
DEFCON 神州 CHINA 1.0

WELCOME TO DEF CON CHINA 1.0!

It is my honor to welcome you to DEF CON China 1.0 on behalf of DEF CON, Baidu Security and XFuture Security.

For our 1.0 launch I am are happy to be in the 751-D Park with you. This space has a much more "DEF CON" feel than a 5 star hotel. Here I feel more freedom of ideas and creativity, and we have space to grow in the years to come.

What's new? Since last year we have gone from 5 DEF CON Groups in China to 11 with more on the way. There are more villages, contests, events, art and music! It has taken the better half of a year to make it here and we are excited and ready to go!

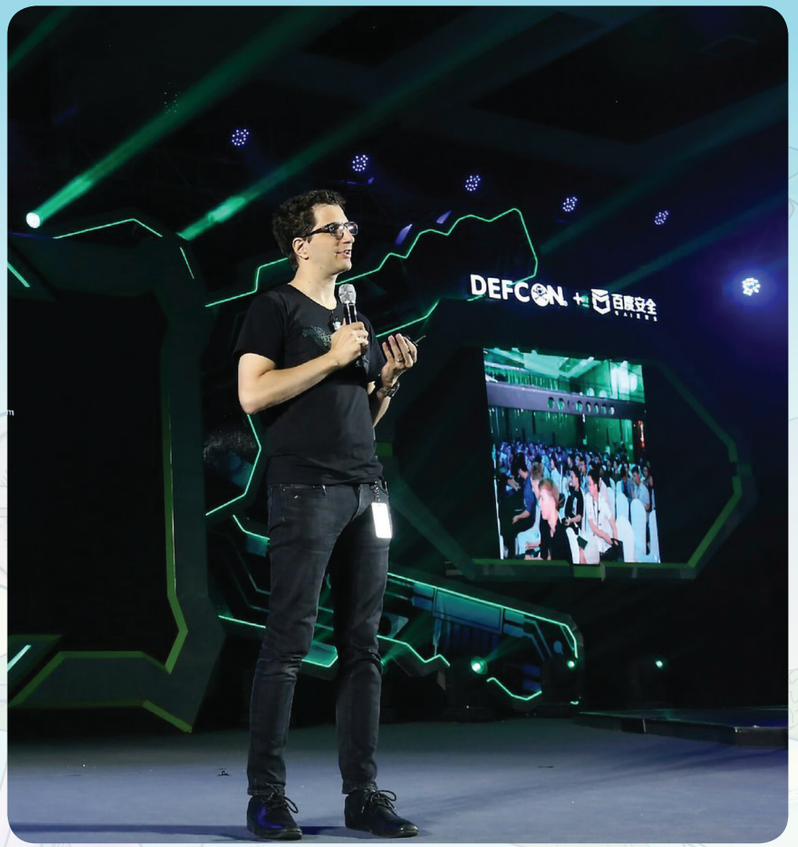
The theme this year is Technology's Promise, a positive vision of what could be if technology enabled our better selves. Instead of tracking and selling to us it could be used to help educate and heal us. In this spirit I want us to build a community of security geeks to solve the problems of today and face the challenges of the future. In this network we will be working with each other for the rest of our careers because internet problems are global problems and we will be the ones called on to help engineer it.

Last year I said that at DEF CON it is your idea that counts, not what you look like, how much money you make, how many followers you have, or what kind of music you listen to. At DEF CON you have the freedom to ask questions, challenge the speakers, and change your opinions.

Just in time for the con I am happy to announce the re-launch of forum.defcon.org, a place to plan all things DEF CON, hang out, talk tech, make friends, start your own blog or share pictures of you latest project. By the time you read this the Android mobile app should be live with iOS not far behind. It is where I will be posting my after-con stories and pictures.

Thank you,

The Dark Tangent



非常荣幸能代表DEF CON、百度安全及未来安全郑重欢迎您至DEF CON 神州 1.0。

我很高兴能在751D Park呈现1.0 版的DEF CON 神州。与一般五星级酒店相比，这里更有"DEF CON"的气息与风格。它也启发了更多的思想自由和创造力，

除此之外还有何不同呢？我们今年预备了更多的Village，比赛，活动，艺术和音乐项目！花了大半年的时间，我们很兴奋得有些迫不及待了！我们的DEF CON Groups（小组）也自去年的5 个团队增长至今年的11支。

今年大会的主题是 科技点燃未来。这是个积极的愿景：倘若科技能改善我们，教育及医治使我们变得更好，而不是关注着目前火热的跟踪及销售。拥着这情怀，我希望能创立一个由安全极客组成的社群面对当下的问题与未来的挑战。我们得相互合作，因为互联网问题是全球性的问题，我们都将是未来的急救员。

我曾说过，在DEF CON，我们不在乎您的样貌，财富，粉丝数量，甚至音乐品味。我们最在乎的是您的思维。在这，我们鼓励您自由探索，对演讲者勇于发问，尝试改变自己的观事的角度。

又一则喜讯 - forum.defcon.org已从新被启动。这是一个计划所有DEF CON相关事项的地方。您可随便游览、谈论技术、交朋友、创建自己的博客或分享最新项目的照片。当您能阅读这篇文章的时候，Android手机应用应该已经和iOS同步了。我将在那里发布本身大会的经历故事与照片。

多谢！

The Dark Tangent 启

DEF CON 神州1.0 欢迎您

10000公里，从拉斯维加斯到北京
15小时时差，从清晨到深夜
1000天，从DEF CON到DEF CON CHINA beta；
1年，从beta到1.0！

DEF CON CHINA 1.0，我们如约而至。

在过去一年中，一如既往，各种网络安全、隐私保护的信息纷至沓来。当下，AI在构建全新的时代，防御体系有了新的强大能力，但其自身的安全性亦变得前所未有的复杂与重要，甚至远远超乎传统安全的边界与范畴。

未来学家凯文·凯利在其《新经济新规则》一书中提出，通过未知的峡谷只有一种可靠的策略，那就是结伴而行。一个企业、社区、技术及经济形态在面临未来不确定性时，应当建立合作伙伴关系，寻找共同目标，通过建立网络来分散风险。这将为通过峡谷带来希望。

在筹备本届1.0的过程中，我反复接触到一个词：复古未来主义（Retro-Futurism），这个词汇的微妙之处，可类比英语语法中的"过去将来时"，其背景可追溯至上世纪60-80年代。

历史是合力的产物。每个时代，都同时被促进开放、合作的力，和封闭、对抗的力拉扯着。短期内总是下坠比上升容易，但长期都是合作的力量取胜。复古未来主义萌生之际，封闭、分裂在全球范围内短暂地占了上风，但与此同时，以原子能、计算机、航天技术为代表的全新世界也如火如荼，全球进入蓬勃的时代，尼克松在中国迈出他的一小步，阿姆斯特朗在月球上迈出他的一小步，但都是人类的一大步！

当下的世界局势更加多元。历史不会真的重复，但总是押韵。在我们微薄之力所能及的范围内，极客这个圈层是能够让人类达成默契结伴而行的机制之一——遵循共同的精神准则，打破边界，形成一个覆盖全球的社区。迈出这一步的可能就是DEF CON CHINA。

结伴而行，没有什么可以阻止人类前进的脚步！



我希望，借助DEF CON CHINA，中国与全世界的极客们可以延续人类的探索与合作精神，可以重拾人类探索"太空时代"的自信与勇气，用科技让未来更美好。

这是我们每一位极客对世界的Technology's Promise。

10,000 kilometers, from Las Vegas to Beijing.
15 hours time difference, from early morning to late night.
1000 days, from DEF CON to DEF CON CHINA beta.
1 year, from beta to 1.0!

DEF CON CHINA 1.0, we are here as promised.

In the past year of 2018, a variety of network security, privacy protection information keep pouring in. At present, AI is building a new era, the defense system has been endowed with new powerful capabilities, but AI its own security has become unprecedented complex and important, even far beyond the boundaries and scope of traditional network security.

In book "New Rules for the New Economy", the futurist Kevin Kelly mentioned that there is only one sure strategy for navigating an unknown canyon, and that is to travel in pairs. When a corparte, community, technology, or economy facing future uncertainties, to build partnerships, seek common goals, establish network to spread the risk would be a wise choice. Only that could bring the hope of getting through the canyon.

In the preparation process of DEF CON CHINA 1.0, I have been repeatedly exposed to a word: Retro-Futurism, which resembles the "Past future tense" of English grammar in its subtlety. The background of "Retro-Futurism" could be traced back to the 1960s and 1980s.

History is the product of forces. Each era is simultaneously pulled by forces of promoting openness and cooperation, and by forces of promoting isolation and confrontation. In the short run, it is always easier to fall than to rise, but in the long run it is the power of cooperation that wins. At the time of germination of Retro-Futurism, closure and division gained the upper hand in the world for a short time, but at the same time, the new world represented by atomic energy, computer and space technology was in full swing, and the world entered a flourishing era. Nixon took a small step in China, Armstrong took a small step on the moon, but they were all giant leaps for mankind!

The world today is more diverse. History does not repeat itself exactly, but it always rhymes. Within our meager strength, hackers would be one of the community who can call the humanity to walk in company in tacit understanding - following a common spiritual code, breaking boundaries, and forming a global community. One possible place to take this step may be DEF CON CHINA.

Navigate together, nothing can stop the pace of human progress!

In virtue of DEF CON CHINA, I hope hackers in China and around the world could continue the exploration and cooperation spirit of human, regain the confidence and courage to explore like the "Space Age", and make the future better with science and technology.

This is the Technology's Promise to the world made by every hacker!

- Ma Jie

THE BADGE

This year's badge was created specifically to bring the DEF CON China community together. As you'll soon discover, the badge is your "passport" while you experience DEF CON. When you complete certain tasks around the event, your roots will start to grow. Complete all the tasks and bring your tree to life! The badge is fully open source and hackable, so you can continue to explore, experiment, and create with it after DEF CON is over.

It has been an honor and challenge to create this badge for you and I'm excited to see it in action. So, embrace your hacker spirit, enjoy all that DEF CON has to offer, and have fun with the badge along the way!

今年的徽章是专门为让DEF CON中国社群聚集在一起而设计的。您很快就会发现，当您体验DEF CON时，徽章将成为您的"护照"。完成了活动的某些任务后，您的"树"就会开始生长。完成所有的任务会让您的树焕发生机！这个徽章是完全用开放源代码而可破解的，因此您还可以在大会结束后继续探索、试验和创建它。

为您创造了这个徽章，既是我的荣誉，也是难度不浅的挑战。我很高兴看到它的实际应用。所以，请您拥抱您的极客精神，享受DEF CON所提供的一切，并且也享受这旅途上徽章带给您的乐趣吧！



QUESTIONS?

PLEASE SEE OUR GOONS AT THE REGISTRATION DESK OR ASK ANYONE IN A STAFF SHIRT FOR HELP

WI-FI

SSID: DEF CON CHINA

USERNAME: DEF CON

PASSWORD: DEF CON CHINA

CODE OF CONDUCT

DEF CON provides a forum for open discussion between participants, where radical viewpoints are welcome and a high degree of skepticism is expected. However, insulting or harassing other participants is unacceptable. We want DEF CON to be a safe and productive environment for everyone. It's not about what you look like but what's in your mind and how you present yourself that counts at DEF CON.

We do not condone harassment against any participant, for any reason. Harassment includes deliberate intimidation and targeting individuals in a manner that makes them feel uncomfortable, unwelcome, or afraid.

Participants asked to stop any harassing behavior are expected to comply immediately. We reserve the right to respond to harassment in the manner we deem appropriate, including but not limited to expulsion without refund and referral to the relevant authorities.

This Code of Conduct applies to everyone participating at DEF CON - from attendees and exhibitors to speakers, press, volunteers, and Goons.

Anyone can report harassment. If you are being harassed, notice that someone else is being harassed, or have any other concerns, you can contact a Goon, go to the registration desk, or info booth.

Conference staff will be happy to help participants contact hotel security, local law enforcement, or otherwise assist those experiencing harassment to feel safe for the duration of DEF CON.

Remember: The CON is what you make of it, and as a community we can create a great experience for everyone.

- The Dark Tangent

DEF CON为参与者提供了一个公开讨论的论坛，在这里，变革性的观点是受欢迎的，并且期望参与者敢于提出质疑。然而，侮辱或骚扰其他参与者是不可接受的。我们想让DEF CON成为一个安全、高效的环境。这不是关于你的外表，你的思想和你如何在DEF CON上展示你自己才是最重要的。

不论任何原因，我们不能容忍对任何参与者的骚扰。骚扰包括蓄意恐吓和以一种使他们感到不舒服、不受欢迎或害怕的方式攻击个人。

参与者被要求停止任何骚扰行为，应立即服从。我们保留以我们认为适当的方式对骚扰作出回应的权利，包括但不限于驱逐而不退款和转介有关当局。

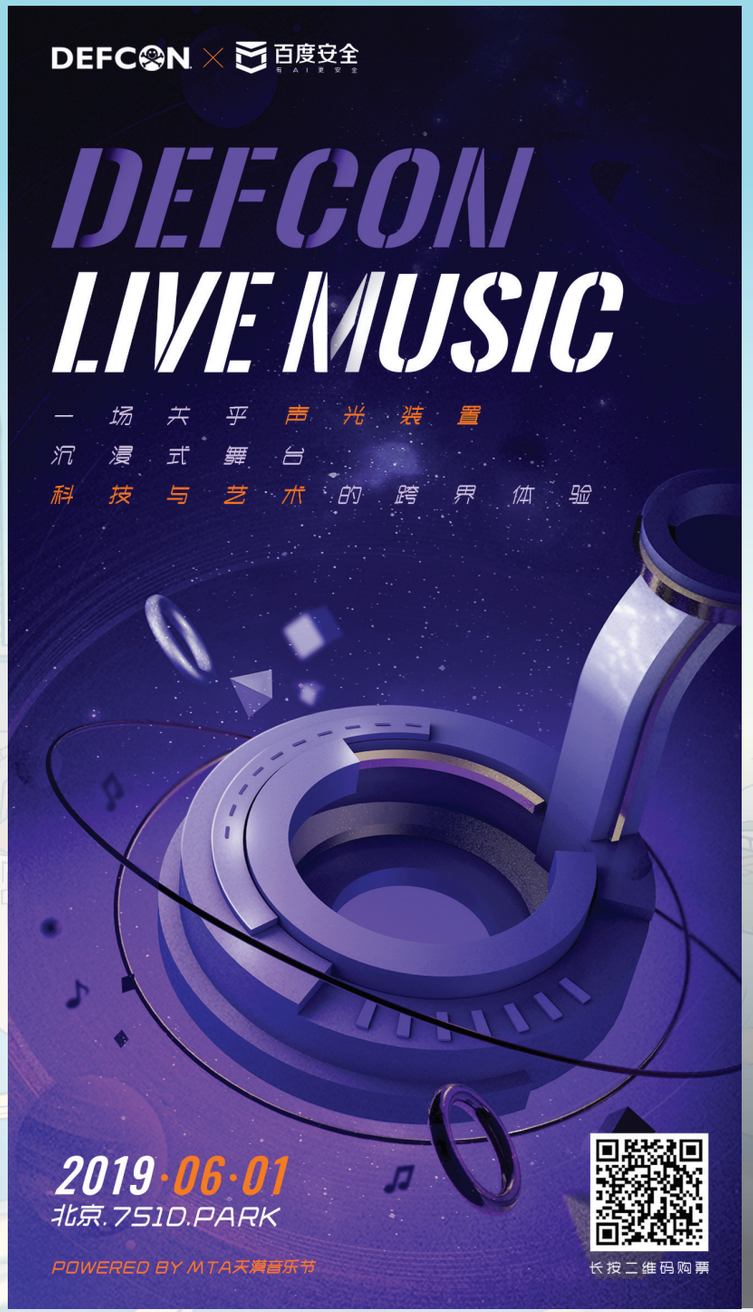
这一行为准则适用于参加DEF CON大会的所有人——从参会者和参展商到演讲者、媒体、志愿者和安保人员。

任何人都可以举报骚扰。假如你遭到骚扰，注意到其他人被骚扰，或有其他问题，可以去登记台或者信息亭联系安保人员。

会议工作人员将乐于帮助与会者联系酒店安保人员、当地执法部门，或帮助那些遭受骚扰的人在DEF CON期间感到安全。

请谨记：此次大会为诸位而举办，作为一个共同体，我们可以为每个人创造一次非凡的经历。

-Jeff Moss （又名The Dark Tangent）



DEF CON LIVE MUSIC简介

主题语：一场关乎声光装置、沉浸式舞台、科技与艺术的跨界体验

时间：6.1晚上630—9点

地点：北京.751D.PARK

音乐会流程：时长2.5小时，五个部分

PART ONE：DJ Abby
PART TWO: 极客音乐（暂定百度音乐社团成员）
PART THREE：电子音乐（777：中国电子音乐的先驱乐队超级市场的主创）
PART FOUR：嘻哈音乐（RAPPER Nineone）
PART FIVE：多媒体艺术舞台(wanwho!)

演出音乐人、艺术家简介:

DJ ABBY是朝鲜族最美90后的女DJ，擅长于TRAP, HipHop, EDM多种音乐风格。

百度音乐社团乐队：截至目前，首批阵容已诞生—百度音乐社团，分别来自百度、爱奇艺、网易的五位极客音乐人，职场上他们的身份是研发工程师、产品经理、市场营销，研究领域涉及AI、智能语音、搜索、视频等，他们的另一身份，则是常年出没于各大音乐节镁光灯中央、拥有丰富的摇滚乐、交响乐、民乐、合唱团管理经验的音乐人，擅长音乐风格遍及摇滚、金属、朋克、迷幻、流行.....在百度音乐社团社长朱胜贤的率领下，DEF CON LIVE MUSIC 的开场曲目将由他们演绎，点燃全场第一乐章。

777: 中国第一支真正意义上的电子乐队超级市场（supermarket）主创。

Nineone：中国人气rapper，单曲《Puma》播放量千万，微博粉丝10

Wanwho!: Wan Who? —— 《流动的命运》流动的命运2.0" (Floating Destiny) 是基于《易经》为灵感创作的交互艺术装置，并伴随现场表演。

DEF CON LIVE MUSIC

Theme: A crossover experience involving sound and light installation, immersive stage, technology and art.

When: June 1st 2019, 6:30 - 9PM

Where: 751 D-PARK Beijing

Program: Approximately 2.5 hours, 5 parts

PART ONE: DJ Abby
PART TWO: Geek Music (Baidu Music Society Band)
PART THREE: Electronic Music (777: China's premier and pioneering electronic music artist)
PART FOUR: Rap (RAPPER Nineone)
PART FIVE: Multimedia art show (Wan Who!)

Artist Bios:

DJ Abby: The prettiest female DJ in the KPOP / Rap / EDM arena.

Baidu Music Society Band is comprised of five geek musicians from Baidu, iQiyi and NetEase. At work, they are R & D engineers, product managers and marketing personnel. Their research fields include AI, intelligent voice, search, video etc. Their alter egos are musicians who have been in the limelight of major music festivals or who have rich experience in various music genres. Under the leadership of Zhu Shengxian, president of Baidu Music Association, they will open for DEF CON LIVE MUSIC.

777: Founder of China's first proper electronic band "supermarket".

NineOne: Popular Chinese rapper, whose single "Puma" launched her into fame with over 100,000 fans on Weibo.

Wan Who?: (Floating Destiny) Floating Destiny 2.0 is an interactive art installation inspired by the I Ching and accompanied by live performance.

由百度安全主办的百度网络安全技术对抗赛（BCTF）将在DEF CON CHINA 1.0期间举行，BCTF 2019正式成为DEF CON CTF预选赛。BCTF线下总决赛的现场邀请到了来自全球十余个国家的12支国际顶尖战队同场竞技。同时，还集结了通过BCTF-RHG人工智能分站赛选拔出的11支AI战队，结合百度安全OPENRASP、KARMA漏洞热修复等开源技术，考察战队的自动化攻防能力。

总决赛冠军战队将直通DEF CON CTF FINALS，TOP3 战队将获得现金奖励，奖励金额等你揭晓。

BAIDU CTF, HOSTED BY BAIDU SECURITY, WILL BE HELD DURING DEF CON CHINA 1.0 AND BCTF 2019 WILL OFFICIALLY BECOME THE PRE-QUALIFIER OF DEF CON CTF. 12 TOP-LEVEL INTERNATIONAL TEAMS WILL BE INVITED TO COMPETE IN THE BCTF FINALS. AT THE SAME TIME, 11 AI TEAMS SELECTED THROUGH BCTF-RHG ARTIFICIAL INTELLIGENCE SUB-STATION COMPETITIONS ARE ASSEMBLED, WHICH CAN USE OPENRASP, KARMA VULNERABILITY HOTFIX AND OTHER OPEN SOURCE TECHNOLOGIES FROM BAIDU SECURITY IN THE AUTOMATIC ATTACK AND DEFENSE COMPETITIONS.

THE FINALS CHAMPION TEAM WILL GO STRAIGHT TO ATTEND DEF CON CTF FINALS, AND THE TOP THREE TEAM WILL RECEIVE CASH AWARDS. CURIOUS ABOUT THE AMOUNT? AHA, WAITING FOR YOU TO EXPLORE!



CONTESTS & EVENTS

SCHEMAVERSE

The Schemaverse [skee-muh vurs] is a space battleground that lives inside a PostgreSQL database. Mine the hell out of resources and build up your fleet of ships, all while trying to protect your home planet. Once you're ready, head out and conquer the map from other DEF CON rivals.

