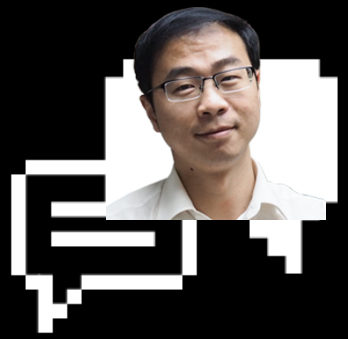


消费类IoT网络安全实现

巫光毅　TUV莱茵

德国电信研究估计，2021年全球将会有380亿物联网设备上线。
其中1/3为智能家居家电，1/3为智慧城市。

消费类物联网


智能电视


智能监控


智能家电


智能照明


无线设备


智能机器人


无人机


智能玩具


智能传感器

智能可穿戴

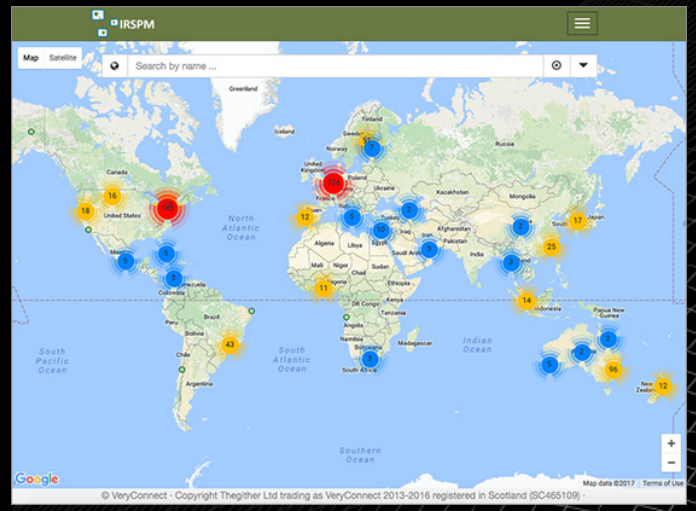

智能控制

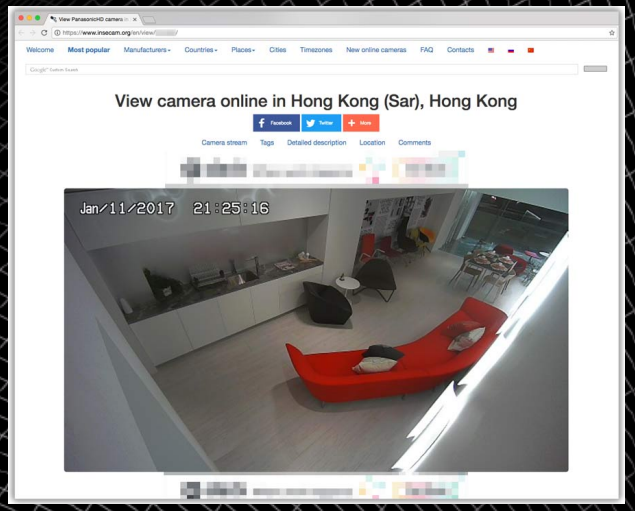

智慧中控

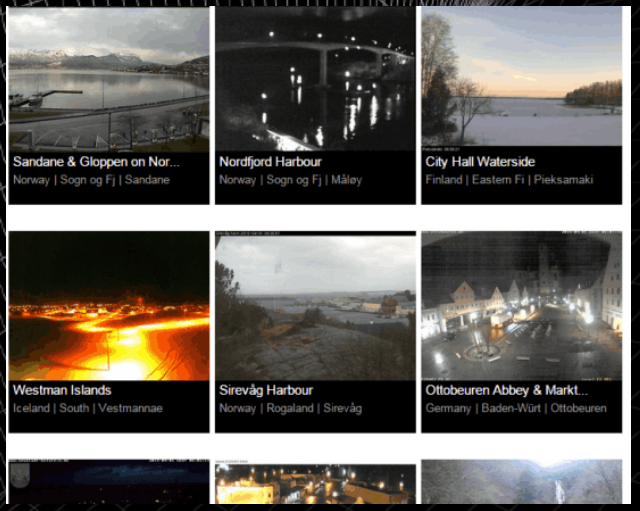
海量设备进入家庭的情况下，到底有多少“好”产品。

IP摄像头弱点暴露

opentopia、geocam、insecam等网站可以在线看到网络摄像头监控画面。
这些摄像头有室内的、室外的、道路监控、商场和酒店监控等。







Samsung and Roku Smart TVs Vulnerable to Hacking, Consumer Reports Finds

Security and privacy testing of several brands also reveals broad-based data collection. How to limit your exposure.

