
DEFCON
+
百度安全
有AI更安全
HOST
DEFCON β
CHINA
神州
SUSTAINING PARTNER
未来安全
XFUTURESECURITY

WELCOME TO DEF CON CHINA [BETA]

On behalf of DEF CON, Baidu Security, and XFuture Security, it is my honor to welcome you to DEF CON China [Beta], the first ever held outside of the USA!

For over 25 years DEF CON has constantly evolved, from 100+ people at DC 1 to over 25,000 at DC 25, and has created a culture of its own. At DEF CON it is your idea that counts, not what you look like, how much money you make, how old you are or what kind of music you like. You need the freedom to ask questions and be able to change your opinions.

It is expected that attendees ask speakers questions, challenge what they think is incorrect, and to improve things. Good ideas get tested, and at DEF CON I want to build an environment where wisdom is challenged and people are free to pursue technical truth.

DEF CON is what you make of it. Attendees come up with ideas for contests, villages, new events and experiences and DEF CON provides a platform for them. DEF CON is a reflection of the hacking and security community, and I invite you to try something new and in return teach something new to another attendee.

As hackers one way we learn is through experimentation, and that is why I am calling this a DEF CON [Beta] conference, because it is a huge learning experiment for us. What we all learn here will help us to build a DEF CON in China for the Chinese community, not just a conference for foreigners in China. It will take years of work to learn a new business culture, a new political culture and a new security community, but we are counting on you to help show us the way. Together we will build a new hacking and learning convention.

Thank you,

The Dark Tangent



FUN AT DEF CON 1

我谨代表DEF CON、百度安全和未来安全，欢迎您来到DEF CON China [Beta]。这是我们首次在美国以外举办DEF CON。

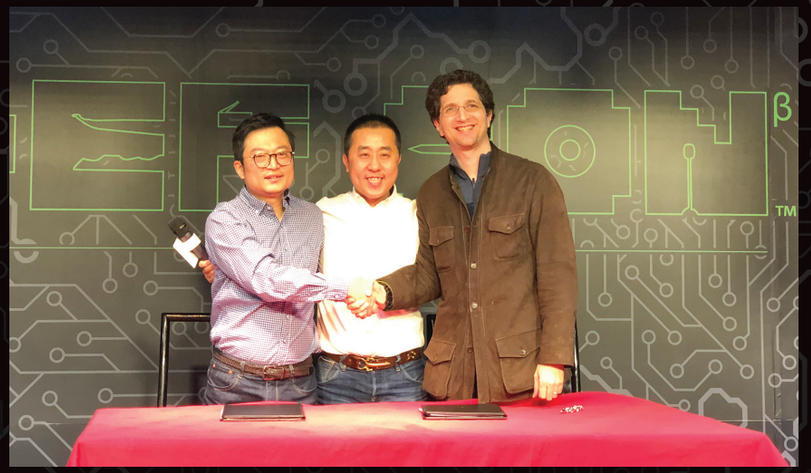
25年来，从第1届DEF CON的100多人到第25届超过25000人，DEF CON一直不断的成长，并形成了自己的风格。不论你的相貌、收入、年龄几许或喜欢什么样的音乐，在DEF CON，最重要的是你的想法。在这里，你可以自由提问，也可以改变你的观点。

我们希望看到参会嘉宾向演讲者发问，挑战他们认为不正确的事，并且去改进它。好想法在这里会被验证。我希望在DEF CON上建立一个挑战智慧，人们可以自由的寻求技术真理的环境。

DEF CON是为大家服务的，为大家提供了一个平台。让参会者将在比赛、Villages、新的活动和实验中迸发新的想法。DEF CON是黑客安全社区的体现，我诚挚的邀请您来尝试一些新的东西，并与其他参会者共同切磋学习。

作为黑客，我们有一种学习方法是“实践中出真知”，这正是为什么我把这个会议称为DEF CON [Beta]会议，这对我们来说是一个巨大的学习经历。我们在这里学到的东西，会帮助DEF CON在中国建立一个华人社区，而不单单是一个在中国举办的国外会议。也许我们将花费数年的时间，学习新的商业文化、政治文化，了解一个新的安全社区，但是我们希望各位来帮助我们走上正轨。让我们大家一起，构建一个全新的黑客学习环境。

谢谢，DT



With nearly two years of meticulous preparation, DEF CON has been carrying 26-year history and for the first time out of Las Vegas to Beijing in May, just after the beginning of summer which is a a sign of new growth for everything. We sincerely thank our friends for their support and assistance in the process. Baidu Security, as the joint organizer of DEF CON China, pays tribute to those who are working on the security front throughout the world, pays tribute to the security community partners, and pays tribute to the geek spirit of exploring the unknown, seeking the essence, and breaking through innovation.

Like many contemporary security workers, the Z80 and the Apple II were the earliest carriers of my contact with the security zone. Without the Internet and even the mouse was not seen as a standard equipment at that time, we were confined to such a machine, regardless of what kind of “innovation” and “destruction” we were engaged in. Thanks to this era, everything is connected by technology and driven by artificial intelligence. Meanwhile, we also saw the security challenges. AI has arrived and the age of big security is approaching. The concept of security has broken through its traditional category. Biometrics and IOT have become popular and have broken the barrier between the virtual world and the real one. In this process, AI technology has been used in offensive and defensive confrontation and there is also such confrontation in itself.

Security is not something that any company, community, or ecology can solve on its own power. It needs to be more open-minded, more cooperative and more inclusive. We hope that with the opportunity of DEF CON China, we will build a platform for cooperation and exchanges, gather all the strength of security circles, and jointly contribute modest strength to the ecological construction of security to make the world better. We are the Blue Team of this world!

Ma Jie

五月的北京，立夏刚过，万物生长。历时将近两年的酝酿与筹备，DEF CON承载着26年的历史，首度走出拉斯维加斯来到北京。真诚感谢广大朋友们在过程中的支持与帮助。百度安全作为DEF CON China的联合主办方，在此向全球奋战在安全战线的工作者致敬，向安全社区合作伙伴致敬，向探索未知、寻求本质、突破创新的极客精神致敬。

与众多同时代的安全工作者一样，Z80与Apple II是我接触安全圈最早的载体，当年我们不管搞什么样的“创新”与“破坏”，都局限在这样一台机器上面，那时候还没有互联网，连鼠标都不是标配。感谢当下这个的时代，这个时代在技术驱动下将所有的东西都联结在一起了，人工智能则赋予无限的可能。与此同时，我们也看到了安全的挑战。AI已至，大安全时代来临，安全的概念突破了传统的范畴，生物识别、物联网的大行其道，打破了虚拟世界与现实世界的屏障，在这个过程中，AI技术被利用在攻防对抗，其自身也存在攻防对抗。

安全不是任何一家公司、一个社区、一个生态能够自己解决的事情，需要以更开放的态度，更广泛的合作与共享应对。希望借助DEF CON China的契机，搭建起一个合作交流的平台，集结所有安全圈的力量，共同为安全生态建设贡献微薄力量，让这个世界变得更加美好。我们是这个世界的蓝军！

马杰

CONNECT

WEBSITE:

HTTPS://DEFCON.ORG

DEF CON MEDIA

HTTPS://MEDIA.DEFCON.ORG

DEF CON GROUPS:

HTTPS:/DEFCONGROUPS.ORG

FORUMS:

HTTPS:/FORUM.DEFCON.ORG

TWITTER:

HTTPS://TWITTER.COM/DEFCON

FACEBOOK:

HTTPS://FACEBOOK.COM/DEFCON/

INSTAGRAM:

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

REDDIT:

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

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全、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）

THE BADGE

We present Defcon Beta's year 1 badge! As badge makers, our philosophy is that each conference's badge should not only reference its history, but create it. DEFCON's game-changing electronic badges started an entire culture of shared electronics, puzzles, and design. One of our favorites informs the medium we use for this first badge, DEFCON 18, created by Joe Grand as evidenced by our use of aluminum PCBs. The soldermask coloring matches that of the standard set by DEFCON where:

Humans = White

Press = Green

Speaker = Blue

Goon = Red

Village = Orange/Yellow

These anonymous categories are taken out of the soldermask layer onto the side of each badge. You might think it inconvenient that you can't write your name, but consider that at a hacker conference, perhaps the most important piece of information you should protect is your identity!

Since we are being graciously hosted in China, it is only fitting that these categories are also, for the first time, presented in Chinese:

Humans = 嘉賓 - attendees

Press = 媒體 - media

Speaker = 演講 - presenter

Goon = 仕事 - staff

Village = 鄉親 - villagers

Each term is inspired by the traditional Chinese seal look.

Our silkscreen colors are the same across each group - though instead of only one silkscreen layer, we have 3 to highlight the awesome art!

现在呈现在你眼前的是DEF CON Beta 的第一年徽章！作为徽章的制作者，我们的理念是每一次会议的徽章，不应只参考它的历史，更要去创造历史。DEF CON的动态电子徽章开启了一个共享电子、智力游戏和设计的时代。最令我们骄傲的一个徽章是由Joe Grand设计的DEF CON 18徽章，我们通过印刷电路板制作出来的。镀在上面的颜色与DEF CON设定的标准匹配，其中：

嘉賓=白色，媒體=绿色，演講=蓝色，
员工=红色，鄉親=橙色/黄色

这些昵称的分类可以通过在每个徽章镀上颜色的那一面区分。你可能会因为无法把你的名字写在上面而认为很不方面，然而从黑客的角度上来讲，最应该受到保护的大概就是你的个人信息了。

我们既然在中国举办，我们将会把这些分类用中文展示出来。不同类别用不同的名称表示：

嘉賓—参会嘉宾

媒體—媒体朋友

演講—演讲者

仕事—我们仕事的工作人员

鄉親—在village呈现节目的朋友

每一个名称的设计灵感都是来自于中国传统印章。

每个类别都使用同一个丝网印颜色——区别于原有的单色印刷，我们使用了三色来突显酷炫的设计。



MUSIC EVENTS

SATURDAY 星期六 19:00 TO 22:00 BALLROOM B 大宴会B厅



The specific form of the concert which is held for DEF CON China Conference on May 12th in 2018 is Electronic Music Party. It is a combination of electronic music and Rave Party with DJ playing djing at the scene. This party is entitled DEF CON China Electronic Night for the reasons that the best music form which is appropriate for "Hacker" and "DEFCON" is an electronic one, and the live music with DJ playing djing is also a best integration with computer and network things. Therefore, Electronic Music Party has become a good performance form with characteristics of science and technology and is becoming more and more popular in the world.

At the same time, we also will add the Peking Opera elements to make the whole concert be a combination of Chinese and western styles which definitely spurt sparks.

The DJ names that we plan to invite are as follows.:

Youdai

Leslie

Danile

The type of of their performance styles respectively including:

HOUSE

TECHNO

DUBSTEP

TRANCE

DEF CON China Electronic Night is mainly played by the electronic music operations team named HANKICK. HANKICK mainly advocates "HOUSE & TECHNO" live performances. DEF CON China.Electronic Night is specially designed for DEF CON China Conference and will be played by the most popular and famous DJ in China with live performances. Definitely speaking, it will make the most stunning electronic music and create a enjoyable experience of feeling the sound of science and technology for people.

"DEFCON中国大会"于2018年5月12日一晚的内部音乐会（晚会）的具体形式是"电音Party"的形式，结合电子音乐与Rave Party，由DJ们现场打碟出演。晚会定名为"DEFCON中国电子之夜"，同"Hacker""DEFCON"最贴切的音乐形式就是电子音乐，同电脑、网络最一体化的现场音乐表演就是DJ打碟，因此，"电音Party"是当今全球最科技感的演出形式，电子音乐正在席卷全球。

同时，我们还将加入京剧元素，使得整台音乐会中西结合，碰撞出不一样的火花。

拟邀DJ：

Youdai

Leslie

Danile

演出风格分别包括的类型：

HOUSE

TECHNO

DUBSTEP

TRANCE

"DEFCON中国电子之夜"由现场电子音乐运营团队HANKICK主推整版，HANKICK主推"HOUSE & TECHNO"现场演出，为百度的"DEFCON中国大会"特别策划的"DEFCON 中国电子之夜"，由中国重量级DJ电子音乐人们打碟出演，会制造出最震撼人心的电子音乐声浪，在振聋发聩的声响里，体会今日的科技之声。

BAIDU CTF

Ballroom A
大宴会A厅



BCTF (Baidu Capture The Flag) will be held during DEF CON China. In the coming BCTF competition, it will adopt two levels of format which combine online preliminaries and offline finals. In the finale, four AI robot teams, dozens of strong domestic CTF teams and internationally famous teams will compete in a final duel. Meanwhile, a security vulnerability will be issued to a public test to win a cash prize. Stay tuned for more information!

