MIDC·2018

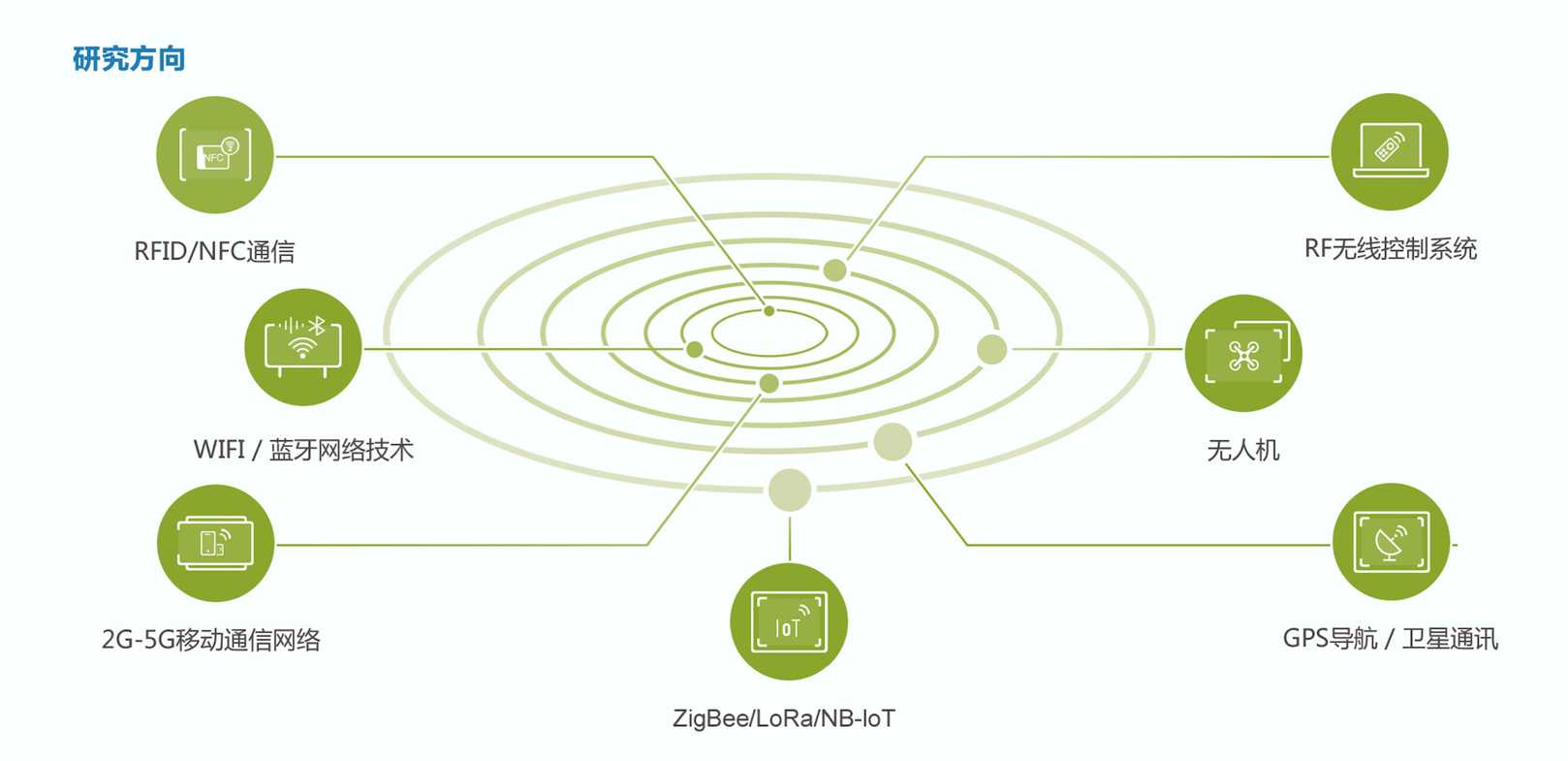
小米IoT安全峰会

大安全下的 IoT 安全威胁演变与应对

杨卿

360黑客研究院&独角兽安全团队

大安全（I'm ABCDE）－太空视角诠释"M"安全



“定位”攻防研究领域，同时创造超级“符号”

独角兽安全攻防团队
360UNICORNTEAM

Re: 谭总，感觉组名霸气真的很重要-.-

杨卿

收件人: 谭晓生

2014年7月11日 15:35

Marvel Team 咋样，我词穷...囧

无线电安全

360无线电安全研究院专注于无线通信、智能设备、汽车、工业系统等新兴安全领域的攻防研究，在信息安全领域拥有极丰富的攻防经验，在国内外安全会议发表研究成果50余次，已出版4部技术专著，申请专利40多项。

无线电安全研究院架构

独角兽安全团队
研究使用无线连接技术的各种系统的安全性

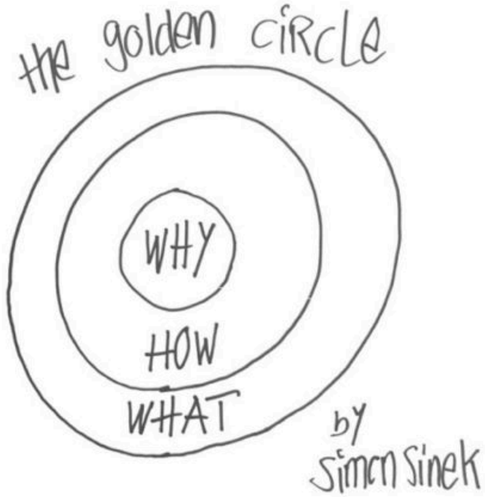
鲲鹏安全团队
硬件类安全攻防产品研发

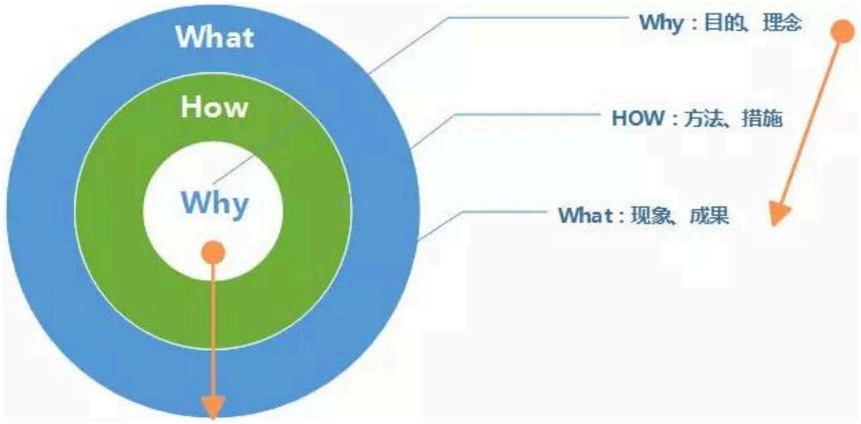
天马安全团队
WiFi安全攻防研究、渗透测试和安全咨询服务

用“黄金圈”法则解释为什么(WHY)执念于”M”无线电通信

People don’t buy what you do,
they buy WHY you do it.