This unique game gives you direct access to the database that governs the rules. Write SQL queries directly by connecting with any supported PostgreSQL client or use your favourite language to write AI that plays on your behalf. This is DEF CON of course so start working on your SQL Injections - anything goes!

Schemaverse [skee-muh vurs] 是一个居住在PostgreSQL数据库中的空间战场。开采地狱资源，建立你的舰队，同时努力保护你的星球。一旦你准备好了，就从其他DEF CON竞争对手那里出发，征服地图。

通过这款独特的游戏，您可以直接访问管理规则的数据库。通过连接任何受支持的PostgreSQL客户端直接编写SQL查询，或者使用您最喜欢的语言编写代表您发挥作用的AI。当然，这是DEF CON，所以开始做SQL注入-随心所欲吧！

SCAVENGER HUNT
寻宝游戏

The DEF CON Scavenger Hunt, though untraditional, has become the spirit of DEF CON. This contest is known for encouraging the hacker mentality and bringing it into uncommon and usually funny challenges. For newer hackers, non-technical hackers, or people looking to find a unique way to interact with the conference, we bring you the longest running contest at DEF CON! For over twenty years the original DEF CON Scavenger Hunt has challenged hackers to think outside of the box. Teams of one to five players compete Friday morning into Sunday, accumulating as many items and completing as many tasks as possible from the list. Will you be the next to stand among the legendary scavengers?

DEF CON寻宝游戏虽然并非传统，但已经融入了DEF CON的精神。这场比赛激发了极客探索欲，因起特别的趣味而长久闻名。对于新极客，非技术极客，或寻找一个独特的方式与会议互动的人，我们带给您在DEF CON活动中保留时间最长的比赛!二十多年来，它一直在挑战极客的思维定式。每队可有一至五名成员，从周五上午到周日进行比赛，尽可能多的收集项目，完成任务。谁会成为下一个寻宝游戏中的传奇赢家呢?

DUNK TANK
水桶惩罚

For the trivial price of a donation to charity you could take a turn trying to dunk various DEF CON luminaries perched over a pool of freezing water. Some geek, maybe even you, with a couple of softballs has a chance at glory.

作为我们活动的一个公益项目，捐款给慈善基金，你就可以获得让DEF CON几个大佬醍醐灌顶的机会， 预设好惩罚绳，桶灌好水，拔下或按下销子，其中有一个销子带动机关，水桶转动水倒下。（游戏规则：大佬坐在水桶下面，完成游戏环境，否则就要被冰水弄湿。

THE D(STRUCTION)20 CTF!



Are you tired of CTFs where contestants' computers aren't in danger of being smashed with a sledgehammer by a person wearing a hot dog costume? Do normal CTFs that don't decide the fate of their competitors at random with a novelty oversized 20-sided die bore you? Then come see the only CTF where the stack isn't the only thing being smashed: The d(struction)20 CTF!

Part CTF, part lemon race, part game show, part demolition derby, the D(struction)20 CTF is a contest to build an affordable, low-cost, usable, and powerful hacking platform, and compete with it! Periodically during the competition, a random contestant from the leaderboard will be chosen to roll the d20 of Destruction to decide what will happen to their rig. If they're very lucky, they roll a natural 20 and no damage will be inflicted! Otherwise, the d20 of Destruction will decide what type of damage will be done to their rig. If the rig survives their chosen fate, the contestant may continue playing, but either way, rolling the d20 of Destruction results in a big point bonus that may make the difference between winning and losing, even if the rig is destroyed in the process!

https://twitter.com/d20ctf

没有穿着热狗套装，拿大锤砸你的CTF比赛。是不是毫无危险系数？对普通的CTF感到无聊？普通的CTF可不会让一个20面的超大骰子来随机决定选手的命运。那就来看看我们的CTF：d(struction)20吧！在这儿，栈可不是唯一要被击碎的东西！

一部分CTF，一部分勒芒拉力赛，一部分游戏秀，还有一部分撞车比赛；这就是我们d(structhe ion)20 CTF。我们为极客们构建了一个参赛者可承担，低成本且实用性强的比赛平台，一起来挑战吧！

比赛期间，会从排行榜中随机抽取一名选手，滚动d20 of Destruction的骰子，滚到什么就决定了他们的装备会发生什么（可能是被破坏摧毁）。如果他们走运，掷出了一个20，他们队就幸免于难。否则d20 of Destruction会决定他们的设备会受到怎样的破坏。如果他们从这场“命中注定”中幸存下来，参赛者就可以继续比赛；但无论如何，摇到大额奖励点数是会影响到你的输赢的——即使你的设备已经被摧毁了，也有可能获胜！

更多详情，请访https://twitter.com/d20ctf

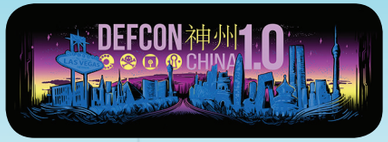
REPLICA OF HALL OF SUPREME HARMONY



The Hall of Supreme Harmony was built in 1416 and completed in 1420. It showcases the exquisite skills and cooperation amongst ancient craftsmen which is difficult to achieve today. This is due to the usage of tenon-and-mortise technology. Because of its complexity, people seldom come into contact with it in today's world. At DEF CON CHINA 1,0, We plan to use tens of thousands of Tang Locks to reproduce the Hall of Supreme Harmony on a reduced scale.

太和殿建于1416年于1420年竣工，距今600年历史，它体现了古代工匠精妙绝伦的手艺与合作能力，如此高水平的配合放在今天也很难企及。这全部得益于榫卯科技，由于榫卯技艺的复杂与习钻很难被人们所接触。在DEF CON 神州 1.0，我们计划用数万块唐块，等比例缩小，复现太和殿。

DEF CON CHINA LIVE ART STORY
现场壁画



For the past decade, the curious and playful work of DEF CON resident artist Mar Williams has been visible all over our convention. Mar's work is a perfect fit with DEF CON's vibe and has become a big part of our visual identity.



For our guests at DEF CON China 1.0, Mar will be creating a mural live onsite. Once the mural is finished, it will be broken down to 18 equal pieces and distributed to guests at the conference. Join us at 751 D Park in Beijing May 31 - June 2 for a chance to bring home some one-of-kind DEF CON art!



在过去的十年里，DEF CON常驻艺术家Mar Williams充满好奇和趣味的作品在我们的大会上随处可见。Mar的作品与DEF CON的氛围完美契合，已经成为我们视觉身份的重要组成部分。

在DEF CON China 1.0大会上，Mar将为我们的嘉宾现场制作一幅壁画。一旦壁画完成，它将被分解成18片个相等的画作，并在会议上分发给参会者。5月31日- 6月2日在北京751D PARK 参加我们的大会，并有机会带回家独一无二的DEF CON艺术!

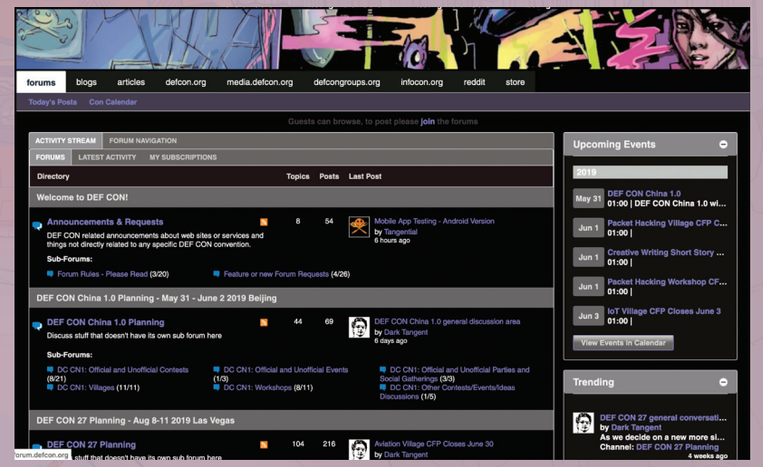


FORUM.DEFCON.ORG

No matter what part of the DEF CON universe you're interested in, you should start at the DEF CON Forums. With a forum account you can reach out to a local DEF CON group, help us plan future events or even chat with other hackers. DEF CON's heart is its community, and the community meets at the DEF CON Forums. Join us!

DEF CON FORUMS

HTTPS://PLAY.GOOGLE.COM/STORE/APPS/DEVELOPER?ID=DEF+CON+COMMUNICATIONS,+INC.



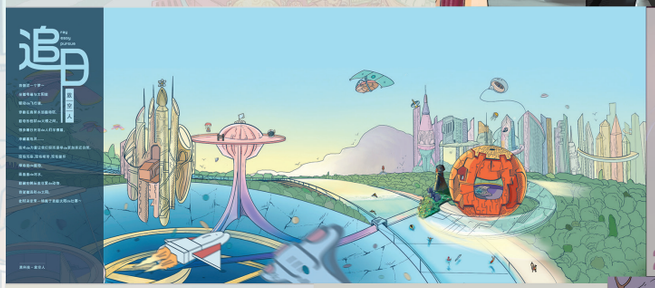
ARTWORK CONTEST WINNERS!

DEF CON is well known for its technical side, but there is a vibrant artistic side as well. Each year, DEF CON invites live musicians and DJs from within the community to perform, and we hold contests for short stories and art to help us bring the year's theme to life.

We expanded the art contest to DEF CON China, and were delighted to find that every entry was amazing! DEF CON thanks everyone who shared their work with us. Extra special congratulations to the winners:



1ST PLACE: "SEARCH" BY ZHAO MENGXI



2ND PLACE: "PURSUE THE SUN" BY LI YUXUAN



3RD PLACE: "CHING MING FESTIVAL RAIN" BY ARVIN DONG

DEMO LABS

JTAGULATOR

Joe Grand (Kingpin)

JTAGulator is an open source hardware hacking tool that assists in identifying on-chip debug interfaces from test points, vias, component pads, or connectors on a circuit board.

Additional information:

http://www.jtagulator.com

http://www.grandideastudio.com/portfolio/jtagulator

On-chip debug (OCD) interfaces can provide chip-level control of a target device and are a primary vector used by engineers, researchers, and hackers to extract program code or data, modify memory contents, or affect device operation on-the-fly. Depending on the complexity of the target device, manually locating available OCD connections can be a difficult and time consuming task, sometimes requiring physical destruction or modification of the device.

JTAGulator is an open source hardware hacking tool that assists in identifying on-chip debug interfaces from test points, vias, component pads, or connectors on a circuit board. It currently supports the detection of JTAG and asynchronous serial/UART interfaces. The tool can save a significant amount of time during reverse engineering, particularly for those who don't have the resources required for traditional hardware reverse engineering processes, and bridges the gap between gaining physical access to circuitry and exploiting it.

JTAGulator continues to be updated with new features and functionality. The project welcomes feedback/contributions/pull requests from the community. JTAGulator hardware and core firmware is distributed under a Creative Commons Attribution-3.0 United States license (http://creativecommons.org/licenses/by/3.0/us/). Supporting Files, Code, etc: Complete design details, documentation, presentations/videos, etc. available at the project page above

JTAGulator是一个开源硬件极客工具，它可以帮助从测试点、过孔、组件板或电路板上的连接器识别芯片上的调试接口。

片上调试(OCD)接口可以提供目标设备的芯片级控制，是工程师、研究人员和极客用来提取程序代码或数据、修改内存内容或实时影响设备操作的主要载体。根据目标设备的复杂性，手动定位可用的OCD连接可能是一项困难且耗时的任务，有时需要对设备进行物理销毁或修改。

JTAGulator是一个开源硬件极客工具，它可以帮助从测试点、过孔、组件板或电路板上的连接器识别芯片上的调试接口。它目前支持JTAG和异步串行/UART接口的检测。特别是对于那些没有传统硬件逆向工程过程所需资源的人来说，该工具可以在逆向工程过程中节省大量时间，并填补物理访问电路和利用电路之间的空白。

JTAGulator不断更新特性和功能。该项目欢迎您的反馈/贡献/参与。

JTAGulator硬件和核心固件是基于知识共享署名3.0美国许可协议发布的

(http://creativecommons.org/licenses/by/3.0/us/)，支持文件、代码等。可从以上链接页面获得完整的设计细节、文档、演示文稿/视频等。

目标人群：硬件、进攻、防守。硬件极客攻击硬件设备的入口。工程师们希望通过使用该工具来测试设备上的开放接口，从而防御性地识别/分类敞口。

Target Audience: Hardware, Offense, Defense

Hardware hackers looking offensively for an entry point in which to compromise a hardware device. Engineers looking to defensively identify/classify their exposure by using the tool to test for open interfaces on their devices.

Joe Grand (@joegrand), also known as Kingpin, is a computer engineer, hardware hacker, DEF CON badge designer, teacher, advisor, runner, daddy, honorary doctor, TV host, member of legendary hacker group L0pht Heavy Industries, and the proprietor of Grand Idea Studio (grandideastudio.com). He has been creating, exploring, and manipulating electronic devices since the 1980s.

Joe Grand (@joegrand)，又名Kingpin，是一名计算机工程师、硬件极客、DEF CON徽章设计师、教师、顾问、跑步者、爸爸、名誉医生、电视主持人、传奇极客组织L0pht Heavy Industries的成员、Grand Idea Studio (granddeastudio.com)的所有者。自20世纪80年代以来，他一直在创造、探索和操纵电子设备。

OSFOOLER

Jaime Sánchez aka segofensiva

Traditional methods to defeat OS Fingerprinting in Linux were written as kernel modules, or at least, as patches to the Linux kernel, like Honeyd, IP Personality, the Stealth Patch, Fingerprint ****er, IPlog... The reason is that if the aim is to change Linux TCP/IP stack behavior, and if we want to achieve it, we need to do it in the kernel layer. Most of these tools are old, doesn't work with actual kernels of can affect tcp/ip stack performance.

OSfooler was presented at Blackhat Arsenal 2013. It was built on NFQUEUE, an iptables/ip6tables target which delegate the decision on packets to a userspace. It transparently intercepted all traffic that your box was sending in order to camouflage and modify in real time the flags in TCP/IP packets that discover your system.

OSfooler-NG has been complete rewriten from the ground up, being highly portable, more efficient and combining all known techniques to detect and defeat at the same time:

- Active remote OS fingerprinting: like Nmap or Xprobe
- Passive remote OS fingeprinting: like p0f or pfsense
- Commercial engines like Sourcefire's FireSiGHT OS fingerprinting

Some additional features are:

- No need for kernel modification or patches
- Simple user interface and several logging features
- Transparent for users, internal process and services
- Detecting and defeating mode: active, passive & combined
- Will emulate any OS
- Capable of handling updated nmap and p0f fingerprint database
- Undetectable for the attacker

Target Audience: Defense and Mobile

建议使用商业工具来保护您的网络，但有必要进一步确保系统的安全性。使用该项技术，您可以执行该步骤，以保护您的服务器免受第一阶段的所有指纹识别攻击。这是通过拦截您的机器正在发送的所有流量来实现的，以便伪装和实时修改发现您的系统的TCP/IP包中的标志。

这项工具擅长检测和击败：

主动远程操作系统指纹识别：如Nmap或Xprobe

被动远程操作系统指纹识别：如p0f或pfsense

商业引擎，如Sourcefire的FireSiGHT OS指纹识别

其它特性：

无需内核修改或补丁

具有高度的可移植性

- 将模拟任何操作系统
- 能够处理Nmap和p0f指纹数据库（beta阶段）
- 对用户透明
- 攻击者无法检测到
- 适用于您的Linux笔记本电脑，服务器和移动设备

有关该工具的更多详情和见解，请关注下方DEF CON 21的演示文稿。

https://www.defcon.org/images/defcon-21/dc-21-presentations/Sanchez/DEFCON-21-Sanchez-Building-an-Android-IDS-Network-level-Updated.pdf

DEMO LABS

该工具将在开放源码许可下发布。

目标人群:防守和移动

Jaime Sánchez (aka @segofensiva) has worked for over 20 years as a specialist advisor for large national and international companies, focusing on different aspects of security such as consulting, auditing, training, and ethical hacking techniques. He holds a Computer Engineering degree and an Executive MBA. In addition, he holds several certifications, like CISA, CISM, CISSP, just to name a few, and a NATO SECRET security clearance, as a result of his role as advisory of many law enforcement organizations, banks and large companies in Europe and Spain.

He has spoken in renowned security conferences nationally and internationally, as in RootedCON, Nuit du Hack, Black Hat, DEF CON, DerbyCON, NocOnName, Deepsec, Shmoocon or Cyber Defence Symposium, among others. As a result of his researches, he has notified security findings and vulnerabilities to top companies and vendors, like Banco Popular, WhatsApp, Snapchat, Microsoft, Apple etc.

He is a frequent contributor on TV (TVE, Cuatro, LaSexta, Telecinco), press (El Pais, El Mundo, LA Times, NBC News) and radio programs, and writes a blog called 'SeguridadOfensiva'

Jaime Sanchez(又名@segofensiva)从事大型国内和国际公司的专家顾问20多年，专注于安全的各个方面，如咨询、审计、培训和道德黑客技术。他拥有计算机工程学位和行政工商管理硕士学位。此外，由于他为欧洲和西班牙的许多执法机构、银行和大公司提供咨询服务，他还持有多项证书，如CISA、CISM、CISSP以及NATO SECRET安全许可等。

Twitter: @segofensiva

Website: https://www.seguridadofensiva.com

Tools: https://github.com/segofensiva

VOIPSHARK: OPEN SOURCE VOIP ANALYSIS PLATFORM

VOIPSHARK: 开源VOIP分析平台是与非

Nishant Sharma
R&D Manager, Pentester Academy

Jeswin Mathai
Security Researcher, Pentester Academy

Ashish Bhangale
Senior Security Researcher, Pentester Academy

Leveraging the packet switched network for making phone calls or VoIP has come a long way now. Today, it has already replaced conventional circuit switching based telephones from the large organizations and now moving to capture the non-commercial users. In this talk, we will focus on the traffic analysis based security analysis of SIP and RTP protocols which are one of the most popular protocols for VoIP. These protocols are already gaining new adopters on high rate and also replacing older protocols like H323.

We will discuss VoIPShark open source VoIP Analysis Platform which will allow people to analyze live or stored VoIP traffic, easily decrypt encrypted SRTP stream, perform macro analysis, generate summary specific to VoIP traffic/nodes and export calls/SMS/DTMF in popular user friendly file formats. We will also be releasing VoIPShark collection of Wireshark plugins written in Lua under GPL. VoIPShark is plug-n-play, easy to modify/extend and platform independent in nature. We will also discuss the currently available open source tools for SRTP decryption, their shortcomings and how VoIPShark address those.

利用分组交换网络进行电话呼叫或VoIP已经取得了很大的进展。如今，它已经取代了传统基于电路交换的电话。从大型机构，至现在正着手吸引非商业用户都用它。在本演讲中，我们将重点放在基于流量分析的SIP协议和RTP协议的安全性分析，这是目前最流行的VoIP协议之一。这些协议已经以很高的速率获得了新的采用者，并取代了像H323这样的旧协议。我们将讨论VoIPShark开源VoIP的分析平台，它将允许人们分析实时或存储的VoIP流量，轻松解密加密的SRTP流，执行宏分析，生成特定于VoIP流量/节点的摘要，并以流行的文件格式导出call /SMS/DTMF。我们还将发布VoIPShark Wireshark插件集合，这些插件是在GPL下用Lua编写的。VoIPShark是即插即用的，易于修改/扩展，本质上不限于任何平台。我们还将讨论当前可用于SRTP解密的开源工具、它们的缺点及VoIPShark如何解决这些问题。

Nishant Sharma is a R&D Manager at Pentester Academy and Attack Defense. He is also the Architect at Hacker Arsenal where he leads the development of multiple gadgets for WiFi pentesting such as WiMonitor, WiNX and WiMini. He also handles technical content creation and moderation for Pentester Academy TV. He has 6+ years of experience in information security field including 4+ years in WiFi security research and development. He has presented/published his work at Blackhat USA/Asia, Wireless Village, IoT village and Demo labs (DEF CON). Prior to joining Pentester Academy, he worked as a firmware developer at Mojo Networks where he contributed in developing new features for the enterprise-grade WiFi APs and maintaining the state of art WiFi Intrusion Prevention System (WIPS). He has a Master's degree in Information Security from IIIT Delhi. He has also published peer-reviewed academic research on HMAC security. His areas of interest include WiFi and IoT security, AD security, Forensics and Cryptography.

LinkedIn: https://www.linkedin.com/in/wifisecguy/

Twitter: @wifisecguy

Facebook: https://www.facebook.com/wifisecguy

Ashish Bhangale is a Senior Security Researcher at Pentester Academy and Attack Defense. He has 6+ years of experience in Network and Web Application Security. He has also worked with the state law enforcement agencies in the capacity of a Digital Forensics Investigator and was instrumental in solving IT fraud/crime cases. He was responsible for developing and testing the Chigula (WiFi Forensics Framework) and Chellam (First pure WiFi Firewall) frameworks. He has also created and managed multiple projects like Vulnerable Web Application OSes, Vulnerable Router Project and Damn Vulnerable Wordpress. He has presented/published his work at Blackhat, Wireless Village, IoT village and Demo labs (DEF CON). His areas of interest include Forensics, WiFi and AD security.

Jeswin Mathai is a Researcher at Pentester Academy and Attack Defense. He has published his work at Blackhat Arsenal and Demo labs (DEF CON). He has a Bachelor's degree from IIIT Bhubaneswar. He was the team lead at InfoSec Society IIIT Bhubaneswar in association with CDAC and ISEA, which performed security auditing of government portals, conducted awareness workshops for government institutions. He was also the part of team Pied Piper who won Smart India Hackathon 2017, a national level competition organized by GoI. His area of interest includes Malware Analysis and Reverse Engineering, Cryptography, WiFi security and Web Application Security.