BCTF（百度国际网络安全技术对抗赛）将在Defcon China间举行。本届BCTF采用线上预选赛、线下总决赛两级赛制。四支AI机器人战队，数十支国内CTF强队和国际知名战队将一同决战紫禁之巅。争夺百万现金大奖。同发出安全漏洞众测百万悬赏征集令，更多彩蛋逐一揭晓。

SCAVENGER HUNT

In order to honor the tradition of the DEF CON Scavenger Hunt that's been run since DEF CON 6, we have created the first ever DEF CON International Scavenger Hunt, in China. We didn't want to leave the tradition behind during our inaugural event! Gather up friends or make some new ones, team up to collect items and experiences. Join us and test your team's hacker mentality! The first challenge? Find us and acquire the secret list, look for a sign.

为了纪念自第六届DEF CON以来传承的DEF CON寻宝游戏的传统，我们设计了在中国的第一个DEF CON国际寻宝游戏。我们的开幕式必将保留此传统。以期八方会友，团队协作获取项目经验。加入我们，测试你们团队的黑客心态!狭路相逢勇者胜，请联系我们获得秘密名单，索取神迹!

DEMO LAB

#WIFICACTUS
#WIFI仙人掌

by d4rkm4tter

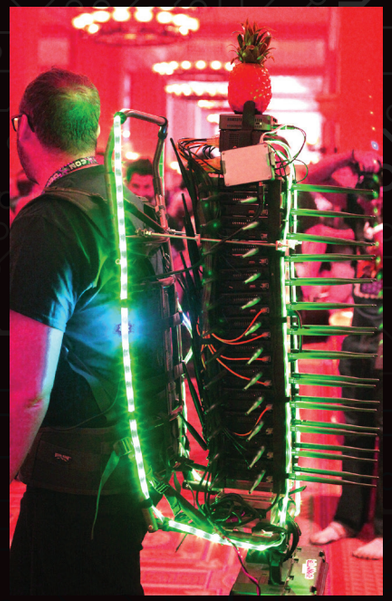
The #WiFiCactus is a passive wireless monitoring device that listens to 50 channels of WiFi all at the same time. The tool is also capable of capturing Bluetooth wireless data as well. This tool uses Kismet to capture the data from the each radio and aggregates them into a single searchable web interface. This tool is also capable of identifying wireless threats such as Broadpwn and Impersonation Attacks.

#WiFi仙人掌是一个被动无线监控设备，可同时收听50个WiFi频道。该工具还能够捕获蓝牙无线数据。该工具使用Kismet从每个无线电收集数据并将数据聚合到单个可搜索的网络界面中。该工具还能够识别无线威胁，比如Broadpwn和模拟攻击。

More info: http://palshack.org/the-hashtag-wifi-cactus-wificactus-def-con-25/

更多信息：http://palshack.org/the-hashtag-wifi-cactus-wificactus-def-con-25/

More Details: Often when capturing wireless data for troubleshooting and analysis a single radio is used which leads to lots of information being missed due to the need to channel hop. The #WiFiCactus fixes this issue by integrating 50 total radios into a single device. This enables the user to cover the vast majority of the Wi-Fi spectrum. This is especially useful when there is a busy environment containing hundreds if not thousands of wireless devices. Due to the far-reaching aspect of wireless technology which is integrated into every part of our lives is important to fully understand the underlying technology. This project provides clarity into what is happening in the air waves around us and demonstrates the need for encryption. Additionally this project has integrated monitoring for Bluetooth as well. Devices used in the #WiFiCactus are Hak5 Pineapple Tetras but a similar project can be accomplished using any Linux compatible radios. This project uses the open source Kismet software to capture and store the data.



更多细节：通常在捕获无线数据以进行故障排除和分析时，使用单个无线电，由于需要跳频，导致大量信息被遗漏。 #WiFi仙人掌 通过将50个无线电收集到一个设备中来解决这个问题。这使用户能够覆盖绝大多数的Wi-Fi频谱。当存在包含数百甚至数千无线设备的繁忙环境时，这是特别有用的。由于集成到我们生活的每个部分的无线技术的深远方面对于充分理解底层技术非常重要。这个项目为我们周围的空中波动发生的事情提供了清晰的信息，并展示了加密的必要性。此外，该项目还集成了蓝牙监控功能。 #WiFi仙人掌使用的设备是Hak5 Pineapple Tetras，但是可以使用任何Linux兼容收音机来完成类似的项目。该项目使用开源Kismet软件来捕获和存储数据。

d4rkm4tter is a mad scientist who likes to hack hardware and software. He is particularly obsessed with wireless. He has a degree in computer science which he has put to use building and breaking a wide variety of systems.

d4rkm4tter是一个喜欢破解硬件和软件的疯狂科学家。他特别痴迷无线。他拥有计算机科学的学位，他已经使用所学来构建并打破各种系统。



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

WORKSHOPS

FRIDAY

	12	15-16	8-9	10-11
14:00-18:00	Mobile App Attack 2.0 Sneha Rajguru	Social Engineering Essentials Valerie Thomas	UAC 0day, all day! Ruben Boonen	Decentralized Hacker Net Eijah

SATURDAY

	12	15-16	8-9	10-11
10:00-14:00	Mobile App Attack 2.0 Sneha Rajguru	Social Engineering Essentials Valerie Thomas	UAC 0day, all day! Ruben Boonen	Decentralized Hacker Net Eijah
14:00-1800	Ncrack and Nmap Paulino Calderon	Scanning the Airwaves Richard Henderson	Practical Malware Analysis: Hands-On Sam Bowne, Devin Duffy-Halseth, & Dylan Smith	Hands-On Exploit Development Georgia Weidman

SUNDAY

	12	15-16	8-9	10-11
10:00-14:00	Ncrack and Nmap Paulino Calderon	Scanning the Airwaves Richard Henderson	Practical Malware Analysis: Hands-On Sam Bowne, Devin Duffy-Halseth, & Dylan Smith	Hands-On Exploit Development Georgia Weidman

UAC 0DAY, ALL DAY!

UAC 0DAY修炼，一天足矣。

Ruben Boonen

This workshop is available to attendees of all levels, however, a basic familiarity with Process Monitor and the Windows API are recommended. The workshop will provide the required knowledge to find, analyze and exploit process workflows which allow an attacker to elevate their privileges from Medium to High integrity. The workshop is divided into the following sections.

Auto-Elevation:
- Identifying auto-elevating processes
- Analyzing process workflows
- Finding UAC bypass targets

Auto-Elevation>Elevated File Operations:
- Using the IFileOperation COM object
- Tricking the Process Status API (PSAPI)

Auto-Elevation>Getting UAC 0day (Pre Windows RS2):
- Analysis of known UAC bypasses
- Understanding the Windows Side-By-Side Assembly
- Creating proxy DLL's
- Using the Bypass-UAC framework
- Dropping 0day(s)!

Auto-Elevation>Triaging Windows RS2:
- Environment variables
- Registry abuse
- COM objects
- Process tokens

The workshop has intense hands-on labs where attendees will put the theory into practice. After

WORKSHOPS

attending, you will immediately be able to apply this knowledge in the field. The next time someone tells you the default UAC settings are sufficient you will be able to set them straight!

只要你对任务管理器和Windows API有基本的认知，就可以参加这个研讨会。本研讨会将会传授攻击者在提权过程中发现、分析与利用相关信息的工作流程，使得攻击者可以将自身在系统的权限从中级向高级提权。 本研讨会分为下列模块：

自动提权：

- 鉴别自动提权进程
- 分析进程工作流程
- 寻找UAC Bypass

自动提权——对文件提权操作：

- 使用the IFileOperation COM 对象
- 欺骗系统状态API（PSAPI）

自动提权——利用UAC 0day（Pre Windows RS2）

- 利用已知UAC Bypass
- 理解Windows Side-By-Side Assembly
- 创建代理DLL文件
- 利用Bypass-UAC 框架
- 发现0days

自动提权——Windows RS2 深入理解

- 环境变量
- 注册表滥用
- COM对象
- 进程Tokens

本研讨会有现场动手实验，可以让与会者将理论付诸实践。参加本研讨会后，你可以将这些知识立即应用在这个领域。下次如果谁告诉你他用默认的UAC配置，你可以立即上手搞定。

My name is Ruben Boonen (@FuzzySec), I have been working in InfoSec since 2012. I have a well-rounded skill set, having taken on many application, infrastructure and bespoke engagements. I have however developed a special interest for Windows: Domain hacking, exploit development, client-side attacks, restricted environments, privilege escalation, persistence, post-exploitation and PowerShell! I love breaking stuff but it is equally important to me to share that knowledge with the wider community. I have previously been a trainer at Black Hat, Def Con and various BSides events in the UK. Additionally, I maintain a InfoSec blog (http://www.fuzzysecurity.com/) where I publish research on a variety of topics!

我的名字是Ruben Boonen (@FuzzySec)，我自2012年起便在InfoSec工作。我拥有全面的技能树，承担了许多应用程序，基础架构和定制的工作。我对Windows也有着特别的兴趣：Domain hacking、exploit development、client-side attacks、 restricted environments、privilege escalation、persistence、post-exploitation 和 PowerShell！

我喜欢搞破坏，但我也喜欢与更广泛的社区分享这些知识。我曾是Black Hat，Def Con和英国各种BSides活动的培训师。另外，我在维护一个InfoSec博客（http://www.fuzzysecurity.com/），在这里，我发布各种研究成果

PRACTICAL MALWARE ANALYSIS: HANDS-ON

恶意软件分析实战：实践

Sam Bowne
Devin Duffy-Halseth
Dylan Smith

Learn how to analyze Windows malware samples, with a hands-on series of projects in a fun, CTF-style environment. There are four levels of analysis challenges.

1. Basic static analysis with file, strings, PEiD, PEview, Dependency Walker, and VirusTotal
2. Basic dynamic analysis with Process Monitor, Process Explorer, RegShot, and Wireshark
3. Advanced static analysis with IDA Pro Free and Hopper
4. Advanced dynamic analysis with Ollydbg and Windbg

The first challenges are easy enough for beginners, and the later ones get difficult enough to interest intermediate security professionals. We will demonstrate the challenges, discuss the technologies and techniques, and help participants get through them as needed.

These challenges use harmless malware samples from the "Practice Malware Analysis" book by Michael Sikorski and Andrew Honig.

All materials and challenges are freely available at samsclass.info, including slide decks, video lectures, and hands-on project instructions. They will remain available after the workshop ends.

在一个有趣的类CTF实践项目里，学习如何分析Windows恶意软件样本。这里有四个层次的分析挑战：

1.使用文件，字符串，PEiD，PEview，Dependency Walker和VirusTotal进行基本静态分析

2.使用Process Monitor，Process Explorer，RegShot和Wireshark进行基本动态分析

3.使用IDA Pro Free和Hopper进行高级静态分析

4.使用Ollydbg和Windbg进行高级动态分析

对初学者来说，第一个挑战是很容易的，后面的则有着足够让中级安全专家们提起兴趣的难度。我们将拆解这些挑战，讨论其中的技术和技巧，并协助参与者完成这些挑战。

这些挑战使用的无害样本来自Michael Sikorski和Andrew Honig所著的《恶意代码分析实战》一书。

所有资料和挑战均可以在samsclass.info上免费获取，包括幻灯片、视频课程和练习项目介绍。这些内容在研讨会结束也会继续提供。

Sam Bowne has been teaching computer networking and security classes at City College San Francisco since 2000. He has given talks and hands-on trainings at DEFCON, HOPE, RSA, B-Sides SF, B-Sides LV, and many other cons. He has a PhD and a CISSP and a lot of T-shirts.

Dylan James Smith Dylan James Smith is a system consultant that now studies and assists with classes as a tutor and TA for Sam Bowne, helping facilitate hands-on workshops at conferences including: BSidesLV/SF, DEF CON, and RSA. Currently tearing things apart and putting them back together while seeking opportunities to practice and teach hacking, or "the cybers" depending on the crowd.

Devin Duffy has assisted Sam Bowne with a hands-on workshop at RSA and other conferences. He's a Script kiddie 4 lyfe.

自2000年起，Sam Bowne便在旧金山城市大学负责计算机网络与安全课程的教学工作。他曾在DEFCON、HOPE、RSA、B-Sides SF、B-Sides LV和很多其他会议上进行主题演讲及实战训练。他拥有博士学位、CISSP认证和一堆T恤衫。

Dylan James Smith 曾协助Sam Bowne在DEF CON、RSA、B-Sides LV和其他会议上举办实战研讨会。他是个Mac大师，擅长解决PC、Linux和网络问题。

Devin Duffy 曾协助Sam Bowne在RSA和其他会议上举办实战研讨会。他可是个 "Script kiddie 4 lyfe"

NCRACK AND NMAP NSE DEVELOPMENT FOR OFFENSE AND DEFENSE

NCRACK和NMAP NSE开发中的攻与守

Paulino Calderon

This workshop will teach participants how to use Nmap, the Nmap Scripting Engine (NSE) and Ncrack to extend the power and capabilities of Nmap. It will cover the basics of the Nmap usage, NSE, and the Lua programming language before diving into how to solve problems by writing custom scripts and modules. By the end of the workshop, you will have in depth knowledge of Nmap, Ncrack, the Nmap Scripting engine and how to develop NSE scripts and Ncrack modules for offensive and defensive tasks. Participants will be provided with a virtual machine that they can use during the training.