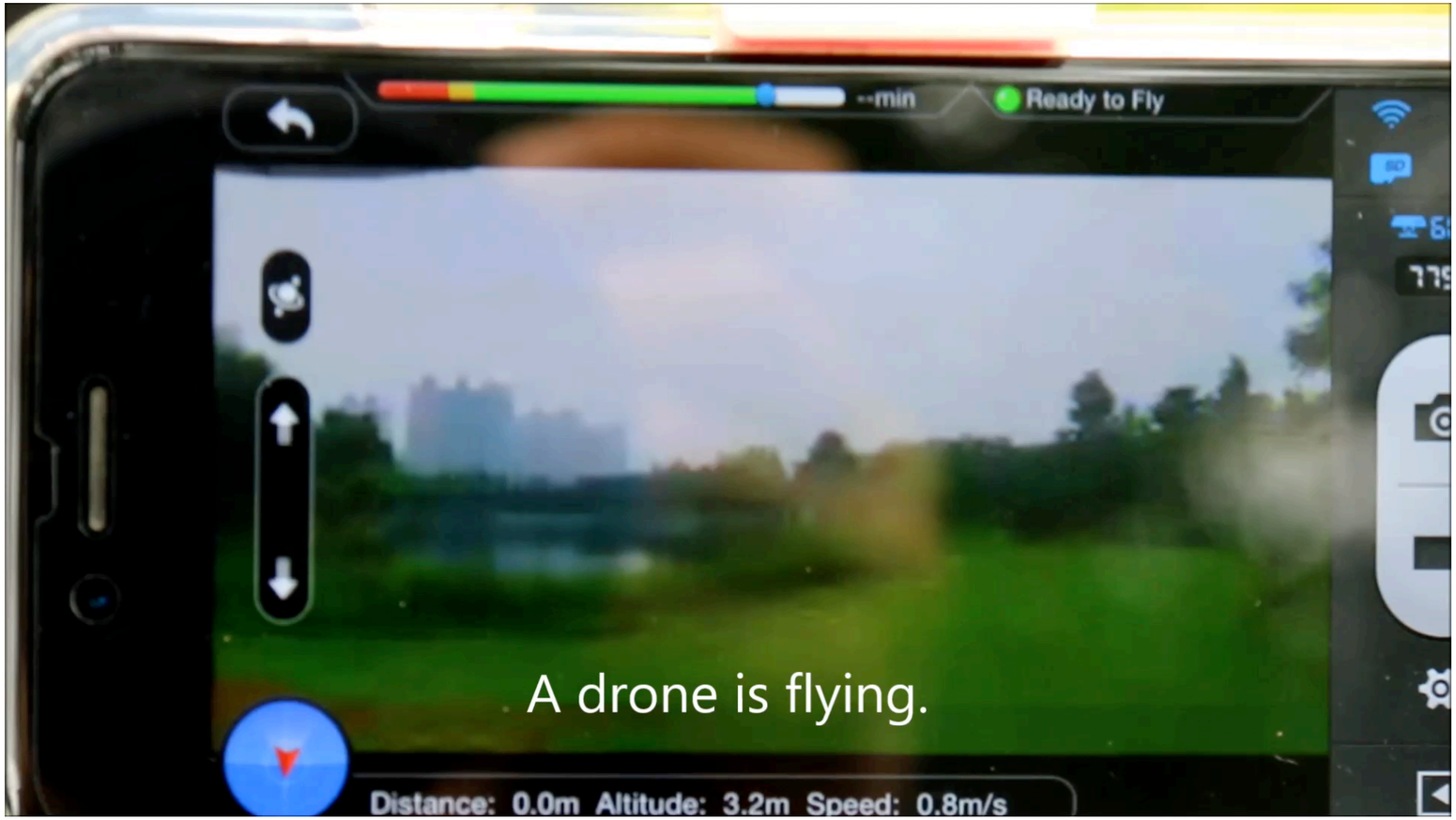
—— Simon Sinek





Because，危害大(应用涉及面广)、修复难度高(甚至不可修复)、修复周期长(以年为时间单位)、重视度低(技术变现难度高、企业投入度低)

危害大(应用涉及面广)



海南灯光秀，开演一分钟300架无人机掉落如雨！主办方：人为恶意干扰

河南都市频道　28万次播放

花费超千万无人机表演成“乱码”专家：或因信号干扰

凤凰新闻　05-04　08:39

演出现场图案的左半部分变成了“乱码”图。 视觉中国图

修复周期长(以年为时间单位)

住房和城乡建设部IC卡应用服务中心文件

建卡服【2013】019号

关于采取若干措施促进城市一卡通系统升级及
加快CPU卡替换M1卡的通知

各有关单位:

近年来我国部分城市一卡通领域陆续出现了因逻辑加密卡安全漏洞导致的各类安全事件，给城市一卡通运营单位及持卡人造成了不必要的损失，也严重影响了城市一卡通行业的安全。为加快系统安全建设步伐，根据国家相关主管部门对城市公共服务信息系统的安全要求，并经上级部门批准，决定自2019年1月1日起不再对使用“建设事业IC卡密钥管理系统”的城市一卡通运营单位提供基于M1卡应用的技术支持，具体要求通知如下。

一、自2014年1月1日起，仍在使用M1卡的城市一卡通运营单位新采购的安全认证卡中将统一设置M1卡控制时效，其时效控制时间截止为2018年12月31日，2019年1月1日起安全认证卡仅支持CPU卡应用。已设置了M1卡应用时效的城市一卡通运营单位不按此规定执行。

修复难度高(甚至不可修复)

安全 https://www.tesla.com/en_EU/about/security

TESLA MODEL S MODEL X MODEL 3 ROADSTER ENERGY SIGN IN

Product Security

Tesla values the work done by security researchers in improving the security of our products and service offerings. We are committed to working with this community to verify, reproduce, and respond to legitimate reported vulnerabilities. We encourage the community to participate in our responsible reporting process.

If you are a security researcher and would like to report a security vulnerability, please send an email to: vulnerability@tesla.com. Please provide your name, contact information, and company name (if applicable) with each report. Priority will be granted to encrypted reports – please include your PGP public key with such reports.

Download the Tesla Motors Inc. PGP key.

Responsible Disclosure Guidelines

We will investigate legitimate reports and make every effort to quickly correct any vulnerability. To encourage responsible reporting, we commit that we will not take legal action against you or ask law enforcement to investigate you if you comply with the following Responsible Disclosure Guidelines:

Provide details of the vulnerability, including information needed to reproduce and validate the vulnerability and a Proof of Concept (POC)
Make a good faith effort to avoid privacy violations, destruction of data and interruption or degradation of our services
Do not modify or access data that does not belong to you
Give us a reasonable time to correct the issue before making any information public

We will attempt to respond to your report within 1-2 business days.

Tesla Security Researcher Hall of Fame

Tesla appreciates and wants to recognize the contributions of security researchers. If you are the first researcher to report a confirmed vulnerability, we will list your name in our Hall of Fame (unless you would prefer to remain anonymous). You may also be considered for an award if you are the first researcher to report one of the top 3 confirmed vulnerabilities in a calendar quarter. You must comply with our Responsible Disclosure Guidelines (above) to be considered for our Hall of Fame and top 3 awards.

2018	UnicornTeam	Jun Li (@bravo_fighter), Qing Yang (@lr0nSmith), Yingtao Zeng, Chaoran Wang
2017	Keen Security Lab	Tencent for CVE-2017-9883 and CVE-2017-6261

特斯拉无钥匙进入系统安全缺陷无法通过固件升级修复只能提供功能关闭来应对漏洞

WIRED Just a Pair of These $11 Radio Gadgets Can Steal a Car SUBSCRIBE

BUSINESS CULTURE DESIGN GEAR SCIENCE SECURITY TRANSPORTATION

SHARE
SHARE 6394
TWEET
COMMENT
EMAIL

ANDY GREENBERG SECURITY 04.24.17 01:34 PM

JUST A PAIR OF THESE $11 RADIO GADGETS CAN STEAL A CAR

QIHOO 360 TEAM UNICORN

FOR YEARS, AUTOMAKERS and hackers have known about a

MOST POPULAR

SCIENCE
Tesla's Super-Battery Could Help Lift an Aircraft Carrier 1,500 Feet
RHETT ALLAIN

PHOTO
'ARAMCO: Above the Oil Fields' Takes You Inside the Surreal, Saudi...
LAURA MALLONEE

SPONSOR CONTENT
When Failure Is Not an Option, We Turn to Plastic
AMERICAN PETROLEUM INSTITUTE

CULTURE
Yes, It Matters That 'Spider-Man: Homecoming' Just Made...
ANGELA

Springer

Search

Home Subjects Services Products Springer Shop About us

» Computer Science » Communication Networks

© 2018

Inside Radio: An Attack and Defense Guide

Authors: **Yang**, Qing, **Huang**, Lin

Provides a practical guide, introducing real-world industrial cases in wireless security attacks and defense

受知名学术出版社Springer邀请
合作出版《无线电安全攻防大揭秘》英文国际版，
著作受多国安全研究者青睐，
成为全球无线电通信安全研究领域的“最佳参考”

Noriaki Hayashi
@v_avenger

@cn0Xroot I'm really inspired by this book.
#SDR #HackRF #RTL-SDR

2018/4/15 22:58

TechWeb > 公司动态 >

360登上GSMA移动安全研究名人堂 成为首家上榜公司

2017.06.15 16:58:07 来源: TechWeb.com.cn 作者:TechWeb.com.cn （0 条评论）

近日，世界著名的全球移动通讯系统协会GSMA更新了安全名人堂名单，360无线电安全研究部的UnicornTeam凭借发现全球首个4G网络协议高危漏洞，成为自GSMA安全研究名人堂设立以来第一个获得该荣誉的公司。

GSMA ABOUT US WHAT WE DO MEMBERSHIP NEWSROOM SEARCH

Mobile Security Research Hall of Fame

Welcome to the GSMA Mobile Security Research Hall of Fame.

The GSMA's Mobile Security Research Hall of Fame lists security vulnerability finders that have made contributions to increasing the security of the mobile industry by submitting disclosures to the GSMA or its members. It is the primary mechanism for the GSMA to recognise and acknowledge the positive impact the finder has had on the mobile industry by following the GSMA's CVD process.

The Hall of Fame also facilitates the nomination and recognition of other finders that may have made significant discoveries of vulnerabilities to individual GSMA member companies.

Entry to the Mobile Security Research Hall of Fame is purely optional and is at the discretion of the finder, the GSMA and/or the nominating GSMA member.

