IoT设备的安全防护——口令安全

海康威视 王滨

First Choice for Security Professionals

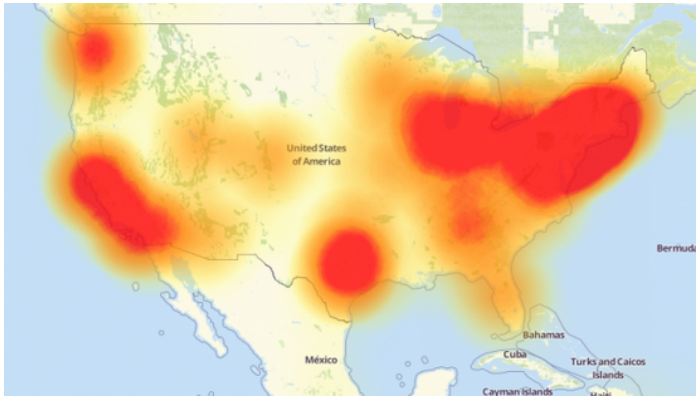
背景介绍

- Gartner预测到2020年，全球的物联网设备数量将达到204亿;
- 联网智能终端一般是部署在开放的环境中接入互联网易被攻击。
- 物联网设备的用户安全意识普遍较薄弱，基础安全能力严重匮乏，攻击门槛低；
- 一旦出现有效的恶意控制方式，影响将迅速扩散；再加上庞大的数量加持，其作为网络武器的威力更是不可小觑！

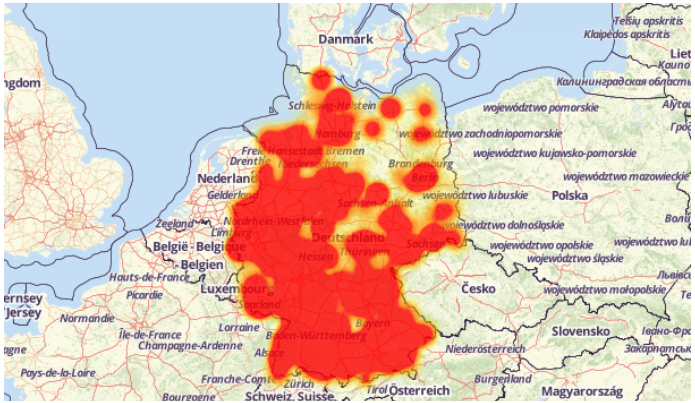
CONTENTS

HIKVISION

事件分析



- 2016年10月21日发生了震惊全球的美国断网事件，黑客通过操控网络摄像头及相关DVR发起DDOS攻击所致。



- 2016年11月28日发生德国电信断网事件，大约90万个路由器被mirai僵尸网络的扫描过程打宕。

事件分析

- 2017年10月21日，以色列安全公司Check Point发布僵尸网络IoTroop正在快速增长，在过去的一个月里感染了100万家企业和机构（国内有数据是感染200万台设备）。IoTroop与Mirai不同，它更加复杂，除了弱凭证，还使用了十几个或更多的漏洞来获取这些设备。如由 D-Link, TP-Link, Avtech, Netgear, MikroTik, Linksys, Synology 和GoAhead 制造的路由器和无线 IP 摄像机

事件分析

部分品牌的联

省市	部分品牌联网摄像头IP数量	部分品牌联网的弱口令摄像头IP数量	弱口令摄像头百分比（%）
江苏	79763	**7024**	8.81
浙江	74253	**17749**	23.9
重庆	12651	4966	**39.25**
山西	12595	1966	15.61
四川	12503	3180	**25.43**

