2015物联网安全年报

阿里聚安全

阿里安全开放平台

摘 要

- ✧ 物联网威胁攻击已摆脱概念，这些物联网设备为人类带来便捷生活的同时，也给黑客提供了新的土壤，所暴露出的安全问题越来越多。2015 年公布了一系列高危漏洞，这些漏洞有的暴露用户隐私，有的影响用户财产，有的甚至对生命安全构成了威胁。由于物联网设备数量大和互联的特性，一个小问题，其影响和严重程度就会被放大到几十倍，甚至更多。
- ✧ 80%的设备暴露硬件调试接口，易被黑客利用。这些设备硬件上都保留了调试接口如 JTAG、SWID、UART，攻击者可通过这些接口获取大量实现上的信息，通过对这些信息的理解，可远程影响更多同类型的设备。
- ✧ 90%固件的安全隐患严重威胁物联网安全。阿里移动安全团队分析发现，90%以上的固件升级更新机制实现不安全、固件对通讯数据的安全检查不完整、大量厂商的固件存在包括密钥等敏感信息、固件中保留了调试命令接口，可远程操作设备等特点将严重威胁物联网安全。
- ✧ 94%传统 Web 安全漏洞同样影响物联网云端 Web 接口。阿里移动安全团队分析发现，传统 Web 安全中的问题同样存在于物联网云端 Web 接口，如跨站脚本、文件修改、命令执行及 SQL 注入等。
- ✧ 位置与时空安全将对用户造成物理性攻击危害。
- ✧ 通信系统及基础设施安全长期不受重视，危害物联网设备安全。包括：利用运营商业务短信系统进行远程诈骗、通信基站设备存在安全隐患、VoLTE 业务漏洞成为另一个攻击平台、4G LTE 安全性还待考验等。
- ✧ 物联网的业务安全将成为新的安全威胁方向。物联网各种业务上产生的数据如个人识别信息、医疗记录、用户账户数据、O2O 业务交易信息等将对生活、工作、娱乐、甚至个体产生极大的关联和影响。但设备在接入、传输、存储等各环节缺少正常的安全防控，甚至缺乏基本的安全考虑。毫无疑问，黑客将会把目标瞄准新的战场，即物联网设备上的业务安全。网络安全领域很多典型防控措施如分隔、域、安全服务最小化等已经不能完全适应物联网带来的安全新挑战，对有价值业务的精确管控和持续防护，才是确保企业和用户安全的关键因素。

目 录

第一章 物联网威胁攻击日益凸显

一时间，我们日常使用的设备多出了智能的概念，小到一块手表，大到一辆汽车，通过有线或无线的方式实现了互联，使得他们不只是具有传统的功能，而是更加的 smart 起来。这些设备被统称为物联网（Internet of Things），他们无处不在，应用的场景有汽车、医疗、物流运输、智能家庭、娱乐等领域。2015 年，设备的数量呈持续增长趋势，据 Gartner 公司预测，到 2020 年物联网设备将达到 260 亿的规模。

物联网利用多种如 Sub-1G、NFC、蓝牙、WiFi、ZigBee 无线通讯技术，又涉及到硬件、设备固件、移动端应用软件、云端服务。可以说物联网融合了很多技术，而且形态各异，但从物理结构上可分成：智能终端设备、手机移动端、云端这三部分。通过手机端下载移动应用，与云端进行通信或直接和终端设备通讯，发送控制指令，再由云端转发控制指令给设备终端，这样就可以实现在任意能够接入互联网的环境下，去控制一台在内网的智能设备，进而实现智能化。