On behalf of the mobile industry, we would like to thank the following people for making a responsible disclosure to us and recognise their contribution to increasing the security of the mobile industry:

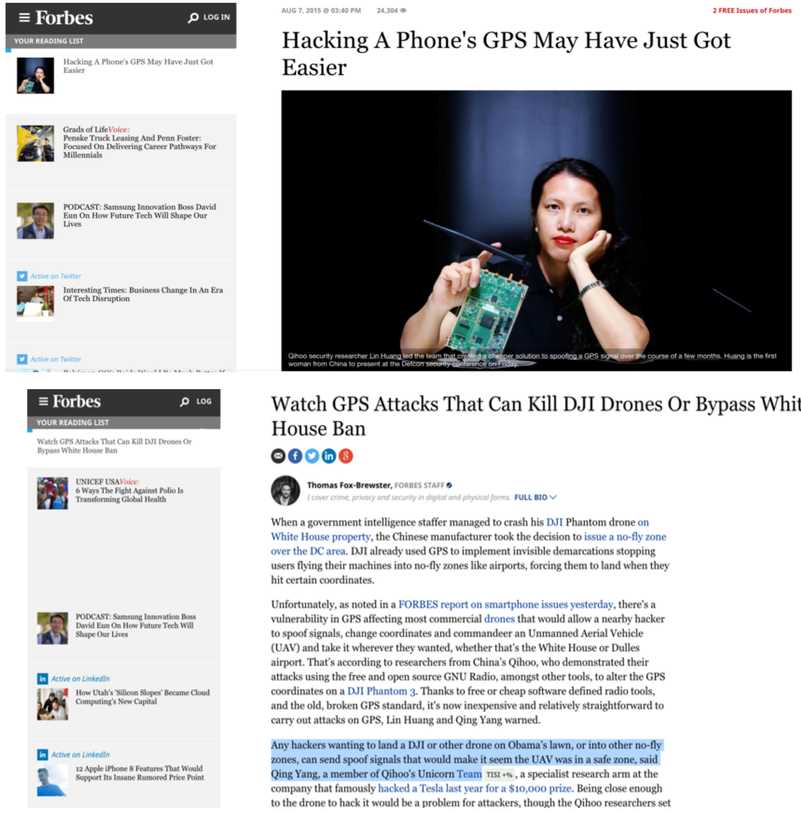
Date	CVD#	Name	Organisation	Link
23/2/2017	0001	Yuwei Zheng, Lin Huang, Haoqi Shan, Jun Li, Qing Yang	Unicorn Team, Radio Security Research Dept., 360 Technology	http://unicorn.360.com
19/6/2017	0003	Vladimir Wolstencroft	BAIKE LTD	
19/6/2017	0003	Fredrik Söderlund	Symsoft	http://www.symsoft.com

For more information about the GSMA Coordinated Vulnerability Disclosure program

全球移动通讯系统协会GSMA（Groupe Speciale Mobile Association）于1995年成立，协会致力于全球通移动电话系统的标准建立、发展等工作。GSMA 广泛联结全球近 800 家移动运营商和近 300 家相关企业，其中包括手机与设备制造商，软件公司，设备供应商，互联网企业，以及相关行业组织。中国移动、中国联通、中国电信等都是该组织的成员。

全球首个发现4G通信协议漏洞，可以实现对通话和短信的劫持，首个入选GSMA名人堂

并获得“CVD#0001”首位漏洞编号



Forbes LOG IN

YOUR READING LIST

Hacking A Phone's GPS May Have Just Got Easier

Grads of LifeVoice: Penske Truck Leasing And Penn Foster: Focused On Delivering Career Pathways For Millennials

PODCAST: Samsung Innovation Boss David Eun On How Future Tech Will Shape Our Lives

Active on Twitter

Interesting Times: Business Change In An Era Of Tech Disruption

Active on Twitter

AUG 7, 2015 @ 03:40 PM 24,304

2 FREE Issues of Forbes

Hacking A Phone's GPS May Have Just Got Easier

Qihoo security researcher Lin Huang led the team that created a cheaper solution to spoofing a GPS signal over the course of a few months. Huang is the first woman from China to present at the Defcon security conference on Friday.

Forbes LOG

YOUR READING LIST

Watch GPS Attacks That Can Kill DJI Drones Or Bypass White House Ban

UNICEF USAVoice: 6 Ways The Fight Against Polio Is Transforming Global Health

PODCAST: Samsung Innovation Boss David Eun On How Future Tech Will Shape Our Lives

Active on LinkedIn

How Utah's 'Silicon Slopes' Became Cloud Computing's New Capital

Active on LinkedIn

12 Apple iPhone 8 Features That Would Support Its Insane Rumored Price Point

Watch GPS Attacks That Can Kill DJI Drones Or Bypass White House Ban

Thomas Fox-Brewster, FORBES STAFF
I cover crime, privacy and security in digital and physical forms. FULL BIO

When a government intelligence staffer managed to crash his DJI Phantom drone on White House property, the Chinese manufacturer took the decision to issue a no-fly zone over the DC area. DJI already used GPS to implement invisible demarcations stopping users flying their machines into no-fly zones like airports, forcing them to land when they hit certain coordinates.

Unfortunately, as noted in a FORBES report on smartphone issues yesterday, there's a vulnerability in GPS affecting most commercial drones that would allow a nearby hacker to spoof signals, change coordinates and commandeer an Unmanned Aerial Vehicle (UAV) and take it wherever they wanted, whether that's the White House or Dulles airport. That's according to researchers from China's Qihoo, who demonstrated their attacks using the free and open source GNU Radio, amongst other tools, to alter the GPS coordinates on a DJI Phantom 3. Thanks to free or cheap software defined radio tools, and the old, broken GPS standard, it's now inexpensive and relatively straightforward to carry out attacks on GPS, Lin Huang and Qing Yang warned.

Any hackers wanting to land a DJI or other drone on Obama's lawn, or into other no-fly zones, can send spoof signals that would make it seem the UAV was in a safe zone, said Qing Yang, a member of Qihoo's Unicorn Team TISI +%, a specialist research arm at the company that famously hacked a Tesla last year for a $10,000 prize. Being close enough to the drone to hack it would be a problem for attackers, though the Qihoo researchers set

全球首次实现低成本GPS欺骗，福布斯连续

两篇媒体报道，并获美国通信协会IEEE高度评价

Lte GPS ZigBee® Bluetooth® GSM NFC LoRa™ WiFi 5G 北斗 NB-IoT

3GPP A GLOBAL INITIATIVE

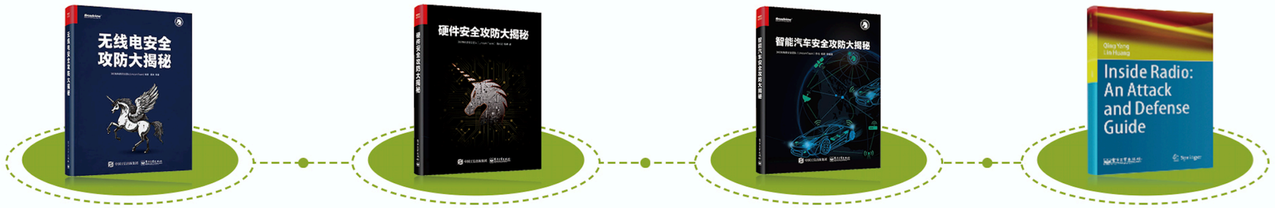
受邀成为3GPP标准组织中唯一一家网络安全公司

GSMA™

首个入选GSMA安全名人堂

安全专著

已出版多部信息安全书籍，包括国内首本无线电安全书籍《无线电安全攻防大揭密》，国内首本硬件安全书籍《硬件安全攻防大揭秘》，国内首本汽车安全书籍《智能汽车安全攻防大揭秘》及与全球知名学术期刊出版社Springer联合出版的《Inside Radio: An Attack and Defense Guide》。



媒体报道

众多成果被中央电视台、北京电视台、北京人民广播电台、福布斯、国家地理、FOX NEWS、WIRED连线、CNET、IEEE、The Register、Hackaday等国内外媒体报道。

国际会议

团队成员多次在BlackHat USA&Europe&Asia、DEFCON、HITB、CanSecWest、IEEE-CNS、POC、RUXCON等国际安全会议及XCon、KCon、MOSEC、ISC互联网安全大会等国内安全会议发表研究成果。