布情况

■ 弱口令问题已经成为当前物联网面临的最严重的安全问题

《2017年我国联网智能设备安全情况报告》国家互联网应急中心CNCERT

弱口令到底是谁的原因？

- 设备制造商？

- 集成商？

- 最终用户？

CONTENTS

HIKVISION

国外研究情况

标准编号	标准名称	主要内容
NIST SP 800-118	企业口令管理向导	介绍了口令以及口令的管理，并从可能会导致用户口令暴露的口令存储、口令传输、用户行为、口令暴力破解、口令重置等技术方面提出了相关的建议。
NIST SP 500-9	使用口令对计算机资源的访问控制	主要内容包括口令机制（口令选择、口令生命周期、口令组成）；口令保护（口令传输、口令存储）
NIST SP 800-63-3	数字身份指南	指南介绍了选择合适的数字身份服务的管理过程，确保对身份、认证的真实性。该标准中也提出了针对口令生命周期、口令复杂性、以及对泄露口令的筛选方面提出了相关建议。
NIST IR 7970	分类规则的口令策略	定义了口令策略相关的规则：口令过期时间、口令通信传输、口令组成、口令存储、认证失败锁定。
NIST IR 8040	衡量移动平台口令的可用性和安全性	本标准主要是对移动平台口令安全性和可用性的研究。从口令的生成、口令的使用、典型的口令攻击、口令强度机制等口令安全方面提出了相关的建议。
NIST IR 7991	美国联邦雇员口令管理行为	抽取了38000名联邦雇员对其口令行为进行研究。研究内容包括口令生成时间、口令生成策略、口令跟踪方法，并对研究发现的问题给出了建议。

国际最新研究情况

- NIST 00-63B《Digital Identity Guidelines Authentication and Lifecycle Management》
  - **去除定期修改口令的要求：**很多研究都显示，要求定期修改口令实际上是有损良好口令安全的。NIST称，该建议的提出，是因为口令应该是用户想改才改，或者有指标表明受到入侵才修改。
  - **放弃口令复杂性要求：**不再要求必须包含大小写字母、特殊符号和数字的复杂性要求。NIST称，即便用户想要只有表情符的口令，也是应该允许的。这里有必要提到存储要求。加盐(salting)、散列（hashing）、介质访问控制(MAC)，以防口令文件被对手获取，离线攻击是非常难以完成的。
  - **对照常用或已泄露口令列表筛选新口令：**提升用户口令强度的最佳方法之一，是对照词典口令和已知泄露口令列表进行筛选。NIST称，词典字、用户名、重复或连续的模式，统统都应该被弃用。