LinkedIn: https://www.linkedin.com/in/jeswinmathai/

Twitter: @jeswinMathai

Facebook: https://www.facebook.com/jeswinMathai

Nishant Sharma是Pentester Academy and Attack Defense的研发经理。他还是Hacker Arsenal的设计师，领导开发Wimonitor、Winx和Wimini等Wifi Pentesting的多个小工具。他还负责Pentester Academy TV的技术内容创建和调整。他在信息安全领域拥有6年以上的经验，包括4年以上的WiFi安全研发经验。他在Blackhat美国/亚洲、无线village、IoT village和DEF CON的演示实验室发表过。在加入Pentester Academy之前，他曾在Mojo Networks担任固件开发员，在那里他为企业级WiFi AP开发了新功能，并维护了最先进的WiFi入侵预防系统（WIPS）。他拥有印度国际信息技术学院德里信息安全硕士学位。他还曾在同行评审的学术研究发表关于HMAC安全。他的兴趣包括WiFi和物联网安全、AD安全、取证和密码技术。

LinkedIn: https://www.linkedin.com/in/wifisecguy

推特：https://twitter.com/wifisecguy

脸谱网：https://www.facebook.com/wifisecguy

Ashish Bhangale是Pentester Academy和Attack Defense的高级安全研究员。他在网络和Web应用程序安全方面有6年以上的经验。他还曾以数字取证调查员的身份与国家执法机构合作，并帮助解决IT欺诈/犯罪案件。他负责开发和测试Chigula（WiFi取证框架）和Chellam（第一个纯WiFi防火墙）框架。他还创建和管理了多个项目，如易受攻击的Web应用程序操作系统、易受攻击的路由器项目和特易受攻击的WordPress。他也曾在Blackhat、无线village、IoT village和DEF CON的演示实验室发表过。他的兴趣包括取证、WiFi和AD安全。

Jeswin Mathai是Pentester Academy和Attack Defense的研究员。他在Blackhat Arsenal和DEF CON的演示实验室发表过。他拥有IIIT Bhubaneswar的学士学位。他是InfoSec Society IIIT Bhubaneswar的团队负责人，与CDAC和ISEA合作，对政府门户网站进行安全审计，为政府机构举办意识研讨会。他也是Pied Piper团队的一员，该团队赢得了由GoI组织的全国水平的"智能印度黑客松2017"。他感兴趣的领域包括恶意软件分析和逆向工程、密码学、WiFi安全和Web应用程序安全。

LinkedIn: https://www.linkedin.com/in/jeswinmathai/

推特: https://twitter.com/jeswinMathai

脸谱网: https://www.facebook.com/jeswinMathai

FROM ZERO OVERHEAD TO MANY VULNERABILITIES: ESCALATING FUZZING EFFECTIVENESS AND EFFICIENCY WITH INTEL PT

通过INTEL PT实现模糊测试提速

Dr. Xinyu Xing
Assistant Professor, Penn State University, Research Scientist, JD.com

Yaohui Chen
PhD student, Northeastern University's College of Computer and Information Science

Dr. Jun Xu
Assistant Professor, Stevens Institute of Technology

Dr.Jimmy Su
Head of security center, JD.com Silicon Valley

In practice, AFL typically exhibits high-performance overhead, particularly when stress-testing target software without access to their source code. Given a commercial off-the-shelf (COTS) binary, AFL needs to perform a black box on-the-fly instrumentation through a customized version of QEMU running in "user space emulation" mode. Despite the best effort of systematic optimization, however, QEMU still incurs substantial overhead to binary-only fuzzing. According to the AFL white paper, the overhead of QEMU based AFL is approximately 2-5x, which significantly surpasses those fuzzing tasks performed through lightweight static instrumentation.

FAST-AFL is a new fuzzing tool to enhance performance for binary-only fuzzing. Technically speaking, the tool is designed and prototyped with Intel PT – a newly available hardware feature – along with a path-sensitive feedback scheme. With this hardware and software co-design principle, the tool could not only accelerate a binary-only fuzzing task for about 29x but, more importantly, explore deeper program behaviors.

当使用AFL测试无源码软件时，AFL需要使用QEMU并对程序进行黑盒插装。这往往为模糊测试带来极高负载。尽管目前已有大量工作尝试减少测试压力，但不幸的是AFL仍然表现出2-5倍的额外负担。在此次演示中，我们介绍FAST-AFL，一种快速模糊测试工具。该工具使用INTEL新型硬件PT来完成对AFL加速及减负。通过此次展示，我们将对AFL在有PT和无PT条件下的性能进行对比。除此之外，我们还将展示如何使用FAST-AFL找到隐藏在软件深处的漏洞。我们将在此次演示中，开源FAST-AFL以供听众测试并使用。

Dr. Xinyu Xing is an Assistant Professor at the Pennsylvania State University, and currently working at JD Inc. as a visiting researcher. His research interest includes exploring, designing and developing tools to automate vulnerability discovery, failure reproduction, vulnerability diagnosis (and triage), exploit and security patch generation. He was the speaker at BlackHat USA, BlackHat Europe and many academic conferences (e.g., USENIX Security and CSS). He has also received best paper awards from academic conferences such as CCS and ACSAC. His works have been featured by many mainstream media, such as Technology Review, New Scientists and NYTimes etc. He was also the organizer of NSA memory corruption forensics competition.

Yaohui Chen is a PhD student in the Computer System Security program at Northeastern University's College of Computer and Information Science, advised by Professor Long Lu. Originally from Sanya, China, Chen earned his bachelor's degree at Tongji University in Shanghai before coming to Northeastern, where he now works in Professor Lu's Research in Software and Systems Security (RiS3) lab. Chen's research centers on security in Android and Linux systems. One of Chen's primary takeaways from his research thus far is the massive vulnerability that exists in cyberspace. By developing defense systems that help to prevent cyberattack, he hopes to address complex issues in system security and help to combat this vulnerability.

Dr. Jun Xu is an Assistant Professor in the Department of Computer Science at Stevens Institute of Technology. He received his PhD from Penn State University, with a focus on cyber security. His research spans the areas of software security, system security, and binary analysis. He has developed new methodologies and techniques for vulnerability finding, analysis, exploitation, and mitigation. His research has led to the discovery of hundreds of previously unknown security defects. Jun is a recipient of ACM CCS Outstanding Paper Award, Penn State Alumni Association Dissertation Award, and RSA Security Scholarship.

Dr. Jimmy Su leads the JD security research center in Silicon Valley. He joined JD in January 2017. Before joining JD, he was the director of advanced threat research at FireEye Labs. He led the research and development of multiple world-leading security products at FireEye, including network security, email security, mobile security, fraud detection, and end-point security. He led a global team including members from the United States, Pakistan, and Singapore from research to product releases on the FireEye's first machine learning based malware similarity analysis Cloud platform. This key technology advance was released on all core FireEye products including network security, email security, and mobile security. He won the Q2 2016 FireEye innovation award for his seminal work on similarity analysis. He earned his PhD degree in Computer Science at the University of California, Berkeley in 2010. After his graduation, he joined Professor Dawn Song's team as a postdoc focusing on similarity analysis of x86 and Android applications. In 2011, he joined Professor Song in the mobile security startup Ensighta, leading the research and development of the automatic malware analysis platform. Ensighta was acquired by FireEye in December of 2012. He joined FireEye through the acquisition. JD security research center in Silicon Valley focuses on these seven areas: account security, APT detection, bot detection, data security, AI applications in security, Big Data applications in security, and IoT security.

邢新宇（助理教授）目前任职于京东安全北美研究中心及宾州州立大学。其研究工作常发表于BlackHat, DEF CON, USENIX Security, CCS，研究成果曾被多家国际知名媒体报道。

Jimmy苏（博士）毕业于美国加州大学伯克利分校，目前担任京东安全北美研究中心负责人。他所领导的团队在企业安全领域取得卓越贡献。其研究成果发表于BLACK HAT（USA），DEF CON，HITB等等。

WORKSHOPS

FRIDAY

	1号会议室	2号会议室	3号会议室
10:30-14:30	HACKING WIFI 破解 WIFI Philippe Delteil & Guillermo Pilleux	INTRODUCTION TO PHYSICAL ACCESS CONTROLS 物理访问控制WORKSHOP Valerie Thomas	EXPLOIT DEVELOPMENT FOR BEGINNERS 初学者漏洞利用环境部署 Sam Bowne & Elizabeth Biddlecome
14:00-1800	CAPTURING, ANALYZING AND FAKING BLE COMMUNICATION 捕获、分析和伪造BLE通信 Yimi Hu & Tao Guo	BADGE HACKING WORKSHOP “破解”DEF CON CHINA 1.0胸卡研讨会 Joe Grand (Kingpin)	ADVANCED CUSTOM NETWORK PROTOCOL FUZZING 高级自定义网络协议模糊测试 Joshua Pereyda

SATURDAY

	1号会议室	2号会议室	3号会议室
10:30-1430	BADGE HACKING WORKSHOP “破解”DEF CON CHINA 1.0胸卡研讨会 Joe Grand (Kingpin)	CAPTURING, ANALYZING AND FAKING BLE COMMUNICATION 捕获、分析和伪造BLE通信 Yimi Hu & Tao Guo	INTRODUCTION TO PHYSICAL ACCESS CONTROLS 物理访问控制WORKSHOP Valerie Thomas
14:00-1800	ADVANCED CUSTOM NETWORK PROTOCOL FUZZING 高级自定义网络协议模糊测试 Joshua Pereyda	REVERSE ENGINEERING MOBILE APPS 对移动应用的逆向工程 Sam Bowne & Elizabeth Biddlecome	HACK TO BASICS - X86 WINDOWS BASED BUFFER OVERFLOWS, AN INTRODUCTION TO BUFFER OVERFLOWS. HACK TO BASICS - 基于X86 WINDOWS的缓冲区溢出案例，对缓冲区溢出进行介绍 Dino Covotsos & Manuel Corregedor

SUNDAY

	1号会议室	2号会议室	3号会议室
10:00-14:00	EXPLOIT DEVELOPMENT FOR BEGINNERS 初学者漏洞利用环境部署 Sam Bowne & Elizabeth Biddlecome	HACK TO BASICS - X86 WINDOWS BASED BUFFER OVERFLOWS, AN INTRODUCTION TO BUFFER OVERFLOWS. HACK TO BASICS - 基于X86 WINDOWS的缓冲区溢出案例，对缓冲区溢出进行介绍 Dino Covotsos & Manuel Corregedor	HACKING WIFI 破解 WIFI Philippe Delteil & Guillermo Pilleux

EXPLOIT DEVELOPMENT FOR BEGINNERS

初学者漏洞利用环境部署

Sam Bowne

Elizabeth Biddlecome

Learn how to take control of Windows and Linux servers running vulnerable software, in a hands-on CTF-style workshop. We begin with easy command injections and SQL injections, and proceed through binary exploits including buffer overflows on the stack and the heap, format string vulnerabilities, and race conditions.

After this workshop, you will understand how memory is used by software, and why computers are so easily tricked into executing bytes as code that entered the system as data.

We will exploit 32-bit and 64-bit Intel systems, and also ARM-based systems. We will examine modern Windows defenses in detail and learn how to defeat them, including ASLR, DEP, stack cookies, and SEHOP.

Previous experience with C and assembly language is helpful but not required. Participants will need a laptop that can run VMware or VirtualBox virtual machines.

All materials and challenges are freely available at samsclass.info, and will remain available after the workshop ends.

在类似CTF环境的研讨会里，你可以学习如何控制可被攻击的Windows和Linux服务器。我们将从简单的命令行注入和SQL注入开始，然后推进到二进制攻击，包括堆栈和缓冲区溢出，字符串格式漏洞和竞争条件。

在参加了这次的研讨会之后，你将理解软件是如何使用内存，以及为什么计算机很容易将被欺骗的字节当作代码来执行。

我们将攻击32位和64位Intel的系统以及基于ARM的系统。我们将详细研究Windows防御体系，并学习如何攻破他们，包括ASLR、DEP、堆栈Cookies和SEHOP。

我们希望你以前有过C语言和汇编语言的基础，不过不是必需的。参会者需要携带一台可以运行VMware或VirtualBox虚拟机的笔记本参会。

所有资料和挑战都可以在samsclass.info上免费获得，在研讨会结束后也会继续提供。

Sam Bowne is an instructor at City College San Francisco, and has been teaching hacking and security classes for ten years. He has presented talks and workshops at DEF CON, HOPE, RSA, BSidesLV, BSidesSF, and many other conferences. He has a CISSP and a PhD and is a DEF CON Black Badge co-winner.

Elizabeth Biddlecome is a consultant and a part-time instructor at City College San Francisco, delivering technical training and mentorship to students and professionals. She leverages her enthusiasm for architecture, security, and code to design and implement comprehensive information security solutions for business needs. Elizabeth enjoys wielding everything from soldering irons to scripting languages in cybersecurity competitions, hackathons, and CTFs.

Sam Bowne是旧金山城市学院的讲师，十年来一直在教授黑客和安全课程。他曾在DEF CON、HOPE、RSA、BSidesLV、BSidesSF和许多其他会议上发表演讲和研讨会。他拥有CISSP和博士学位，并且是DEF CON Black Badge的联合获奖者。

Elizabeth Biddlecome是旧金山城市学院的顾问和兼职讲师，为学生和专业人士提供技术培训和指导。她自己对架构、安全性和代码有巨大的热情，为业务需求设计和实施全面的信息安全解决方案。Elizabeth喜欢在网络安全竞赛、黑客马拉松和CTF中使用脚本语言。

REVERSE ENGINEERING MOBILE APPS

对移动应用的逆向工程

Sam Bowne

Elizabeth Biddlecome

Practice finding flaws in real Android and iOS apps in this fun, CTF-style hands-on workshop, and you will be ready to avoid making security errors in your own apps.

Android apps are very easy to unpack, analyze, modify, and repack; partly because of the open nature of the system, and partly because most companies neglect basic security measures. In this workshop, participants will hack apps from the Bank of America, IBM, Harvard, Home Depot, the Indian government, and other large organizations. We will find insecure network transmissions, broken cryptography, improper logging, and pervasive lack of binary protections. We will also analyze the way iOS apps use network transmissions, and observe serious vulnerabilities in iOS apps from major companies.

We will analyze Android internals in details, using the Drozer attack framework to inspect and manipulate intents to exploit insecure activities and content providers. We will perform a protection level downgrade attack on an Android 4.3 device,| removing security protections from the Twitter app.

All class materials are freely available on the Web, and will remain available after the workshop. All vulnerabilities were reported to the affected companies long ago, where appropriate.

在类似CTF的实践研讨会里体验在真实Android与iOS应用找到缺陷的乐趣，你将学到如何避免在自己的应用上出现这些安全错误。

Android应用非常容易被拆包、分析、修改和再打包：部分原因是系统天然的开放性，还有部分原因是大多数公司都忽略了基本的安全措施。在这个研讨会里，参会者将破解来自于美国银行、IBM、哈佛、家得宝、印度政府及其他大型组织的应用。我们将会发现不安全的网络传输、破解加密、不正确的日志和普遍缺乏的二进制安全防护。我们也将分析iOS应用程序的网络传输方法，并观察主要公司的iOS应用中的漏洞。

我们将详细分析Android内部，利用Drozer攻击框架去检查内容来利用其中不安全的活动和内容提供。我们将对一台Android 4.3系统的设备进行安全等级保护降级的攻击，并将Twitter应用的安全保护措施删除。

课程所有资料均可在网上免费获得，并且在研讨会结束后也会继续提供。所有漏洞均为很早以前已经报告给受影响公司的漏洞。

Sam Bowne is an instructor at City College San Francisco, and has been teaching hacking and security classes for ten years. He has presented talks and workshops at DEF CON, HOPE, RSA, BSidesLV, BSidesSF, and many other conferences. He has a CISSP and a PhD and is a DEF CON Black Badge co-winner.

Elizabeth Biddlecome is a consultant and a part-time instructor at City College San Francisco, delivering technical training and mentorship to students and professionals. She leverages her enthusiasm for architecture, security, and code to design and implement comprehensive information security solutions for business needs. Elizabeth enjoys wielding everything from soldering irons to scripting languages in cybersecurity competitions, hackathons, and CTFs.

Sam Bowne是旧金山城市学院的讲师，十年来一直在教授黑客和安全课程。他曾在DEF CON、HOPE、RSA、BSidesLV、BSidesSF和许多其他会议上发表演讲和研讨会。他拥有CISSP和博士学位，并且是DEF CON Black Badge的联合获奖者。

Elizabeth Biddlecome是旧金山城市学院的顾问和兼职讲师，为学生和专业人士提供技术培训和指导。她自己对架构、安全性和代码有巨大的热情，为业务需求设计和实施全面的信息安全解决方案。Elizabeth喜欢在网络安全竞赛、黑客马拉松和CTF中使用脚本语言。

HACK TO BASICS - X86 WINDOWS BASED BUFFER OVERFLOWS, AN INTRODUCTION TO BUFFER OVERFLOWS

HACK TO BASICS - 基于X86 WINDOWS的缓冲区溢出案例，对缓冲区溢出进行介绍

Dino Covotsos

Manuel Corregedor

Want to learn about exploit development but feeling overwhelmed at all the latest technologies and buzzwords?

Hack to basics is a course which will provide you with foundational level exploit development skills with real world exploitation techniques. This will range from “Vanilla” EIP overwrites through to Structured Exception Handler(SEH) exploitation and how egg hunters work with practical examples.

By the end of the course, Students can expect to know the basics of x86 assembly, including some real world examples of exploiting vanilla EIP overwrites, SEH exploitation and using egg hunters. This will provide an entry to the world of exploit development and a strong foundation to work off in order to make it easier to transition to the newer, more advanced technologies which are in place today.

We will be using Python to construct our exploits, combined with a debugger such as Immunity or OllyDBG, it it is recommended to be familiar with both.

想了解漏洞利用开发，但对所有最新技术和流行语感到不知所措?

Hack to basics是一门通过现实世界的开发技术提供基础级别的漏洞利用开发技能的课程。这将包括“Vanilla”EIP覆盖到结构化异常处理程序（SEH）开发以及如何使用Egg Hunter实际示例。

在课程结束后，学生会了解x86组装的基础知识，包括利用Vanilla EIP覆盖，SEH开发和使用Egg Hunter的一些真实的例子。这将为渗透测试世界提供一个入口，并打下强大的工作基础，以便更容易地过渡到现有的更新的，更先进的技术。

我们将使用Python来构建我们的工具，结合Immunity或OllyDBG等调试器，建议您提前熟悉它们。

WORKSHOPS

Dino Covotsos is the founder and CEO of Telspace Systems, a 100% South African-owned IT security firm, which started in 2002. Covotsos has many years of experience in the information security sector and has been involved in hundreds of information security projects worldwide. He is also a well-known presenter at international conferences, including Hack In the Box, Sector, H2HC, DEF CON (Recon Village) and many more. Covotsos is also passionate about the information security community and is involved various community based projects. Covotsos is on the advisory board for the ITWeb Security Summit and has several industry certifications, such as the OSCE, OSCP, OSWP and CREST CRT.

Manuel is currently employed as the Chief Operating Officer at Telspace Systems. Manuel has a passion for information security and over the years has gained a significant amount of knowledge and experience in the both the technical (operational) and management areas of information security. Throughout his career he has been involved in information security-related research, training, awareness and advisory projects targeting industry sectors, large financial/government institutions, multinational organisations and SMEs. He has overseen a large number of projects, Manuel also facilitates and speaks at numerous conferences as well as taking part in radio interviews and forming part of specialist panels.

Dino Covotsos是Telspace Systems的创始人兼首席执行官，Telspace Systems是一家由南非全资投资的IT安全公司，始于2002年。Covotsos在信息安全领域拥有多年经验，并参与了全球数百个信息安全项目。他还是国际会议的著名主持人，包括Hack In the Box（HITB），Sector，H2HC，DEF CON（Recon Village）等等。Covotsos也对信息安全社区充满热情，并参与各种社区项目。Covotsos是ITWeb安全峰会的顾问委员会，并拥有多项行业认证，如OSCE，OSCP，OSWP和CREST CRT。

HACKING WIFI

破解 WIFI

Philippe Delteil

Guillermo Pilleux

Wireless Networks (Wifi) are the most used type of network nowadays and most people don't know really how vulnerable they are, even WPA/WPA2 Enterprise.

In this workshop we will cover most wifi encryptions being used today, how they work behind the scenes and the theory of the cracking process. Also, you will be able to apply this knowledge on the spot with some real-life-scenario wifi networks.

Some encryptions are mathematically difficult to crack, where the cracking process could take lifetimes. But not to worry, there still are ways to get around this with an attack called Man-in-the-middle (MITM). Be wary! You never know to whom's Internet Access Point you're connecting and who's eavesdropping on you.

Ever wondered how to get somebody's passwords of a website? After this workshop you will be able to supplant a website without the victim ever knowing it with Wifiphishing or DNS Spoofing the client's router.

What to know before

- Linux commands (sed, awk, grep and the basic ones)
- Basic shell scripting
- Basic knowledge about WEP/WPA/WPA2/WPS

What you will learn

- How wifi security works
- How to audit a wireless network
- How to perform and automate Wifi attacks (WEP/WPA/WPA2 (personal & enterprise)/WPS)
- How to use the cloud to crack passwords (GpuHash.me, AWS EC2)
- How to use your own GPU to crack passwords. (in case you have one)

How technical is the class

- 40% theory and concepts
- 60% writing and testing commands/scripts and attacking wifis.