技术实力

发现4G网络协议高危漏洞，成为全球移动通讯系统协会GSMA安全研究名人堂首支上榜团队，获首个漏洞编号CVD#0001。

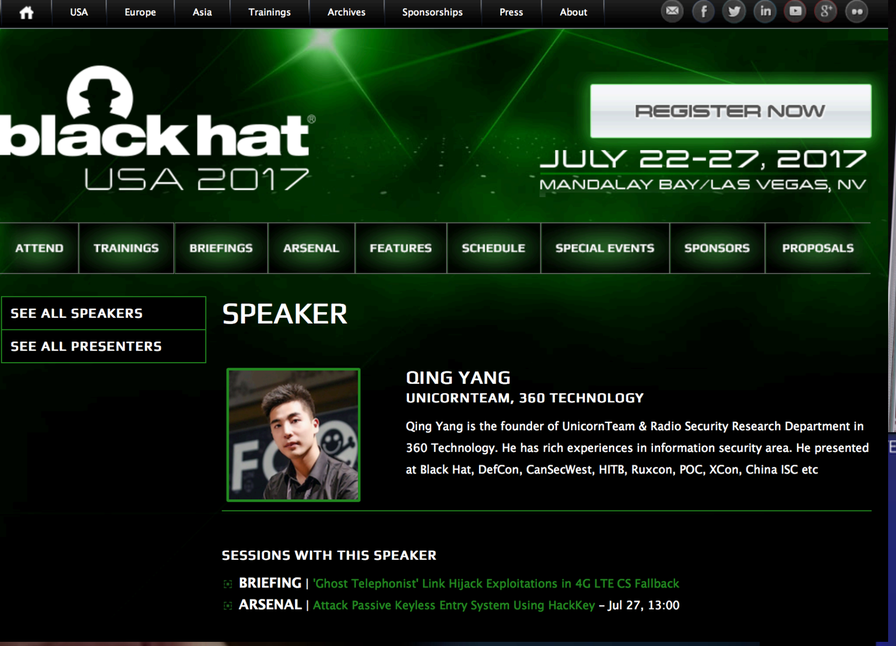
发现汽车无钥匙进入与启动系统高危漏洞，该漏洞影响全球众多汽车厂商旗下智能汽车，入选特斯拉安全研究名人堂。

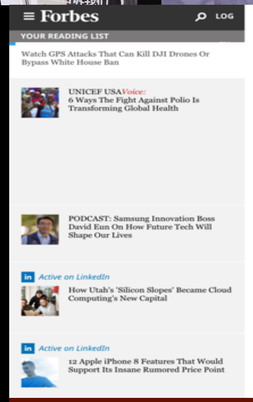
获全球知名半导体制造公司NXP（恩智浦）关于芯片层面的首个漏洞致谢。

获得DEFCON官方授权及全球顾问委员会成员身份，负责中国首个DC010安全社区，及管理协助全国各个地区DEFCON GROUPS，连接中国与全球安全人员生态圈。

幽灵接线员“Ghost Telephonist”研究成果，荣获美国BlackHat Pwnie Awards（黑客奥斯卡）最具创新研究奖提名，也是历史上中国安全研究员获得该奖项首次提名。

凭借移动网络协议安全研究突出成绩，入选全移动通信标准化组织3GPP，是现今该标准组织中国成员中唯一的互联网安全公司。





Watch GPS Attacks That Can Kill DJI Drones Or Bypass White House Ban

Thomas Fox-Brewster, FORBES STAFF
I cover crime, privacy and security in digital and physical forms. FULL BIO

When a government intelligence staffer managed to crash his DJI Phantom drone on White House property, the Chinese manufacturer took the decision to issue a no-fly zone over the DC area. DJI already used GPS to implement invisible demarcations stopping users flying their machines into no-fly zones like airports, forcing them to land when they hit certain coordinates.

Unfortunately, as noted in a FORBES report on smartphone issues yesterday, there's a vulnerability in GPS affecting most commercial drones that would allow a nearby hacker to spoof signals, change coordinates and commandeer an Unmanned Aerial Vehicle (UAV) and take it wherever they wanted, whether that's the White House or Dulles airport. That's according to researchers from China's Qihoo, who demonstrated their attacks using the free and open source GNU Radio, amongst other tools, to alter the GPS coordinates on a DJI Phantom 3. Thanks to free or cheap software defined radio tools, and the old, broken GPS standard, it's now inexpensive and relatively straightforward to carry out attacks on GPS, Lin Huang and Qing Yang warned.

Any hackers wanting to land a DJI or other drone on Obama's lawn, or into other no-fly zones, can send spoof signals that would make it seem the UAV was in a safe zone, said Qing Yang, a member of Qihoo's Unicorn Team TISI +%, a specialist research arm at the company that famously hacked a Tesla last year for a $10,000 prize. Being close enough to the drone to hack it would be a problem for attackers, though the Qihoo researchers set

SHARE
SHARE 6394
TWEET
COMMENT
EMAIL

ANDY GREENBERG SECURITY 04.24.17 01:34 PM

JUST A PAIR OF THESE $11 RADIO GADGETS CAN STEAL A CAR

QIHOO 360 TEAM UNICORN

FOR YEARS, AUTOMAKERS and hackers have known about a

MOST POPULAR

SCIENCE
Tesla's Super-Battery Could Help Lift an Aircraft Carrier 1,500 Feet
RHETT ALLAIN

PHOTO
'ARAMCO: Above the Oil Fields' Takes You Inside the Surreal, Saudi...
LAURA MALLONEE

SPONSOR CONTENT
When Failure Is Not an Option, We Turn to Plastic
AMERICAN PETROLEUM INSTITUTE

CULTURE
Yes, It Matters That 'Spider-Man: Homecoming' Just Made...
ANGELA WATERCUTTER

独角兽安全攻防团队
360UNICORNTEAM

360
无线电安全研究院

HACKNOWN
BUILD LEGENDS FOR THE FUTURE

杨卿，360黑客研究院负责人、国际知名安全团队独角兽UnicornTeam创始人，也是首个企业无线电通信安全研究机构“360无线电安全研究院”的建立者。 国科大网络空间安全学院客座教授，广州大学企业导师。51CTO俱乐部讲师。

技术成果入选特斯拉、GSMA等安全名人堂，并获得GSMA“CVD#0001”首位漏洞编号。曾获Blackhat Pwnie Awards黑客奥斯卡最具创新研究奖提名，也是黑帽大会Blackhat USA&Europe&ASIA 、黑客大会DEFCON 、HITB、CanSecWest、IEEE－CNS等国际知名安全会议演讲者。

著有《无线电安全攻防大揭密》、《硬件安全攻防大揭秘》、《智能汽车安全攻防大揭秘》、Springer学术《Inside Radio: An Attack and Defense Guide》等技术专著。众多成果被福布斯、美国国家地理、WIRED连线、福克斯新闻、CNET、The Register、IEEE ComSoc等知名媒体报道。

全球通信标准化组织3GPP参会代表。网络安全试点示范项目评审专家。 WitAwards互联网安全年度评选评委专家。 ANZER安在安全新媒体荣誉顾问。 DC010(DEFCON Group)技术顾问。

央视CCTV《汽车百年II》大型纪录片安全专家，2015、2017年两届央视CCTV《315》晚会出镜安全专家。国内首部黑客微电影“I’m Here”男主角。《东方黑客》小说人物原型。

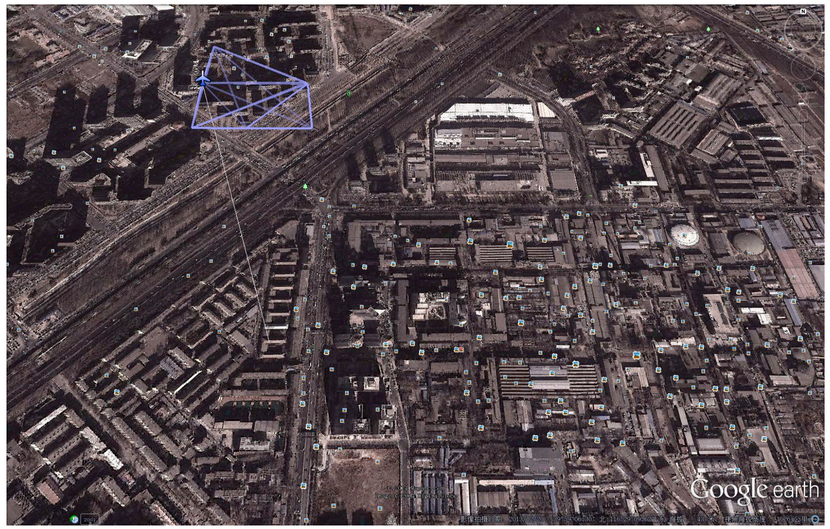
从0到1，从1到 N，未来的新威胁攻防要仰仗各位同行了

“想要我的财宝吗？想要的话拿去吧！去找吧！我把所有的财宝都放在那里！”