本研讨会将向参会者传授如何使用Nmap、Nmap脚本引擎（NSE）和Ncrack来拓展Nmap的应用能力。在编写自定义脚本与模块前，我们会先学习Nmap基本用法、NSE和Lua编程。通过本次研讨会后，你将深入的了解Nmap、NCrack、NSE的相关知识和如何通过开发NSE脚本与Ncrack模块来做攻击与防御。参会者现场可获取到一个培训用虚拟机环境。

Paulino Calderon (@calderpwn) has been in Information Security for more than 10 years. He is the co-founder of Websec, a company offering information security consulting services based in Mexico and Canada. He loves learning new technologies, conducting big data experiments, and developing and destroying software. In 2011 Paulino joined the Nmap team during the program Google Summer of Code to work on the project as a NSE developer. He focused on improving the web scanning capabilities of Nmap and has kept on contributing to the project since then. He has also published 'Nmap 6:Network Exploration and Security Auditing Cookbook' and 'Mastering the Nmap Scripting Engine' covering practical tasks with Nmap and NSE development. He loves attending information security conferences and has given talks and workshops in over 30 events in Canada, United States, Mexico, Colombia, Peru, Bolivia and Curacao.

Paulino Calderon (@calderpwn)已在信息安全领域工作了十多年。他是Websec的联合创始人，Websec是一家在墨西哥和加拿大提供信息安全咨询服务的公司。他喜欢学习新技术，做大数据分析实验，开发和分析软件。2001年，Paulino在Google的Summer ofCode项目里作为一名NSE开发者加入到Nmap团队。他专注于提高Nmap扫描网站的能力，并一直为该项目做贡献。他曾著有《Nmap 6:Network Exploration and Security Auditing Cookbook》和《Mastering the Nmap Scripting Engine》等书，这些书涵盖了Nmap和NSE开发的基础内容。他喜欢参加信息安全会议，曾在加拿大、美国、墨西哥、哥伦比亚、秘鲁等国家超过30个活动里进行主题演讲和开办研讨会。

DECENTRALIZED HACKER NET

去中心化黑客网络

Eijah

As hackers, sometimes we need to send data without anybody knowing anything. We don't want anybody to know what we're sending, so we use encryption. That's the easy part. We also don't want anybody to know that we're sending any data. That's the hard part. The observation of our presence on the network could be enough to get us in trouble. And that's just not acceptable. We need to figure out a way to hide in plain sight.

Creating an environment where data can be sent securely and our presence on the network is hidden, is not an easy thing to do. We can't rely on centralized technologies, which means we need to build a decentralized network. The network should be adaptive and flexible enough to send any type of data to any number of users. But how do we inject anonymity into a network while still supporting the verification of identity between parties? Can we establish trust without having to trust?

This workshop takes you through the process of creating a decentralized network that allows you to circumvent detection by governments and corporations. You'll be able to securely communicate and share data while masking your online identity. You'll create an adaptive, node-based infrastructure where data is shared via Distributed Hash Tables (DHT) backed by real-time asymmetric Elliptic-curve cryptography (ECC). If you've ever wanted to punch a hole through a great (or not-so-great) firewall, this workshop is for you.

Please note that this is a medium-level, technical workshop and requires that attendees have prior experience in at least one programming language, preferably C or C++. Bring your laptop, a USB flash drive, and your favorite C/C++ 11 compiler (>= gcc/g++ 4.9.2 or msvc 2015).

作为一个黑客，有时候，我们需要在任何人都不知道的情况下传输数据。我们不想让别人知道我们传了什么，这时候我们会对数据加密，这还算比较容易。更深入的，我们也不想让别人知道我们在传输数据，这部分就难了。我们在网络上的行为有可能令我们摊上麻烦事，这我们就无法接受了。我们需要找出一种在众目睽睽之下隐匿的方法。

创建一个可以让数据安全传输并隐藏我们上网足迹的环境并不是容易的事。我们不能依赖中心化的技术，这就意味着我们需要构建一个去中心化的网络。这个网络应该具有兼容性和灵活性，以便可以向任意数量用户传输任意类型文件。但是，我们怎样在使用匿名网络的同时仍然可以鉴别双方的身份呢？我们可以在不认证的情况下进行认证吗？

这个研讨会将带你逐步创建去中心化网络，让你远离与公司的监测。你将可以在隐藏在线身份的情况下安全的沟通和分享数据。你将学会创建一个自适应的基于节点的基础架构，其中数据通过分布式哈希表（DHT）共享，该分布式哈希表（DHT）由实时非对称椭圆曲线密码术（ECC）支持。如果你曾想通过一个强势的（可能没那么强势）防火墙，那么这个研讨会很适合你。

请注意，这是一个中等水平的技术研讨会，需要参会者至少熟练使用一种编程语言，最好是C或C++。需要携带笔记本、U盘和你喜欢的C/C++编译器（gcc/g++≥4.9.2或MS VC2015）

Eijah is the founder of Promether and has 20+ years of software development and security experience. He is also the creator of Demonsaw, an encrypted communications platform that allows you to chat, message, and transfer files without fear of data collection or surveillance. Before that Eijah was

WORKSHOPS

a Lead Programmer at Rockstar Games where he created games like Grand Theft Auto V. He has been a faculty member at multiple colleges, has spoken about security and development at DEFCON and other security conferences, and holds a master's degree in Computer Science. Eijah is an active member of the hacking community and is an avid proponent of Internet freedom.

Eijah是Promether的创始人，有二十多年的软件开发和安全经验。他也是Demonsaw的创始人，Demonsaw是一个加密沟通平台，用户可以在无需顾虑隐私或监控的情况下聊天、留言和传输文件。在此之前，Eijah是RockStar Games的首席程序员，他开发了例如“侠盗猎车手5”（GTA V）等游戏。他曾在多所大学任教，在DEF CON和其他安全会议上进行安全与开发相关的主题演讲。Eijah是黑客社区的活跃分子，而且热衷于网络自由。

SCANNING THE AIRWAVES: BUILDING A SIMPLE RADIO SCANNING SYSTEM USING SDR

扫描电波：用SDR建立一个简单的无线电扫描系统

Richard Henderson

Every second of every day, radio communications are flying through the air: shortwave radio, broadcast AM, FM and television, ham radio users. Taxi drivers, buses, parents using small toy radios to keep in touch in amusement parks. Have you ever wondered what's being said over the air? Many of these systems are easily listenable with some basic software and very inexpensive hardware dongles originally designed for capturing over-the-air television broadcasts. This workshop will walk you through the basics of radio systems, how they work, and how you can set up a listening post to decode these systems and listen in. We'll also cover the legalities of listening in, and where to find information online about popular frequencies to listen in on. If you have an SDR stick, please bring one. A number of sticks will be available to borrow for those without.

每时每刻，无线电都在大气中穿梭：短波通讯，AMFM广播，电视，业余无线电爱好者，出租司机，公交车，以及家长通过随身玩具来掌握孩子的位置。你有没有想过这些无线电在大气中会是什么样？有很多无线电是可以通过一些简单的软件和很便宜的电视信号接收器进行监听。这个研讨会将会带你了解无线电系统的基本知识、工作原理，以及如何通过搭建一个监听点对无线电进行解码和监听。我们还会介绍监听的注意事项以及一些比较常见的可以实时监听的信息。你可以借用会议现场的SDR USB存储棒

Richard Henderson is a writer, researcher, and ham radio/electronics nerd who has worked in infosec and technology for well over a decade. Richard is currently co-authoring a book on cybersecurity for ICS/Scada systems.

Richard Henderson不仅是一名作家、研究员，还是一个无线电/电路学业余爱好者，他在信息安全与技术领域已经工作了十多年。Richard目前在协助撰写一本关于在ICS/Scada系统中的网络安全的书籍。

MOBILE APP ATTACK 2.0

移动APP攻击 2.0

Sneha Rajguru

This full-fledged advance hands-on workshop which will get the attendees familiar with the various Android as well as iOS application analysis techniques and bypassing the existing security models in both the platforms. The main objective of this workshop is to provide a proper guide on how the mobile applications can be attacked and provide an overview of how some of the most important security checks for the applications are applied and get an in-depth understanding of these security checks. The workshop will also include a CTF challenge designed by the trainer in the end where the attendees will use their skills learnt during the workshop to solve this challenge.

This workshop will mainly focus on the following :

1. Reverse engineer Dex code for security analysis.
2. Jailbreaking/Rooting of the device and also various techniques to detect Jailbreak/Root.
3. Runtime analysis of the apps by active debugging.
4. Modifying parts of the code, where any part can be specified as some functions, classes and to perform this check or to identify the modification, we will learn how to find and calculate the checksum of the code. Our objective in this section will be to learn, Reverse Engineering an application, get its executable binaries , modify these binaries accordingly, resign the application.
5. Runtime modification of code. Objective is to learn how the programs/codes can be changed or modified at runtime. we will learn how to perform introspection or overriding the default behavior of the methods during runtime and then we will learn how to identify if the methods have been changed). For iOS we can make use of tool Cycript, snoop-it etc.
6. Hooking an application and learn to perform program/code modification.
7. By the end of workshop, based on the course content CTF challenges written by the trainer will be launched, where the attendees will use their skills learnt in the workshop to solve the CTF challenges.

The workshop will begin with a quick understanding on the architecture, file system,permissions and security model of both iOS and Android platform.

Newly designed CTF challenges apps (both Android and iOS apps) will be distributed to the attendees to solve and practice for the mobile app's exploitation.

NOTE:

The tools and techniques used in the workshop are all open source and no special proprietary tools need to be purchased by the attendees for analysis post the training. Some of the tools taught in the training will be helpful in analysis and automating test cases for security testing of the mobile apps:

Drozer, Introspy, Apktool, Dex2jar, Cycript, JD-Gui, SSL Trust killer

这个高阶实践研讨会将引导参会者熟悉各种Android与iOS应用分析技术，并绕过这两个平台现有的安全模块。本次研讨会的主要目标是概述移动应用软件应该怎么攻击以及简要说明应用程序使用的一些重要的安全检查并对其进行深入理解。研讨会的最后还有由讲师设计的CTF挑战，参会者可以通过利用在研讨会里学到的东西去完成挑战。 本研讨会将着重关注以下几点：

1. 逆向分析Dex代码用来做安全性分析
2. 对设备进行越狱/Root并利用多种方法检测越狱/Root状态
3. 对正在运行的软件进行实时分析
4. 修改一部分代码，这些代码可能被识别为一些函数、类，它们会被执行或者被校验完整性。我们将会学到如何计算代码的校验和。这部分的目标是学习逆向一个应用，获取其可执行二进制文件，适当的修改这些二进制文件并对应用重新签名。
5. 运行时修改代码。目标是学习如何在程序运行时修改或更换自身的代码。我们将会学到如何在运行时检查自身代码或在运行时修改自身代码。
6. 在应用程序里挂钩子并学会如何实现程序/代码的修改
7. 在研讨会的结尾，基于本课程，有一个由讲师编写的CTF挑战。参会者可以通过他们刚学到的知识来解决这个CTF挑战。

这个研讨会将对iOS和Android平台的结构、文件系统、权限和安全模组进行快速入门。

新开发的CTF挑战应用程序（Android与iOS平台）将会提供给参会者，该应用适用于学习应用程序的漏洞利用。

注意事项：

在研讨会里使用的工具与技术都是开源的，与会者无需为本次研讨会购买其他特殊软件。培训中教授的一些工具对未来进行移动应用分析与自动化安全测试将有很大的帮助：

Drozer, Introspy, Apktool, Dex2jar, Cycript, JD-Gui, SSL Trust killer

Sneha works as Senior Security Consultant with Payatu Software Labs LLP. Her interests lies in web, mobile application security and fuzzing. She has discovered various security flaws within various open source applications such as PDFLite, Jobberbase, Lucidchart and more. She has spoken and provided trainings at various conferences such as DEFCON, BSides LV, BSidesVienna, OWASP AppSec USA, DeepSec, DefCamp, FUDCon, and Nullcon. Sneha is passionate about promoting and encouraging Women in Security and has founded an initiative called WINJA-CTF through which she hosts women-only CTFs and Workshops at conferences and other events. Sneha is also active in the local security community and hosts local security meetups in Pune. She leads the Pune chapter of null community.

Sneha在Payatu Software Labs LLP任高级安全顾问。她的兴趣包括网络、移动应用安全和模糊测试。她在很多的开源程序中发现了各种安全问题，例如PDFLite、Jobberbase和Lucidchart。她曾在例如DEFCON、BSides LV、BSidesVienna、OWASP AppSec USA、DeepSec、DefCamp、FUDCon和Nullcon等会议上进行演讲并开展研讨会。Sneha致力于促进与鼓励女性进入安全圈，并成立了名为WINJA-CTF的企划，在企划中只有女性参赛者的CTF、研讨会和其他活动。Sneha还活跃在本地的安全论坛，并在Pune举行了安全聚会。

SOCIAL ENGINEERING ESSENTIALS

社会工程概要

Valerie Thomas

Are you a penetration tester in need of social engineering training? Perhaps you just want an understanding of what social engineering is all about. This workshop has something for everyone. First we'll begin with the basics of social engineering and why it works, then dive into non-traditional topics such as spycraft, acting, pressure sales, and the psychology behind them. Next we'll build upon that knowledge to create social engineering attacks. We'll cover the steps of the social engineering process from planning to post-attack including real-world examples. We'll end the day with the basics of appearance hacking and utilizing social engineering in physical penetration testing.