这些设备让我们的生活变得便利的同时，也给黑客提供了新的土壤，所暴露出的安全问题越来越多，被关注度也与日俱增。2015 年公布了一系列高危漏洞，这些漏洞有的暴露用户隐私，有的影响用户财产，有的甚至对生命安全构成了威胁。如 2015 年 7 月，菲亚特克莱斯勒美国公司宣布召回 140 万辆配有 Uconnect 车载系统的汽车，黑客可通过远程软件向该车载系统发送指令，进行各种操作如减速、关闭引擎、让刹车失灵等，严重危害人身安全。2015 年 8 月的黑帽大会和世界黑客大会上，包括汽车在内的各种智能设备都被爆出安全漏洞，黑客利用安全漏洞可以控制智能手机、汽车、交通红绿灯，甚至搭载有智能狙击镜的高级狙击步枪，让人惊叹不已。因为物联网设备数量和互联的特性，一个小问题，其影响和严重程度就会被放大到几十倍，甚至更多。

根据阿里移动安全团队对物联网安全性的调查，以及对设备如物联网汽车的中控显示、智能路由器、网络摄像头、智能开关、家庭网关、门锁、家用告警器等的分析，发现一些共有的安全问题，以作学习和思考。

图 1 物联网安全隐患

第二章 物联网安全问题

1.1 80%的设备暴露硬件调试接口，易被黑客利用

硬件接口，例如 JTAG、SWID、UART，用于设备制造商在设计时的前期调试，生产时的程序烧录，以及诊断测试的目的。我们发现 80%的设备的硬件上都保留了调试接口，攻击者通过这些接口获取到大量实现上的细节信息。例如设备与云端和移动应用软件的通讯协议、信息完整性校验的算法、加密过程中所使用的秘钥，再利用对这些信息的理解，远程影响更多同类型的设备。

