE-200：信息泄露	攻击者可以监控无线网络并进行暴力破解，以恢复密钥并解密通信流量。
	路由器Dlink 850L	CWE-319：以明文形式传输的敏感信息	攻击者可以远程控制设备。
	Skaterboards Boosted, Revo, E-Go	CWE-300：通过非端点访问通信信道（中间人攻击漏洞）	攻击者可以向设备发送各种命令来指挥它。
	LIFX智能LED灯泡	CWE-327：使用可破解或危险的加密算法攻	击者可以捕获并解密流量，包括网络配置等。
	DJI Spark无人机	CWE-327：使用可破解或危险的加密算法	攻击者可以访问设备的设置。

OWASP IoT TOP10

8

Lack of Device Management

Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.

8

缺乏设备管理

对已部署在生产过程中的设备，缺乏安全支持，包括：资产管理、更新管理、安全解除、系统监控和响应能力。

OWASP IoT TOP10

9

Insecure Default Settings

Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.

9

不安全的默认设置

设备或系统的默认设置不安全，或缺乏限制操作者修改配置的方式让系统更加安全的能力。

设备类型	设备名称	CWE	安全影响
	ADSL设备ZTE ZXDSL	CWE-15：允许外部人员控制系统或进行相关配置	攻击者可以重置设备的配置。
	毛绒玩具	CWE-521：弱密码	儿童及其父母的录音的存储机制不够安全，这使得它们可以在互联网上轻松搜索到。
	Canon打印机	CWE-269：权限管理不当& CWE-295：证书验证不当	攻击者可以访问保护不当的设备并更新其固件。
	Parrot AR.Drone 2.0	CWE-285：授权不当	攻击者可以通过移动应用程序无线控制无人机。
	Smart Nest Thermostat	CWE-269：权限管理不当	未经授权的攻击者可以访问Nest帐户。

OWASP IoT TOP10

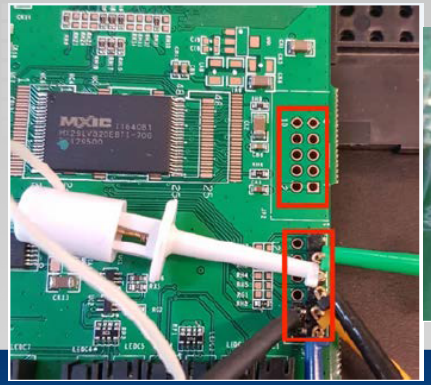
10 Lack of Physical Hardening

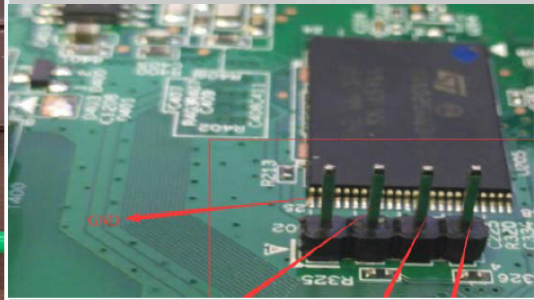
Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.