你是需要社会工程培训的渗透测试人员吗？大概你只是想了解社会工程到底是什么吧。这个研讨会对每个人都有用。首先，我们将从社会工程的基础和它如何运作谈起。然后切入到特殊主题如间谍、演技、压力营销和这些行为背后的心理学。接下来我们将利用这些知识去构建社会工程攻击。我们将结合真实案例，从攻击计划开始到攻击完成后的完整流程，逐步介绍社会工程攻击的每一步。我们将以基础社交黑客与利用社会工程进行物理渗透作为今天的尾声。

Valerie Thomas is an Executive Information Security Consultant for Securicon LLC that specializes in social engineering and physical penetration testing. After obtaining her bachelor's degree in Electronic Engineering, Valerie led information security assessments for the Defense of Defense before joining private industry. Her unique Defense and civilian background provides her with a solid understanding of intrusion detection, data loss prevention, and endpoint (in)security. Her electronic and RFID training became a crucial element of her physical security specialization. While some choose to focus on cyber of physical security, she has chosen to exploit the weaknesses of the combination of the two. As an ethical hacker and consultant, she holds multiple industry certifications. Valerie is the coauthor of "Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats" with Bill Gardner. Throughout her career, Valerie has conducted penetration tests, vulnerability assessments, compliance audits, and technical security training for executives, developers, and other security professionals. She has provided briefings and workshops for DEF CON, Derbycon, Blackhat, and multiple BSides events.

Valerie Thomas是Securicon LLC的执行信息安全顾问，专注于社会工程和物理渗透测试。在获得电子工程学士学位后，她在加入私营企业前曾领导国防部的信息安全测评。她独特的国防与民间背景，对她在入侵检测、数据安全和终端安全等方面的理解有着深远的影响。她的电子与RFID训练已经成为她的物理安全专业化课程的一个关键要素。虽然很多人选择专注于物理安全，她选择利用两者的弱点。作为有道德的黑客和顾问，她拥有多个行业认证。Valerie与Bill Gardner合著《Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats》。在她的职业生涯中，她为很多高管、开发人员和其他安全专家进行过多次关于渗透测试、漏洞评估、合规性审计和技术安全培训。她曾在DEF CON、Derbycon、Blackhat和多个BSides活动进行简报和举行研讨会。

HANDS-ON EXPLOIT DEVELOPMENT

动手开发渗透框架

Georgia Weidman

This course will provide a hands-on foundation in discovering and exploiting memory corruption issues. Complex memory corruption issues are discovered in software by security researchers regularly, resulting in bug bounties and exploit sales. In this workshop we will discuss how memory corruption works and gain some experience using the tools of the trade for developing working exploits such as GDB, Immunity Debugger, and Mona.py. Participants will exploit beginner friendly examples of common memory corruption issues allowing students to get familiar with how memory corruption works without getting stuck behind all the latest and greatest anti-exploitation methods. Both Windows and Linux examples will be included. Students will be provided with target virtual machines with vulnerable

WORKSHOPS

software running as well as additional exercises for continued practice after class. By popular demand this course has moved to more modern operating systems, though the bugs used are still beginner friendly. Exploits will be written in the Python programming language but exploit skeletons will be provided for those unfamiliar with the language. This workshop prepares students for future study in vulnerability discovery and exploits development.

这个课程将提供一个关于发掘和利用内存错误的基础实践。安全研究者们经常挖掘到的复杂内存错误问题，并将其提供给漏洞奖励平台或高价售出。在本研讨会上，我们将讨论内存错误是如何发生的以及用一些开发工具去搭建利用环境，例如GDB、ImmunityDebugger和Mona.py。参会者将利用对初学者友好的例子来熟悉常见的内存错误的利用方法，但不会被操作系统中的安全措施干扰。Windows和Linux的例子这里都会讲。学员们将获得一个虚拟机，其中内含有漏洞的软件，可用于课上及课后练习。本课程已升级至较新的操作系统，不过漏洞利用依旧是对新手友好的。渗透脚本是用Python编程语言写的，但是漏洞利用框架还是会提供给不熟悉这门语言的人。这个研讨会将会为学员们未来更深入的学习漏洞挖掘与漏洞利用打下坚实的基础。

Shevirah founder and CTO Georgia Weidman is a serial entrepreneur, penetration tester, security researcher, speaker, trainer, and author. She holds a MS in computer science as well as holding CISSP, CEH, and OSCP certifications. Her work in the field of smartphone exploitation has been featured internationally in print and on television. She has presented or conducted training around the world including venues such as NSA, West Point, and Black Hat. Georgia founded Bulb Security LLC, a security consulting firm specializing in security assessments/penetration testing, security training, and research/development. She was awarded a DARPA Cyber Fast Track grant to continue her work in mobile device security culminating in the release of the open source project the Smartphone Pentest Framework (SPF). She founded Shevirah Inc. to create product solutions for assessing and managing the risk of mobile devices in the enterprise and testing the effectiveness of enterprise mobility management solutions and is a graduate of the Mach37 cybersecurity accelerator. She is the author of Penetration Testing: A Hands-On Introduction to Hacking from No Starch Press. She was the recipient of the 2015 Women's Society of CyberJutsu Pentest Ninja award. She is on the board of advisors of the angel backed security training startup Cybrary and the nonprofit Digital Citizens Alliance and is a member of the CyberWatch Center's National Visiting Committee. She served as a judge for the FTC Home Inspector IoT security challenge.

Shevirah创立者兼首席技术官 Georgia Weidman是位连续创业者、渗透测试人员、安全研究者、讲师、训练家，还有作者。她拥有计算机科学硕士学位，同时还持有CISSP、CEH和OSCP认证。她在智能手机渗透领域的成就已经传遍全球。她曾在世界各地展示或开展培训，例如NSA、西点军校和Black Hat。Georgia成立了Bulb安全公司，一家从事安全评估/渗透测试、安全培训和研发的安全咨询公司。她被授予DARPA Cyber Fast Track大奖，因其在移动安全前沿的持续研究，并发布了开源项目“智能手机渗透框架”（SPF）。她成立了Shevirah公司，评估与管理移动设备的风险，通过测试移动管理解决方案的有效性。并且是Mach37网络安全孵化器的产品。她也是No Starch Press出版的《Penetration Testing: A Hands-On Introduction to Hacking》一书的作者。她获得了2015年Women's Society of CyberJutsu Pentest Ninja大奖。她是安全培训初创品牌Cybrary的天使投资人，非营利组织Digital Citizens Alliance的顾问，也是CyberWatch Center's National Visiting Committee的成员。她曾担任FTC 家庭IoT安全评审的裁判。

soma fm

listener-supported, commercial-free, underground/alternative internet radio broadcasting from San Francisco

网络电台












www.somafm.com

VILLAGES

LOCKPICK VILLAGE

2nd Floor, Room 5
5号会议室
http://toool.us/

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.

想要修补一些你只能在电影中看到的警察，间谍和特务的使用的锁和工具吗？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如何运作以及如何妥协。

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，以及如何利用漏洞的技术，以及练习自行难以尝试的各种级别的锁。

专家将亲自演示并提供大量试用锁，拾取工具和其他设备供您使用。通过探索许多流行的锁具设计中的缺陷和错误，您不仅可以了解开锁这项运动的趣味，还可以获得关于保护自己的财产的最佳方法和实践的更多知识。

AI VILLAGE

3rd Floor, Room 20
20号会议室
https://twitter.com/aivillage_dc

The AI Village at DEFCON is a place where experts in AI and security (or both!) can come together to learn and discuss the use, and misuse, of artificial intelligence in traditional security. Artificial Learning techniques are rapidly being deployed in core security technologies like malware detection and network traffic analysis, but their use has also opened up a variety of new attack vectors against the systems that use them. Using techniques such as Generative Adversarial Networks, would-be attackers could target non-traditional platforms, such as deep learning based image recognition systems used in self driving cars. These same attack methods could be leveraged to extract confidential training data from a deployed model itself, adding another layer of privacy and security risks to an ever-growing list of concerns.

The AI Village will explore these issues and encourage open discussion for possible solutions (and any interesting attacks the attendees can come up with). For those who would rather learn through practice, a practice workshop session will also be available.

Come participate in introductory workshops where you can learn how to use (and misuse!) machine learning models as part of your arsenal. Talks include:

- A discussion of the recently released report on the Malicious Use of AI

- Red-teaming machine learning systems using adversarial techniques

- Vulnerabilities of machine learning tools

DEFCON的AI Village是一个人工智能、安全领域专家们(或两者都包括)一起学习和讨论在传统安全中使用和误用人工智能的地方。人工学习技术正迅速被部署到核心安全技术中，比如恶意软件检测和网络流量分析，但它们的使用也为使用它们的系统开辟了各种新的攻击向量。利用生成的对抗网络等技术，潜在的攻击者可以瞄准非传统的平台，例如用于自驾车的基于深度学习的图像识别系统。可以利用这些相同的攻击方法从已部署的模型中提取机密的培训数据，在日益增长的关注列表中增加另一层的隐私和安全风险。

AI Village将探讨这些问题，并鼓励公开讨论可行的解决方案（包括与会者能提出的任何有趣的攻击）。如果想通过实践去学习，也可以参加实践讲习班。

快来参加介绍性的学习班，在那里你可以学习如何使用(或误用!)机器学习模型成为你自身的一部分实力。主题包括:

-关于近期发布的人工智能恶意使用报告的讨论

-使用抗辩技术的红队机器学习系统

-机器学习工具的弱点

CAR HACKING VILLAGE

Front entrance
https://www.carhackingvillage.com/

Car Hacking Village is an interactive, hands-on village with the goal of teaching village goers what car hacking is, introducing village goers to the tools of car hacking, and working with hackers to create a community of car hackers at DEF CON China.

汽车极客village是一个互动的实践村庄，目标是向参加者讲授汽车极客攻击行为，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

2nd Floor, Room 3
3号会议室
http://reconvillage.org/

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是一个开放空间。包括共同关注侦查的会谈，现场演示，研讨会，讨论，CTF。这个village较适向对开源智能（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意识。

HARDWARE HACKING VILLAGE

Ballroom C
大宴会C厅

https://www.dchhv.org

Come join us for hardware hacking, teaching, learning, and exploration.

Lots of prizes to go around, and lots of puzzles to learn new things or show off your skills.

来加入我们的硬件极客攻击，教学，学习和探索。 有许多奖品可获得，还有许多难题可以用来学习新事物或展示自己的技能。

PACKET HACKING VILLAGE

2nd Floor, Rooms 7-8
7-8 号会议室

https://www.wallofsheep.com/

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，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DEFCON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的建立是为了为了通过培训和安全意识来启发参与者，同时关注红蓝对抗与防御技巧。

BLUE TEAM VILLAGE

3rd Floor, Room 19
19 号会议室

https://twitter.com/BlueTeamVillage

For many, DEF CON epitomizes hacking which traditionally involves an offensive mentality. However, in recent years, attacks have become trivially easy to exploit in any environment meaning that effective defense has been difficult. Defenders have to deal with legacy, politics, and resource constraints and typically have less public information on how to best protect their environment when compared to the red side. This leaves defenders at DEF CON feeling a bit left out with most, if not all, of the content favoring red. This village is a DEF CON paradigm shift providing an area where Blue Teams can gather, learn basic and advanced defensive techniques, swap war stories, and have fun.

Blue Team Village at DEF CON (BTV) promotes defensive security knowledge and its dissemination throughout the greater DEF CON community. At the BTV, you'll find valuable information on defensive security from the very basic 101-level concepts through the latest, most advanced techniques we can get past NDAs. We also have contests, so you can prove your skills in securing systems – and perhaps even show some of those red teamers what's what.

对许多人来说，DEF CON是黑客攻击的缩影，而黑客攻击通常是一种心理攻击。然而，近年来，攻击在任何环境下都很容易被利用，这意味着有效的防御是困难的。防御者必须处理遗留问题、政治问题和资源限制问题，并且在如何更好地保护环境的问题上，与红色方面相比，他们的公共信息通常较少。这样一来，DEF CON的辩护者就会觉得有点不受欢迎了。这个village是一个DEF CON范式转换，它提供了一个蓝色团队可以聚集的区域，学习基本的和先进的防御技术，交换战争故事，并且玩得很开心。

在DEF CON (BTV)的Blue Team Village推广防御性的安全知识，并在更大的DEF CON社区传播。在BTV中，从最基本的101-层概念中通过最新的、最先进的技术能够得到过去的NDAs，进而您将找到关于防御安全性的有价值的信息。我们也有比赛，所以你可以在安全的系统中证明你的技术，甚至可能展示一些红色团队的诀窍。

BIOMETRICS IDENTIFICATION VILLAGE

Ballroom C
大宴会C厅



In biometrics identification village, you will learn how biometric identification technology works. Such technology includes fingerprint, iris, face, and vein recognition etc., You will also learn how to circumvent the authentications based on these biometrics by simply spoofing the sensors. We will bring our hacking methods to the audience by breaking down the sensor devices, capturing and faking the biometric characteristics.