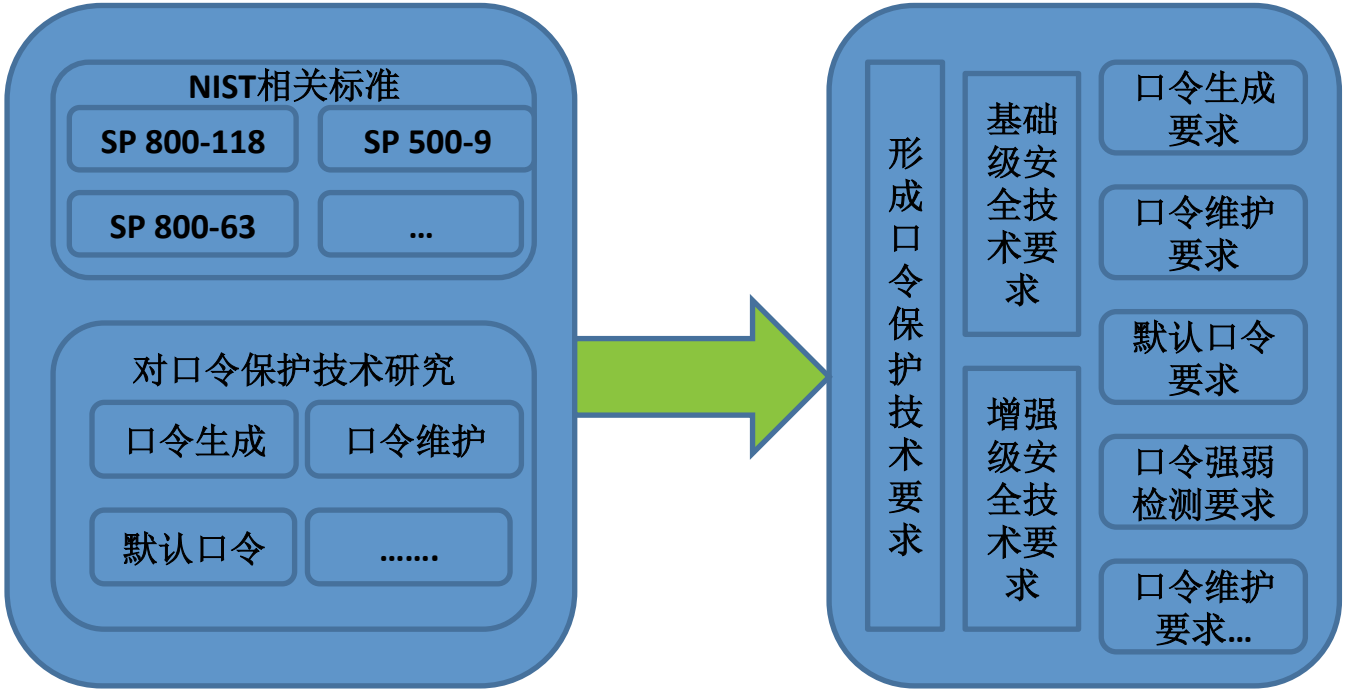
国内研究情况

- 部分国家安全标准提及了口令的部分安全要求，但都没有完整的关于口令保护的相关标准，如《信息安全等级保护》；
- 通过对当前物联网设备口令安全风险评估，发现口令在生成、维护、传输、存储等方面存在的安全隐患和风险；
- 需要形成物联网设备口令的保护标准，对在我国销售或使用的智能联网设备进行安全规范，避免由于默认口令、弱口令等口令保护不足带来的安全风险，提高物联网设备整体安全防护能力和水平。

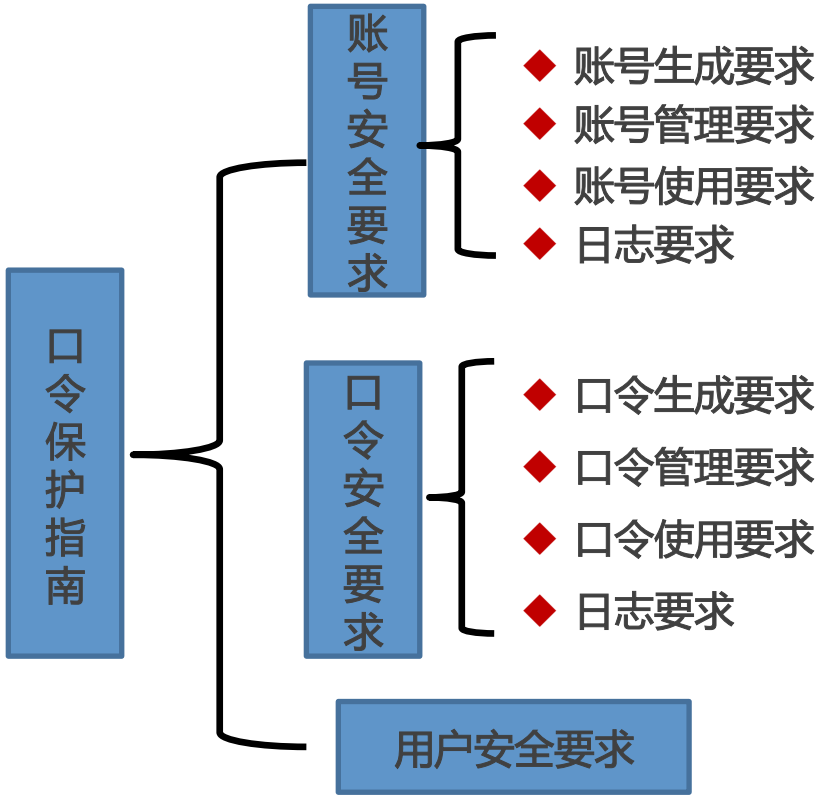
CONTENTS

HIKVISION

口令安全技术路线


NIST相关标准
SP 800-118
SP 500-9
SP 800-63
...
对口令保护技术研究
口令生成
口令维护
默认口令
.....
形成口令保护技术要求
基础级安全技术要求
增强级安全技术要求
口令生成要求
口令维护要求
默认口令要求
口令强弱检测要求
口令维护要求...