10 缺乏物理加固措施

缺乏物理加固措施，导致潜在攻击者能够获取敏感信息以便后续进行远程攻击或对设备进行本地控制。

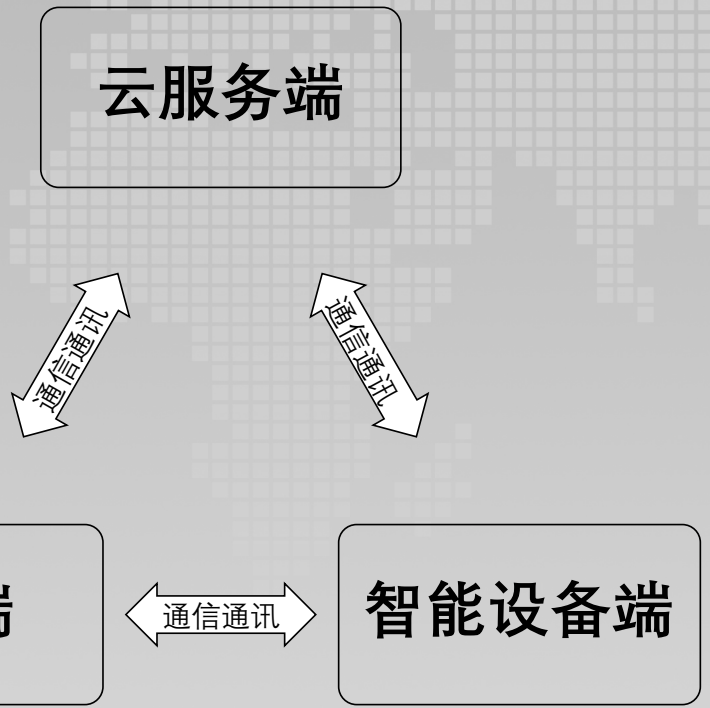
设备类型	设备名称	CWE	安全影响
	D-Link相关设备	CWE-284：访问控制不当	攻击者可以访问用户的私人信息，如照片等。
	婴儿监视器Mi-Cam	CWE-284：访问控制不当	攻击者可以监视用户。
	TOTOLINK路由器	CWE-20：输入验证不当	攻击者可以在设备中植入后门。
	路由器TP-Link	CWE-284：访问控制不当	攻击者可以获得root权限并将设备变为僵尸网络的一部分。
	Smart Nest恒温器	CWE-284：访问控制不当	攻击者可以从外设（例如USB或UART）启动处理器。





OWASP
Open Web Application Security Project

IoT安全威胁分析-IoT技术架构



物联网安全开发生命周期

定义

- 型的物联网环境软件包括1、从设备接收数据以进行进一步处理的软件，例如通常位于云端的基于Web或其他的应用程序，这些应用程序对接收到的数据进行分析；2、用于控制的移动设备软件，例如各类智能家居APP、安卓/ios操作系统等；3、驻留在智能设备上的软件，例如设备固件、物联网产品操作系统、物联网设备驱动程序等；4、物联网通信通讯协议栈，例如tcp/ip、802.1、coap、mqtt等；5、在不同组件之间格式化和传输数据的中继服务，例如API、在智能设备、移动端和其他物联网组件之间传输数据的Web服务等

需求

- 典型的物联网环境在物理上（适用大量设备）和逻辑上（适用多种技术和应用程序）分布广泛，所以在安全需求识别阶段应该满足整个物联网产品和服务生命周期的灵活性。

设计

- 对于每个物联网组件、应列举威胁因素和可能的威胁情况，考虑攻击者的潜在动机、意图、能力以及攻击途径、影响和可能性并对此设计特定的安全控制来防止潜在的安全问题。其中尤为重要的是物联网中网络与物理世界高度相关，所以针对智能设备的安全性也应该在设计阶段考虑。

物联网安全开发生命周期

开发

- 虑到物联网设备的硬件和软件限制，在其生态系统中的代码融入安全性对开发人员是一种挑战安全开发指南适用于不同组件的开发过程，包括常见语言（JAVA、J2EE、PHP）的安全编码指南，以及基于特定硬件的代码和控制嵌入式系统的代码（C、C++）。同时还应培养开发人员有关物联网攻击和威胁防御的意识

测试

- 物联网架构下需要包括对物理设备的评估测试，其不仅涉及软件还包括各类组件以及物理架构以预防诸如拆解、物理端口模糊测试、总线攻击、流量分析等

部署

- 物联网解决方案通常部署在广泛开放的环境中，其中管理员和支持团队可能无法完全控制。物联网部署的另一个特殊性即在异构性，如智能设备的固件、用于后端物联网服务的云服务器，实现物联网通信通讯协议的网关和网络组件等。