1 AUG 2017 NEWS

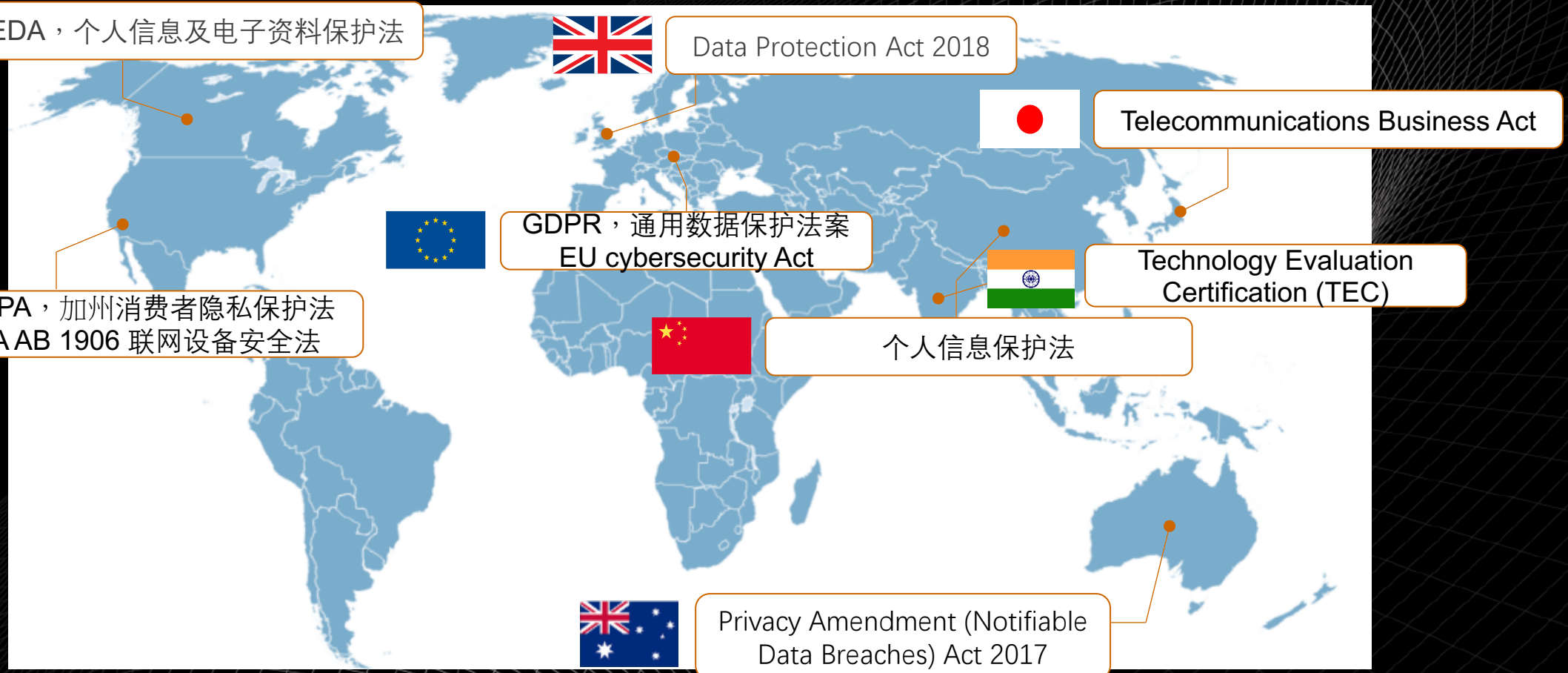
Alexa Hack Allows Continuous Eavesdropping