口令安全内容框架


口令保护指南
账号安全要求
账号生成要求
账号管理要求
账号使用要求
日志要求
口令安全要求
口令生成要求
口令管理要求
口令使用要求
日志要求
用户安全要求

口令安全详细内容

分类	要求	具体内容
账号安全要求	账号生成	➢ 设备中帐号应具有唯一性； ➢ 在新建或修改帐号时，应提供命名规则检查功能。
	账号使用	➢ 所有帐号都应公开； ➢ 应禁用或删除第三方或开源软件中不使用的默认帐号。
	账号管理	➢ 应为管理员提供帐号添加、删除、修改、查询等功能； ➢ 应提供可配置的帐号锁定策略。如帐号到期锁定，连续多次输入错误口令锁定帐号等； ➢ 所有帐号都应被设备管理员管理。
	日志要求	➢ 全部用户对帐号的所有操作均应记录日志，日志内容应包括用户ID、操作内容、IP地址、时间、操作结果等信息。

口令安全详细内容

HIKVISION

分类	要求	具体内容
口令安全要求	口令生成	➢ 应支持可扩展的口令复杂度策略 ➢ 应提供弱口令检测功能； ➢ 自动生成的口令应具有随机性； ➢ 应为每个设备帐号随机生成默认口令； ➢ 对于使用默认口令的智能联网设备，每次登录时应提醒用户修改口令，直到修改默认口令为止。
	口令使用	➢ 口令传输应采用安全传输通道或者加密后传输； ➢ 应默认对输入框中的口令进行掩盖显示； ➢ 应禁止口令从输入框中复制的功能； ➢ 用户登录成功后无法查看自己的口令； ➢ 对口令的鉴别过程应具备防暴力破解功能，如错误登录尝试超过设定次数后锁定操作帐号或者操作IP一段时间。
	口令管理	➢ 所有口令都应可修改，如应禁止使用硬编码口令等； ➢ 用户修改口令前，应提供验证旧口令以及对新口令再次确认的功能； ➢ 存储口令时应加密，加密算法按照国家有关规定执行；

口令安全详细内容

分类	要求	具体内容
口令安全要求	口令管理	➢ 存储的口令应具有防暴力破解机制，如加盐等； ➢ 应使用操作系统的访问控制功能限制对口令文件的访问； ➢ 应防止口令存储文件被篡改； ➢ 应提供在忘记帐号或者口令的情况下将设备恢复到出厂状态的功能； ➢ 口令复杂度策略应可配置，应支持管理员根据应用场景配置强化的口令复杂度策略； ➢ 应具备显示口令安全强度的能力。
	日志要求	➢ 全部用户对口令的所有操作均应记录日志，日志内容应包括用户ID、操作内容、IP地址、时间、操作结果等信息。
用户安全要求	用户安全要求	➢ 用户应修改设备的默认口令； ➢ 用户应为不同的设备设置不同的口令； ➢ 用户不应使用过去曾被泄露的口令； ➢ 用户应妥善保管所使用的帐号和口令； ➢ 用户不应明文存储、传输口令； ➢ 用户应定期对口令进行修改； ➢ 当有迹象足以显示账号口令可能遭破解时，应立即更改口令，并以安全事件方式及时上报； ➢ 设备人机帐号、机机帐号应采用不同的帐号。

CONTENTS

HIKVISION

总结

- 国家信息安全标准委员会（TC260）
  - 《信息安全技术-智能联网设备口令保护指南》
  - 已经形成送审稿

Thanks

Hikvision Digital Technology Co., Ltd.
No.555 Qianmo Road, Binjiang District
Hangzhou 310052, China
T +86 571 88075998
F +86 571 89935635
overseasbusiness@hikvision.com

www.hikvision.com