在生物特征识别village，你将看到类似指纹、虹膜、人脸、静脉等常见的生物识别方式是如何工作的，以及如何用及其简单的方法对这些传感器进行欺骗，从而通过验证。我们会通过拆解、捕获特征、制作假特征等展示，通过实际操作，让大家更加直观的感受这一切。

CHIP-OFF VILLAGE

Ballroom C
大宴会C厅

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.

During the chip-off village, visitors shall have an opportunity to remove the embedded emmc chip from the devices and re-solder on the small circuit board. And our experts will demonstrate how to attack the IoT/mobile devices to obtain privilege and gain access control as well as the data stored. We will also introduce some inexpensive JTAG/ISP and chip-off equipments on-site and for your testing.

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。

PRESENTATION SCHEDULE

FRIDAY 星期五

11:30-11:50	Welcome to DEF CON China The Dark Tangent
12:00	Spreading malware with Google (Nice Quilombo) 演讲题目：用谷歌传播恶意软件（Nice Quilombo） Fabian Cuchietti & Gonzalo Sanchez
13:00	You Logged Into My Account 议题名称：你上了我的账号 Daizibukaikou 呆子不开口
14:00	When Memory-Safe Languages Become Unsafe 当内存安全变得不再安全 Mingshen Sun 孙茗珅, Yulong Zhang 张煜龙, & Dr. Wei Tao 韦韬博士
15:00	Lessons Learned from Five Years of Building Capture the Flag 5年搭建CTF上的经验 Vito Genovese
16:00	Triton and Symbolic Execution on GDB Triton 和符号执行在 GDB 上 Weibo Chen 陈威伯
17:00	General ways to find and exploit Path Traversal Vulnerabilities on Android APPs 几种通用的安卓平台路径穿越漏洞的挖掘与利用姿势 Xiaobo Xiang 向小波 (Elphet)

SATURDAY 星期六

10:00	Keynote: Bugs Aren't Random: A Unified Perspective on Building and Breaking 漏洞并非无章可循：建立与打破统一视角 Dan Kaminsky
11:00	Blasted to Bits: Mutilating Media in a Minute 爆炸：一分钟内销毁存储设备 Zoz
12:00-12:20	Fooling Image Search Engine 欺骗图片搜索引擎 Yuanjun Gong 弓媛君, Bin Liang 梁彬, & Jianjun Huang 黄建军
12:30-12:50	Transparent Malware Debugging on x86 and ARM x86和ARM环境下的透明恶意软件分析 Zhenyu Ning 宁振宇 & Fengwei Zhang 张锋巍
13:00	From Memory Safety to Non-bypassable Security 从内存安全到非可越安全范式（NbSP） Dr. Wei (Lenx) Tao 韦韬博士
14:00	Beyond Adversarial Learning — Data Scaling Attacks in Deep Learning Applications 对深度学习系统的数据流攻击 Kang Li 李康
15:00	Security Research Over the Windows (kernel) Peter Hlavaty
16:00	Smart Contract Hacking 智能合约黑客 Konstantinos Karagiannis
17:00	DEF CON Groups Panel Peter Wesley, Tielei Wang王铁磊, Changsheng Gao高昌盛, Xinpeng Liu刘新鹏, Jun Li李均, April C. Wright, & Jayson E. Street
19:00 - 21:00	Live Music

SUNDAY 星期日

10:00	From Dark Visitors to Valued Allies: The Evolution of the Hacker Community in Asia and Around the World! 从灰色访客到重要盟友：论亚洲及全球的黑客社区的演变 Jayson E. Street
11:00	Hacking Intranet from Outside: Security Problems of Cross Origin Resource Sharing (CORS) Dr. Haixin Duan 段海新 & Jianjun Chen 陈建军
12:00-12:20	Passwords in the Air: Harvesting Wi-Fi Credentials from SmartCfg Provisioning 路上Wi-Fi欲断魂：攻击SmartCfg无线配网方案 Changyu Li 李昶蔚 & Quanpu Cai 蔡泉朴
12:30-12:50	I Am Groot: Examining the Guardians of Windows 10 Security 我是格鲁特：Windows 10 的安全护卫队 Chuanda Ding 丁川达
13:00	Androsia: Securing 'Data in Process' for your Android Apps Androsia：保证Android程序中'正在使用的数据'安全 Samit Anwer
14:00	Closing Talk

PRESENTATIONS

ANDROSIA: SECURING 'DATA IN PROCESS' FOR YOUR ANDROID APPS

ANDROSIA：保证ANDROID程序中‘正在使用的数据’安全

Samit Anwer

Each Android app runs in its own VM, with a limited heap size for creating new objects. The Android OS/app doesn't differentiate between regular objects and objects that contain security sensitive information. These critical objects are kept around in the heap until the OS hits a memory constraint. The OS then chooses to invoke garbage collector in order to reclaim memory from the apps. Java does not provide explicit APIs to reclaim memory occupied by objects. This leaves a window of time where the security critical objects live in the memory and wait to be garbage collected. During this window a compromise of the app can allow an attacker to read the credentials. This is a needless risk every Android application lives with today. We propose a tool called Androsia, which performs a summary based interprocedural data flow analysis to determine the points in the program where security sensitive objects are last used (so that their content can be cleared). Androsia then performs bytecode transformation of the app to flush out the secrets resetting the objects to their default values. Attendees will learn: a) why java.security.* APIs for destroying objects are not upto the mark?, b) the key terms used in data flow analysis with live examples and finally, c) how Androsia protects data in process of Android apps?

每个Android程序都运行在自己的虚拟机中，该虚拟机有规定大小的堆内存用于分配新对象。而Android系统并不会区分这些新对象是常规对象或是包含敏感信息的对象。这些包含敏感信息的关键对象会一直驻留在内容中，直到Android系统发现内存不足，然后系统会调用垃圾回收函数用以回收内存给程序使用。Java本身并不提供可以直接回收内存的函数。这就导致在敏感数据被回收释放前会在内存中驻留很长一段时间，而在这段时间中，恶意程序就可能读取这些内存获得敏感信息。目前，所有Android程序都面临着这个不必要的风险。

我们提出了一个名叫Androsia的工具，该工具会通过数据流分析找到包含敏感信息的对象的最后一次使用时间（此后该对象就可以被清理）。进而，Androsia会通过调整该程序的字节码，将包含敏感信息的对象重置为默认值。

参会者可以学到：a)为什么java.security.*中关于销毁对象的APIs远远没有达到要求？b)数据流分析中使用的关键技术。c) Androsia是如何保护Android程序中的敏感数据?

Samit Anwer is a Web/Mobile Application security researcher. Soon after completing his Master's degree from IIIT Delhi in Mobile and Ubiquitous Computing he joined Citrix R&D India as a Product Security researcher.

He is actively involved with vulnerability research in popular Web/Mobile apps and has responsibly disclosed several security vulnerabilities with Google Cloud Print API, XSS filter evasion on IE 11/MS Edge, code execution on Microsoft Windows 10, Microsoft's OAuth 2.0 implementation and buffer overflows on MS Edge/IE 11.

He is an active member of the Null Bangalore Chapter, IEEE community and has spoken on various security topics at BlackHat Asia Singapore (2018), AppSec USA, Orlando (2017), c0c0n X, Kerala (2017), CodeBlue, Tokyo (2017), and Null meets (2015, 2016, 2017)

His technical interests lie in using static program analysis techniques to mitigate security and performance issues on mobile/web apps, breaking web/mobile apps, and researching on cutting edge authentication and authorization mechanisms. His publications can be found here: https://dblp.uni-trier.de/pers/hd/a/Anwer:Samit.

Twitter: @samitanwer1

Samit Anwer是一位Web/Mobile程序安全研究院，毕业于IIIT Delhi的Mobile and Ubiquitous Computing专业，目前在Citrix R&D India任职产品安全研究，从事Web/Mobile程序的漏洞研究。 他多次发现Google，IE，Edge和win10的漏洞，活跃于Null Bangalore Chapter和IEEE community， 并在BlackHat Asia Singapore (2018), AppSec USA, Orlando (2017), c0c0n X, Kerala (2017), CodeBlue, Tokyo (2017), and Null meets (2015, 2016, 2017) 发表议题。他研究方向为使用静态程序分析方法发现Web/Mobile程序的安全问题，部分出版物可以在此处找到： https://dblp.uni-trier.de/pers/hd/a/Anwer:Samit.

TRITON AND SYMBOLIC EXECUTION ON GDB

TRITON 和符号执行在 GDB 上

Weibo Chen
陈威伯

I Introduce the concept of symbolic execution and Triton. (https://github.com/JonathanSalwan/Triton). Detailed steps of how I design and develop SymGDB(https://github.com/SQLab/symgdb). I Will also explain the architecture design, what kind of problem I met, and how to debug when I develope SymGDB. At the end, compare the differences between Triton and other symbolic execution framework.

介绍符号执行的原理和 Triton 框架，详细阐述自己设计和实作 SymGDB(https://github.com/SQLab/symgdb) 的过程，当初如何设计架构，在过程中所遇到的困难，以及如何解决和除错的技巧，在最后，比较其他符号执行的框架。

Weibo Chen, is Co-founder of NCTUCSC(https://www.facebook.com/NCTUCSC/) and member of Bamboofox CTF team. Recently, he got his master degree from National Chiao Tung University. He focuses on symbolic execution and binary exploit. His passion is for security education and security research. He loves to share knowledge with other people.

我的名字是陈威伯 (@bananaappletw)，自大三后开始学习资安，创立交大网路安全策进会(https://www.facebook.com/NCTUCSC/)，也是 Bamboofox CTF team 的成员，最近刚从 SQLab (http://sqlab.cs.nctu.edu.tw/) 毕业，研究的领域是符号执行和二进位胁迫。 致力於教导资安知识以及研究资安技术，这是我们部落格(https://bamboofox.github.io/) 和训练平台(https://bamboofox.cs.nctu.edu.tw/) 的链接，我喜欢和大家分享知识。

SPREADING MALWARE WITH GOOGLE (NICE QUILOMBO)

Fabian Cuchietti
Gonzalo Sanchez

Google products have a good reputation and are synonymous with reasonably high and reliable levels of security. However, in this talk, Fabian and Gonzalo will focus to show a case of how Google Earth will be the vector attack to make an antimalware evasion by a technique of malware injection into memory, and evading the Google Earth sandbox.

Three scopes will be covered during the conference:

- Google Session Hijacking

- Remote Code Execution (Remote Shell)

- Javascript malware execution (Monero Minning)

谷歌产品有良好的声誉，并且是相当高和可靠的安全级别的代名词。然而,在这个演讲中, Fabian和Gonzalo将集中展示谷歌地球如何通过使用恶意软件进行防病毒逃避而成为攻击载体,并逃避谷歌地球沙箱。

这次会议将涵盖三个领域:

- Google Session Hijacking

- Remote Code Execution (Remote Shell)

- Javascript malware execution (Monero Minning)

-谷歌会话劫持

-远程代码执行(远程Shell)

- Javascript执行恶意软件(Monero挖掘)

Fabian Cuchietti (Argentina '90) started in the security world at a very young age. Member of the Hall of Fame of companies such as Google, Facebook, Apple, Microsoft, Mozilla or Paypal. He was one of the first south american members of Synack's Red Team. Since 2015 he has been working as Red Team Member at Internet Security Auditors.

Gonzalo Sanchez (Spain '81) is Red Team Leader in Internet Security Auditors and is manager of the hacking team of Madrid, Barcelona and Bogotá.

Fabian and Gonzalo meet at ISEC Auditors and are working together building crazy big things.

Fabian Cuchietti （人名）(阿根廷90年)年轻时就加入到安全领域中。是名人堂公司如谷歌,Facebook,苹果,微软, 摩斯拉或贝宝的成员。他是南美Synack红队早期的成员之一。自2015年以来,他一直以红队成员身份在互联网安全审计工作。

Gonzalo Sanchez (西班牙81年)以红队leader身份加入到互联网安全审计中,并且是马德里,巴塞罗那和波哥大黑客团队的负责人。

Fabian与Gonzalo同ISEC审计员们一起在做一些伟大而疯狂的事情。

YOU LOGGED INTO MY ACCOUNT

议题名称：你上了我的账号

Daizibukaikou
呆子不开口

This topic describes some ways for inducing victims to log into an attacker's account on the Internet, which can result in some vulnerabilities and attack scenarios.Meanwhile, this topic will also mention how to fix it.This kind of security risk is often overlooked, while it can provide important help for some use of vulnerabilities, even combining some of the low-risk vulnerabilities or features of CSRF, selfxss, OAuth, and SSO, etc. to steal login credentials, bind third-party backdoors accounts, steal privacy, access others' resources, conduct phishing attacks and implement fraudulent use of identity, etc.