What tools are we going to use

- aircrack-ng (ifconfig, iwconfig, airmon-ng, airodump-ng, aireplay-ng, aircrack-ng, airbase-ng, airdecap-ng)
- Reaver (reaver, wash)
- Radius Servers (radiusd)
- Pyrit
- tshark/Wireshark/tcpdump
- Ettercap

What to read in advance

- Vivek Ramachandran & Cameron Buchanan, 2015, Kali Linux Wireless Penetration Testing Beginner's Guide, Birmingham B3 2PB, United Kingdom.

无线网络（Wifi）是现在最常用的网络模式并且人们并不是真的知道它有多么可被攻击，即使时是使用WPA/WPA2 企业级加密。 在本次的研讨会中，我们将介绍现在广泛应用的wifi加密方式与他们如何工作的以及破解理论。此外，你将可以在一些真实场景的无线网络应用这些知识。 一些加密方法在数学方面很难破解，因为破解可能需要使用毕生的时间。 不过不用担心，我们依旧有方法通过中间人（MITM）攻击来解决这个问题。注意！你永远不知道你正在连接的热点是哪个网络接入点，谁在监听你。 有没有想过如何获得某人的密码？ 在本次研讨会之后，你就会在受害者什么都不知道的情况下通过wifi钓鱼或DNS客户端欺骗来获得密码。 你需要提前了解：

- Linux命令行（sed、awk、grep和基础命令）；
- 基本的shell脚本；
- 关于WEP/WPA/WPA2/WPS的基本知识。

在这里你将学到：

- Wifi安全是如何运作的；
- 如何监听一个Wifi网络；
- 如何进行并自动化Wifi攻击（WEP/WPA/WPA2(个人级与企业级)/WPS）；
- 如何使用云计算破解密码（GpuHash.me、亚马逊云计算 EC2）；
- 如何使用你自己的GPU破解密码（如果你有GPU）。

这门课的课时计划

- 40%理论和概念；
- 60%编写并测试命令/脚本并对wifi进行攻击。

我们将使用这些工具：

- aircrack-ng (ifconfig, iwconfig, airmon-ng, airodump-ng, aireplay-ng, aircrack-ng, airbase-ng, airdecap-ng)；
- Reaver (reaver, wash)；
- Radius Servers (radiusd)；
- Pyrit；
- tshark/Wireshark/tcpdump；
- Ettercap。

你需要提前阅读的内容：

- Vivek Ramachandran & Cameron Buchanan, 2015, Kali Linux Wireless Penetration Testing Beginner's Guide, Birmingham B3 2PB, United Kingdom

译者注：中文版书名为《Kali Linux无线渗透测试指南》 ISBN：9787115483683 各大电商有售。

Philippe Delteil is Computer Science Engineer from the University of Chile, he gave his first talk at DEF CON 26 Skytalks. Most of the time, he gives classes for free in various topics: CTF, pentesting, programming, Basic computer knowledge. He's been working with Wifi hacking during the last 3 months. He has a company with a very clever name: Info-sec.

Guillermo Pilleux has a B.CS. in Computer Science at University de Chile. Trainee in Info-Sec company doing Wifi hacking research. Founder and CEO of OneClick, an automation solution for real estate bill paying. Worked in Guatemala for Opticality doing HTR (Handwritten-text-recognition) research. DEF CON 27 will be his first time at DEF CON, he hopes to survive.

Philippe Delteil是智利大学的计算机科学工程师，他在DEF CON 26 Skytalks上发表了他的第一个演讲。大多数时候，他在各种网站上免费提供各种课程：CTF，渗透测试，编程，基本的计算机知识。在过去的3个月里，他一直在研究Wifi破解。他的公司名称非常睿智：Info-sec。

Guillermo Pilleux在智利大学计算机科学专业取得了计算机科学学士学位。“CTF和渗透测试简介”研讨会的前学生。 Info-Sec公司的实习生，在做Wifi破解研究。 OneClick的创始人兼首席执行官，OneClick是一种房地产账单支付的自动化解决方案。曾在危地马拉从事光学领域的HTR（手写文本识别）研究。 DEF CON 27将是他第一次在DEF CON，他希望能够讲好。

DEF CON CHINA 1.0 BADGE HACKING WORKSHOP

“破解”DEF CON CHINA 1.0胸卡研讨会

Joe Grand

Want to dive deeper into the DEF CON China 1.0 Badge and discover some of the secrets hidden within? In this workshop, badge designer Joe Grand will discuss low-level details of the badge and guide you through setting up the development environment, exploring and modifying the firmware, and more!

想要深入了解DEF CON CHINA 1.0 的胸卡并发现其中隐藏的秘密吗？在这个研讨会，胸卡设计者Joe Grand将讨论胸卡的基本细节，并指导你搭建开发环境，探索和自定义固件等等。

Joe Grand (@joegrand), also known as Kingpin, is a computer engineer, hardware hacker, DEF CON badge designer, teacher, advisor, runner, daddy, honorary doctor, TV host, member of legendary hacker group L0pht Heavy Industries, and the proprietor of Grand Idea Studio (grandideastudio.com). He has been creating, exploring, and manipulating electronic devices since the 1980s.

Joe Grand（@joegrand），也被称为Kingpin，他是一名计算机工程师、硬件极客、DEF CON胸卡设计者、教师、顾问、跑步者、父亲、名誉医生、电视主持人、传奇极客组织L0pht Heavy Industries的成员，还有Grand Idea Studio (grandideastudio.com)的所有者。他自从20世纪80年代就一直在创造、探索和操控电子设备。

CAPTURING, ANALYZING AND FAKING BLE COMMUNICATION

捕获、分析和伪造BLE通信

Yimi Hu

Tao Guo

胡一米

郭韬

In this workshop, we will talk about BLE communication security. As far as we know, BLE communication has been widely used in healthcare, beacons, and home entertainment industries. Thus, capturing BLE communication and doing some security research on BLE communication seems to be interesting. During this workshop, all necessary equipment is provided, such as CC2540, CC Debugger and corresponding software. Besides, BLE-based devices, such as smart bulb, smart doorlock and smart bracelet which we can find in our daily lives, will be analyzed and attacked. We hope our participants are familiar with Android development/reverse-engineering or Embedded development/reverse-engineering. It's also ok, if they don't. And participants need to take his laptop with Win 7 or higher version. The whole workshop will be divided into 3 parts. And some challenges are left for participants in each part.

Taking part in our workshop, you will get the following skills:

1) Basic knowledge about BLE communication

2) Sniffing BLE communication on the air

3) Sending BLE packets to control devices unauthorized

4) Faking BLE packets to deceive the controller

我们的workshop涉及到的内容是BLE通信安全。我们在日常生活中可以体会到，BLE通信在诸如健康护理或家庭娱乐等行业的应用越来越广泛。所以抓取BLE通信并进行安全分析是一件很有趣的事情。

在我们的workshop中，所有必需的工具，比如CC2540 Dongle、CC Debugger以及相应的软件，都已经备好。参与者只需要携带一台笔记本电脑（预装Win 7或更高版本的操作系统）即可。

针对BLE通信，我们准备了三款生活中常见的设备：智能灯泡、智能门锁以及智能手环。我们将整个workshop分成了三个部分，每个部分会针对一款设备进行研究。此外我们还设置了一些挑战，每位参与者都可以用我们提供的工具对之前研究的设备进行攻击。

参与到我们的workshop中来，需要你：最好熟悉安卓开发/逆向或嵌入式开发/逆向，当然我们也会考虑到没有相关经验的同学们。

你将学到：

1、BLE的基础知识；

2、嗅探周围的BLE通信；

3、发送数据包，“非法”控制设备；

4、伪造数据包，欺骗控制端；

Yimi Hu, member of DC0086, senior security researcher at PwnMonkey Security Lab of Beijing xFutureSecurity Information Technology Co., Ltd., has working on IoT security for several years. During his career, he has committed many CVEs and CNNVDs on smart door locks, IP cameras and other devices from well-known manufacturer such as Samsung or Honeywell. He is also a public speaker. He has made many speeches at his country and is good at public speaking.

Tao Guo, security researcher of xFutureSecurity Information Technology Co., Ltd., member of PwnMonkey Security Lab and DC0086, has been working on development of embedded devices for many years, and now mainly focuses on security analysis of embedded devices. Since when his attention is drawn to smart door locks, many vulnerabilities on world-famous smart door locks have been committed to CVE and CNNVD.

胡一米，DC0086成员，就职于北京未来安全信息技术有限公司，胖猴实验室高级安全研究院。胡一米在IoT安全研究领域拥有数年工作经验，对如三星、霍尼韦尔等知名厂商的产品进行过深入研究，向CVE及CNNVD提交了许多关于智能门锁、IP摄像头和其他设备的漏洞。

郭韬，北京未来安全信息技术有限公司安全研究员，胖猴实验室和DC0086成员，曾有多年嵌入式设备开发经验，现专注于嵌入式设备的安全研究，目前已经发现了数个国内外知名智能门锁品牌的安全漏洞。

WORKSHOPS

ADVANCED CUSTOM NETWORK PROTOCOL FUZZING

高级自定义网络协议模糊测试

Joshua Pereyda

Get hands on experience writing custom network protocol fuzzers. This class will cover the basics of network protocol "smart fuzzing." Exercises will utilize the open source network protocol fuzzing framework, boofuzz. Attendees will gain practice reverse engineering a network protocol, implementing and iterating on a custom fuzzer, and identifying vulnerabilities.

After:

- You will know the basics of fuzzing.
- You will know how to write custom network protocol fuzzers using state of the art open source tools.
- You will have hands on experience with this widely-discussed but still largely mysterious test method.

Before (Prerequisites): You should:

- Be comfortable doing some basic programming in Python.
- Understand basic network protocol concepts (e.g. what is a protocol and what is a network layer).
- Be familiar with WireShark and how to use it.
- Have a laptop with at least 8 GB of RAM.

What you won't learn:

- Exploit development.
- Python programming. Because you can already do that (see above). ;)

Fuzzing is a wide and deep field with a wide array of technologies. This class is a beginner-friendly deep dive into one niche of the fuzzing world.

亲身体验编写自定义网络协议模糊测试。这门课将介绍"智能测试"网络协议的基础知识。练习利用开源模糊测试框架boofuzz进行测试。参会者将获得对网络协议进行逆向工程的实践、实现与自定义模糊器迭代，以及识别漏洞。

在此之后：

- 你将了解模糊测试的基础知识；
- 你将了解如何使用最先进的开源工具编写自定义的网络协议模糊器；
- 你将亲身体验这种广泛讨论却很神秘的测试方法。

在此之前，你需要：

- 习惯用Python写一些基本的程序；
- 理解网络协议的基本概念（例如什么是协议以及什么是网络层）；
- 熟练使用WireShark并知道如何使用；
- 携带一台至少8GB内存的笔记本电脑。

在这里你不会学到：

- 漏洞开发；
- Python编程，因为你已经可以做到了。

模糊测试是一个广泛而深入的领域，并拥有相当大的技术含量。这门课程对初学者很友好，是深入了解模糊测试的一个基石。

Joshua is a software engineer specializing in information and network security. He has worked in the critical infrastructure and cloud computing industries with employers heavily invested in software and hardware security. Among his passions are hacking, teaching kids to program, attending orchestral concerts with his wife, and figuring out how he can get paid to do it all... legally.

Joshua is the maintainer of the boofuzz network protocol fuzzing framework.

Joshua是一名专注于信息和网络安全的软件工程师。他曾在关键基础设施和云计算行业工作，他的雇主在软件和硬件安全方面投入巨大。他的热情包括，教孩子们编程，和他的妻子一起参加管弦乐音乐会，并弄清楚他是如何合法得到报酬的呢？。

Joshua是boofuzz网络协议模糊测试框架的维护者。

INTRODUCTION TO PHYSICAL ACCESS CONTROLS

物理访问控制WORKSHOP

Valerie Thomas

Physical Access can be controlled by a variety of intelligent and simple devices. If you are wanting an overview of what these controls are and how they work, then this workshop is for you. In this class, we will discuss the fundamentals of physical security, current and upcoming technologies, and how to put them all together in order to perform a red team style assessment.

Basics

- Facility access overview
- Credential and identity concepts
- Physical Access Control System (PACS) fundamentals
- What is RFID and why does it matter?

Attacks

- RFID hacking
- Control system attacks
- Defeating physical controls (fences, gates, cameras)
- The human element of physical security

Putting it all together

- Offsite/onsite reconnaissance
- Attack planning and execution
- Post-attack strategies
- Reporting physical access finding
- Remediation approaches and reference material

物理访问可以由多种智能设备和简单设备控制。如果您想了解这些控件是什么，它们的工作原理如何，那么这个Workshop非常适合您。在本课程中，我们将讨论物理安全的基本原理、目前已有的和未来的新技术，还有如何将它们相结合来进行red team评估。

基本要素

- 设备访问概述
- 认证和识别概念
- 物理访问控制系统(PACS)基础知识
- 什么是RFID？为什么它很重要?

安全攻击

- 无线射频识别入侵
- 控制系统攻击
- 攻破物理控制（栅栏，门点，摄像头）
- 物理安全的人为要素

综合包含

- 线下/线上侦查
- 攻击的策划和执行
- 攻击发生后的策略
- 汇报物理访问的发现
- 修复措施和参考资料

Valerie Thomas is a technical director for Securicon that specializes in social engineering and physical penetration testing. After obtaining her bachelor's degree in electronic engineering, Thomas led information security assessments for the Defense Information Systems Agency (DISA) before joining private industry. Throughout her career, Thomas has conducted penetration tests, vulnerability assessments, compliance audits and technical security training for executives, developers and other security professionals.

Valerie Thomas是Securicon的技术总监，Securicon是一家专门从事社会工程和物理渗透测试的公司。取得电子工程学士学位后，Valerie成为了国防信息系统局(DISA)信息安全评估的带头人，之后入职了私企。在她的职业生涯中，为管理人员、开发人员和其他安全专业人员进行了渗透测试、漏洞评估、遵从性审计和技术安全培训。



VILLAGES

LOCKPICK VILLAGE
开锁VILLAGE

Want to tinker with locks and tools the likes of which you've only seen in movies featuring police, spies, and secret agents? Then come on by the Lockpick Village, run by The Open Organization Of Lockpickers, where you will have the opportunity to learn hands-on how the fundamental hardware of physical security operates and how it can be compromised.

The Lockpick Village is a physical security demonstration and participation area. Visitors can learn about the vulnerabilities of various locking devices, techniques used to exploit these vulnerabilities, and practice on locks of various levels of difficultly to try it themselves.

Experts will be on hand to demonstrate and plenty of trial locks, pick tools, and other devices will be available for you to handle. By exploring the faults and flaws in many popular lock designs, you can not only learn about the fun hobby of sport-picking, but also gain a much stronger knowledge about the best methods and practices for protecting your own property.

想要像电影中警察，间谍和特务那样破解各类锁和工具吗？那么来开锁village吧，开锁village由开锁匠的开放组织运营，您将有机会亲身体验实体安全的基本硬件的运作及妥协。

开锁village是一个实体安全示范和参与区域。访问者可以了解各种锁定设备的漏洞，以及如何利用这些漏洞破解各种级别的锁具。

专家将亲自演示并提供大量试用锁具，破解工具和其他设备供您使用。通过探索许多流行锁具设计中的缺陷和漏洞，您不仅可以感受开锁这项活动的趣味，还可以获得关于保护自己的财产的最佳方法和实践性知识。

CAR HACKING VILLAGE
汽车极客VILLAGE

Car Hacking Village is an interactive, hands-on experience. There you can use vehicle network tools, software, and electronic control modules to learn or practice vehicle hacking. Connect to cars where you don't have to worry about breaking. Bring your laptop and RF tools to play our Def Con China CTF.

Learn about Key Fobs, CAN Bus, Automotive Ethernet, and vehicle electronics. The CHV will host several hands on work shops throughout the day, please check out the village or CarHackingVillage.com for information.

汽车极客village是一个互动性的实践Village，目标是向参加者展示汽车极客的攻击行为，介绍汽车极客攻击的工具，并与极客合作在DEF CON 中国创建汽车极客社区。

RECON VILLAGE
侦查VILLAGE

Recon Village is an Open Space with Talks, Live Demos, Workshops, Discussions, CTFs with a common focus on Reconnaissance. The village is meant for professionals interested in areas of Open Source Intelligence (OSINT), Threat Intelligence, Reconnaissance, and Cyber Situational Awareness, etc. with a common goal of encouraging and spreading awareness around these subjects.

侦察Village是一个开放的空间。包括共同关注侦查的会谈，现场演示，研讨会，讨论及CTF。这个village较适合对开源智能（OSINT），威胁情报，侦察和网络情景意识等领域感兴趣的专业人士，旨在鼓励和传播有关这些主题的安全意识。

HARDWARE HACKING VILLAGE
硬件极客VILLAGE

Come join us for hardware hacking, teaching, learning, and exploration. We help you make your own use for things. We provide the tools and supplies for your hardware hacking pleasure; our volunteers help facilitate that. We might not have every tool under the sun, but we can help cobble something together in order to break, make, and repurpose.

来加入我们的硬件极客攻击，教学，学习和探索。 我们准备了许多奖品，还有许多难题等待技艺超群的您前来破解。

PACKET HACKING VILLAGE
数据包攻防极客VILLAGE

The Packet Hacking Village is where you'll find network shenanigans and a whole lot more. PHV welcomes all DEF CON attendees and there is something for every level of security enthusiast. This village was created to help enlighten attendees through education and awareness while focusing on defense and blue team techniques.

在数据包攻防极客village中，你将会看到网络欺骗以及更多有趣的东西。数据包攻防极客village欢迎所有DEF CON的参加者，并且对每个级别的安全爱好者都有相应的准备。这个village的建立是为了通过安全意识的培训启发参与者，同时关注红蓝对抗与防御技巧。

BLOCKCHAIN VILLAGE
区块链 VILLAGE

Bits and Blocks

At Bits and Blocks we showcase networks built on blockchain technology. Applications controlling assets with distributed transactions are examined. Mandarin speakers and English speakers are welcome to experience a free blockchain workshop for beginners in the Bits and Blocks village.

https://www.bitsblocks.org/

Developments at BAT (Baidu, Alibaba, Tencent) as well as IBM, Amazon, and Opensource projects like cryptocurrencies and the Hyperledger are explained. Please come to Bits and Blocks to share your blockchain experience and meet other security engineers.

For advanced hackers, Bits and Blocks features detailed guidance on the Schnorr signature algorithm, the cryptographic Merkle tree, and confidential transactions. Several hardware projects showcase developments in device driven blockchain applications.

在Bits and Blocks，我们展示了基于区块链技术的网络。研究使用分布式事务控制资产的应用程序。欢迎所有讲中文或英语的人士在Bits and Blocks体验免费的区块链工作坊。https://www.bitsblocks.org/ 解释了BAT(百度、阿里巴巴、腾讯)、IBM、亚马逊以及加密货币和超级账本等开源项目的发展。请到Bits and Blocks分享您的区块链经验，并与其他安全工程师聚集。对于高级极客，Bits and Blocks提供了关于Schnorr签名算法、加密Merkle树和机密事务的详细指导。几个硬件项目展示了设备驱动的区块链应用程序的开发。因为区块链village随着区块链技术的创新每天都有新的突破，我们在安全方面还有很多需要赶上。

BCOS Blockchain Village

As innovations in Blockchain Technology are making new breakthroughs every day, we have a lot to catch up on security front. Blockchain Village at DEF CON brings the latest of cool and exciting research, breaches, hacks, discussions, innovations and papers with hands workshop all focused on Blockchain Security.

DEF CON的区块链Village带来了最新的酷炫和令人兴奋的研究、入侵、破解、讨论、创新和亲身体验的研讨会。以上这些的重点都在区块链安全。

VXCON VILLAGE

VXCON (Variety eXploitation) Village is held by VXRL Hong Kong. VXRL is founded by a group of passionate security researchers and white-hat hackers in Hong Kong. Our team has deep expertise in software and hardware security, and we have hands-on domain knowledge in several vertical industries. Our mission is to make the cyberspace a safe place for the future. Our village this time will cover not only chip-off technique but alos some hardware like SMD badge soldering skill. It is an in-depth hand-on playground.

VXRL 是建基於香港的科技公司，由一群熱愛資訊保安研究的白帽駭客組成。在今次「晶片數據分析」工作坊中，參與者有機會利用一些簡單工具及儀器，從平版，手機，物聯網的晶片中取得重要的資訊，並會在展覽中展示多種實用及價錢平宜的工具及儀器。

AI VILLAGE

Artificial Learning techniques are becoming more prevalent in core security technologies like malware detection and network traffic analysis. Their use has opened up new vectors for attacks against non-traditional targets, such as deep learning based image recognition systems used in self driving cars. There are unique challenges in defending and attacking these machine learning systems that the security community needs to be made aware of. This AI Village will introduce DEF CON attendees to these systems and the state of the art in defending and attacking them. We will provide a setting to educate DEF CON at large through workshops and a platform for researchers in this area to share the latest research.

在恶意软件检测和网络流量分析等核心安全技术中，人工学习技术越来越普遍。它们的使用为针对非传统目标的攻击开辟了新的载体，比如用于自驾车的基于深度学习的图像识别系统。在防御和攻击这些机器学习系统方面存在独特的挑战，需要让安全社区意识到这一点。这个AI village将向DEF CON的参与者介绍这些系统，以及防御和攻击它们的最新技术。我们将通过研讨会为DEF CON提供一个广泛的教育平台，并为该领域的研究人员提供一个分享最新研究成果的平台

Baidu mesaTEE

百度MesaTEE

Curious on Intel SGX? Come and join us at the MesaTEE Village! Learn anything you want to know about Intel SGX and secure SGX programming in Rust or Python. Lots of fun with hands-on experiments and challenges on MesaTEE. Surprising gifts for challenge winners!