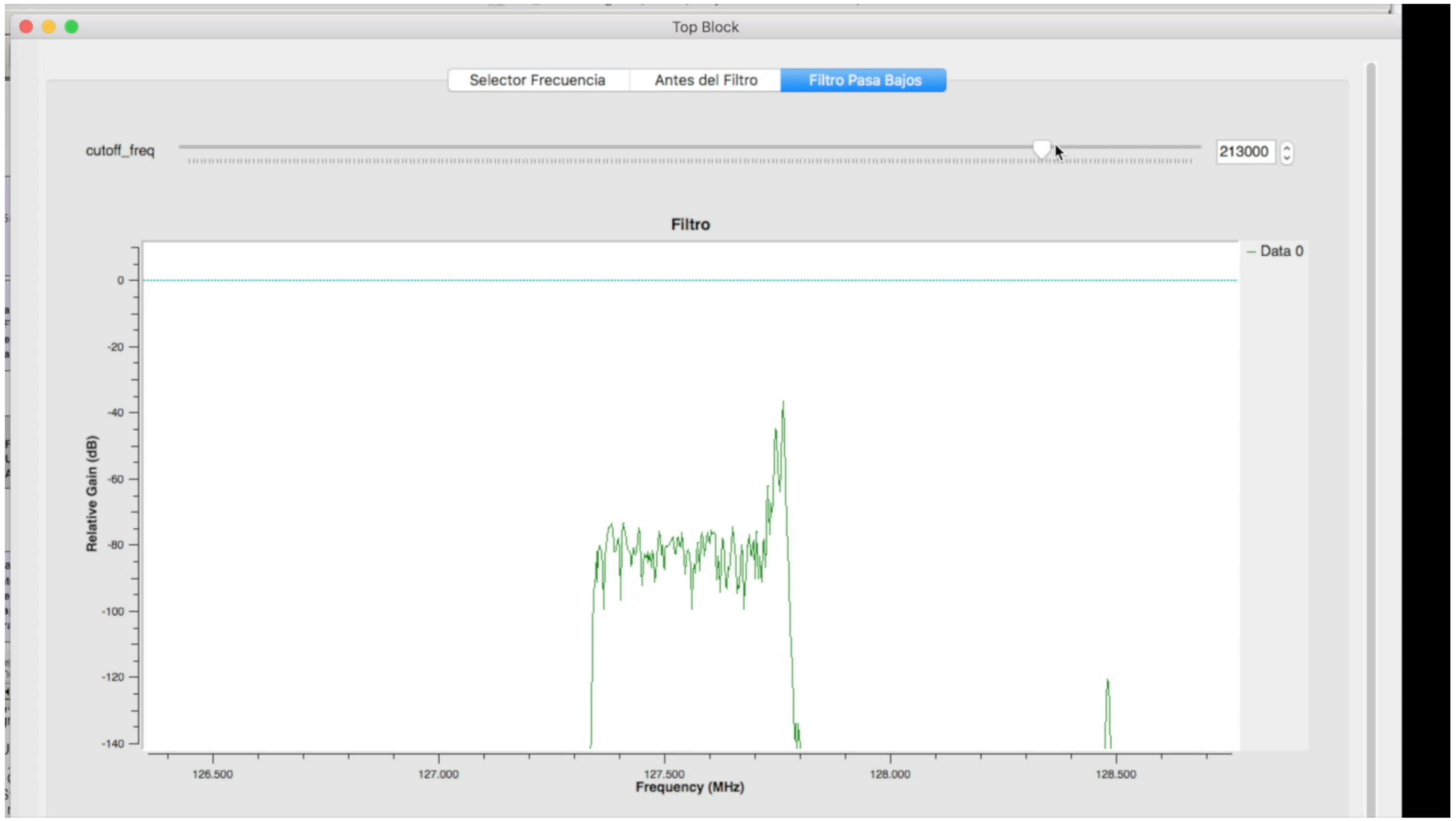
GPS 欺骗攻防技术对于 IoT场景不单是位置欺骗威胁

新浪科技讯 北京时间2月15日早间消息，根据最新报告的一个漏洞，如果用户将iPhone的日期调整至1970年1月1日，那么iPhone就会变砖。

利用GPS 、短波NTP授时欺骗将引发更大的安全问题，如针对金融、工业等基础设施云，这种通过恶意攻击影响系统时间的威胁造成的“内伤”值得深挖以及防护思考。



历史悠久的基础交通设施通信系统面临新威胁



各类通过无线通信触发的灾害报警系统安全堪忧

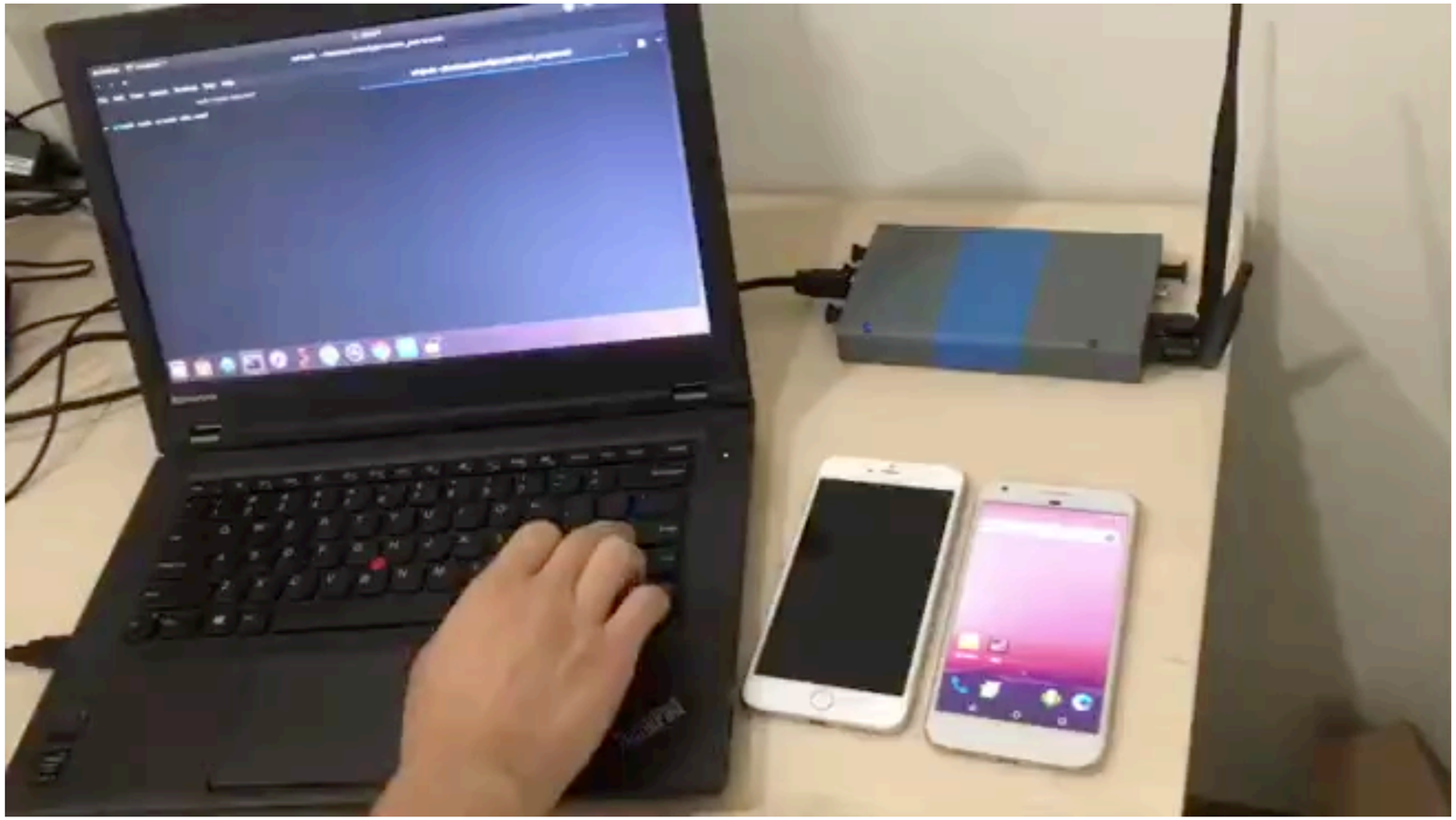
紧急报警系统中存在严重漏洞 攻击者可远程触发误报

品味智能
百家号 | 04-12 09:23

紧急报警系统 (EAS) 中被曝存在一个严重的漏洞，攻击者可通过射频远程激活所有警报器从而触发误报。

全球各地都在使用紧急报警警报器提醒公民注意自然灾害、人为灾难和紧急情况如危险的天气状况、风暴、龙卷风和恐怖主义攻击等。

误报可人为制造恐慌和混乱，正如去年美国德克萨斯州达拉斯市经历的那样。当时156个紧急警报器一直响了2个小时左右的时间，导致居民从睡梦中惊醒且引发恐慌。



美国达拉斯警报器遭黑客入侵 警笛声持续一小时

2017-04-10 14:11

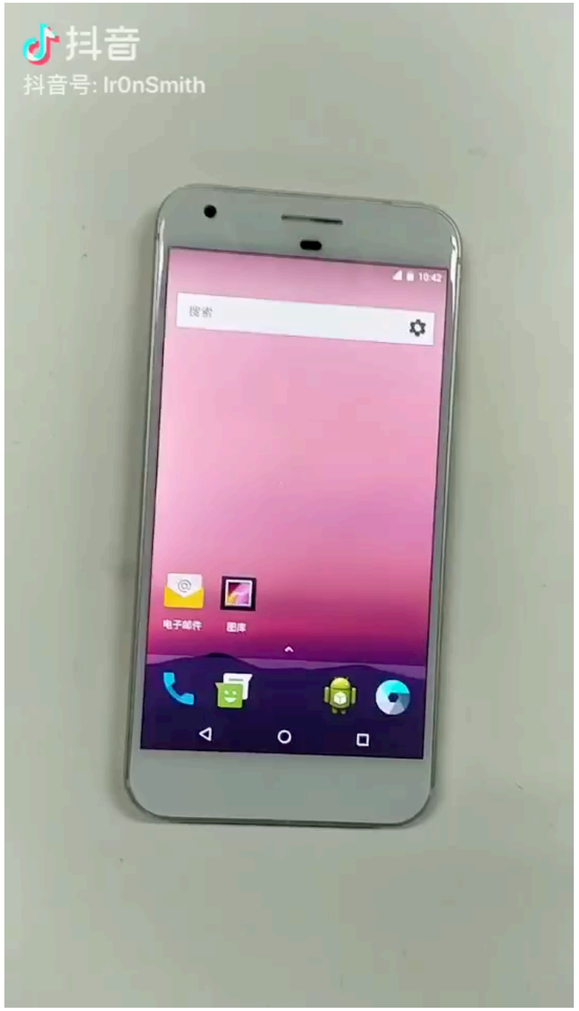
德克萨斯州达拉斯周围的夜间紧急警报器在星期五晚上启动，报警声超过一个小时，促使大量的电话打入该市911中心。市应急管理处的官员已经确认没有紧急情况，而是达拉斯紧急警报器系统被入侵。该市新闻办公室主任萨娜·赛义德告诉记者，这个城市的156个紧急警报器被激活。

各种老旧无线灾害报警系统

移动网络（4G）警报特性

可能被恶意利用，造成社会

恐慌等恶性安全事件。



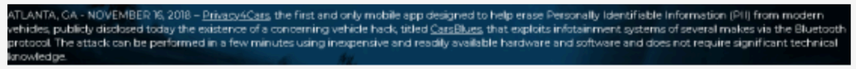
CarBlues蓝牙攻击预计影响数以千万计的车辆

来源：工业互联网安全应急响应中心　时间：2018-11-21　阅读次数：14