本议题介绍了一些互联网上诱导受害者登录攻击者账号的方式，以及由此产生的一些漏洞和攻击场景，同时也会聊聊如何修复此类问题。这种安全风险往往被人忽视，但它可以给某些漏洞利用过程提供重要的帮助，甚至结合csrf、selfxss、oauth、sso的一些低危漏洞或特性可以形成盗取登录凭证、第三方后门账号、窃取隐私、钓鱼攻击、盗取资源、冒用身份等攻击。

Network ID: Daizibukaikou. He is skillful in web security and once worked for Internet companies such as Sina, Nokia, Meituan, and Xiaomi on information security. He is currently working for Antfin as a security expert, and is responsible for the system and network security.

网名: 呆子不开口，熟悉web安全，曾任职于新浪、诺基亚、美团、小米等互联网公司从事信息安全工作。现任蚂蚁金服安全专家，负责蚂蚁金服系统网络安全。

I AM GROOT: EXAMINING THE GUARDIANS OF WINDOWS 10 SECURITY

我是格鲁特: WINDOWS 10 的安全护卫队

Chuanda Ding
Tencent Security Xuanwu Lab
丁川达
玄武实验室的高级研究员

Being one of the main targets of 3 Pwn2Own competitions, Microsoft Windows 10, along with Microsoft Edge, is proven more and more difficult to exploit.

Now Windows 10 has been released for more than 2 years, Microsoft has been constantly updating the security mitigations integrated with the operating system. After 5 major releases, multiple levels of protections have been added to prevent a programming error from turning into a full system compromise.

You may have heard many of them marketed as "Guards" under the Windows Defender brand. But how do they actually work?

As Pwn2Own participants (and winners), we closely watched Windows 10 security evolve over the years.

In this talk, you will get a behind-the-scene view of Windows 10 security mitigation implementations, how it helped make attackers' life harder, and how the attackers overcame it.

作为连续三届Pwn2Own竞赛的目标，Windows 10以及Microsoft Edge的漏洞利用的难度越来越高了。

PRESENTATIONS

现在Windows 10已经发布2年了，微软持续为其增加新的安全防护机制。在它的5个大版本里，增加了多层防护以避免编程错误被利用而造成系统沦陷。

你可能听说了其中的某些防护机制被放进Windows Defender品牌来宣传。但它们实际上是如何工作的?

我们身为Pwn2Own参与者（和获胜者），紧跟着这些年Windows 10安全进化的步伐。

在这个演讲里，你将看到Windows 10安全防护机制的幕后实现，它如何让攻击者的工作更艰难，以及攻击者如何绕过他们。

Chuanda Ding is a senior security researcher at Tencent Security Xuanwu Lab, conducting research on Windows security.

He spoke at CanSecWest 2016, QCon Beijing 2016 and CanSecWest 2017.

Twitter: @XuanwuLab

丁川达 是腾讯安全玄武实验室的高级研究员，负责Windows安全研究。

他曾在CanSecWest 2016、QCon 北京 2016 和CanSecWest 2017演讲。

HACKING INTRANET FROM OUTSIDE: SECURITY PROBLEMS OF CROSS ORIGIN RESOURCE SHARING (CORS)

Dr. Haixin Duan
Professor, Institute for Network Science and Cyberspace, Tsinghua University

Jianjun Chen
PhD student, Tsinghua University

段海新
教授就职于清华大学网络研究院

陈建军
清华大学网络研究院博士研究生

The default Same Origin Policy essentially restricts access of cross-origin network resources to be “write-only”. However, many web applications require “read” access to contents from a different origin, so developers have come up with workarounds, such as JSON-P, to bypass the default Same Origin Policy restriction. Such ad-hoc workarounds leave a number of inherent security issues. CORS (cross-origin resource sharing) is a more disciplined mechanism supported by all web browsers to handle cross-origin network accesses. In this talk we present our empirical study about the real-world uses of CORS. We find that the design, implementation, and deployment of CORS are subject to a number of new security issues: 1) CORS relaxes the cross-origin “write” privilege in a number of subtle ways that are problematic in practice; 2) CORS brings new forms of risky trust dependencies into web interactions; 3) CORS is generally not well understood by developers, possibly due to its inexpressive policy and its complex and subtle interactions with other web mechanisms, leading to various misconfigurations. Finally, we propose protocol simplifications and clarifications to mitigate the security problems uncovered in our study.

出于安全的目的，Web浏览器的同源策略（Same Origin Policy）限制了跨域的网络资源访问。然而，开发者由于业务的需要许多时候必须访问跨域的资源。跨域资源共享CORS（Cross-Origin Resource Sharing）是目前解决跨域资源访问的最为正规的方案，也得到了所有主流浏览器的支持。然而，我们发现CORS的设计、实现与现实网络中的配置都存在大量的安全问题。本报告介绍我们对现实世界的CORS所做的大规模实证研究，我们发现攻击者可以利用CORS安全漏洞可以绕过防火墙攻击内网二进制服务、利用之前不可利用的CSRF漏洞和获取任意网站敏感的Cookie信息等。此外，我们还对Alex 排名5万的域名下9千多万的网站进行大规模的测量，发现支持CORS的网站中有27.5%的网站存在配置安全风险，其中包括mail.ru、fedex.com、washingtonpost.com以及国内知名的网站和搜索引擎。最后，我们对CORS的设计和部署提出了改进建议以降低风险。

Dr. Haixin Duan is a professor at the Institute for Network Science and Cyberspace, Tsinghua University. He was once a visiting scholar at UC Berkeley and a senior scientist in International Computer Science Institute(ICSI). Dr. Duan has been working on network security for more than 20 years. His recent research interests include protocol security, intrusion detection, underground economy detection and etc. Some of his research results were deployed by industries like Baidu, and published in top security conferences like Security & Privacy, USENIX Security, CCS and NDSS.

Jianjun Chen is a PhD student at Tsinghua University supervised by Prof. Haixin Duan. In 2015, he visited UC Berkeley under the direction of Prof. Vern Paxson. Currently he has published three papers on top security conferences(NDSS, CCS, IEEE S&P). Among them, the NDSS paper on CDN forwarding loop attacks has won the conference’s “Distinguished Paper Award”. It is the first time that a Chinese scholar wins this award as the first author in top security conferences. His research work are not only recognized by the academic community, but also help many well-known industrial companies(eg. AKamai, Cloudflare, Tencent) and open-source software(eg. Squid) to fix multiple severe vulnerabilities.

段海新教授就职于清华大学网络研究院，网络空间安全实验室主任。他在网络安全领域从事科研、教学20多年，近期的研究方向包括网络协议安全、入侵检测、地下经济检测等。他的许多研究成果发表在网络安全国际顶级的学术会议（Security&Privacy、CCS、USENIX Security、NDSS等），曾获NDSS2016年杰出论文奖，并获得中央网信办首届“网络安全优秀人才”奖。网络安全战队蓝莲花联合创始人，网络安全国际学术论坛“InForSec”联合发起人。

陈建军，清华大学网络研究院博士研究生，导师段海新教授，曾师从Vern Paxson 教授加州大学Berkeley做访问研究。主要从事网络安全方向的研究，在网络安全顶级学术会议Security&Privacy、CCS和NDSS上发表三篇学术论文，并获NDSS2016杰出论文奖。他的研究不仅获得了学术界的认可，也帮助许多世界知名的互联网企业（如Akamai、CloudFlare、腾讯等）和开源软件（如Squid等）修复了安全漏洞。

LESSONS LEARNED FROM FIVE YEARS OF BUILDING CAPTURE THE FLAG
5年搭建CTF上的经验

Vito Genovese
Member, Legitimate Business Syndicate
LegitimateBusinessSyndicate会员

Capture the Flag is the ultimate test of hacker skill, and DEF CON is the oldest and most prestigious CTF venue. After five years running DEF CON CTF with Legitimate Business Syndicate, our journey running this series of games has come to a close, but what remain are the lessons we learned along the way.

This presentation will cover topics about all aspects of CTF organization: the history of CTF, building a cross-functional organizing team that sticks together year after year, developing a game infrastructure that handles the onslaught of attacks from players, and the stories behind some of the most difficult CTF challenges ever built.

CTF是对黑客技能的终极测试，而DEF CON是历史最悠久同时也是最负盛名的CTF场地。在Legitimate Business Syndicate合作的DEF CON CTF运行五年之际，虽然我们运营这个比赛的行程到达了尾声，但是我们在这里学到了很多。

这个演讲将涵盖了CTF组织的各方面的主题：CTF的历史，组建多年稳定的跨职能组织团队，建立一个可以承受参赛者猛烈攻击的比赛架构，和一些最难的CTF挑战背后的故事。

Vito Genovese is a founding member of Legitimate Business Syndicate, organizers of DEF CON Capture the Flag from 2013 to 2017. Vito’s work included building infrastructure for distributed software development, designing and building both cloud-based and on-site scoring systems for CTF, visual design and branding of competition materials, picking fonts, sourcing coffee and other beverages, and writing public material for the Legitimate Business Syndicate blog and Twitter accounts.

legitbs.net/

Twitter: @vito_lbs

Vito Genovese 是Legitimate Business Syndicate的初创会员，2013年至2017年DEF CON CTF的组织者。Vito的工作包括分布式软件开发的基础架构构建，设计与构建CTF云端与本地端的计分系统，比赛物料的视觉设计与品牌推广，·选择字体，采购咖啡和其他饮料，并且为”合法商业组织”的博客与推特帐号撰写更新内容。

FOOLING IMAGE SEARCH ENGINE
欺骗图片搜索引擎

Yuanjun Gong
弓媛君

Bin Liang
梁彬

Jianjun Huang
黄建军

Our work brings to light that Content-Based Image Retrieval (CBIR) systems, which are commonly used in image search engines, can be potential attack targets of adversaries. In this work, we present the threat model of evading the CBIRs. Specifically, we focus our work on the SIFT/SURF based CBIRs and propose several algorithms for removing/injecting the key points in images to bypass the algorithms. We apply the RMD algorithm and our algorithm to remove the SIFT and SURF key points respectively. Moreover, we inject SIFT key points into images with our IMD algorithm (inverting the operation of RMD) or surround an image with a frame filled with ‘basic bricks’. We evaluate the algorithms on an image indexing engine VisualIndex with three strategies: removal only, injection only and hybrid. The experimental results show the effectiveness of bypassing the engine. With the algorithms and strategies, we succeed in evading Google Image Search Engine, which can be considered as a black-box CBIR system, while the utility of the image is preserved. We also demo the possibility of source/target attack. To conclude, our work proves the existence of threats to CBIR systems and demonstrates that industrial-level Image Search Engines, such as Google Image Search, are prone to be attacked with adversarial images.

演讲工作揭示了一种新的安全威胁：被用于图片搜索引擎中的基于内容的图像检索系统（CBIR，即”以图搜图”）可能成为潜在的攻击目标。针对基于SIFT/SURF的CBIR系统，我们提出了几种用于移除/注入图片中关键点以绕开检索的算法：通过RMD算法和我们所提出算法来去除SIFT和SURF关键点、应用IMD算法（RMD的逆操作）在图片中注入SIFT关键点和在图片周围添加填充了特殊构造的边框以注入关键点等。基于这些算法我们设计了三种扰动策略：仅移除，仅注入和混合。实验结果表明其能有效地欺骗实验性的图片搜索引擎VisualIndex。利用以上的算法和策略，我们还成功地绕开了Google图片搜索引擎，使得目标图片不能够被”以图搜图”的方式被检索到，同时还保留了图片的可用性。我们的工作表明了CBIR系统确实面临着被绕开的风险，并证明了工业级图片搜索引擎（如Google图片搜索引擎）也容易受到恶意构造的图片的欺骗。

Yuanjun Gong is an undergraduate student at Rennin University of China, majoring in Information Security.

Bin Liang received the Ph.D. degree in Computer Science from Institute of Software, Chinese Academy of Sciences. He is currently a Professor at School of Information, Renmin University of China. His research interests focus on program analysis, vulnerability detection, and Web security.

Jianjun Huang received the Ph.D. degree in Computer Science from Purdue University. He is currently an Assistant Professor in Renmin University of China. He is now focusing on detecting vulnerability in destktop/mobile/Web applications.

弓媛君：中国人民大学信息学院信息安全专业本科生，即将开始攻读博士学位。

梁彬：中国人民大学信息学院教授，博士毕业于中国科学院软件研究所，研究方向为程序分析、漏洞检测和Web安全。

黄建军：中国人民大学信息学院计算机系讲师，博士毕业于博士美国普渡大学，研究方向为桌面/移动/Web应用程序中的漏洞检测。

SECURITY RESEARCH OVER THE WINDOWS (KERNEL)

Peter Hlavaty
Senior Security Researcher at Keenlabs Tencent

Past several years Microsoft Windows undergo lot of fundamental security changes. Where one can argue still imperfect and bound to tons of legacy issues, on the other hand those changes made important shifts in attacker perspective. From tightened sandboxing, restricting attack surface, introducing mitigations, applying virtualization up to stronger focus even on

PRESENTATIONS

win32k. In our talk we will go trough those changes, how it affects us and how we tackle them from choosing targets, finding bugs up to exploitation primitives we are using. While also empathize that windows research is not only about sandbox, and there are many more interesting target to look for.