对英特尔SGX感到好奇吗？ 快来加入我们的MesaTEE Village吧！ 通过Rust或Python了解有关英特尔SGX和安全SGX编程的任何信息。MesaTEE的动手实验和挑战趣味颇多。挑战赢家还有惊喜礼物！

BUGZEE SOLDERING VILLAGE
BUGZEE焊接 VILLAGE

BugZee soldering Village is here to teach soldering and basic electronics in the most creative and fun way possible. Since hackers love bugs, we took inspiration from nature and OWASP logo to make an electronic rendition of a bee. We call it BugZee and it's our tribute to the OWASP community. Its entirely made out of electronic components and stands tall on its resistor legs. When soldered and powered to life, it moves around making a buzzing sound and glows wings in the dark. It's very intuitive and not too technical for anyone and everyone who wants to learn to solder or just wants to have a physical rendition of OWASP hacking bug.



BugZee焊接village是以富有创意和乐趣的方式教授焊接和基础电子技术。出于对昆虫的喜爱，所以我们从大自然和OWASP的logo中得到了灵感，制作了一个蜜蜂的电子板。我们称之为BugZee，这是我们对OWASP社区的敬意。它完全由电子元件组成，电阻腿直立。当焊接并为其供电时，它会四处移动，并发出嗡嗡的声音，同时翅膀会发亮。这个一个非常直观的案例，对于任何人和每个想学习焊接或想了解OWASP破解漏洞的基础原理的人来说都更加浅显易懂，便于理解。

BLACK WINDOW
黑窗极客

Black window village offer the basic physical penetration teaching for participant. We also build the model office for the participant to try the physical penetration. Content include the least of bypassing infrared alerts, drop the detectaphone, stealing the secret files and so on.

You can defend better only when you know how to attack. Physically experiencing the physical penetration protection helps protect the property of your individual and your enterprise.

黑窗village为参与者提供物理渗透入侵基础教学，并搭建模拟办公室等环境提供参与者尝试物理入侵。内容包括但不限于躲避红外报警器、安装窃听器、获取文件等。

CONNECT

OFFICIAL SITES

WEBSITE: HTTPS://DEFCON.ORG

DEF CON MEDIA: HTTPS://MEDIA.DEFCON.ORG

DEF CON GROUPS: HTTPS:/DEFCONGROUPS.ORG

DEF CON FORUMS: HTTPS:/FORUM.DEFCON.ORG

U.S. SOCIAL MEDIA

TWITTER: HTTPS://TWITTER.COM/DEFCON

FACEBOOK: HTTPS://FACEBOOK.COM/DEFCON/

INSTAGRAM: HTTPS://WWW.INSTAGRAM.COM/WEAREDEFCON/

REDDIT:HTTP://WWW.REDDIT.COM/R/DEFCON

CHINA SOCIAL MEDIA

DEF CON

WECHAT ID: DEFCONCHINA

DEFCON
DEF CON Security Geek Hacking Community
Scan TikCode with latest version of Dou Yin to follow me
抖音 记录美好生活

DOU YIN ID: 2268283217 "DEFCON"

知乎

ZHIHU.COM:
"THEDARKTANGENT"

DOWNLOAD THE PRESENTATION MATERIALS AND MORE FROM THE DEF CON MEDIA SERVER AT:

HTTPS://MEDIA.DEFCON.ORG/DEF CON CHINA 1/

InfoCon
Hacking Conference Archive
www.infocon.org

PRESENTATION SCHEDULE

FRIDAY 星期五

10:00	CREATING THE DEF CON CHINA 1.0 BADGE DEF CON CHINA 1.0徽章创生记 Joe Grand
11:00	TRANSFERABILITY OF ADVERSARIAL EXAMPLES TO ATTACK CLOUD-BASED IMAGE CLASSIFIER SERVICE 花费少成效快 攻破云端图像分类"黑盒"防线 Liu Yan, Wei Tao, Hao Xin, Wang Yang 兜哥, 韦韬, 郝新, 王洋
12:00-12:20	BRIDGE ATTACK: DOUBLE-EDGED SWORD IN MOBILESEC 桥接攻击：移动安全中的双刃剑 Zidong Han 韩紫东
12:30-12:50	WARNING: MAGNITUDE 10 EARTHQUAKE IS COMING IN ONE MINUTE 警告：10级地震将在一分钟内发生 Weiguang Li, Lin Huang & Yuwei Zheng
13:00	TAG-SIDE ATTACKS AGAINST NFC 攻陷 NFC Christopher Wade
14:00	HACKING DRIVERLESS VEHICLES 有的放矢 打造无人驾驶汽车金钟罩 Zoz
15:00	THE ART OF GAME SECURITY 游戏安全攻防艺术论 Joey Zhu
16:00	YOU ARE NOT HIDING FROM ME .NET .NET没有秘密 Aden Chung

SATURDAY 星期六

10:00	DEREVOLUTIONIZING OS FINGERPRINTING: THE CAT AND MOUSE GAME 猫鼠游戏：终结特征识别神话 Jaime Sanchez
11:00	CHINESE MECHANICAL LOCKS - AN INSIGHT INTO A UNIQUE WORLD OF LOCKS 机械锁中国造：欢迎来到锁之秘境 Lucas Zhao
12:00-12:20	FACE SWAPPING VIDEO DETECTION WITH CNN 使用CNN进行人脸交换视频检测 Yang Wang, Hao Xin, Junfeng Xiong, Liu Yan & Wei Tao 王洋, 郝新, 熊俊锋, 刘焱 & 韦韬
12:30-12:50	HOW TO PERFORM SECURITY ANALYSIS ON IOT EQUIPMENT THROUGH BUILDING A BASE STATION SYSTEM 反间谍计划：自建基站与数据嗅探方法论 Xiao HuiHui 小灰灰
13:00	ATTACKS YOU CAN'T COMBAT: VULNERABILITIES OF MOST ROBUST MOBILE OPERATORS 挡不住的攻击：移动运营商的基因缺陷 Sergey Puzankov
14:00	IPV666 - ADDRESS OF THE BEAST IPV666: 魔鬼地址 Christopher Grayson & Marc Newlin
15:00	GOT TO GLITCH THEM ALL: 10+ YEARS OF WAR STORIES GLITCHING EMBEDDED AND IOT DEVICES 全面沦陷：噪声攻击与IOT设备的10+年战争 Ramiro Pareja
16:00	MODERN MALWARE: DE-OBFUSCATION, EMULATION AND ROOTKITS 反击恶意软件：源头做起不挖坑 Alexandre Borges

SUNDAY 星期日

10:00	BREAKING THE BACK END! IT IS NOT ALWAYS A BUG. SOMETIMES, IT IS JUST BAD DESIGN! 打破后端限制！坏设计惹的祸，不全是BUG的锅 Gregory Pickett
11:00	VOIPSHARK: OPEN SOURCE VOIP ANALYSIS PLATFORM VOIPSHARK：开源VOIP分析平台是与非 Nishant Sharma, Ashish Bhangale & Jeswin Mathai
12:00	FROM ANCIENT TO MODERN: DIAGNOSING ROOT CAUSE OF SOFTWARE VULNERABILITIES FROM UNEXPECTED CRASHES Dr. Xinyu Xing & Dr. Jimmy Su
13:00	MISSION IMPOSSIBLE: STEAL KERNEL DATA FROM USER SPACE Yueqiang Cheng & Panel 程越强, 陈兆丰, 张煜龙, 丁羽, 韦韬
14:00	CLOSING CEREMONIES

PRESENTATIONS

MODERN MALWARE: DE-OBFUSCATION, EMULATION AND ROOTKITS

反击恶意软件: 源头做起不挖坑

Alexandre Borges

Security Researcher, Blackstorm Security

Blackstorm Security, 安全研究员

Modern advanced malware samples are used to infect countries and they make part of the current cyber war, cyber espionage and financial attacks. Furthermore, critical actors, who write these malicious codes, try to make the static and dynamic analysis really hard by heavily obfuscating and, eventually, virtualizing codes using techniques such as CFG, call stack manipulation, dead code, opaque predicate and so on. Understanding these concepts and how they are used with virtualized packers is an advantage to learn the main anti-reversing techniques.

Therefore, to manage complex scenarios as exposed above, we are able to use frameworks such as METASM, MIASM and several dynamic static emulation techniques to make code simpler. At end, the goal is to reduce the code (most of time by using symbolic analysis), making us able to get a better understanding about the threat. Additionally, the introduction of dynamic tracing (DTrace) on Windows can help us to having a better understanding about programs and their behavior.

This presentation aims to show concepts and a practical approach on how to handle these reverse engineering challenges and techniques.

现代高级恶意软件的危害程度已上升至国家层面，成为了当前网络战争、网络间谍活动和金融攻击的重要手段。编写这些恶意代码的黑客试图通过诸如CFG、堆栈调用、死代码撰写及不透明谓词使用等技术进行大量混淆并最终虚拟化代码，从而增加静态分析和动态分析的难度。因此了解这些概念以及如何通过虚拟封隔器的共同使用破解难题，是我们学习防反转技术的关键核心。

针对上述复杂的环境场景，我们可以使用METASM、MIASM等框架和一些动态静态仿真技术来简化代码，这不仅能帮助我们更好的应对威胁，更能帮我们实现减少代码的最终目标。此外，在Windows上引入动态跟踪(DTrace)也可以帮助我们更好地理解程序及其行为。

本演讲将向参会者有效地展示处理并解决这些逆向工程的技术与实用方法。

Alexandre Borges is a Security Researcher, who has been working on Reverse Engineering, Malware Analysis and Digital Forensic Analysis for many years.

Usually, he teaches training courses about Malware and Memory Analysis, Digital Forensics, Mobile Forensics and Mobile Malware Analysis around the world. Furthermore, Alexandre is the creator and maintainer of Malwoverview triage tool: https://github.com/alexandreborges/malwoverview

Alexandre has spoken in several conferences such as DEF CON 2018, H2HC conference (2015 and 2016), BSIDES (2016, 2017 and 2018), BHack (2018), HITB 2019 (Amsterdam) and CONFidence Conference 2019 (Poland).

Alexandre Borges是一名安全研究员，多年来始终致力于逆向工程、恶意软件分析和数字取证分析。

常年在世界各地教授关于恶意软件和内存分析、数字取证、移动取证和移动恶意软件分析的培训课程。此外，Alexandre还是Malwoverview 分类工具的创建者和维护者: https://github.com/alexandreborges/malwoverview

Alexandre曾在多个会议上发表过演讲，如DEF CON 2018，H2HC会议（2015年和2016年），BSIDES（2016年，2017年和2018年），BHack（2018年），HITB 2019年（阿姆斯特丹）和2019年CONFidence会议（波兰）。

MISSION IMPOSSIBLE: STEAL KERNEL DATA FROM USER SPACE

Yueqiang Cheng

程越强

Staff Security Scientist, Baidu USA X-Lab

Zhaofeng Chen

张煜龙

Staff Security Scientist, Baidu X-Lab

Yulong Zhang

张煜龙

Principle Security Scientist, Baidu

Yu Ding

丁羽

Staff Security Scientist, Baidu X-Lab

Tao Wei

韦韬

Chief Security Scientist, Baidu X-Lab

With the introduction of GDPR and the emphasis on privacy, more and more companies and research institutions have begun to pay attention to data privacy protection. Among the protection schemes, using the kernel to protect private data plays an important role.

However, Meltdown and Spectre as a CPU vulnerability allow a rogue process to read the kernel data in CPU L1-d cache, even when it is not authorized to do so. Until now, the only effective mitigation approach was to isolate kernel memory from user-mode processes. This solution has different names on different platforms: Kernel Page-Table Isolation (KPTI) on Linux, Kernel Virtual Address (KVA) Shadow on Windows, and Double Map (DM) on OS X.

In this talk, however, we will prove the illusion that the strong isolation of KPTI has perfectly defeated Meltdown to be incorrect. First, we propose Variant V3r to demonstrate that Meltdown can be improved to be more powerful and reliable than what people originally thought. Variant V3r significantly increases the reliability for a rogue process to read any kernel data (not necessary in L1-d cache) on multiple platforms. Next, we further propose an even more powerful attack, Variant V3z, that allows a rogue process to bypass KPTI and reliably read any kernel data. To the best of our knowledge, V3z is the first Meltdown variant that is able to defeat KPTI.

To demonstrate the reliability, efficiency, and effectiveness of these two new variants, we will show demos that unprivileged processes can reliably leak secrets from anywhere in the kernel space, even in the presence of KALSR.

Finally, we will offer suggestions to mitigate our proposed threats, and we call for more and more parties to join in this effort to improve the security of processors and operating systems.

随着GDPR的引入和人们对隐私的重视，越来越多的公司和研究机构开始关注数据隐私保护。在保护方案中，使用内核来保护私有数据起着重要作用。

但是，Meltdown和Spectre作为CPU漏洞允许恶意进程读取CPU L1-d高速缓存中的内核数据，即使它没有被授权这样做。到目前为止，唯一有效的缓解方法是组合KPTI + SMAP + KUI（内核用户隔离）。KPTI将内核内存与用户模式进程隔离开来。此解决方案在不同平台上具有不同的名称：Linux上的内核页表隔离（KPTI），Windows上的内核虚拟地址（KVA）阴影和OS X上的双映射（DM）。

然而，在本次演讲中，我们将证明强大的保护组合（KPTI + SMAP + KUI）完全击败了Meltdown的错觉。首先，我们使用Variant V3r来改进Meltdown，使其比人们原先想象的更强大和可靠。Variant V3r显着提高了恶意进程在多个平台上读取任何内核数据（在L1-d缓存中不必要）的可靠性。接下来，我们进一步提出了一个更强大的攻击Variant V3z，它允许恶意进程绕过（KPTI + SMAP + KUI）并可靠地读取任何内核数据。据我们所知，V3z是第一个能够击败的Meltdown变种（KPTI + SMAP + KUI）。

为了证明这两个新变体的可靠性，效率和有效性，我们将展示无特权进程可以可靠地从内核空间中的任何位置泄露秘密的演示，即使在KALSR存在的情况下也是如此。

最后，我们将提供缓解的建议，并呼吁越来越多的研究者加入这项工作，以提高处理器和操作系统的安全性

Yueqiang Cheng is a Staff Security Scientist at Baidu USA X-Lab. His research interests focus on System Security (e.g., SGX, Virtualization), Blockchain Security, and Side Channel Security.

Zhaofeng Chen is a security researcher from Baidu X-Lab, focusing on iOS/macOS security.

Yulong Zhang is currently working at Baidu conducting the research and development of the next generation methodologies to analyze advanced mobile malware, and to design security products to detect and defend mobile threats.

Yu Ding is a staff security scientist at Baidu X-Lab. His research interests are security issues around Intel SGX, secure decentralized systems, and security protocol analysis .

Dr. Tao (Lenx) Wei is the head of Baidu X-Lab. Prior to joining Baidu, he was an associate professor at Peking University. His research interests include software analysis and system protection, web trust and privacy, programing languages, and mobile security.

程越强博士是百度美国X-Lab的资深安全科学家。他的研究专注于构建安全可信的系统和软件，包括SGX安全，侧通道攻防，硬件安全和无人驾驶安全。

陈兆丰，百度安全资深安全研究员，主要研究移动和系统安全。

张煜龙是百度安全实验室研究员，主要负责移动安全、无人驾驶安全、可信安全计算等领域。

丁羽博士是百度 X-Lab 的安全科学家，致力于研究 Intel SGX 技术和协议安全分析。他是软件安全的狂热爱好者，致力于打造一个内存安全的世界。

韦韬博士是百度首席安全科学家（T11）、百度安全实验室负责人、北大客座教授。曾任UC Berkeley大学著名安全团队 BitBlaze 协办人，MITBBS联合创立者，在系统安全学术界和工业界均有不凡建树。目前在百度担任安全技术通道主席、基础技术体系TC联席主席，推动百度在安全、边缘计算、开源生态等多个领域工作获得了长足的进展。

YOU ARE NOT HIDING FROM ME .NET

.NET没有秘密

Aden Wee Jing Chung

Threat Hunter, F-secure Countercept

F-secure Countercept之威胁搜寻员

For years, we at Countercept have seen adversaries across the threat pyramid make use of PowerShell tool-kits for lateral movement, data exfiltration and persistence over different environments. As defenders, we have done a pretty good job – PowerShell is a fading threat in time. Mimikatz execution through PowerShell? AMSI and PowerShell logging can handle that relatively well.

However, adversaries being adversaries don't just give up. They have migrated tool-kits to areas where visibility is still limited – such as .NET. Favoured by adversaries due to its wide range of functionalities, ease of development, and default presence on modern Windows platforms, we have seen a significant increase in exploitation toolkits leveraging .NET to perform usual activities - but in an area where they are relatively hidden.

First, we'll take a look at these tools - what they do, and how they work. Techniques such as DCOM object abuse, run-time code compilation and in-memory assembly loading (performed by the DotNetToJscript project) would be examine in detail. These techniques are used by exploitation tool-kits such as GhostPack, SharpShooter, and SilentTrinity, and thus are very relevant to defenders. We'll then focus on detection. We'll examine the indicators such toolkits and techniques leave behind, and how we can detect them utilising various sources of telemetry, collected via open-source tooling, such as process logging, DLLs imports and ETW tracing of JIT compilation or Interop events.

At the end of the day, attendees will walk away with an understanding of the inner workings of various .NET techniques as well as how they can be used to compromise a windows machine stealthily. Additionally, attendees will learn how a defender can leverage on open source tooling to detect and hunt for .NET attacks.

Countercept多年来都已看到威胁金字塔中的对手使用PowerShell工具包在不同的环境中进行横向移动、数据过滤和持久攻击。作为安全的守护者，我们正在努力让PowerShell成为一个逐渐消失的威胁。我们发现通过PowerShell执行Mimikatz ?AMSI和PowerShell日志可以使问题得到有效的解决。

然而，对手从不会轻易放弃。他们已将工具包迁移到可见性的有限领域(如.NET)。凭借.NET广泛的功能、易于开发以及在现代Windows平台上的默认存在，备受对手的青睐。我们已经看到利用.NET执行常规活动的开发工具包显著增加，但始终局限于一个相对隐蔽的领域。

首先，在活动中，我们会对这些工具的功能及操作加深了解，并对DCOM对象滥用、运行时代码编译和内存中程序集的加载(由DotNetToJscript项目执行)等技术进行详细的研究。这些技术会在诸多开发工具，如GhostPack，SharpShooter和SilentTrinity得到利用，因此与安全守护者密切相关。之后我们将关注检测。对工具包和技术所留下的指示符进行研究，同时利用开放源码工具收集的各种遥测源(如进程日志记录、DLL导入和ETW跟踪)IT编译或互操作事件)对它们进行检测。

通过活动，参会者将了解到各种.NET技术的内部工作原理，以及如何使用这些技术悄悄地破坏Windows机器。此外，参会者也会了解到守护者如何利用开放源码工具对.NET的检测和搜索进行攻击。

Aden performs hand to hand detection and response combat, with real world adversaries as part of his life as a Threat Hunter at Countercept. Armed with a rainbow colored keyboard, ensuring no activity is left undetected is Aden's focus, regardless of toolkit, geographical origin, or sophistication.

Aden 在Countercept以一名威胁搜寻员的身份与现实世界中的敌人进行对抗。无论工具包的地理来源或复杂程度如何，确保安全是Aden工作的内核。

CREATING THE DEF CON CHINA 1.0 BADGE

DEF CON CHINA 1.0徽章创生记

Joe Grand

(Kingpin)

In honor of the first official DEF CON China event, we present to you a badge with a purpose. Created with the specific goal of bringing the DEF CON China community together, the badge is a fun, open source, hackable, and reusable electronic device.

Join badge designer Joe Grand as he guides you through the entire badge development process, including early concepts, prototyping, manufacturing, and all of the challenges he faced along the way.

为纪念首届官方DEF CON China活动的举办，我们为您准备了一枚具有特殊意义的徽章。这个徽章是一个有趣的、开源的、可编程、可重复使用的电子设备，它的目标是将中国的DEF CON社区聚集在一起。

徽章设计师Joe Grand将引导您重温整个徽章开发过程；包括最早的概念构思、原型创意、设计制造，以及他在开发过程中遇到的挑战。

Joe Grand (@joegrand), also known as Kingpin, is a computer engineer, hardware hacker, DEF CON badge designer, teacher, advisor, runner, daddy, honorary doctor, TV host, member of legendary hacker group L0pht Heavy Industries, and the proprietor of Grand Idea Studio (grandideastudio.com). He has been creating, exploring, and manipulating electronic devices since the 1980s. @joegrand (Twitter) and http://www.grandideastudio.com

Joe Grand (@joegrand)，又名Kingpin，计算机工程师、硬件极客、DEF CON徽章设计师、教师、顾问、跑步爱好者、父亲、名誉医生、电视主持人、传奇极客组织L0pht Heavy Industries的成员、Grand Idea Studio (granddeastudio.com)的所有者。自20世纪80年代以来，他一直不断地创造、探索和操纵电子设备。@joegrand (Twitter) http://www.grandideastudio.com

PRESENTATIONS

IPV666 - ADDRESS OF THE BEAST

IPV666: 魔鬼地址

Christopher Grayson
Security Engineer, Bird Ride
Bird Ride 的安全工程师

Marc Newlin
Security Engineer
安全工程师

Global adoption of IPv6 continues to grow, with Google reporting IPv6 as 25% of its client traffic. IPv6 comes with a slew of improvements from larger address space to self-organizing addressing to required support of multicast, but these improvements are a double-edged sword. With NAT going away, DHCP no longer being required, modern operating systems and networks supporting and preferring IPv6 over IPv4, ICMP being required for network operation, iptables not applying to IPv6, and multiple IP addresses being associated with individual interfaces, IPv666 conjures the perfect storm of fail open defaults.