Privacy4Cars昨天公开披露一个严重的安全漏洞，该漏洞可能会影响数百万辆汽车，其通过攻击利用几类车辆上的信息娱乐系统，上述系统可以通过蓝牙访问用户标识（PII）。

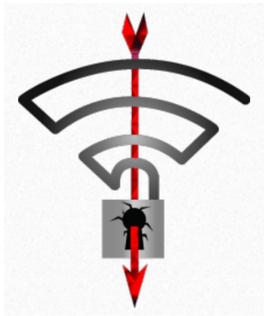
Privacy4Cars警告说，一种新的蓝牙黑客技术，被称为CarsBlues，有可能会影响数百万辆汽车。CarsBlues攻击通过蓝牙利用了安装在几类车辆上的信息娱乐系统中的安全漏洞，它会影响已经将智能手机与汽车同步的用户，导致车主的隐私数据暴露给攻击者，并用于各种非正当的目的。攻击者可以访问已存储的联系人、呼叫日志、文本日志，在某些情况下还可以访问文本消息，而且无需将用户的手机连接到系统。

该公司发布的报告中称："攻击可以用廉价且容易获得的硬件和软件在几分钟内完成攻击，而且这还不需要大量的技术知识"。

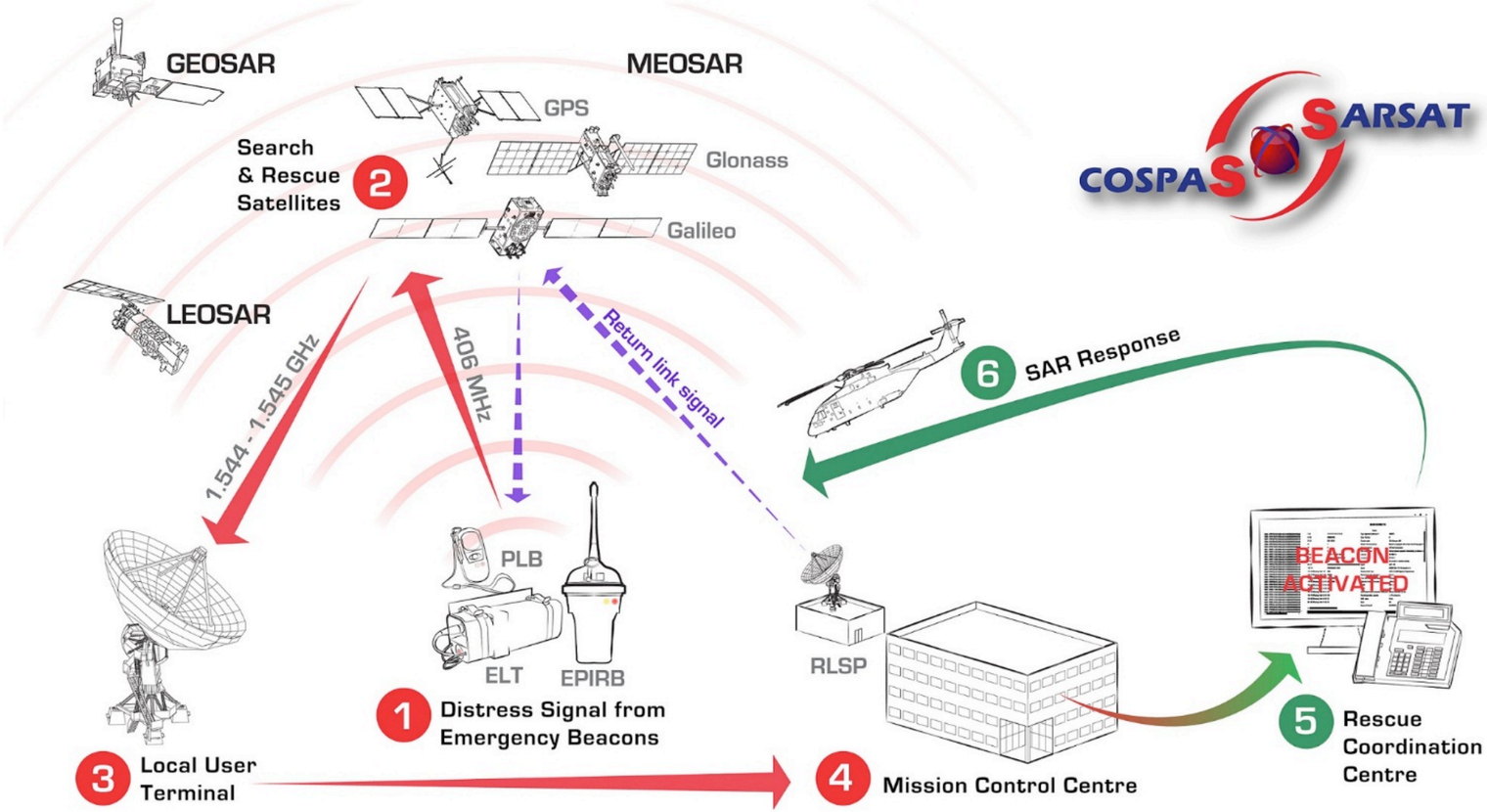

ATLANTA, GA - NOVEMBER 16, 2018 – Privacy4Cars, the first and only mobile app designed to help erase Personally Identifiable Information (PII) from modern vehicles, publicly disclosed today the existence of a concerning vehicle hack, titled CarsBlues, that exploits infotainment systems of several makes via the Bluetooth protocol. The attack can be performed in a few minutes using inexpensive and readily available hardware and software and does not require significant technical knowledge.