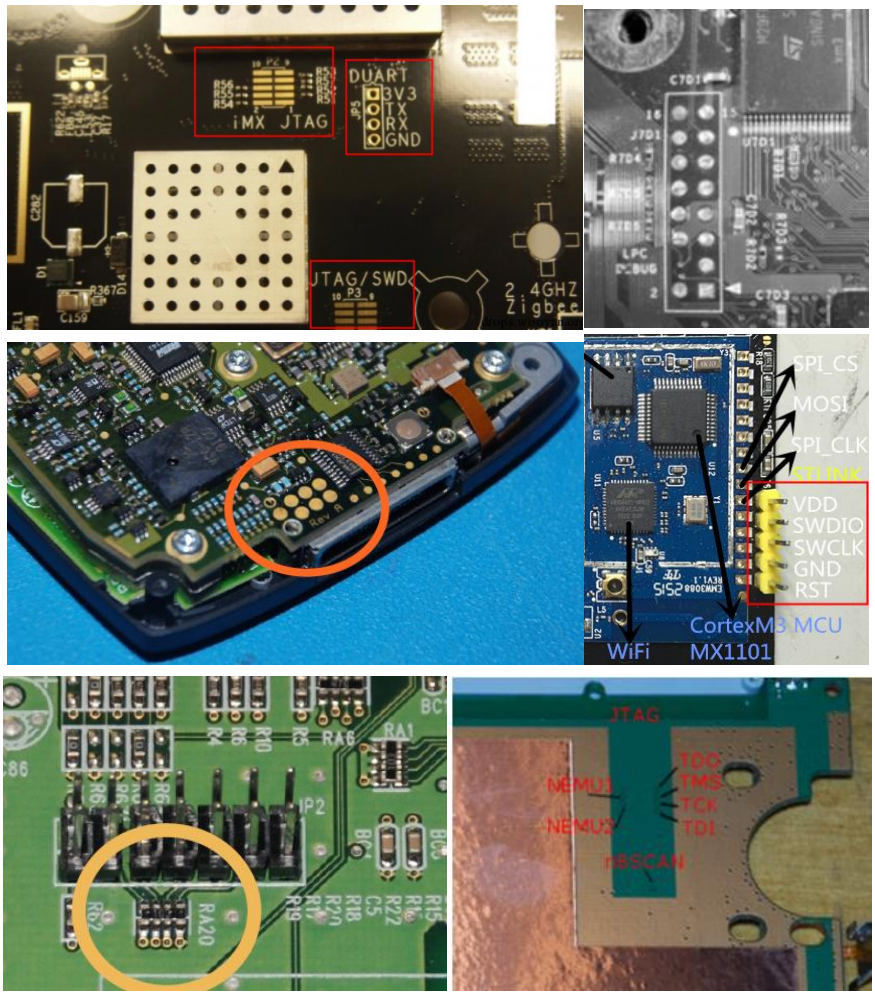

图 2 暴露调试接口的硬件示例

1.2 90%固件上的安全隐患严重威胁物联网安全

1. 90%以上的固件升级更新机制实现不安全

固件升级的问题包括：升级包的来源是否安全、升级包下载传输是否安全、升级文件是否存在敏感数据、执行升级操作是否进行完整性检查、是否对升级包的版本进行检查、升级包的内容是否进行加密处理。这些问题都会影响到攻击者是否可获得固件、解压、分析并进行篡改，最终烧录到设备上导致持续性影响。

测试项	博联智能开关	极路由	Wink Hub	某型汽车多媒体中控	Ubi	MyQ Garage
来源不安全	YES	YES	NO	NO	NO	NO
内容没有加密	YES	NO	YES	YES	YES	YES
升级部署没有签名检查	YES	NO	YES	YES	YES	YES
没有版本降级限制	YES	YES	YES	YES	YES	YES

表 1 部分厂商固件上安全隐患的对比

2. 固件对通讯数据的安全检查不完整

虽然通讯协议中定义了序号、校验值，但固件在实现时没有进行校验和检查，或检查的方式过于简单，可被攻击者轻易绕过。例如汽车钥匙系统中使用了 KEELOQ 滚码，钥匙每发送一次命令后，内部的序号会增加，汽车 ECU 本应检测正确的序号才认为有效。但因为车厂在实现上的问题，容易导致此类危害。如比亚迪某些车型在连续发送两条命令（A 和 B）后，序号会被重置到 A，如果捕获到连续 2 次解锁车门的命令信号，就可以实现无限次开车门。类似的问题在沃尔沃、别克君威等部分型号的车辆中得到验证。

3. 大量厂商的固件存在包括密钥等敏感信息

敏感信息泄露无论在应用层还是系统层，都是一个普遍存在的安全隐患。多数物联网固件中信息存放过于简单（不经过任何计算或明文），通过对多个厂商的固件进行分析，对获取到的密码 HASH 进行破解，发现很多弱口令如： admin, pass, logout，helpme 等。多个厂商在固件中不但包含自签名的 HTTPS 证书，且由于不正确的版本发布管理和设计缺陷，一些厂商还包含私钥。SEC Consult 在本年度调查中发现来自 50 个厂商的超过 900 款产品中存在硬编码密钥重用问题，其中受影响的厂商如下：

```
ADB, AMX, Actiontec, Adtran, Alcatel-Lucent, Alpha Networks, Aruba Netw
orks, Aztech, Bewan, Busch-Jaeger, CTC Union, Cisco, Clear, Comtrend, D-
Link, Deutsche Telekom, DrayTek, Edimax, General Electric(GE), Green Pa
cket, Huawei, Infomark, Innatech, Linksys, Motorola, Moxa, NETGEAR, NetC
omm Wireless, ONT, Observa Telecom, Opengear, Pace, Philips, Pirelli, Ro
bustel, Sagemcom, Seagate, Seowon Intech, Sierra Wireless, Smart RG, TP
-LINK, TRENDnet, Technicolor, Tenda, Totolink, unify, UPVEL, Ubee Intera
ctive, Ubiquiti Networks, Vodafone, Western Digital, ZTE, Zhone, ZyXEL。
```