Why, then, haven't more boxes been popped via IPv6? It turns out finding live hosts over IPv6 is a non-trivial problem (2^128 is a little bit bigger than 2^32)!

In this talk we will cover how we've approached solving the IPv6 address discovery problem. We'll cover the various mistakes we made, the predictive clustering model and neighboring address discovery that we've built into our ipv666 toolkit (with a new and improved discovery rate of 343 addresses per second), and the new web portal we've created that provides access to our aggregated IPv6 address data set. In providing this data and tool set we hope to enable researchers to evaluate the security posture of IPv6 hosts.

IPv6的使用量在全球范围内持续增长。谷歌报告显示，IPv6的使用率现已占其客户端流量的25%。从更大的地址空间到自组织寻址再到多播支持，IPv6带来了一系列令人惊喜的改进，但这些改进也是把双刃剑。随着NAT的消失，DHCP也不再被需要。现代操作系统中对于网络支持优先使用的是IPv6而不是IPv4，网络操作需要ICMP，iptables无法试用于IPv6，以及与单个接口关联的多个IP地址，IPv666正在上演一场故障风暴。

那么，为何没有更多的盒子通过IPv6弹出呢?事实证明，找到IPv6上的实时主机是一个不小的问题(2^128比2^32稍微大一点)!

在本次演讲中，我们将介绍如何解决IPv6地址发现的各类问题。分享我们收集到的各种经验、我们在ipv666工具包中内置的预测性群集模型和相邻的地址发现(具有每秒343个地址的新的和改进的发现速率)，以及我们创建的Web新门户，该门户将提供我们整合的IPv6地址数据集。通过提供这些数据和工具集，我们希望使研究人员能够对IPv6主机的安全状况有更好的评估。

Chris Grayson (OSCE) is a security engineer at Bird Ride. In this roles he designs and implements distributed systems and addresses security issues at scale. Prior to joining Bird Rides Chris was a security engineer at Snap, Inc., a founder at Web Sight, a senior penetration tester at Bishop Fox, and a research scientist at the Georgia Institute of Technology. During his tenure at these organizations Chris grew into both a breaker and a builder, becoming adept at compromising all manners of systems as well as designing and implementing mechanisms to protect them. Chris has spoken at numerous security conferences such as DEF CON, ToorCon, ShmooCon, and HushCon, and attended the Georgia Institute of Technology where he received two degrees and organized and lead the Grey H@t student hacking organization.

Marc is a security engineer by day, and SDR hacker by night, having disclosed wireless vulnerabilities to 21 vendors in the last two years. A glutton for challenging side projects, he competed solo in two DARPA challenges, although he never went to college. In 2013-14, Marc got into SDR by competing in the DARPA Spectrum Challenge, placing second in the preliminary tournament. In 2011, he wrote software to reassemble shredded documents, finishing the DARPA Shredder Challenge in third place out of 9000 teams.

Chris Grayson (OSCE)是Bird Ride的安全工程师。在这个角色中，他设计并实现了分布式系统，并有效处理了大规模的安全问题。在加入Bird Ride之前，Chris是Snap公司的安全工程师、Web Sight的创始人、Bishop Fox公司的高级渗透测试人员和乔治亚理工学院的研究科学家。在这些组织任职期间，Chris成为了兼顾攻击和维护能力的专业性人才。他通晓所有破坏系统的方式，并设计和实现了保护系统的机制。Chris曾在DEF CON、ToorCon、ShmooCon和HushCon等多个安全会议上发言，并在佐治亚理工学院(Georgia Institute of Technology)获得了双学位，同时还组织和领导了Grey H@t学生黑客组织。

Marc白天是一名安全工程师，晚上是一名SDR黑客，在过去的两年中，他向21家供应商披露了数十个无线漏洞。他酷爱挑战性的业余项目，尽管从未上过大学，他还是独自参加了DARPA的两项挑战。2013-2014年，通过参加DARPA频谱挑战赛进入SDR，并在预赛中取得第二名的成绩。2011年，他编写了重新组装碎文件的软件，在9000个团队中脱颖而出，名列第三，完成了DARPA碎纸机挑战赛。

BRIDGE ATTACK: DOUBLE-EDGED SWORD IN MOBILESEC

桥接攻击：移动安全中的双刃剑

Zidong Han
Tencent Mobile Security Labs, Razor Team

韩紫东
腾讯移动安全实验室 安全研究员

Bridge Attack(BA) is new attack surface for mobile phone and IoT devices in LAN. The abstract bridge is usually implemented by some custom schemes or protocols, such as Javascript Bridge in webview, Upnp Protocol in IoT. In some cases, the Bridge's expanded ability makes the risks of devices in LAN, and the vulnerability can be persistently exploited with a common web attack (Eg. XSS/CSRF)

Bridge Attack finds the potential vulnerability in communication between internal and external components. We think that external component gives more data-flow attack entries which should be checked identification in the internal component. That means bridge attack makes devices in LAN face more attack risks which can lead to remote code execution, sensitive data leak and IOT devices being controlled.

桥接攻击（BA）是局域网中智能手机和物联网设备的一类新攻击面。这种抽象的桥通常由一些自定义方案或协议实现，例如webview中的Javascript Bridge，IoT中的Upnp协议等。在某些情况下，Bridge的扩展能力会降低局域网中智能设备的风险，并且可以通过常见的Web攻击达到持续利用漏洞的效果（例如， XSS / CSRF）

桥接攻击利用内部和外部组件之间通信的潜在漏洞，我们认为外部组件提供了更多的数据流攻击入口，这些入口应当在内部组件中进行合理的身份校验。这意味着桥接攻击使局域网中的设备面临更多的攻击风险，这些风险可能导致远程代码执行，敏感数据泄漏以及IOT设备遭受控制。

Zidong Han, is an android security researcher from Tencent Mobile Security Lab, Razor Team. Focuses on mobile security research, especially App vulnerability and IOT related security research, Attended HITB-SECCONF-2018-Beijing,as a speaker in CommSec: "Who Hijacked My Smart Home: One URL to Hack ALL IoT Device" Attended GeekPwn 2018, Hack Pwn in House. Found and exploited more than 20 vulnerabilities in eight kinds of IoT devices.

韩紫东是来自腾讯移动安全实验室Razor团队的安全研究员。专注于移动安全研究，主要是App漏洞和物联网相关的安全研究，参加HITB2018年（北京），演讲议题《"谁劫持了我的智能家居：一个破解所有物联网设备的URL"》； 参加GeekPwn2018黑客屋挑战赛，在八种智能家居设备中发现并利用了20多个漏洞。

WARNING: MAGNITUDE 10 EARTHQUAKE IS COMING IN ONE MINUTE

警告：10级地震将在一分钟内发生

Weiguang Li
LTE Security Researcher from 360 Technology

JingLi Hao

Yuwei Zheng

Public warning system (PWS) based on mobile communication system is used to alert the public to emergency events such as earthquakes, tsunamis, hurricanes, etc. We carefully study the PWS in LTE network and uncover the vulnerability of PWS in LTE air interface, i.e., the warning messages of the PWS are not encrypted or signed when they are transmitted over the air. Thus, it is possible that malicious PWS warning messages can be transmitted.

We simply use a low cost soft define radio (SDR) device and modify not much code of the LTE open source project srsLTE in order to forge the warning messages. Both Apple and Android test mobile phones are affected by our forged warning messages.

Fake PWS warning messages will cause serious panics among the population, they also could be used to send advertising or spam messages. The public warning system may become paralyzed and useless under the threat of the abuse of fake warning messages.

本议题将讨论LTE协议中与PWS(Public Warning System公共预警系统)相关的安全漏洞。 PWS是向公众播报地震海啸以及其他紧急事件的预警系统，在灾难发生前，PWS系统可以为人民的生命安全争取极其宝贵的时间。

我们仔细研究了LTE协议中与PWS相关部分，发现LTE空口中承载的预警信息是不经过加密以及完整性保护的，我们通过常用的软件无线电设备即可以伪造虚假的灾难预警信息，并且成功的迫使支持PWS的Android和iPhone手机发出灾难警报。通过对LTE协议中参数的精心配置，我们还实现了将灾难警报信息伪装成诈骗钓鱼以及广告短信的形式。最后我们提出了一些相应的解决办法，来防止PWS系统沦为摆设甚至成为电信诈骗的工具。

Weiguang Li is a mobile network security researcher from UnicornTeam of 360 Technology Co. Ltd in China. He mainly focuses on GSM and LTE security, He is also interested in NB-IOT baseband reverse engineering and software-defined radio development. WeChat: ColorLight

Yuwei Zheng is a senior security researcher from 360 technology. He focuses on the security issues of embedded hardware and IOT systems. He was the speaker of DEF CON, HITB and BlackHat.

JingLi Hao is a researcher of 360 Security Research Institute, member of Unicorn Team, satellite hacker

李伟光 是360 IOT安全研究部UnicornTeam研究员，主要从事移动通信网络GSM,WCDMA与LTE网络协议的安全研究，擅长对NB-IoT基带芯片的逆向以及软件无线电开发等工作，同时也是360集团3GPP标准代表。

GOT TO GLITCH THEM ALL: 10+ YEARS OF WAR STORIES GLITCHING EMBEDDED AND IOT DEVICES

全面沦陷：噪声攻击与IOT设备的10+年战争

Ramiro Pareja
Technical Leader, Riscure Security Lab China
技术负责人@Riscure 安全研究实验室中国区

Fault injection, also known as glitch attacks, is a hardware hacking technique that has been successfully used to attack all kind of targets for more than 20 years. However, most of the security experts ignore about its existence or understates its risks. With the recent decrease on the tooling cost required to perform fault injection, these type of attacks have become affordable for the masses. At the same time, the generalization of secure coding practices and the rise of the IoT devices based on small SoCs is increasing the interest on these and other hardware attacks, as quite often nowdays they are the only resort to attack some electronic devices.

In this talk, we tell our war stories about performing fault injection attacks on a wide variety of devices used by different industries. Our real stories - a compendium of more than 10 years of experience as hardware security analysts - will cover the full spectrum what fault injection is about. We will be talking about shooting lasers, breaking military grade cryptography, unblocking locked devices, revealing the deepest secrets hidden in the hardware and much more. But not everything is lost for your electronic devices! We will also talk about how you can protect your hardware and software against these powerful attacks.

故障注入，也称为噪声攻击，是一种已成功用于攻击各种目标的硬件黑客攻击技术。但是，大多数安全专家都会忽视它的存在或低估它的风险。如今执行故障注入所需的工具成本正在持续降低，与此同时，安全编码实践的普及和基于小型SoC的物联网设备的流行正在增加人们对这些和其他硬件攻击的兴趣，因此这也成为了攻击某些电子设备唯一的手段。

在本次演讲中，我们将讲述关于不同行业使用各种设备进行故障注入攻击的斗争故事。通过真实故事的案例分享，展示一名硬件安全分析师超过10年的宝贵经验。我们将带来关于镭射激光，军用级密码术的破解，已锁定的设备解锁等内容，揭示隐藏在硬件中最深层秘密。但并非所有电子设备都被攻陷了，我们还将讨论如何保护你的硬件和软件免受这些强大的攻击。

Ramiro Pareja is the technical leader of the Riscure security testing laboratory located in China. He has large experience on hardware security and he specializes on Embedded Systems and SoC security. In the last years, Ramiro has developed an interest and expertise in the automotive industry (embedded and connected technologies deployed in modern vehicles), applying fault injection and side channel attacks – very common in other markets like smartcards or content protection – to the automotive electronic systems.

If it has chips, he can break it ;)

Ramiro Pareja是Riscure位于中国的安全测试实验室的技术负责人。他在硬件安全方面拥有丰富的经验，专注于嵌入式系统和SoC安全。在过去的几年里，Ramiro对汽车行业（现代车辆中部署的嵌入式和互联技术）方面有着强烈兴趣并储备了丰富的专业知识，将故障注入和侧信道攻击广泛应用于汽车的电子系统中。

（如果它有芯片，他可以攻破它）。

BREAKING THE BACK END! IT IS NOT ALWAYS A BUG. SOMETIMES, IT IS JUST BAD DESIGN!

打破后端限制! 坏设计惹的祸，不全是BUG的锅

Gregory Pickett
Cybersecurity Operations, Hellfire Security
Hellfire Security之网络安全行动部

Reverse engineering is critical to exploitation. However, going through the process of reverse engineering can often lead to a great deal more than just uncovering a bug. So much so that you might find what you need for exploitation even if you don't find a bug.

That's right. If you go through object data, object representation, object states, and state changes enough you can find out quite a lot. Yes. Poor application logic is a bitch. Just ask any application penetration tester. This time it is not the magstripe. It's appsec and you will get to see how application attacks can be used against a hardware platform.

In this talk, I will go through the journey that I took in reverse engineering the public transportation system of an east asian mega-city, the questions that I asked as I wondered "How does this work?", the experiments that I ran to answers those questions, what I learned that lead me to an exploit capable of generating millions of dollars in fake tickets for that very same system, and how other designers can avoid the same fate. Not without risk, this research was done under a junta so I will also be telling you how I kept myself out of jail while doing it. Please join me. You won't want to miss it.

逆向工程对开发研究至关重要。因为，逆向工程的过程往往能察觉到比发掘bug更有用的内容，即使没有发现bug，也可发掘到开发所需的关键东西。

PRESENTATIONS

如果你对对象数据、对象表示、对象状态和状态变化做了足够的研究，你就能发现很多有用的东西。对任何应用程序渗透测试仪进行研究与分析，不尽人意的应用程序逻辑比比皆是，这并不是磁条的问题，这正是AppSec。在活动中您将了解如何对硬件平台使用应用程序攻击。

演讲中，我将分享一段自己在东亚大城市公共交通系统中进行逆向工程的经历。在这段经历中，我常想着"这是如何操作的"问题，为了寻求问题的答案，我不断的进行试验并从中有所收获。这不仅让我成功地攻破了这一系统同时也许会了对于此类攻击的防护手段，从而让系统有效的避免攻击。这项研究还是在一个军政府的领导下进行的，风险极高，相信您一定不会想要错过。

Gregory Pickett CISSP, GCIA, GPEN has a background in intrusion analysis for Fortune 100 companies but now heads up Hellfire Security's Managed Security Services efforts and participates in their assessment practice as a network security subject matter expert. As a security professional, his primary area of focus and occasional research is networks with an interest in using network traffic to better understand, to better defend, and sometimes to better exploit the hosts that live on them. He holds a B.S. in Psychology which is completely unrelated but interesting to know. While it does nothing to contribute to how he makes a living, it does demonstrate how screwed up he actually is.

Gregory Pickett CISSP， GCIA， GPEN拥有入侵分析Fortune 100公司的背景，现任职于Hellfire Security，从事托管安全服务工作并作为网络安全主题专家参与其评估实践。作为一名安全专业人士，他主要关注的领域是网络，其兴趣在于如何使用网络流量更好地理解、防御，甚至更利用其上的主机。他拥有心理学学士学位，虽然该学位与安全领域相距甚远，但却让他收获了很多有趣的知识。

ATTACKS YOU CAN'T COMBAT: VULNERABILITIES OF MOST ROBUST MOBILE OPERATORS

挡不住的攻击：移动运营商的基因缺陷

Sergey Puzankov
Telecom Security Expert, Positive Technologies
Positive Technologies，电信安全专家

The mobile world is moving to 5G. However, there are billions of subscribers who still use old 2G and 3G networks. These networks rely on the SS7 (Signaling System #7) protocol stack that was developed in the 1970s. The SS7 stack was supposed to be used as an isolated network within a small club of large telephone operators, so nobody thought about upper-layer security mechanisms. Further development of SS7 brought the possibility of sending signaling traffic over IP networks. Thus, the SS7 stack got vulnerabilities "by-design" that allow an external intruder to perform such attacks as location tracking, service disruption, SMS and voice call interception. Mobile operators, equipment vendors, and non-commercial organizations (such as the GSMA - the association of mobile operators) are aware of the problem. They develop and implement security solutions mitigating threats from SS7 networks.

Our recent research shows that SS7 has vulnerabilities that allow bypassing any protection tools. Manipulation of parameters on different layers of an SS7 message may help an intruder to cheat a security tool and achieve the goal even with subscribers served by a well-protected network. The research findings were reported to the GSMA Coordinated Vulnerability Disclosure Programme and FASG (Fraud and Security Group). The report was used for a security recommendations update.

In this presentation, I will demonstrate how an intruder can use new SS7 vulnerabilities to bypass security tools. I will explain why it is possible and how network equipment reacts to malicious traffic. In addition, I will give recommendations to operators on how to make their networks more secure.

移动世界已向5G迈进。 然而，仍有数十亿用户在使用旧的2G和3G网络。 这些网络依赖于20世纪70年代开发的SS7（信令系统＃7）协议栈。SS7堆栈本来是作为一个由大型电话运营商组成的小俱乐部中的一个隔离网络使用的，所以没有人考虑过上层的安全机制。SS7的进一步发展带来了通过IP网络发送信令流量的可能性。因此，SS7堆栈具有"按设计"的漏洞，允许外部入侵者执行诸如位置跟踪、服务中断、SMS和语音呼叫拦截等攻击。移动运营商、设备供应商和非商业组织（例如GSMA - 移动运营商协会）都意识到了这个问题。 他们开发并实施安全解决方案，以减轻SS7网络的威胁。

我们最新的研究显示，SS7存在可以绕过任何保护工具的漏洞。 在SS7消息的不同层上操纵参数可以帮助入侵者骗取安全工具并实现目标；即便用户受到良好保护的网络提供服务也是如此。 研究结果已报给GSMA协调漏洞披露计划和FASG（欺诈与安全组）。 该报告会用于更新安全建议。

在这个演讲里，我将演示入侵者如何使用新的SS7漏洞来绕过安全工具，解释它为何能成功，以及网络设备应对恶意流量的做法。此外，我也会提出如何令网络更安全的建议。

Sergey was born in 1976. He graduated from Penza State University with a degree in automated data processing and management systems in 1998. Before joining Positive Technologies in 2012, he worked as a quality engineer at VimpelCom. Being a security expert in telecommunication systems at Positive Technologies, he researches signaling network security and participates in audits for mobile operators around the world.

Sergey is also the general developer of the PT Telecom Vulnerability Scanner tool, member of the PT Telecom Attack Discovery development team, writes Positive Technologies annual reports on telecom security.

He is part of the team that revealed vulnerable points in popular two-factor authentication schemes using texts and demonstrated how easy it is to compromise Facebook, WhatsApp, Telegram accounts, and a Bitcoin wallet. Apart from that, Sergey actively contributes the results of security research and discovered vulnerabilities to global organizations, such as GSMA and ITU.

Sergey生于1976年。1998年，他从奔萨州立大学(Penza State University)毕业，获得自动化数据处理和管理系统学位。在2012年加入Positive Technologies之前，他在VimpelCom担任质量工程师。作为Positive Technologies的电信系统安全专家，他研究信号网络安全，并参与全球移动运营商的审计。

Sergey也是PT Telecom Vulnerability Scanner工具的总开发人员，是PT Telecom Attack Discovery开发团队的成员，并负责撰写Positive Technologies关于电信安全的年度报告。

他与团队轻而易举地展示如何利用文本揭示了流行的双因素认证方案的弱点，并入侵Facebook、WhatsApp、Telegram账户和比特币钱包。除此之外，Sergey还积极地发掘及提交漏洞及研究成果至全球组织(如GSMA和ITU)，对安全研究有一定的贡献。

DEREVOLUTIONIZING OS FINGERPRINTING: THE CAT AND MOUSE GAME

猫鼠游戏：终结特征识别神话

Jaime Sanchez
Global Security Research Lead, Telefónica
Telefónica全球安全研究主管

With the explosive growth and distributed nature of computer networks, it has become progressively more difficult to manage, secure, and identify Internet devices. An outsider has the capability to discover general information, such as which operating system a host is running, by searching for default stack parameters, ambiguities in IETF RFCs or non-compliant TCP/IP implementations in responses to malformed requests. By pinpointing the exact OS of a host, an attacker can launch an educated and precise attack against a target machine.

There are lot of reasons to hide your OS to the entire world:

- Revealing your OS makes things easier to find and successfully run an exploit against any of your devices.
- Having and unpatched or antique OS version is not very convenient for your company prestige. Imagine that your company is a bank and some users notice that you are running an unpatched box. They won't trust you any longer! In addition, these kind of 'bad' news are always sent to the public opinion.
- Knowing your OS can also become more dangerous, because people can guess which applications are you running in that OS (data inference). For example if your system is a MS Windows, and you are running a database, it's highly likely that you are running MS-SQL.
- It could be convenient for other software companies, to offer you a new OS environment (because they know which you are running).
- And finally, privacy; nobody needs to know the systems you've got running.

This talk aims to present well-known methods that perform classification using application-layer traffic (TCP/IP/UDP headers, ICMP packets, or some combination thereof), old style approaches to defeat remote OS fingerprinting (like tweaking Windows registry or implement patches to the Linux kernel) and why this doesn't work with nowadays and could affect TCP/IP stack performance. We'll also present a new approach to detect and defeat both active/passive OS fingerprint with OSfooler-NG, a completely rewritten tool, highly portable, completely undetectable for the attackers and capable of detecting and defeating famous tools like nmap, p0f, Xprobe, pfsense and many commercial engines.