过去的几年里MS Windows经历了许多基础的安全性变化，一方面来说这些改变并不完美，无法避免得产生许多遗留问题，另一方面这些改变也让攻击者的视角产生了重要的转变，从更紧密的沙箱，限制攻击面，引入缓解机制，即使在win32k上也启用虚拟化来增强，在我们的谈话中，我们会通过这些变化，它们如何影响我们，我们如和在选择攻击目标，寻找bug直到我们使用的破解手段中来处理这些变化，同时也可以理解windows的研究不仅仅只是关于沙箱，也有许多有趣的目标可以研究

Peter (@zer0mem) is Senior Security Researcher at KeenLab, Tencent. Focusing mainly on sandbox escapes on windows platform, virtualization, and mitigation bypasses. Pwn2Own 2016..2017 winner, frequent speaker at software security conferences like recon, bluehat, zeronights, syscan, and others.

Twitter: @zer0mem

Peter(@zer0mem)是腾讯安全科恩实验室的高级研究员，这几年主要关注Windows平台的沙箱逃逸，虚拟化技术以及漏洞利用缓解的绕过。他是Pwn2Own 2016和2017多个Windows相关项目的冠军，曾多次在RECon, Bluehat, Zeronights, Syscan等国际著名安全峰会上发表演讲。

BUGS AREN'T RANDOM: A UNIFIED PERSPECTIVE ON BUILDING AND BREAKING
漏洞并非无章可循：建立与打破统一视角

Dan Kaminsky
Chief Scientist, White Ops
White Ops首席科学家

It can take looking at a few thousand bugs, but eventually hacking feels like getting really good at telling the same joke, over and over again.

It's OK, the computer still laughs, but why isn't software engineering delivering the reliability and predictability of other engineering disciplines?

That's a question with an answer. It's not an easy answer, like "devs are lazy" or "tools are bad". Who are hackers to complain about either? But it's an answer I intend to explore, in true hacker fashion, by seeing traditional boundaries as mostly false, but useful for identifying what to fuzz.

Why should we separate the humans that write bugs, from the tools the tools they use? Humans write tools. Why these tools in particular?

Why would we separate forward and reverse engineering, dev from test? Wait, are those the same thing? Does any other field isolate the creator from the consequences of their creation?

Is this going to be just some fluffy exploratory keynote? No, this is way too long a flight for that. We're going to talk about where I think software and hardware architecture is going to go, with actual code you're welcome to try to break. I'll tell you exactly where to look.

Should be fun.

也许你看过数千个漏洞，但是hacking这些漏洞的感觉却很搞笑，像是开了无数次的同一个玩笑。还好吧，计算机一直都认为这个玩笑很有意思。为啥软件工程不能像其他学科一样，提供稳定可靠、风险可控的服务呢？

这个问题是有答案的，但是答案不是很简单，例如“开发就是偷懒”或者“工具都是垃圾”。都是谁在吐槽这些答案呢？这个问题的答案将是我们的主题：通过观察传统的错误然后去找到真正有价值的问题。

为啥我们应该将写bug的人与他们使用的工具拆开处理呢？因为是人类写了工具。为啥这些工具特别重要？

为什么我们要分开正向与逆向工程和开发测试呢？等等，这些是类似的事情吗？有其他领域会把创造者与被创造的工具拆分开吗？

难道我们只是要根据主题闲聊吗？不，这要说的太长了。我们将会去讨论我认为软件和硬件应该何去何从，并结合实际代码进一步说明。我会告诉你他们的真正意义。

祝你尽兴。

Dan Kaminsky has been hacking professionally for almost twenty years. A well known speaker at conferences such as Black Hat and Defcon, Dan is the Co-Founder and Chief Scientist of White Ops, and is one of seven Recovery Key Shareholders for the Internet's Domain Name System. Dan's research spans a wide variety of topics, but he gets the coolest emails from kids who use his iPhone app to correct their color blindness. It's called DanKam, because of course it is, and he's telling you this so he has to get it back on the iPhone store already.

Twitter: @dakami

Dan Kaminsky 近20年来在黑客攻击领域很专业。作为例如DEF CON和Black Hat等会议上都是很知名的讲师，Dan是White Ops的联合创始人兼首席科学家，并是互联网末日重启计划的七人之一。Dan的研究领域很宽广，但是他认为最酷的成就是获得了色盲孩子通过iPhone发送的彩色邮件。这个软件叫DanKam，正因为这样，他才将这个软件重新带入iPhone应用商城。

SMART CONTRACT HACKING

Konstantinos Karagiannis
CTO, Security Consulting, BT Americas

Smart contract hacking always makes headlines. Typical incidents can cost millions or even hundreds of millions in losses. And the problem doesn't seem to be going away. Recent independent scans show 34,200 vulnerable smart contracts lurking on the Ethereum blockchain. It's time to help these developers secure their code and foster a new generation of hardened SDLC practices. Ethereum has fantastic Turing-complete functions awaiting our use, and Solidity smart contracts are a crucial way that the Enterprise Ethereum Alliance, Quorum, and other entities plan on moving to Web 3.0. Ethical hacking of all this new code is a necessary service and excellent way to cash in (ethically).

Join Konstantinos for a look at a Solidity hacking methodology that can be applied right away, including the latest open source tools.

智能合约黑客经常会成为头条。典型的事故可以造成数百万甚至上亿的损失，并且问题似乎并没有解决。最近的独立扫描显示34200弱势智能合约潜伏在以太坊区块链。是时候帮助这些开发人员确保他们的代码安全和培养新一代的硬化SDLC实践。以太坊有着神奇的图灵完整功能等待我们使用，可靠性智能合约是企业以太坊联盟, Quorum和其他实体计划迁移到Web 3.0的一种重要方式。这些道德入侵的新代码是兑现的一个必要服务和优秀方式 (从道德观上讲)。

从Konstantinos那里可以了解下可以立即应用的可靠性黑客方法,包括最新的开源工具。

Konstantinos Karagiannis is the Chief Technology Officer for Security Consulting at BT Americas. In addition to guiding the technical direction of ethical hacking and security engagements, Konstantinos specializes in hacking financial applications, including smart contracts and other blockchain implementations. He has spoken at dozens of technical conferences around the world, including DEFCON, Black Hat Europe, RSA, and ISF World Security Congress.

Twitter: @konstanthacker

Konstantinos Karagiannis（人名同上）是安全咨询在BT美洲的首席技术官。除了指导道德黑客的技术方向和安全活动,Konstantinos专门从事黑客金融应用程序,包括智能合同和其他区块链实现。他已经在世界各地的数十场技术会议中发言,包括黑客大会、欧洲黑帽,RSA和安全部队世界安全大会。

BEYOND ADVERSARIAL LEARNING · DATA SCALING ATTACKS IN DEEP LEARNING APPLICATIONS
对深度学习系统的数据流攻击

Kang Li
Director, Institute for Cybersecurity and Privacy, University of Georgia
李康

In this presentation the speaker will demonstrate attacks that target the data scaling process in popular deep learning examples. By carefully crafting input data that mismatches with the scales used by deep learning models, the speaker will show how an attacker can successfully evade image classification even when applications use well-trained deep learning models. The speaker will also present a few potential defending strategies to detect or mitigate such data-flow attacks.

此次演讲将展示对深度学习系统的数据流攻击。 通过改变输入数据的维度特性，攻击者可以针对深度学习的数据处理进行攻击，对深度学习图像识别等应用造成逃逸攻击和数据污染攻击的效果。演讲也会介绍对这类攻击的基本防御方法以及相关工具。

Kang Li is a professor of computer science and the director of the Institute for Cybersecurity and Privacy at the University of Georgia. His research results have been published at academic venues, such as IEEE S&P, ACM CCS and NDSS, as well as industrial conferences, such as BlackHat, SyScan, and ShmooCon. Dr. Kang Li is the founder and mentor of multiple CTF security teams, including SecDawg and Blue-Lotus. He is also a founder and player of the Team Disekt, a finalist team in the 2016 DARPA Cyber Grand Challenge.

李康是美国乔治亚大学计算机终身教授，目前担任乔治亚安全与隐私学院院长。主要关注的研究方向包括系统和网络安全，成果在IEEE S&P, ACM CCS，NDSS等多个学术会议上发表。李康也多次受邀在 BlackHat，SyScan，ShmooCon 等国际黑客会议上发表演讲。 李康曾参与创建多只CTF战队，他是清华蓝莲花战队的启蒙导师。他组建的Disekt战队在2016年网络自动攻防超级对抗赛CGC中闯入决赛。

PASSWORDS IN THE AIR: HARVESTING WI-FI CREDENTIALS FROM SMARTCFG PROVISIONING
路上WI-FI欲断魂：攻击SMARTCFG无线配网方案

Changyu Li
李昶蔚
Quanpu Cai
蔡泾朴

Smart devices without an interactive UI (e.g., a smart bulb) typically rely on specific provisioning schemes to connect to wireless networks. Among all the provisioning schemes, SmartCfg is a popular technology to configure the connection between smart devices and wireless routers. Although the SmartCfg technology facilitates the Wi-Fi configuration, existing solutions seldom take into serious consideration the protection of credentials and therefore introduce security threats against Wi-Fi credentials.

We conduct a security analysis against eight SmartCfg based Wi-Fi provisioning solutions designed by different wireless module manufacturers. Our analysis demonstrates that six manufacturers provide flawed SmartCfg implementations that directly lead to the exposure of Wi-Fi credentials: attackers could exploit these flaws to obtain important credentials without any substantial efforts on brute-force password cracking. Furthermore, we keep track of the smart devices that adopt such Wi-Fi provisioning solutions to investigate the influence of the security flaws on real world products. Through reversely analyzing the corresponding apps of those smart devices we conclude that the flawed SmartCfg implementations constitute a wide potential impact on the security of smart home ecosystems.

伴随着家庭智能化的趋势，大量传统家居装置开始逐步升级为可以无线接入互联网的智能家居设备。为了协助这些缺少输入接口的设备（如智能洗衣机，智能门锁）认证并接入加密无线网络，无线芯片供应商设计了各种配网方案，用以传输Wi-Fi密码及SSID，无线配网也成为智能家居生态系统中的代表性应用场景之一。

PRESENTATIONS

作为一类广为流行的配网方案，SmartCFG为诸多无线芯片提供了自动化获取Wi-Fi密码并连接到无线网络的功能。不幸的是，这类方案从设计到实现往往都忽视了安全保护，在攻击者面前往往显得极为脆弱。我们深入分析了市场上八家主流无线芯片供应商所提供的SmartCFG方案，发现其中六款方案存在严重安全隐患：攻击者无需接入受保护的无线网络（WPA2/WPA/WEP）即可解密所传输的Wi-Fi密码！我们进一步大规模扫描了常见智能家居设备并分析了那些使用SmartCfg方案的设备的对应代码实现，发现有三分之二的实现方式可被利用（甚至在所集成SmartCFG方案原本足够安全的情况下，部分设备仍然因为实现中的密码学误用而破坏了安全性）。分析表明，现有SmartCFG方案的配网安全性防护亟需增强。

Changyu Li graduated from Xidian University with the major of Information Security. After graduated, he continues studying at Shanghai Jiao Tong University, focusing on software security. He is now a member of Lab of Cryptology and Computer Security (LoCCS). He takes an interest in the security and privacy of Internet of Things; especially, smart home. Also, he is a big fan of CTF games.

Quanpu Cai, a undergraduate student at Shanghai Jiao Tong University with the major of Cyber Security, now as a member of Lab of Cryptology and Computer Security (LoCCS). His interest covers a large span of security, including reversing and exploiting, mainly related to the area of Internet of Things.

李昶蔚 本科毕业于西安电子科技大学信息安全专业， 毕业后保送为上海交通大学密码与计算机安全实验室（LoCCS）硕士研究生，就读期间的研究方向包括智能设备的私有协议分析，智能设备的软件安全分析等。他还热衷于参加CTF竞赛，曾多次在安全竞赛中获得优异成绩。

蔡淦朴, 上海交通大学网络安全专业大三本科生，现为上海交通大学密码学与计算机安全实验室（LoCCS）成员。 研究兴趣涵盖了一系列安全相关的领域，主要包括软件及嵌入式设备逆向工程及漏洞利用，尤其是物联网安全领域。

TRANSPARENT MALWARE DEBUGGING ON X86 AND ARM
X86和ARM环境下的透明恶意软件分析

Zhenyu Ning
Ph.D. candidate, Wayne State University
宁振宇
韦恩州立大学计算机系助理教授
Fengwei Zhang
Assistant Professor, Wayne State University
张锋巍
韦恩州立大学系统安全方向博士研究生

With the rapid proliferation of malware attacks on the Internet, understanding these malicious behaviors plays a critical role in crafting effective defense. Existing malware analysis platforms leave detectable fingerprints like uncommon string properties in QEMU, signatures in Linux kernel profiles and artifacts on basic instruction execution semantics. Since these fingerprints provide the malware a chance to split its behavior depending on whether the analysis system is present or not, existing analysis systems are not sufficient to analyze the sophisticated malware. In this talk, we present the framework for transparent malware analysis, which leverages the hardware features in existing PC and mobile devices to increase the transparency of malware analysis. In particular, we introduce MalT on the x86 architecture and Ninja on the ARM architecture. MalT uses the system management mode as the execution environment and performance monitor unit as hardware assistant to facilitate the analysis, whereas Ninja involves the TrustZone technology and embedded trace macrocell to improve the transparency. Moreover, both MalT and Ninja are OS-agnostic, and do not require modification to the operation system or the target application.