图 3 存在硬编码密钥重用问题的 50 家厂商

4. 固件中保留的调试命令接口

物联网固件中调试命令多用于工厂测试以及开发调试，例如预留后门、启动 rootshell 进行排错，虽然在移动端应用软件中不会使用，但攻击者在理解协议的基础上，可封装出对应的调用接口，远程操作设备，例如可对设备恢复出厂配置进行拒绝服务攻击，或者窃取设备上保存的用户敏感数据。通过研究，发现多数设备存在如下共性问题：

a) 调试接口服务访问没有正确限制：多数设备运行 HTTP 服务、ADB 服务、Telnet 服务，并没有正确限制访问，即可通过远程 LAN 或 Internet 访问。

b) 调试接口服务没有正确进行验证：使用简单的 password 或空密码，可简单绕过验证服务，达到未授权访问的目的。

c) 调试接口服务允许执行任意代码：该接口提供高权限的任意代码执行功能，通过漏洞或设计权限，攻击者访问该接口服务后就可以完全控制设备。

测试	博联智能开关	极路由	Wink Hub	哈曼汽车多媒体中控	Ubi	MyQ Garage
调试接口访问没有正确限制	YES	YES	YES	YES	YES	YES
调试接口是否可在未授权时访问	YES	NO	NO	YES	YES	NO
调试接口是否允许代码执行	NO	YES	YES	YES	NO	YES

表 2 部分厂商固件中保留调试命令接口的安全隐患对比

5. 设备和云端、移动应用端通讯时的安全问题

通讯链路的安全篡改或者监听，可导致劫持、敏感信息泄露及未授权访问。设备和云端、移动应用端通讯时的安全基本问题如下：

a) 设备到服务没有使用正确验证：设备没有在整个通信会话过程使用验证凭据或者唯一标识符，允许攻击者未授权访问。

b) 设备到服务端没有对中间人攻击进行保护：通过 MITM 攻击，攻击者可以在设备和服务端之间获取和修改通信。

c) 信道无加密：设备和云端以及移动应用端通信传输时，控制命令和采集的数据没有加密，攻击者通过监听获取敏感数据。

d) 存在重放攻击：设备没有重放保护，允许攻击者重用之前截获的消息，实现未授权访问以及执行恶意操作。

测试	博联智能开关	极路由	Wink Hub	哈曼汽车多媒体中控	Ubi	MyQ Garage
允许未授权访问	NO	NO	YES	YES	NO	NO
存在 MiTM 劫持	YES	NO	YES	N/A	YES	YES
信道没有加密	NO	NO	NO	N/A	YES	NO
存在重放攻击	YES	NO	NO	N/A	YES	YES

表 3 部分厂商设备和云端、移动端通讯时的安全隐患对比

1.3 94%传统 Web 安全漏洞同样影响物联网云端 Web 接口

通过对部分物联网厂商后台接口的扫描检测，传统 Web 安全中的问题同样存在于物联网云端 Web 接口，跨站脚本、文件修改、命令执行及 SQL 注入继续是 Web 接口的重要安全漏洞：