Sorry guys, OS fingerprinting is over...

随着计算机网络的爆炸式增长和分布式特性，管理、保护和识别Internet设备变得越来越困难。外部人员能够通过搜索默认堆栈参数、IETF RFC中的歧义或不兼容的TCP/IP实现来发现一般信息，比如主机运行的操作系统。通过精确定位主机的操作系统，攻击者可以对目标机器发起有针对性的精确攻击。

隐藏操作系统的意义：

- 操作系统的暴露更容易触发漏洞
- 不安全的操作系统会让公司的声誉受损。想象一下，若您的公司是一家银行，一些用户注意到您正在用一个未打包的盒子。他们不会再相信你了！此外，这种"坏"消息会给公司带来负面影响。
- 了解您的操作系统也会变得更加危险，因为人们可以猜测您在那个操作系统中运行的应用程序(数据推断)。例如，如果您的系统是一个MS Windows，并且正在运行一个数据库，那么很可能正在运行MS- SQL。
- 对于其他软件公司来说，为您提供一个新的操作系统环境可能很方便（因为他们知道您在运行哪个操作系统）。
- 出于对隐私的保护，没有人需要知道您用的系统。

这个演讲的目的是介绍一些常见的方法,使用应用程序层执行分类交通(TCP / IP / UDP报头,ICMP包,或一些组合),阐释为何旧式的方法无法打败远程操作系统指纹识别(如调整Windows注册表或实现Linux内核补丁)。我们还将提出一种新的方法来检测和击败主动/被动操作系统指纹与OSfooler - NG，这是一个全新的工具，高度便携，不仅针对完全无法检测到的攻击者，还能够检测和击败著名的工具，如nmap, p0f, Xprobe, pfsense和许多商业引擎。

对不起，OS指纹识别已结束了……

Jaime Sánchez (aka @segofensiva) has worked for over 20 years as a specialist advisor for large national and international companies, focusing on different aspects of security such as consulting, auditing, training, and ethical hacking techniques. He holds a Computer Engineering degree and an Executive MBA. In addition, he holds several certifications, like CISA , CISM , CISSP , just to name a few, and a NATO SECRET security clearance, as a result of his role as advisory of many law enforcement organizations, banks and large companies in Europe and Spain.

He has spoken in renowned security conferences nationally and internationally, as in RootedCON , Nuit du Hack , Black Hat , DEF CON , DerbyCON , NocOnName , Deepsec , Shmoocon or Cyber Defence Symposium , among others. As a result of his researches, he has notified security findings and vulnerabilities to top companies and vendors, like Banco Popular, WhatsApp, Snapchat, Microsoft, Apple etc.

He is a frequent contributor on TV (TVE, Cuatro, LaSexta, Telecinco), press (El Pais, El Mundo, LA Times, NBC News) and radio programs, and writes a blog called 'SeguridadOfensiva'

Jaime Sánchez(又名@segofensiva)20多年来一直是大型国内和国际公司的专家顾问，专注于安全的不同方面，如咨询、审计、培训和道德黑客技术。他拥有计算机工程学位和工商管理硕士学位。此外，由于他是欧洲和西班牙许多执法机构、银行和大公司的顾问，他持有若干证书，如CISA、CISM、CISSP(仅举几例)和北约的秘密安全许可。

VOIPSHARK: OPEN SOURCE VOIP ANALYSIS PLATFORM

VOIPSHARK：开源VOIP分析平台是与非

Nishant Sharma
R&D Manager, Pentester Academy
Pentester Academy 的研发经理

Jeswin Mathai
Security Researcher, Pentester Academy
Pentester Academy的安全研究员

Ashish Bhangale
Senior Security Researcher, Pentester Academy
Pentester Academy的高级安全研究员

Leveraging the packet switched network for making phone calls or VoIP has come a long way now. Today, it has already replaced conventional circuit switching based telephones from the large organizations and now moving to capture the non-commercial users. In this talk, we will focus on the traffic analysis based security analysis of SIP and RTP protocols which are one of the most popular protocols for VoIP. These protocols are already gaining new adopters on high rate and also replacing older protocols like H323.

We will discuss VoIPShark open source VoIP Analysis Platform which will allow people to analyze live or stored VoIP traffic, easily decrypt encrypted SRTP stream, perform macro analysis, generate summary specific to VoIP traffic/nodes and export calls/SMS/DTMF in popular user friendly file formats. We will also be releasing VoIPShark collection of Wireshark plugins written in Lua under GPL. VoIPShark is plug-n-play, easy to modify/extend and platform independent in nature. We will also discuss the currently available open source tools for SRTP decryption, their shortcomings and how VoIPShark address those.

利用分组交换网络进行电话呼叫或VoIP已经取得了很大的进展。如今，它已经取代了传统基于电路交换的电话。从大型机构，至现在正着手吸引非商业用户都用它。在本演讲中，我们将重点放在基于流量分析的SIP协议和RTP协议的安全性分析，这是目前最流行的VoIP协议之一。这些协议已经以很高的速率获得了新的采用者，并取代了像H323这样的旧协议。我们将讨论VoIPShark开源VoIP的分析平台，它将允许人们分析实时或存储的VoIP流量，轻松解密加密的SRTP流，执行宏分析，生成特定于VoIP流量/节点的摘要，并以流行的文件格式导出call /SMS/DTMF。我们还将发布VoIPShark Wireshark插件集合，这些插件是在GPL下用Lua编写的。VoIPShark是即插即用的，易于修改/扩展，本质上不限于任何平台。我们还将讨论当前可用于SRTP解密的开源工具、它们的缺点及VoIPShark如何解决这些问题。

Nishant Sharma is a R&D Manager at Pentester Academy and Attack Defense. He is also the Architect at Hacker Arsenal where he leads the development of multiple gadgets for WiFi pentesting such as WiMonitor, WiNX and WiMini. He also handles technical content creation and moderation for Pentester Academy TV. He has 6+ years of experience in information security field including 4+ years in WiFi security research and development. He has presented/published his work at Blackhat USA/Asia, Wireless Village, IoT village and Demo labs (DEF CON). Prior to joining Pentester Academy, he worked as a firmware developer at

PRESENTATIONS

Mojo Networks where he contributed in developing new features for the enterprise-grade WiFi APs and maintaining the state of art WiFi Intrusion Prevention System (WIPS). He has a Master's degree in Information Security from IIIT Delhi. He has also published peer-reviewed academic research on HMAC security. His areas of interest include WiFi and IoT security, AD security, Forensics and Cryptography.

Ashish Bhangale is a Senior Security Researcher at Pentester Academy and Attack Defense. He has 6+ years of experience in Network and Web Application Security. He has also worked with the state law enforcement agencies in the capacity of a Digital Forensics Investigator and was instrumental in solving IT fraud/crime cases. He was responsible for developing and testing the Chigula (WiFi Forensics Framework) and Chellam (First pure WiFi Firewall) frameworks. He has also created and managed multiple projects like Vulnerable Web Application OSes, Vulnerable Router Project and Damn Vulnerable Wordpress. He has presented/published his work at Blackhat, Wireless Village, IoT village and Demo labs (DEF CON). His areas of interest include Forensics, WiFi and AD security.

Jeswin Mathai is a Researcher at Pentester Academy and Attack Defense. He has published his work at Blackhat Arsenal and Demo labs (DEF CON). He has a Bachelor's degree from IIIT Bhubaneswar. He was the team lead at InfoSec Society IIIT Bhubaneswar in association with CDAC and ISEA, which performed security auditing of government portals, conducted awareness workshops for government institutions. He was also the part of team Pied Piper who won Smart India Hackathon 2017, a national level competition organized by GoI. His area of interest includes Malware Analysis and Reverse Engineering, Cryptography, WiFi security and Web Application Security.

Nishant Sharma是Pentester Academy and Attack Defense的研发经理。他还是Hacker Arsenal的设计师，领导开发Wimonitor、Winx和Wimini等Wifi Pentesting的多个小工具。他还负责Pentester Academy TV的技术内容创建和调整。他在信息安全领域拥有6年以上的经验，包括4年以上的WiFi安全研发经验。他在Blackhat美国/亚洲、无线village、IoT village和DEF CON的演示实验室发表过。在加入Pentester Academy之前，他曾在Mojo Networks担任固件开发员，在那里他为企业级WiFi AP开发了新功能，并维护了最先进的WiFi入侵预防系统（WIPS）。他拥有印度国际信息技术学院德里信息安全硕士学位。他还曾在同行评审的学术研究发表关于HMAC安全。他的兴趣包括WiFi和物联网安全、AD安全、取证和密码技术。

Ashish Bhangale是Pentester Academy和Attack Defense的高级安全研究员。他在网络和Web应用程序安全方面有6年以上的经验。他还曾以数字取证调查员的身份与国家执法机构合作，并帮助解决IT欺诈/犯罪案件。他负责开发和测试Chigula（WiFi取证框架）和Chellam（第一个纯WiFi防火墙）框架。他还创建和管理了多个项目，如易受攻击的Web应用程序操作系统、易受攻击的路由器项目和特易受攻击的WordPress。他也曾在Blackhat、无线village、IoT village和DEF CON的演示实验室发表过。他的兴趣包括取证、WiFi和AD安全。

Jeswin Mathai是Pentester Academy和Attack Defense的研究员。他在Blackhat Arsenal和DEF CON的演示实验室发表过。他拥有IIIT Bhubaneswar的学士学位。他是InfoSec Society IIIT Bhubaneswar的团队负责人，与CDAC和ISEA合作，对政府门户网站进行安全审计，为政府机构举办意识研讨会。他也是Pied Piper团队的一员，该团队赢得了由GoI组织的全国水平的"智能印度黑客松2017"。他感兴趣的领域包括恶意软件分析和逆向工程、密码学、WiFi安全和Web应用程序安全。

TAG-SIDE ATTACKS AGAINST NFC

攻陷 NFC

Christopher Wade

This talk covers tag-side attacks against NFC communication protocols, including cracking of Mifare encryption keys and performing targeted attacks against NFC readers. In addition, it will cover the design and creation of devices capable of emulating NFC tags down to the raw protocol using standard components and tools, with no abstraction to dedicated hardware, covering and expanding on the capabilities of available products. This talk will contain how 13.56MHz NFC works at a raw level, how tools can be built for analysing it, how the protocol can be implemented in full on standard Microcontrollers, and the security weaknesses present in its design.

本演讲涵盖针对NFC通信协议的标签端攻击，包括破解Mifare加密密钥和针对NFC读取器执行针对性攻击。此外，它还将涵盖设计和创造能够使用标准组件和工具模拟NFC标签到原始协议的设备，不需要专用硬件，覆盖和扩展可用产品的功能。本演讲将包括运行在13.56MHz的NFC如何在基本功率下工作，如何构建工具以进行分析，如何在标准微控制器上完全实现该协议，以及其设计中存在的安全弱点。

Chris is a seasoned security researcher and testing consultant. His main focuses are in reverse engineering hardware, fingerprinting USB vulnerabilities and playing with Software Defined Radios, with his key strength lying in firmware analysis, which he utilises as part of the hardware testing team at Pen Test Partners.

克里斯是一位经验丰富的安全研究员和测试顾问。他的主要工作重点是逆向工程硬件，指纹识别USB漏洞和使用软件定义无线电，其主要优势在于固件分析，他将其作为Pen Test Partners硬件测试团队的一部分。

HOW TO PERFORM SECURITY ANALYSIS ON IOT EQUIPMENT THROUGH BUILDING A BASE STATION SYSTEM

反间谍计划: 自建基站与数据嗅探方法论

XiaoHuiHui
Senior Security Researcher, Baidu,Inc.

小灰灰
百度高级安全研究员

Every year billions more smart devices, like those in vending machines\automobile central controls\shared bicycles\ smart watches, are connecting to the network using 2/3/4G technology. On one hand, we need to obtain the data of connections between devices and cloud to analyze and find the vulnerabilities. On the other hand, as latest devices do not have as many direct break-in points to exploit, sniffing and man-in-the-middle into 2/3/4G traffic seem to be the trending and effective attacks, which may cause serious security issues such as leaking confidential information and remote command execution etc.

In this talk, we will first show how to build a test GSM base station system under legal premise, and then introduce a new method (inspired from learnings on malicious BTS practices in China) which make the mobile devices connected to the test base station system automatically. Using this method, we can sniff and run MITM attack easily. This affects all kinds of devices using 2/3/4G. We will demonstrate 4 examples, which use this method to find the vulnerability and take control of the devices. At the end, we will present how to build a 4G LTE test base station to perform the fast and stable testing on mobile devices.

现在越来越多的智能设备拥有2/3/4G连接功能，例如自动售货机、汽车中控、共享单车、智能手表....一方面，我们需要通过获取到234G数据，了解设备和云端的通讯内容，另一方面，很多设备已经没有太多的攻击入口，而针对234G流量的嗅探甚至是中间人无疑是一个很好的攻击点，很有可能会造成重要信息泄露、远程命令执行等安全问题。

在本次议题中，我们会介绍如何在合法前提下搭建GSM基站系统，会介绍一种让移动设备自动连接到基站系统的方法，实现对GPRS数据进行嗅探、MITM，这种攻击方法影响所有的通过移动网络进行通讯的设备，然后介绍4个实际漏洞利用例子。同时我们也会介绍如何搭建4G LTE测试基站，对移动设备进行快速、稳定的测试，以及如何利用运营商内网问题进行安全测试。

Shupeng is a member of Baidu Security Lab. He is an expert on IoT security, AI security, penetration testing, etc. He was invited to talk on multiple security conferences, and successfully pwned IOT equipments on XPwn 2016/2017/2018, GeekPwn May/October 2017, the biggest pwn competitions in China.

小灰灰是百度安全实验室高级安全研究员，主要研究方向为硬件安全、AI安全、攻防对抗。曾被邀请参加多个安全会议，在XPwn、 GeekPwn等破解大赛中多次成功破解硬件设备。

FROM ANCIENT TO MODERN: DIAGNOSING ROOT CAUSE OF SOFTWARE VULNERABILITIES FROM UNEXPECTED CRASHES

从远古到现代: 使用软件运行错误自动化诊断软件漏洞

Xinyu Xing
Assistant Professor, Penn State University. Research Scientist, JD.com

Jimmy Su
Head of Security Center, JD.com Silicon Valley

Despite the best efforts of developers, software inevitably contains flaws that may be leveraged as security vulnerabilities. Modern operating systems integrate various security mechanisms to prevent software faults from being exploited. To bypass these defenses and hijack program execution, an attacker therefore needs to constantly mutate an exploit and make many attempts. While in their attempts, the exploit triggers a security vulnerability and makes the running process terminate abnormally.

After a program has crashed and terminated abnormally, it typically leaves behind a snapshot of its crashing state in the form of a core dump. While a core dump carries a large amount of information, which has long been used for software debugging, it barely serves as informative debugging aids in locating software faults, particularly memory corruption vulnerabilities. As such, previous research mainly seeks full reproducible execution tracing to identify software vulnerabilities in crashes. However, such techniques are usually impractical for complex programs. Even for simple programs, overhead of full tracing may only be acceptable at the time of in-house testing.

In this talk, we will introduce a reverse execution technique, which takes as input a core dump, reversely executes the corresponding crashing program and automatically pinpoints the root cause of the vulnerable site hidden behind the crash. In the process of performing reverse execution, our technique typically encounters uncertainty (e.g., uncertain control or data flow) which significantly influence the capability of identifying vulnerabilities. To tackle this problem, we augment the technique with deep recurrent neural network, which poses reverse execution with the ability to perfectly infer the control and data flow leading up to the program crash. To demonstrate the utility of this technique, we have already used it to analyze hundreds of crashes pertaining to more than 300 CVEs, and successfully pinpoint the vulnerable site corresponding to each crash. Along with this talk, we will release the tool developed under our technique and make it publicly available.

尽管软件开发者投入大量精力，但计算机软件仍然充满未知缺陷。在现实世界中，未知缺陷不仅导致程序错误，更可以成为发起黑客攻击的武器。为解决未知漏洞可能带来的危害，现代操作系统整合各种安全机制。为了绕过这些安全机制为黑客带来的枷锁，黑客往往会不断调整并试错针对漏洞所准备的攻击脚本。在调整及试错的过程中，漏洞往往被触发并由此导致程序的异常终止。

当程序异常终止时，现代操作系统往往会为该程序生成一份程序终止报告。在该份报告中，系统会将程序终止时刻的内存及寄存器快照保存以帮助程序开发人员和安全分析人员诊断错误。目前使用该程序终止报告来实现错误诊断往往花费开发人员和安全分析人员大量时间。当该报告由内存安全漏洞所导致时，人工分析甚至需要更久时间。

在本次讲演中，我们将首先介绍分析程序终止报告的历史，各项技术的优缺点。而后，我们将介绍一种全新的逆向执行技术来提升程序终止报告的分析。该技术使用动态与静态分析，并辅助深度学习技术来完成对漏洞成因的迅速诊断。配合此次报告，我们将开源此项技术，并通过上百个CVE来演示该技术的效果。

Dr. Xinyu Xing is an Assistant Professor at the Pennsylvania State University, and currently working at JD Inc. as a visiting researcher. His research interest includes exploring, designing and developing tools to automate vulnerability discovery, failure reproduction, vulnerability diagnosis (and triage), exploit and security patch generation. He was the speaker at BlackHat USA, BlackHat Europe and many academic conferences (e.g., USENIX Security and CSS). He has also received best paper awards from academic conferences such as CCS and ACSAC. His works have been featured by many mainstream media, such as Technology Review, New Scientists and NYTimes etc. He was also the organizer of NSA memory corruption forensics competition. xingxinyu1983 (wechat) http://xinyuxing.org (personal site)

Dr. Jimmy Su leads the JD security research center in Silicon Valley. He joined JD in January 2017. Before joining JD, he was the director of advanced threat research at FireEye Labs. He led the research and development of multiple world leading security products at FireEye, including network security, email security, mobile security, fraud detection, and end-point security. He led a global team including members from the United States, Pakistan, and Singapore from research to product releases on the FireEye's first machine learning based malware similarity analysis Cloud platform. This key technology advance was released on all core FireEye products including network security, email security, and mobile security. He won the Q2 2016 FireEye innovation award for his seminal work on similarity analysis. He earned his PhD degree in Computer Science at the University of California, Berkeley in 2010. After his graduation, he joined Professor Dawn Song's team as a post doc focusing on similarity analysis of x86 and Android applications. In 2011, he joined Professor Song in the mobile security startup Ensighta, leading the research and development of the automatic malware analysis platform. Ensighta was acquired by FireEye in December of 2012. He joined FireEye through the acquisition. JD security research center in Silicon Valley focuses on these seven areas: account security, APT detection, bot detection, data security, AI applications in security, Big Data applications in security, and IoT security.

邢新宇（助理教授）目前任职于京东安全北美研究中心及宾州州立大学。其研究工作常发表于BlackHat, DEF CON, USENIX Security, CCS，研究成果曾被多家国际知名媒体报道。

Jimmy苏（博士）毕业于美国加州大学伯克利分校，目前担任京东安全北美研究中心负责人。他所领导的团队在企业安全领域取得卓越贡献。其研究成果发表于BLACK HAT（USA），DEF CON，HITB等等。

TRANSFERABILITY OF ADVERSARIAL EXAMPLES TO ATTACK CLOUD-BASED IMAGE CLASSIFIER SERVICE

花费少成效快 攻破云端图像分类"黑盒"防线

Liu Yan (Dou Goodman)
Senior Security Researcher, Baidu X-Lab

Hao Xin
Security Researcher, Baidu X-Lab

Wang Yang
Security Researcher, Baidu X-Lab

Wei Tao
Chief Security Scientist, Baidu

兜哥
百度安全实验室 资深研究员

郝新
百度安全实验室 资深研究员

王洋
百度安全实验室 资深研究员

韦韬
百度首席安全科学家(t11)

PRESENTATIONS

In recent years, Deep Learning(DL) techniques have been extensively deployed for computer vision tasks, particularly visual classification problems, where new algorithms reported to achieve or even surpass the human performance . While many recent works demonstrated that DL models are vulnerable to adversarial examples.Fortunately, generating adversarial examples usually requires white-box access to the victim model, and real-world cloud-based image classifier services are more complex than white-box classification and the architecture and parameters of DL models on cloud platforms cannot be obtained by the attacker. The attacker can only access the APIs opened by cloud platforms. Thus, keeping models in the cloud can usually give a (false) sense of security.In this paper, we mainly focus on studying the security of real-world cloud-based image classifier services. Specifically, (1) We propose a novel attack methods, Fast Featuremap Loss PGD (FFL-PGD) attack based on Substitution model ,which achieve a high bypass rate with a very limited number of queries. Instead of millions of queries in previous studies, our methods find the adversarial examples using only two queries per image ; and (2) we make the first attempt to conduct an extensive empirical study of black-box attacks against real-world cloud-based classifier services. Through evaluations on four popular cloud platforms including Amazon, Google, Microsoft, Clarifai, we demonstrate that Spatial Transformation (ST) attack has a success rate of approximately 100% except Amazon approximately 50%, FFL-PGD attack have a success rate over 90% among different classifier services.