受该漏洞影响程度最大的为各类租赁车辆，因其车载信息系统需要与用户手机应用通过WiFi或蓝牙方式进行绑定，包括但不限于各类共享车辆、通过订阅服务租赁或出售的车辆。

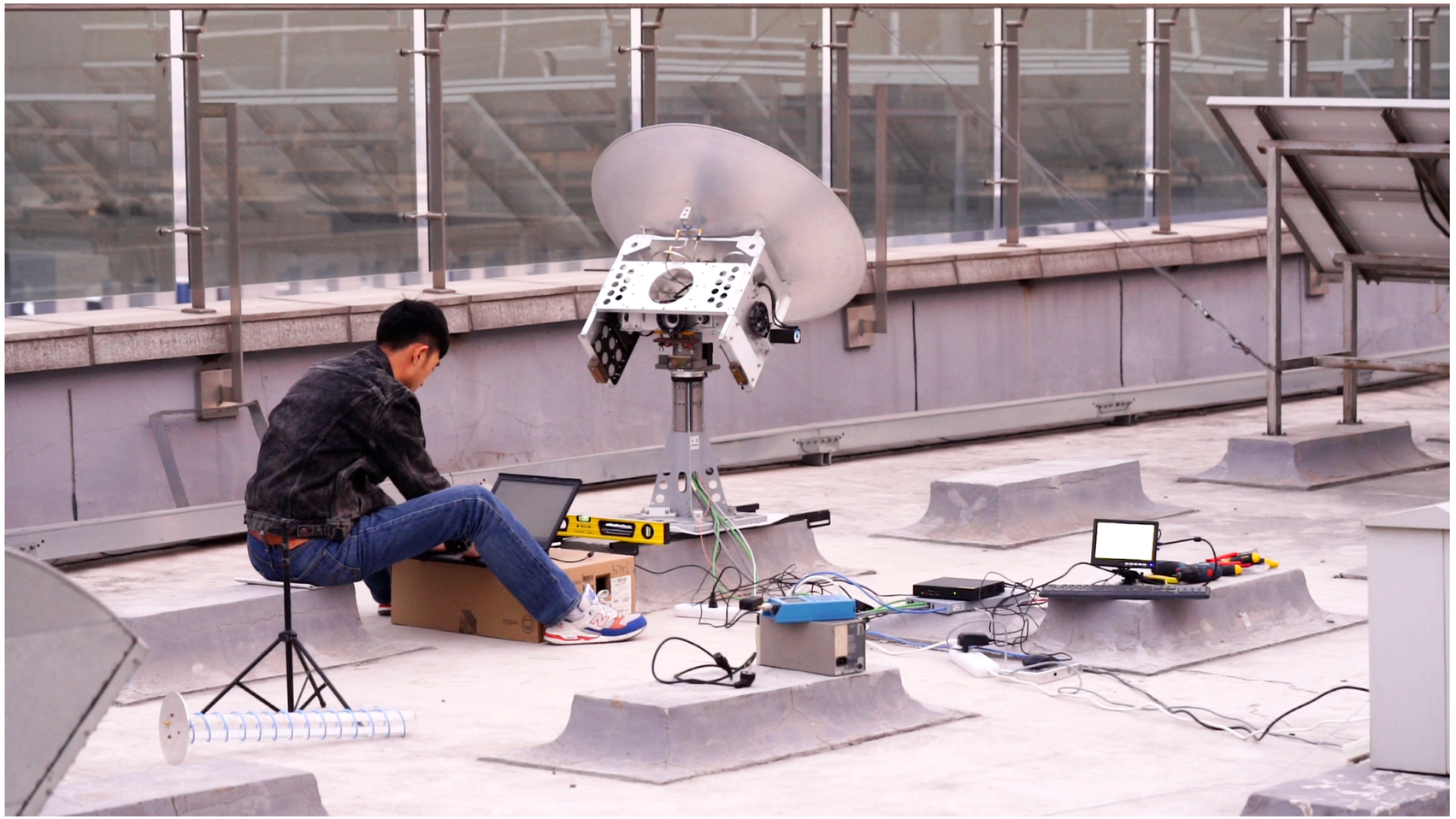
参加漏洞比赛的从业者可以考虑适当"跨界"，从系统漏洞挖掘的红海换到以移动基带、WiFi、蓝牙、GPS模块等"必备"模块为主的漏洞挖掘蓝海，不被注意而漏洞多是其特点，一旦有所突破将会成为通杀攻击手段，引发"地图炮"效果，手机、汽车、智能音箱等 IoT 设备都将受到影响。



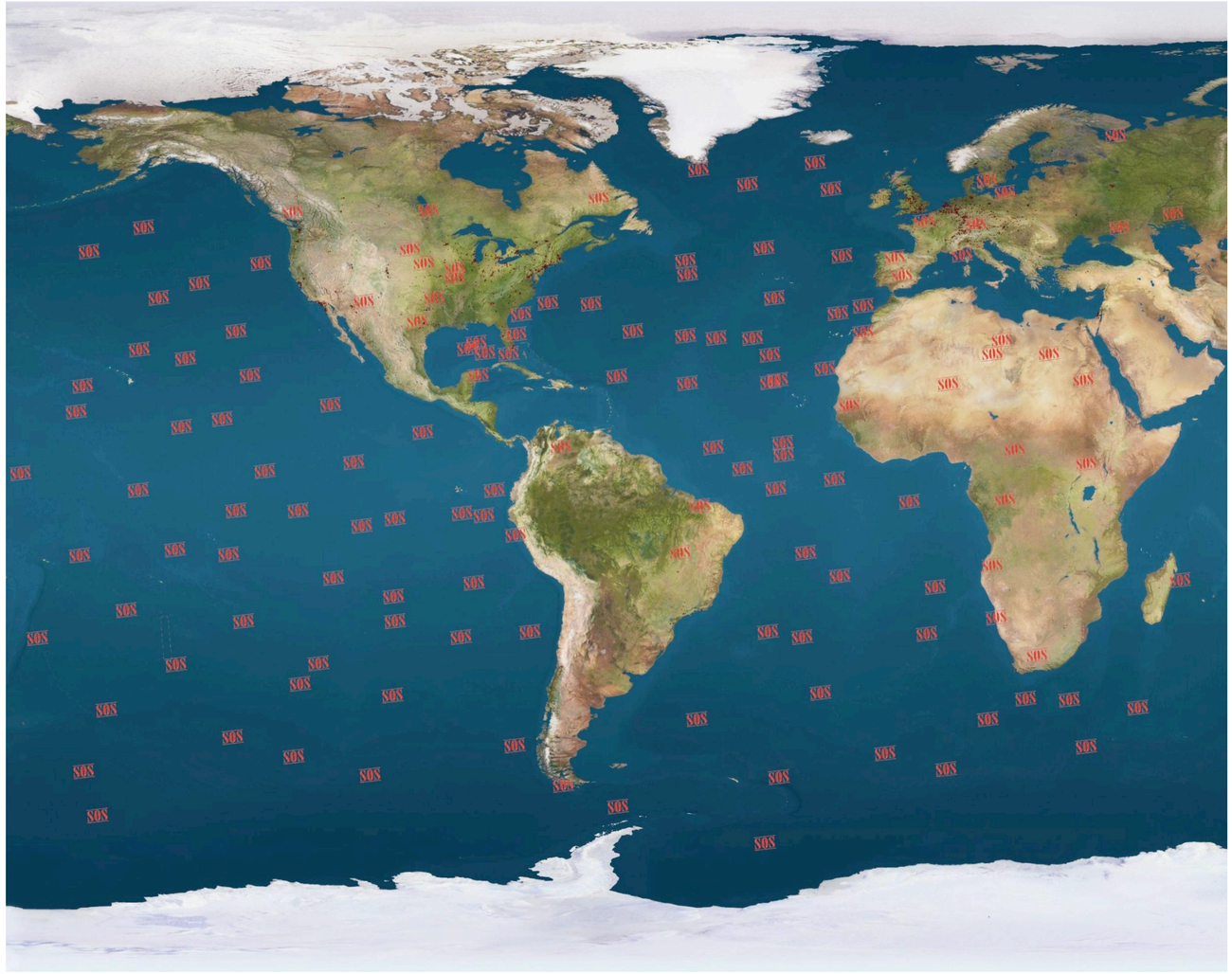
卫星通信系统的各类安全将会是下一个问题大户




AZ: 46 EL: 23



MH370(Boeing 777-200ER) have 4 ELTs
But no message , unusual…



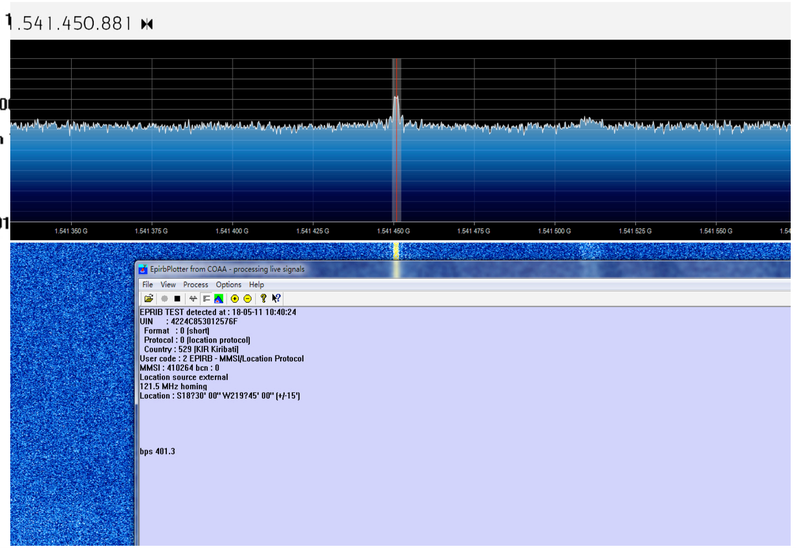
ITU List of MID Country Code Numbers

ITEM	BITS	VALUE
Message format: Not provided in 15 hex id	25	
Protocol: User	26	1
Country code: 227 - **France**	27-36	0011100011
User type: Orbitography	37-39	000
Identification Bits, Hex value: D38AAD42490	40-85	1101001110001010101011010000010010010010000000
15 Hex ID:	N/A	9C634E2AB509240