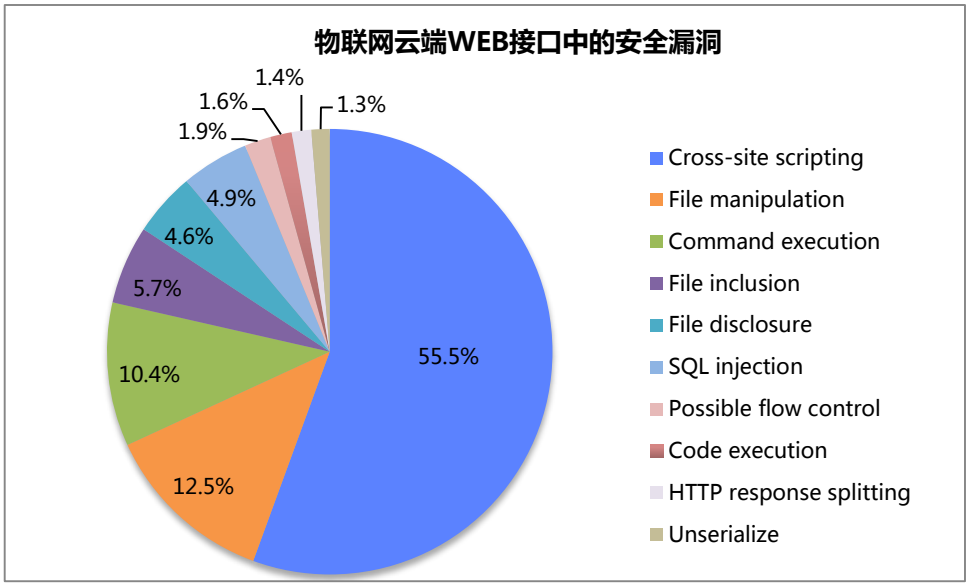

图 4 物联网云端 WEB 接口中的安全漏洞

1.4 位置与时空安全会对用户造成物理性的攻击危害

智能设备更加依赖于时间信息和位置信息，来实现设备的功能特性。常见的时间与位置的获得方法，主要是依赖于以下几种方式：

1. GNSS 系统。如 GPS、北斗、GLONASS 等。GNSS 系统在定位的同时，也对终端完成了授时过程。
2. WiFi 辅助定位。由于 GNSS 系统的信号极弱，在室内信号强度便不足以提供定位所需。因此，大部分的位置信息提供商都提供了基于 WiFi 特征的辅助定位功能，基于 WiFi 的 SSID 和 BSSID 进行定位。
3. 通信基站的标识信息。通信基站中的特征标识如 LAC 和 CellID 信息可以被用于终端进行快速定位。