近年来，深度学习（DL）技术已广泛用于计算机视觉任务，特别是视觉分类问题，其中报告新算法实现甚至超过人类表现。许多最近的工作证明DL模型容易受到对抗样本攻击，幸运的是，生成对抗样本通常需要对受害者模型进行白盒访问，而真实世界的基于云的图像分类器服务比白盒分类模型复杂多。攻击者无法获取云平台上DL模型的体系结构和参数，只能访问云平台开放的API。因此，云中的DL模型通常可以给出（错误的）安全感。本文主要研究基于云的图像分类器服务的安全性。具体来说，（1）我们提出了一种新的攻击方法，即基于替身模型的FFL-PGD攻击，它以非常有限的查询数量实现高攻击成功率。我们的方法不像在以前的研究中使用黑盒攻击那样需要数千到数百万个查询，基于替身模型的FFL-PGD攻击平均生成每个对抗样本仅查询2次。（2）我们首次尝试对真实世界基于云的图像分类器服务的黑盒攻击进行广泛的实证研究。通过对包括亚马逊，谷歌，微软，Clarifai在内的四个流行云平台的评估，我们证明Spatial Transformation (ST) 攻击的成功率约为100％，除了亚马逊大约50％，FFL-PGD攻击的成功率超过90％在不同的分类服务中。

Liu Yan (Dou Goodman), Head of AI security team of Baidu X-Lab, is a technology writer of AI Safety Trilogy. His research interests include AI and network security. He starts the open source project Advbox.

Wang Yang is a senior security researcher of Baidu X-Lab. His interests lie in face recognition, adversarial learning, and data mining. He maintains and actively contributes to Advbox project that is an open source toolbox for AI safety.

Hao Xin has been engaged in security product development for many years in Baidu. His main research directions include object detection and image classification.

Dr. Tao (Lenx) Wei is the head of Baidu X-Lab. Prior to joining Baidu, he was an associate professor at Peking University. His research interests include software analysis and system protection, web trust and privacy, programming languages, and mobile security.

刘焱（兜哥，Dou Goodman），百度安全AI模型安全团队负责人，研究方向为人工智能与网络 安全。他是AI安全三部曲的作者，著有《web安全之机器学 习入门》、《web安全之深度学习实战》、《web安全之强化学习与GAN》。他同时是著名 开源项目AI安全工具箱Advbox的作者。

王洋，百度安全研究员，主要研究方向为人脸识别、对抗样本学习、数据挖掘。

郝新，在百度从事安全产品研发多年。其目前从事AI模型安全相关研究，主要研究方向是 目标检测和图像分类。

韦韬，百度首席科学家，加入百度前为北大副教授，主要研究领域为安全架构、 编程语言、 人工智能、网络与信息安全。

FACE SWAPPING VIDEO DETECTION WITH CNN

使用CNN进行人脸交换视频检测

Wang Yang
Security Researcher, Baidu X-Lab

Junfeng Xiong
Security Researcher, Baidu X-Lab

Liu Yan
Security Researcher, Baidu X-Lab

Hao Xin
Security Researcher, Baidu X-Lab

Wei Tao
Chief Security Scientist, Baidu

王洋
百度安全实验室 资深研究员

熊俊锋
百度安全实验室 资深研究员

兜哥
百度安全实验室 资深研究员

郝新
百度安全实验室 资深研究员

韦韬
百度首席安全科学家(t11)

Recent developments of fabricating faces in videos such as Deepfakes have raised significant concerns that these deep learning techniques may be abused to create pornographic video or fake propaganda. In Deepfakes videos, the faces of a person are replaced with the faces of another one. And these faked videos are nearly indistinguishable for human. We find CNN-based networks can effectively distinguish DeepFakes videos from the real ones and present two effective methods. Firstly, we use a simple yet effective CNN architecture with several convolutional layers to build a powerful DeepFakes detector. Secondly, we find a FaceNet based method is an effective binary classifier. FaceNet is one of the state-of-the-art convolutional neural networks for face recognition, which could catch high-level features of faces. We use these features to train an SVM classifier. The two methods demonstrate successful detection reaching an accuracy rate of 99% and 94% respectively among our tests.

随着AI技术的发展，基于深度学习模型的图像换脸技术让眼见也未必为实。“换脸视频”引 发了公众对于版权与肖像权保护的担忧，甚至担心此技术被用于制作假新闻与 色情业。“换脸视频”中的假脸对于人眼和人脸识别模型是难以分辨的。我们提出两种基 于CNN网络的方法可以有效的识别此种假脸。一种是简单而有效的CNN图像分 类网络，其只需几个卷积层就能构造一个假脸识别器。另一种方法是利用FaceNet这个流 行的人脸识别模型提取特征，然后再训练SVM进行二分类。这两种方法分 别达到了99%、93%的准确率。

Wang Yang is a senior security researcher of Baidu X-Lab. His interests lie in face recognition, adversarial learning, and data mining. He maintains and actively contributes to Advbox project that is an open source toolbox for AI safety.

Junfeng Xiong(Jay Xiong) is an AI security researcher at Baidu X-Lab. His research interests cover deep learning security, privacy and IOT.

Liu Yan (Dou Goodman), Head of AI security team of Baidu X-Lab, is a technology writer of AI Safety Trilogy. His research interests include AI and network security. He starts the open source project Advbox.

Hao Xin has been engaged in security product development for many years in Baidu. His main research directions include object detection and image classification.

Dr. Tao (Lenx) Wei is the head of Baidu X-Lab. Prior to joining Baidu, he was an associate professor at Peking University. His research interests include software analysis and system protection, web trust and privacy, programming languages, and mobile security.

王洋，百度安全研究员，主要研究方向为人脸识别、对抗样本学习、数据挖掘。

熊俊锋，AI安全研究员，百度X-lab、硕士毕业于华盛顿大学。他的研究方向包括深度学习安全、隐私和物联网。

刘焱（兜哥，Dou Goodman），百度安全AI模型安全团队负责人，研究方向为人工智能与网络安全。他是AI安全三部曲的作者，著有《web安全之机器学 习入门》、《web安全之深度学习实战》、《web安全之强化学习与GAN》。他同时是著名开源项目AI安全工具箱Advbox的作者。

郝新，在百度从事安全产品研发多年。其目前从事AI模型安全相关研究，主要研究方向是目标检测和图像分类。

韦韬，百度首席科学家，加入百度前为北大副教授，主要研究领域为安全架构、 编程语言、 人工智能、网络与信息安全。

THE ART OF GAME SECURITY

游戏安全攻防艺术论

Joey Zhu
Expert/Director
专家/主任

The game security is a branch of security without noteworthy, but the problems is critical for game survival. The underground economy cost billions of dollars loss from game, the presentation will discover some founding at underground economy at first. In the main part of presentation will show some techniques details of game hacks with comparison of traditional security problem. The last part will discuss some protection countermeasures against those hacks and exploits.

尽管游戏安全是一个没有太多关注的安全细分领域，但是它存在的安全风险对游戏来说是非常关键的。黑色产业每年给游戏带来数以亿计的损失。这个分享将首先会揭示这其中一些关于黑产的发现；然后通过类比的方法，对比传统安全和游戏安全的攻击手段，帮助听众理解游戏安全风险；最后我们将介绍一些游戏安全保护手段和安全实践，帮助大家打造更安全健康的游戏。

Joey Zhu is an expert and director at Tencent, and working on Game Security since 2013. Previously, he was an architect and researcher at Trend Micro China from 2005 to 2012. His major work focus on PE virus sandbox, Script Analysis Engine on web threats and Game Security solution. He was honored to be a speaker on the topic “Chinese phishing at DEF CON 19”, in Las Vegas, in 2011.

从2013年开始至今在腾讯游戏担任技术专家，负责游戏安全的相关保护方案建设。在此之前，2005年到2012年在趋势科技担任架构师，负责病毒分析沙盒，恶意JS脚本引擎等相关工作。有幸在2011年DEF CON19做过关于中国钓鱼趋势的分享。

CHINESE MECHANICAL LOCKS - AN INSIGHT INTO A UNIQUE WORLD OF LOCKS

机械锁中国造：欢迎来到锁之秘境

Lucas Zhao
UrbanHawk

In most of the world, the lock market is pretty unremarkable. However, there is a whole other world of lock designs that are sold exclusively to the Chinese domestic market. This presentation will discuss a variety of topics regarding Chinese mechanical lock designs, from the unique dynamics of the market that fostered these designs, to flaws present in these designs, as well as how we can use some of these principles present in these locks for use in other situations.

在世界大部分地区，锁市场是级平凡的。然而，专门出售给中国国内市场的锁具设计属异。本演讲将探讨有关中国机械锁设计的主题，从培育这些设计的独特市场动态，到这些设计中存在的缺陷，以及如何将这些锁中的一些原理用于其他情况。

Lucas Zhao (UrbanHawk) is a 19-year-old lockpicker (albeit a mediocre one) with a special interest in Chinese locks, and an avid collector of locks from all over the world. He has been dissecting and researching locks since he was 10 years of age, and has a fairly comprehensive knowledge of all things related to locks. He loves to talk endlessly about his lock interests to anyone who will listen, much to the annoyance of his friends, who now avoid actively avoid him. He currently attends Case Western Reserve University in Cleveland, OH as an undergraduate student.

Lucas Zhao(市鹰) 是一个19岁的锁匠(虽属平庸之辈)，对中国锁有着特殊的兴趣，并且热衷于收藏来自世界各地的锁。他从10岁起就开始解剖和研究锁具，对锁具相关的一切都有相当全面的了解。他喜欢和任何愿意听的人没完没了地谈论他对锁的兴趣，恼火朋友们，使人家积极地回避他。他目前就读于俄亥俄州克利夫兰的凯斯韦斯特储备大学，是一名本科生。

HACKING DRIVERLESS VEHICLES

有的放矢 打造无人驾驶汽车金钟罩

Zoz

Did you watch Total Recall and wish you could fuck up JohnnyCab? Driverless vehicles are here at last and practically ripe for the hacking. Autonomous and unmanned systems already patrol our skies and oceans, and are being tested on our streets, highways and sidewalks. All trends indicate these systems are at an inflection point that will show them rapidly becoming commonplace. It is therefore a salient time for a discussion of their capabilities and potential vulnerabilities.

This session will be an informative and light-hearted look at the current state of civil driverless vehicles and what hackers or other reprobates might do to mess with them. Topics covered will include the full suite of common and proposed sensors, decision profiles and potential failure modes that could be exploited. This talk aims to both inspire unmanned vehicle designers and end users to think about robustness to adversarial and malicious scenarios, and to give the paranoid false hope of resisting the robot revolution.

你是否看过《宇宙威龙》（Total Recall 1990）并希望你能攻破JohnnyCab？无人驾驶车辆终于变为现实并且已经可以面对黑客攻击了。自动驾驶和无人系统已经在协助我们管控天空和海洋，并且正在街道，高速公路和人行道上进行测试。所有趋势都表明这些系统处于历史的拐点，这将使它们迅速变得司空见惯。因此，现在就是讨论它们的能力和潜在安全性重要时刻。

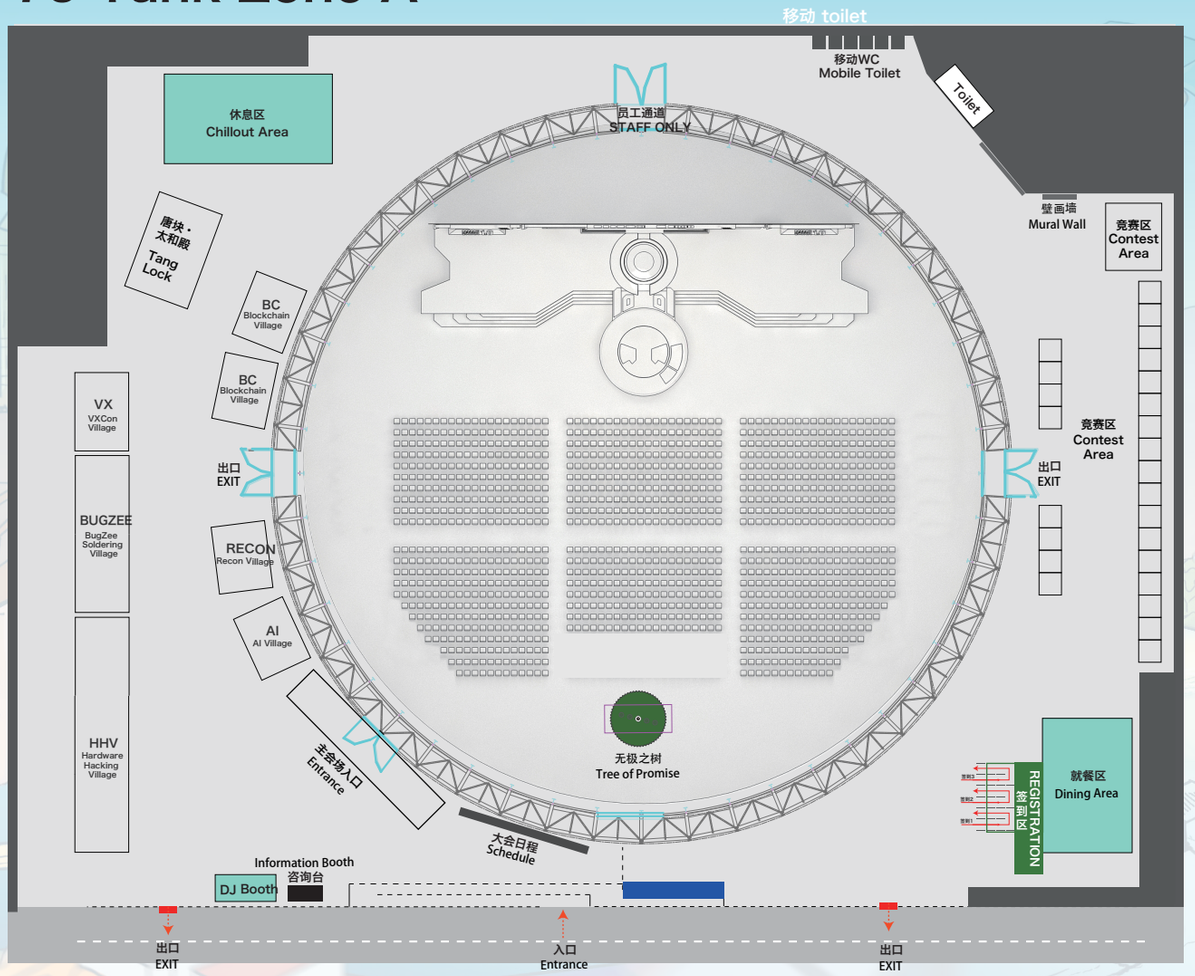
这次会议将是一个信息丰富，轻松的分析民用无人驾驶车辆现在的状态，以及黑客或其他捣蛋鬼可能会做些什么来搞坏它们。涵盖的主题包括全套通用和建议使用的传感器，决策模块和可能被利用的潜在故障模式。本演讲的目的是激励无人驾驶汽车设计师和终端用户思考攻击和恶意场景的稳定性，并对抵制机械革命进行批判。

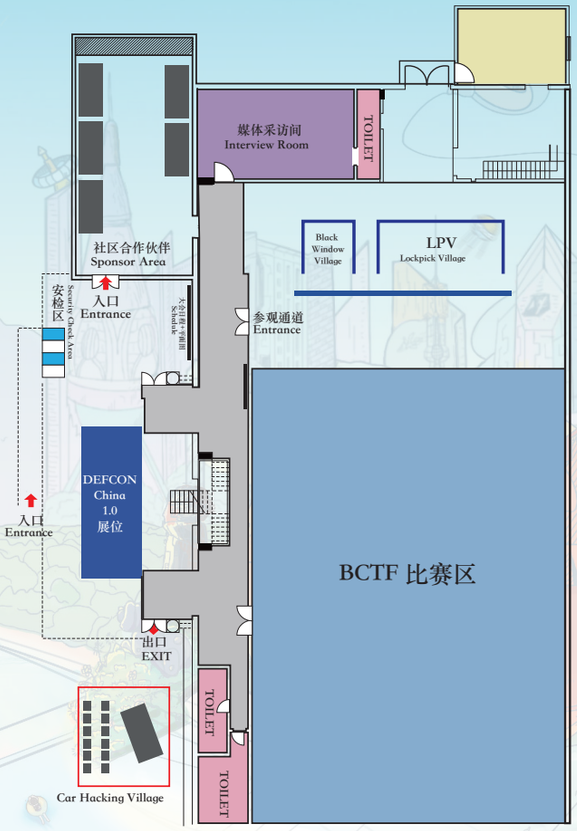
Zoz is a robotics interface designer and rapid prototyping specialist. As co-host of the Discovery Channel show ‘Prototype This!’ he pioneered urban pizza delivery with robotic vehicles, including the first autonomous crossing of an active highway bridge in the USA, and airborne delivery of life preservers at sea from an autonomous aircraft. He, for one, welcomes our new robot chauffeurs, and would only mess with them out of tough love.

Zoz是一名机器人界面设计师和快速原型制作专家。作为Discovery Channel节目’Prototype This！’的主持人，他率先使用机器人车辆进行市内比萨饼外送，包括美国第一条在运营的公路桥的自动穿越，以及用无人飞机空运海上救生设备。他期待见到新的机器人司机，并且只会因为强烈的爱而去研究他们。

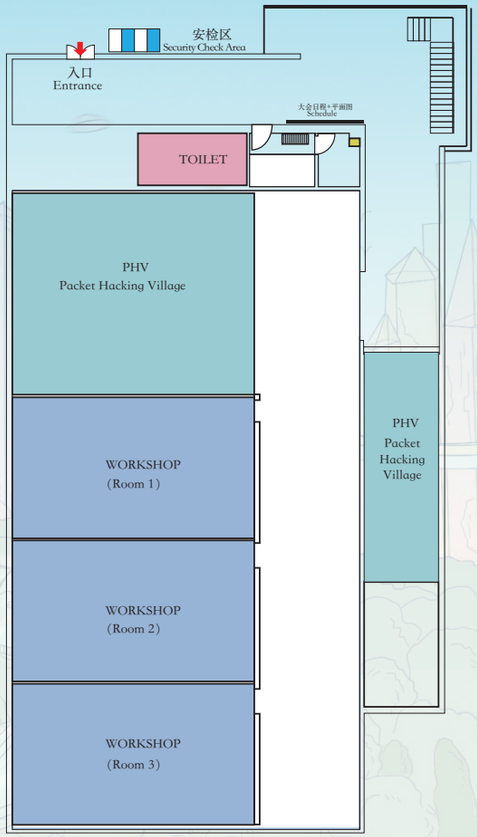
751 D PARK

79 Tank Zone A





第一车间
(Zone B)



中央大厅
(Zone C)

THANK YOU! 致谢

I want to thank everyone who has helped to make DEF CON China 1.0 possible.

Thank you to Ma Jie and Baidu Security for their long term vision to bring DEF CON to China, and Wang Yingjian, Zhao Xuan and Zhang Jin from XFuture for their excellent operational and professional support. Without these people we wouldn't be here. Liu Ye, Ma Meng, Wu Qiong and Song Ai from Baidu Security. Translating language and culture between Chinese and English was critical, a big thank you to Cayce for all her late night work.

Thank you to the DEF CON staff: Nikita, Neil, Darington, Cayce, Will, Linda, and Janet for helping make this happen. Zant from Villages, Tottenkoph from Workshops, Grifter from Contests and Events, Kampf from Entertainment, and the entire CFP Review Team.

Thank you to the speakers, workshop trainers, villages, demo labs, and contest organizers who brought the content and knowledge to share. I hope that people will leave here with new ideas, friends, and a desire to share what they have learned.

I'd like the thank Kingpin for coming out of badge design retirement and building an amazing flexible badge and showing off some amazing one man power management tricks. Our resident artist, Mar, made their first trip to China and their vision surrounds us with much of the art they created. Thank you for the live mural painting and ability to try and capture the hacker spirit through art.

Thank you to the DEF CON Groups in China and all of the community supporters, sponsors and press who helped spread the word of our conference.

Finally I want to thank you for taking your time and money to help make DEF CON something special. We are trying hard to build a different kind of conference in China and while the road may be difficult I believe in the value of the journey.

I look forward to seeing everyone next year at DEF CON China 2 next year,

- The Dark Tangent

我想感谢所有为DEF CON 神州1.0作出贡献的人们。

首先，要感谢马杰及百度安全的坚持，让我们再次来到中国。同时也要感谢未来安全的王英键， 赵萱及张晋为活动所提供的出色运营和专业支持。若没有你们的努力，也不会有今天DEF CON 神州1.0的成功举办。我还要感谢百度安全的刘叶，马濛，吴琼和宋艾，而作为我们沟通桥梁的凯熙更是功不可没，感谢你无数次的熬夜。

感谢DEF CON 的职员： Nikita, Neil, Darington, Cayce, Will, Linda 和 Janet对这项活动的全力支持与无私奉献。也感谢负责Village的Zant, 负责研讨会的Tottenkoph,负责竞赛与项目的Grifter， 负责娱乐项目的Kampf 及整个CFP评审团。

非常感谢所有的演讲者，研讨会的培训人员，villages， 演示实验室及竞赛的主办团队，感谢你们所带来的专业的知识与技术分享。我希望所有的参会者都能在活动中有所收获，并将这份收获持续的传递下去。

在此，我还想要感谢Kingpin重出江湖，为此次活动设计了一枚令人惊艳的徽章，这枚徽章将为活动带来意想不到的效果。我们的常驻艺术家Mar也首次来到了中国，在现场我们始终被他绝妙的创作所围绕。谢谢你呈现的现场壁画，让极致的极客精神与艺术的表达完美融合。

感谢国内的DEF CON Groups 及所有的社区支持者，赞助商，和为活动宣传作出贡献的媒体成员。

最后，我要感谢在座的每一个人，感谢您花费宝贵的时间和金钱参与到DEF CON的活动中来。我们希望通过不断的努力让活动变得与众不同，更为参会者带来绝佳的会议体验，尽管我深知任重道远，但我坚信未来可期。期待明年的DEF CON CHINA 2与您再会。

- The Dark Tangent启