Home › News › Hacker Takes Over 'Smart Home' by Hacking into Google Nest System

Hacker Takes Over 'Smart Home' by Hacking into Google Nest System

IANS - September 24, 2019 7:50 pm

全球数据保护法和网络安全法



- 发现风险: 使用明文协议

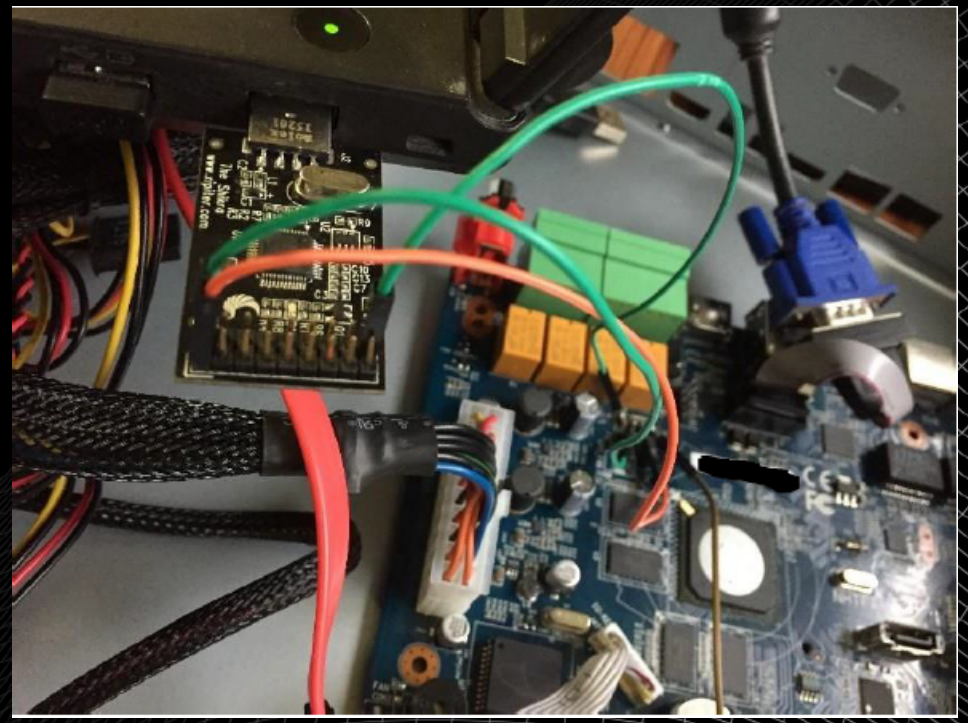
造成的危害：网络中的攻击者可能能够窃听通信信道，访问甚至操纵敏感信息。

建议的修复方式：敏感数据的传输都使用最新的加密协议。

- 发现风险: UART接口开放，并且可以使用root shell

造成的危害：攻击者可以连接到调试接口，并可以全权访问硬件设备。

建议的修复方式：禁用UART访问或者增加设备访问凭证



```
/etc # whoami
root
/etc # uname -a
Linux (none) 3.10.0_hi3536 #2 Fri Oct 30 15:46:53 CST 2015 armv7l GNU/Linux
/etc #
```

- 发现风险: 固件逆向

造成的危害：固件可以被逆向。可能暴露硬编码凭证，并且暴露更多的攻击界面。

建议的修复方式：固件加密。

```
rootkill3r@arun:~/office/clients/nvr/_N0I_UI1A_180623_133_18300.fls.extracted/cramfs-root$ ls
bin   dev  home  lib      lost+found    mknod_console  nfsroot  proc  sbin   sys  usr
boot  etc  init  linuxrc  mkimg.rootfs  mnt            opt      root  share  tmp  var
rootkill3r@arun:~/office/clients/nvr/_N0I_UI1A_180623_133_18300.fls.extracted/cramfs-root$ cd etc/
rootkill3r@arun:~/office/clients/nvr/_N0I_UI1A_180623_133_18300.fls.extracted/cramfs-root/etc$ cat passwd
root:$1$$qRPK7m23GJusamGpoGLby/:0:0::/root:/bin/sh
rootkill3r@arun:~/office/clients/nvr/_N0I_UI1A_180623_133_18300.fls.extracted/cramfs-root/etc$ cat passwd-
root:ab8nBoH3mb8.g:0:0::/root:/bin/sh
rootkill3r@arun:~/office/clients/nvr/_N0I_UI1A_180623_133_18300.fls.extracted/cramfs-root/etc$
```

常见风险

开放debug端口

弱密码、密码重置

不安全TLS配置

明文传输

不安全的运行库

本地明文存储

不安全函数

Portal权限设置

消费类IoT安全规范

- 没有通用默认密码
- 保持软件更新
- 安全存储凭据和敏感数据
- 安全传输
- 最大限度地减少暴露的攻击面
- 确保软件完整性
- 检查系统遥测数据
- 验证各渠道输入数据

安全实现，基于规范化开发。

SDLC流程

需求

开发

测试

发布

安全实现，也基于规范化流程。

网络安全创新大会
Cyber Security Innovation Summit

THANKS

巫光毅

TUV莱茵深圳

Tel: +18025477830