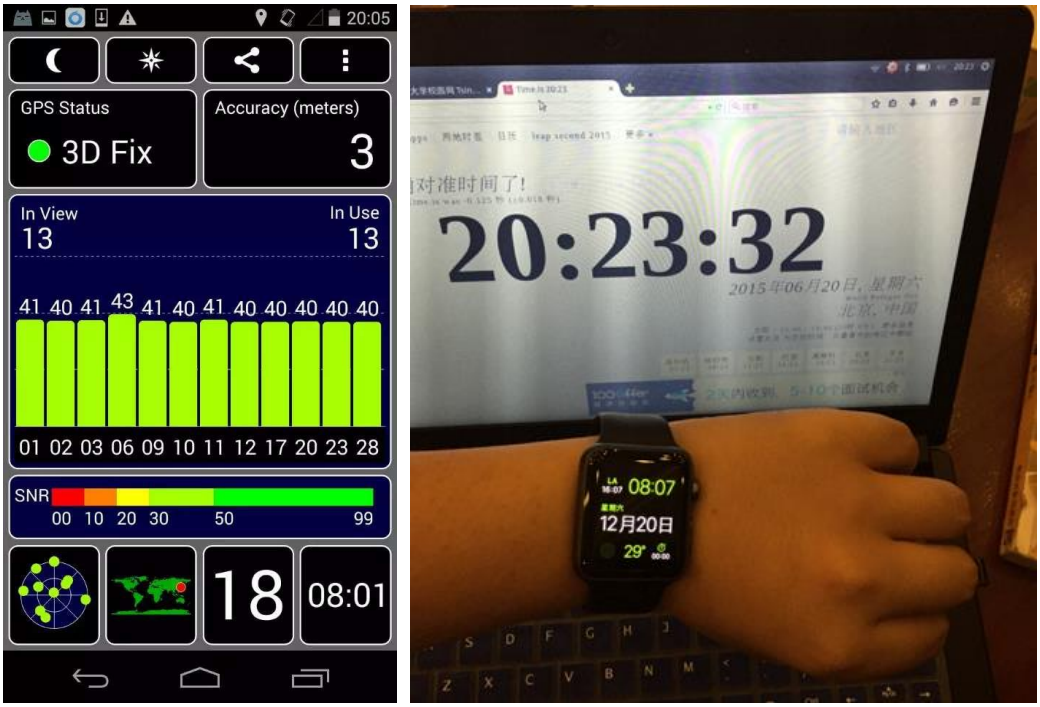

图 5 伪造的 GPS 信号被 Android 设备接收，伪造的 GPS 信号干扰 Apple Watch 的时间

这几种位置时空信息获取方式的实现上，目前仍处于关注其功能完整性及有效性的阶段，对于安全方面的考虑较少。

近期业界发布了不少关于位置时空安全的研究。例如在 BlackHat Europe 2015 安全大会中，来自赫尔辛基大学的安全研究者演示了在 LTE 环境下，从基站的广播信息中嗅探到用户的地理位置。该团队在大会中也展示了两种位置时间的欺骗攻击方式：利用软件无线电设备实施 GPS 位置时间欺骗，和基于普通计算机无线网卡 WiFi 辅助定位系统的位置欺骗，iPhone 和 Apple Watch 均受影响。特别地，我们发现基于 WiFi 的位置欺骗比 GPS 欺骗更容易被攻击者利用，攻击者甚至都不需要使用任何特殊的硬件设备，只需要一部普通的笔记本电脑，即可对市面上常见的地图类应用进行攻击。这将会给地图位置信息提供商带来较大的安全挑战，例如应对位置数据采集过程中的防投毒技术。同时，随着室内定位技术的逐渐成熟，室内定位基站大规模部署之后，如何应对一脉相承的位置安全问题，也将是接下来物联网安全技术的一个挑战。

1.5 通信系统及其基础设施安全性长期不够重视

通信系统及其基础设施是物联网的基石与骨干，但在万物互联的时代里，通信系统及其业务的安全性长期没有得到重视，间接危害物联网设备的安全。2015 年披露了多起涉及到通信系统的安全漏洞，相信之后对通信系统和基础设施的攻击会持续增加。

1. 运营商业务短信系统安全

2015 年 12 月出现的一种利用运营商短信业务平台实现远程换卡的诈骗手法。据报道，“诈骗短信的特色是发送以 HK 开头的一串指令，后面的数字代表的是新的 SIM 卡卡号，当用户根据短信提醒，回复退订指令至 10086 后，手机卡就可能落入犯罪分子手里，致使银行卡、或支付账户资金被盗。”目前在运营商的业务受理系统中，除可通过短信办理业务外，还有电话拨号信令办理，这些业务受理系统大部分是从有线电话时代继承下来的，有很多遗留问题。

2. 通信基站设备安全

2015 年第一季度，国内运营商某型家庭基站被发现了多枚重大漏洞，可导致用户的短信、通话、数据流量被窃听。恶意攻击者可以在免费申领一台设备之后，迅速地将其改造成伪基站短信群发器和流量嗅探器，影响公众的通信安全。传统通信厂商以物理隔离为主的安全策略，在通信网核心设备 IP 化的趋势下，面临着较大的挑战。

3. VoLTE 业务漏洞成为另一个攻击平台

运营商正在大力推进部署的高清语音 VoLTE 业务，给用户带来了更好的通话体验，更短的接通时间，同时逐步替换掉原有的短信业务。但是 VoLTE 业务背后所依赖的 SIP 协议，给安全研究者们提供了又一个新的攻击面。韩国 KAIST 研究团队在 2015 年 10 月发布了他们对于当地 VoLTE 业务的分析报告，找到了当地运营商的 VoLTE 业务漏洞。

4. 4G LTE 安全性还待考验

虽然 4G 业务相对于 2G 在安全方面有了较大的提升，伪基站在 4G 业务中基本得到了杜绝，但是 LTE 的信令中，仍然存在着一些没有被考虑到的安全风险。例如在今年 11 月位于荷兰举办的 Blackhat 大会中，来自赫尔辛基大学的研究团队，演示了如何使用 LTE 的信令泄漏出来的信息，对小区范围内的用户进行跟踪。