UIN (?): 9D1FCFA7AB0D990 detected on 11/12/18 09:16:39 UTC
Message type: distress / short
Protocol: user
Registered in: United Kingdom (MID=232)
Test User Protocol
Test Data: 3CFA7AB0D990 (111100111110100111101010110000110110011001000 0)
Beacon activated manually
No non-protected data field

UIN (?): 9C6000000000001 detected on 1
Message type: distress / long
Protocol: user
Registered in: France (MID=227)
Orbitography Protocol
Orbitography data: 000000000001 (0000

UIN (?): 9C634E2AB509240 detected on
Message type: distress / long
Protocol: user
Registered in: France (MID=227)
Orbitography Protocol
Orbitography data: 34E2AB509240 (1101

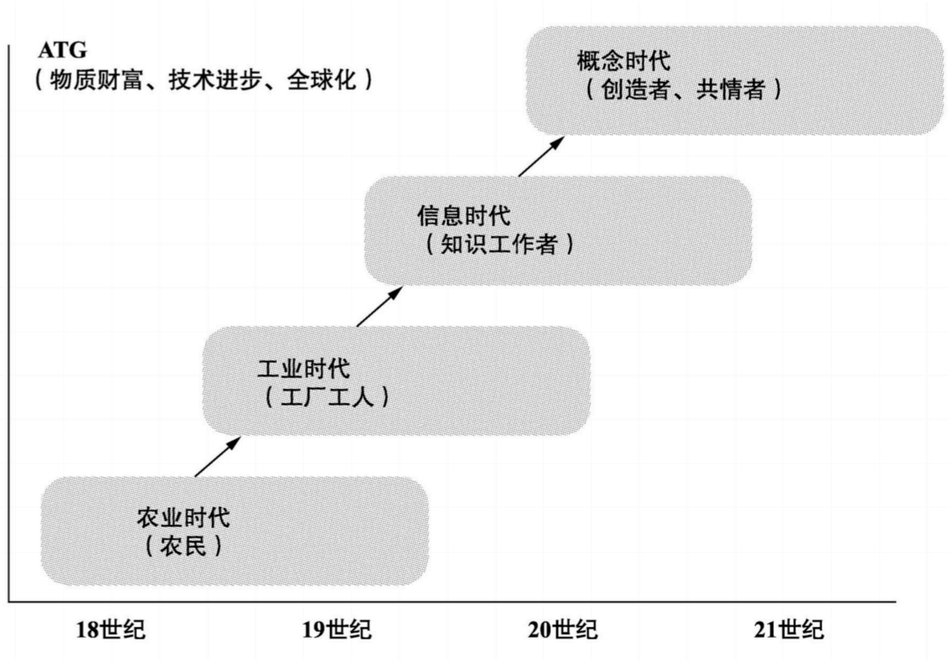


近地轨道卫星存在被攻击入侵后恶意变换轨道姿态的可怕假想，卫星通信安全与卫星系统本身的安全都不容忽视

大安全（I'm ABCDE）－每个人都有自己的哈姆雷特“E”教育

我们可以把过去的150年看作一场三幕剧。

- 第一幕是工业时代，推动经济发展的是无数的工厂和高效的流水线工作。这一幕的主角是从事大规模生产的工人，基本特征是体力和个人毅力。
- 第二幕是信息时代，美国和其他国家逐步发展起来。大规模生产退居幕后，信息和知识成为驱动发达国家经济发展的主要力量。这一幕的主角是知识工作者，其特征是擅长左脑思维。
- 第三幕是概念时代，当今，物质财富的充裕、亚洲的崛起和自动化的影响在不断深化，其影响力越来越大，第三幕正渐渐拉开帷幕。我们把这一幕称为概念时代。这一幕的主角是创造者和共情者，其特征是擅长右脑思维。



借力黑客Hack文化，诠释创新故事，寄希望于“未来“推动安全技术革新

混沌大学创办人 李善友

“今天每一个职场人都必须学习创新，就像在工业时代，每一个人必须学习商业管理一样。”

趋势专家 丹尼尔平克 在其畅销书《全新思维》中关于高概念与高感性的解释

- **高概念能力包括：创造艺术美感和情感美，辨析各种模式，发现各种机会，创造令人满意的故事，以及将看似无关的观点组合成某种新观点。**
- **高感性能力包括：理解他人，了解人际交往的微妙，找到自己的快乐并感染他人，以及打破常规、探寻生活的目标和意义。**

多数安全人才生来就拥有离经叛道不走寻常路的思维优势，如果创造出一种有趣的“模式”，用黑客文化故事内容与玩具娱乐加深对于Hack这种心智思维逻辑的正反馈，就会使他们获得一种自驱的“驱动力”，藉而通过刻意练习补充多元认知模型，那么一定会产生神奇的“化学效果”，也一定会从他们身上诞生创新的黑科技。

Hack技术能力之外，更重要的通识能力品质

独角兽安全攻防团队
360UNICORNTEAM

360 无线电安全研究院

HACKNOWN
BUILD LEGENDS FOR THE FUTURE

自驱（情怀、志向、理想、梦想力）

有趣（会玩、游戏力、审美力、专注力）

耐心（滞后满足、坚韧不拔、等待力）

创新（离经叛道之心、与众不同之事、概念想象力）

好奇（感受世界、感知变化、细节洞察力）

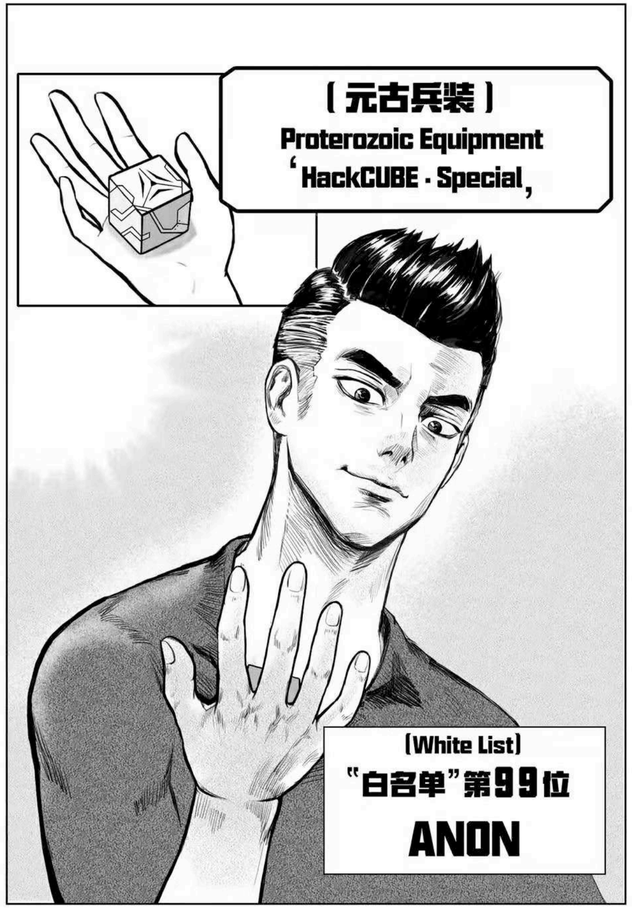
自律约束（风骨、格局、德行、极致力）

韧性（不屈、钝感力、黑色生命力）

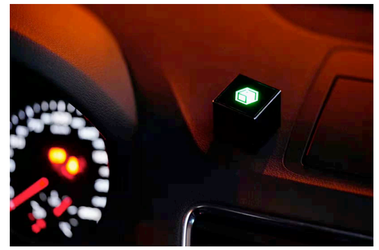
沟通（协作协同、共情移情力、故事营销力）

升级（提升多元认知模型、学习成长力）

寓教于乐，从学中玩，从玩中学，兴趣是最好的老师



1 网络军火交易 (完) 下集待续...



“这里已经没有可以反抗的固有规则、没有可以打破的预期了，让创造力显得惊人并且有意义的背景都失去了，那我们还能颠覆什么呢？如果你想颠覆传统，最好先去了解它。所以外行或新手很少能够想出真正有创造性的东西。”

《直觉泵》关于“跳出系统”（jootsing）这种思维工具的表述某种维度上也是一种黑客(Hack)思维

谢谢！