5. USIM 卡安全密钥可提取

目前已经有团队可以实现对于 4G USIM 卡的密钥进行提取。4G USIM 卡在当前的互联网生活中，处于较为重要的安全中心的位置上，一旦 USIM 卡的安全被攻破，将会给支付、通信、账号体系带来巨大的冲击。

第三章 物联网安全未来发展趋势

1. 物联网的业务安全会成为新的安全威胁方向

人类对世界的了解，会随着智能设备和传感器的互联不断延伸和增长，而相应的其业务和数据也会不断增加。根据调查，90%的数据从未被分析或采取任何安全措施。毫无疑问，利益最大化的黑客会把目标瞄准新的战场，即物联网设备上的业务安全。

物联网各种业务上产生的数据如个人识别信息，医疗记录，用户账户数据，020 业务交易信息等将对生活、工作、娱乐、甚至个体产生极大的关联和影响。但设备在接入、传输、存储等各环节缺少正常的安全防控，甚至缺乏基本的安全考虑。

网络安全领域很多典型防控措施如分隔、域、安全服务最小化等已经不能完全适应物联网带来的安全新挑战，对有价值的业务的精确管控和持续防护，才是确保企业和用户安全的关键因素。

2. Web of Things（WoT）安全将是物联网技术趋势的重要一环

物联网的发展将聚焦在 Advanced Sensor Fusion 与 Physical-World Web 层面，这二个层面简单来说，就是 WoT。根据维基百科上的定义，WoT 是物联网的 Application Layer，并且是使用 Web 技术来打造 Application。简单来说物联网+ Web-enabled technologies 就是 WoT。对 WoT 来说就是以 URL 来表示物联网装置：

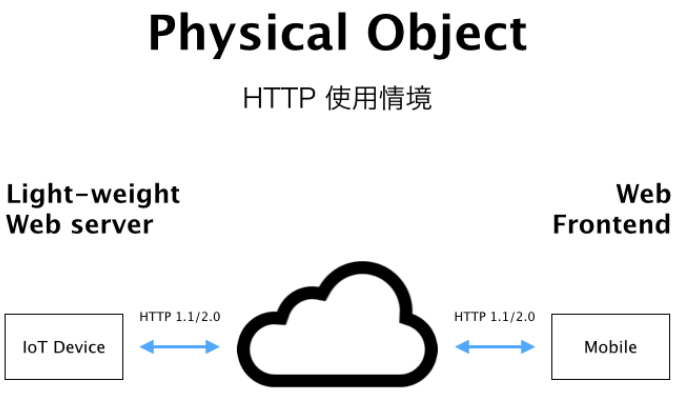

图 6 移动设备上使用 Web 前端通过云中转来访问设备

而基于 Web 的传统安全攻击手段，如 SQL injection, XSS, Command Exec 等都会在 WoT 上继续存在，并由于防护机制的薄弱，更容易受到攻击，显而易见 WoT 的安全防护需要成为物联网安全中的重要一环。

3. 加密算法的硬件化

加密是保证通讯不被篡改的关键，将加密算法固化在一个专用的芯片或使用芯片内部的专用控制器，这种方式可有效避免因为通过软件计算而导致的 Key 泄露。加上硬件成本越来

越低，以及芯片厂商在设计芯片时本身的安全性考虑，这样的趋势后续会明显起来。而设备厂商是否可以让这些新技术无缝融合到产品中，也是产品是否安全的关键。

4. 认证的标准化

专用的、安全的认证协议会逐渐取代目前仅从功能实现考虑的简单协议，相信安全性会得到整体提升。

阿里聚安全微信公众号

阿里聚安全官网

阿里聚安全官网：http://jaq.alibaba.com

官方邮箱：mobilesecurity@service.alibaba.com