近年来，恶意软件攻击对网络的威胁日益严重，而分析这些恶意软件的行为对有效地防御这些恶意软件有着至关重要的作用。现有的恶意软件分析系统在分析环境中留存了很多可被检测到的痕迹，如QEMU环境下的不正常的字符串属性，Linux内核配置文件中的残留痕迹，以及基础执行时语义上的差别。而恶意软件可以通过检测这些痕迹来确定分析系统是否存在，并根据自身是否被监控来做出不一样的反应。因此，现有的恶意软件分析系统并不足以用来分析这类复杂的恶意软件。而我们利用PC和移动设备上广泛存在的硬件特性来构建一个恶意软件分析框架，并利用该框架来提高恶意软件分析的透明度。具体来说，我们在x86架构中设计了MalT系统，在ARM架构中提出了Ninja系统。其中，MalT系统将系统管理模式(SMM)作为运行环境，并利用性能监控单元(PMU)这一硬件特性来辅助进行恶意软件分析，而Ninja系统则利用可信区域(TrustZone)技术以及嵌入式跟踪宏单元(ETM)来提高系统的透明度。值得一提的是，MalT系统和Ninja系统都与我们通常使用的操作系统无关，无需对操作系统或是目标恶意软件进行任何修改。

Zhenyu Ning is a Ph.D. candidate with the Computer Science Department at Wayne State University. He received his master degree in computer science from Tongji University in 2011. His research interests are in the areas of hardware-assisted system security, embedded systems, and trusted execution environments.

Twitter: @Hackin9

Fengwei Zhang is an Assistant Professor with the Computer Science Department at Wayne State University. He received his Ph.D. degree in computer science from George Mason University in 2015. His research interests are in the areas of systems security, with a focus on trustworthy execution, transparent malware debugging, transportation security, and plausible deniability encryption. He is a recipient of the Distinguished Paper Award in ACSAC 2017.

From Dark Visitors to Valued Allies: The Evolution of the Hacker Community in Asia and Around the World!

宁振宇，韦恩州立大学系统安全方向博士研究生。2011年于同济大学获得计算机应用硕士研究生学位，曾就职于华为、银联等企业。主要研究方向为硬件辅助的系统安全，嵌入式系统以及可信执行环境。

张锋巍，韦恩州立大学计算机系助理教授。2015年于乔治梅森大学取得博士研究生学位。主要研究方向为系统安全，可信计算，透明恶意软件分析，交通系统安全，以及可否认加密技术。曾获ACSAC 2017杰出论文奖。

FROM DARK VISITORS TO VALUED ALLIES: THE EVOLUTION OF THE HACKER COMMUNITY IN ASIA AND AROUND THE WORLD!
从灰色访客到重要盟友: 论亚洲及全球的黑客社区的演变

Jayson E. Street

Jayson E. Street will take the attendees on a journey through time and around the world. Exploring one of the most difficult questions that faces our community. What is a Hacker? He'll focus on famous Chinese hackers throughout history and how we all connect through a global community. Be prepared to have your beliefs challenged and hopefully some questions answered.

Jayson E. Street is an author of the "Dissecting the hack: Series". Also the DEF CON Groups Global Ambassador. Plus the VP of InfoSec for SphereNY. He has also spoken at DEF CON, DerbyCon, GRRCon and at several other 'CONs and colleges on a variety of Information Security subjects. *He was a highly carbonated speaker who has partaken of Pizza from Beijing to Brazil. He does not expect anybody to still be reading this far but if they are please note he was chosen as one of Time's persons of the year for 2006.

Twitter: @jaysonstreet

Jayson E. Street是《Dissecting the hack系列》图书的作者之一，同时他也是DEF CON团队的全球大使，SphereNY的信息安全副总裁。他曾在DEFCON、DerbyCon、GRRCon、各种其他CON和学校里进行关于信息安全的各种主题演讲。*他是一名高度依赖碳酸饮料的演讲者。从北京到巴西，他到处分享披萨。他从不期待有人会读到这部分，不过如果有人看到了，请注意，他曾经被选为时代周刊2006年的年度人物。

WHEN MEMORY-SAFE LANGUAGES BECOME UNSAFE
当内存安全变得不再安全

Mingshen Sun
孙茗珅
Researcher, Baidu X-Lab
Yulong Zhang
张煜龙
Senior Staff Security Scientist, Baidu X-Lab
Dr. Wei Tao
韦韬博士
Chief Security Scientist, Baidu

Fatal bugs introduced by non-memory-safe languages (C/C++/etc.) are one of the oldest yet persistent problems in computer security. To alleviate this issue, there has been an emerging trend to re-implement programs using memory-safe languages (Rust/Go/Swift/etc.). By using such languages, developers usually have an illusion that they have obtained 100% guarantees of type soundness, memory-safety, and thread safety.

However, through our assessment of a wide range of open-source projects, we found that this assumption is not correct and sometimes can lead to dangerous consequences. We collected and analyzed more than 10,000 Rust programs. All of these programs rely on libc, and at least 25% depend on extra unsafe C/C++ libraries. These libraries break Rust's memory-safety promise and also expose users to great threats. Unfortunately, the inclusion of C/C++ libraries are agnostic to developers, leaving the issue unnoticed. What's more, some of the C/C++ libraries are statically linked. This leads to fragmentation and makes it challenging to carry out a scalable patching.

Even if a program is fully developed using memory-safe languages, memory security issues can still occur. Rust allows developers to write unsafe code using "unsafe" keyword, but some libraries wrap unsafe code and re-export as "safe" functions. If developers use these "safe" functions, they are not aware of the unsafety introduced by these libraries. Moreover, we will show that some of the memory-safe languages fail to zero-out memory regions on object destruction, which can lead to secret memory leakages.

To illustrate the real-world threats, we will provide a few detailed case studies and live demos where programs developed by memory-safe languages can still be exploited via memory bugs. Finally, we will offer suggestions and provide tools for developers/users to achieve a sustainable ecosystem.

由非内存安全的编程语言（例如 C 和 C++ 等）带来的致命 bug 是计算机安全史上最古老、最长久的安全问题。近年出现了使用内存安全语言（例如 Rust、Go、Swift 等）重构安全要求高的组件的趋势。但是开发者在使用这些语言的时候会有一种错觉：认为只要用这些语言编写的程序就能 100% 保证类型安全、内存安全以及线程安全。

但是我们的研究表明上述假设并不成立，并且有可能导致危险的后果。我们收集并分析了 10,000 个使用 Rust 编写的程序或库。我们发现几乎所有的 Rust 程序都依赖 libc 库，并且至少 25% 的 Rust 库都依赖其它 C/C++ 的库。这些库破坏了 Rust 的内存安全特性，暴露了一些潜在的威胁。更加不幸的是，开发者并不知道程序使用了这些 C/C++ 库，也没有注意这些威胁的存在。除此之外，因为一些静态链接的 C/C++ 库的存在，引起了库依赖的碎片化，使大规模的更新升级更有挑战。

近一步的研究表明，即使完全使用内存安全语言做开发，内存安全问题依然存在。比如，Rust 允许开发者使用 “unsafe” 关键字编写非内存安全的代码以绕过编译器的限制。但是，一些库使用了这些 “unsafe” 代码，并把这些代码重导出为 “安全” 的函数给其它开发者使用。其他开发者使用这些 “安全” 的函数的时候并不知道 “非内存安全” 代码的存在，埋下了内存安全的隐患。

为了说明这些威胁，我们将详细展示几个案例。这些程序使用内存安全代码编写，但是仍然有安全问题的。为了内存安全生态的可持续发展，我们提供了一些使用内存安全语言的建议，并同时给开发者提供工具检测上述问题。

Mingshen Sun is a senior security researcher of Baidu X-Lab at Baidu USA. He received his Ph.D. degree from The Chinese University of Hong Kong. His interests lie in solving real-world security problems related to system, mobile, IoT devices and cars. He maintains and actively contributes to the MesaLock Linux project, a memory-safe Linux distribution.

Twitter: @MingshenSun

https://mssun.me

Dr. Wei (Lenx) Tao is the Chief Security Scientist at Baidu, and Adjunct Professor at Peking University. He was also a co-organizer of the BitBlaze Group in UC Berkeley. His research interest lies in security architecture, programming languages and machine

PRESENTATIONS

learning. Beside defending Baidu against various kinds of attacks, he also initiates, directs and promotes several important open-source security projects of Baidu, such as MesaLock Linux (a memory-safe Linux distribution), Rust SGX SDK, OpenRASP, etc.

孙茗珅博士是百度安全实验室安全研究员，毕业于香港中文大学，研究方向包括系统安全、移动安全、IoT 设备和车辆安全。曾在 CCS，ACSAC 等顶级安全会议上发表论文或演讲。同时，他是 MesaLock Linux 项目（一个内存安全的 Linux 发行版）的维护者。Twitter: @MingshenSun， https://mssun.me

张煜龙是百度安全实验室高级资深研究员，曾在 Black Hat、RSA、USENIX Security、IEEE S&P 等世界各大顶级安全会议上发表论文或演讲，被 BBC、CNN、Reuters 等诸多媒体报道，同时还为一系列知名学术会议和杂志审稿。他们还获得过三星、苹果、高通、Google、Pebble等公司的致谢。

韦韬博士是百度首席安全科学家兼北京大学教授，曾组建了 UC Berkeley BitBlaze 小组。他的研究兴趣为安全架构、编程语言、机器学习。他在保护百度免受安全攻击的同时发起了几个重要的开源安全项目，比如说 MesaLock Linux 项目（一个内存安全的 Linux 发行版），Rust SGX SDK，Open RASP 等。

FROM MEMORY SAFETY TO NON-BYPASSABLE SECURITY

从内存安全到非可越安全范式（NBSP）

Dr. Wei (Lenx) Tao
Chief Security Scientist at Baidu, and Adjunct Professor at Peking University

韦韬博士
百度首席安全科学家.北京大学兼职教授

Security researchers and engineers have worked hard for decades to protect software written in memory unsafe languages like C or C++, but real world exploits show that all currently deployed protections can be defeated. Therefore, memory safe programming languages like Rust or Go get more and more attention. However, there is still a significant gap between memory safety and formal verification – i.e. memory safety cannot guarantee that your software is vulnerability-free, and formal verification for general software is still too complex to be adopted widely.

In this talk, we propose Non-bypassable Security Paradigm (NbSP), which bridges memory safety and formal verification. The "Non-bypassable" property was introduced by MILS (Multiple Independent Levels of Security/Safety) and it requires that one component cannot use another communication path, including lower level mechanisms to bypass the security monitor. NbSP combines program analysis and specifications to ensure that critical check points are non-bypassable. In this way, NbSP reduces attack surfaces significantly, and makes it practical for either detailed manual inspection or further formal verification of authentication, authorization and auditing.

安全界花费了数十年的努力来试图保护那些用C/C++等非内存安全语言编写的系统，然而每年Pwn2Own残酷的现实显示这些防护都是可以被绕过的。因此Rust, Go这样的内存安全语言越来越被业界重视。但内存安全与严格的形式化验证安全之间依然有着一道鸿沟，即内存安全依然无法保障程序是无漏洞的，而通用的严格形式化验证的代价过于高昂导致无法广泛应用。

为此，我们提出非可越安全范式Non-bypassable Security Paradigm (NbSP)。我们认为NbSP范式是内存安全迈向形式化验证安全的一个实用化的关键步骤。”非可越”(Non-bypassable)安全属性是在著名的多重独立安全等级（MILS，Multiple Independent Levels of Security/Safety)中提出。NbSP范式采用模型检验与编程规范相结合的方式来确保内存安全的程序中关键检查点不会被绕过。这样，NbSP范式可以大幅度缩小目标程序的攻击面（Attack Surface），并且使得后继针对认证、授权、审计等关键安全功能的人工审查或者是形式化验证变得可行

Dr. Wei (Lenx) Tao is the Chief Security Scientist at Baidu, and Adjunct Professor at Peking University. He was also a co-organizer of the BitBlaze Group in UC Berkeley. His research interest lies in security architecture, programming languages and machine learning. Beside defending Baidu against various kinds of attacks, he also initiates, directs and promotes several important open-source security projects of Baidu, such as MesaLock Linux (a memory-safe Linux distribution), Rust SGX SDK, OpenRASP, etc.

韦韬博士，百度首席安全科学家，百度安全实验室负责人，北京大学客座教授，也曾是UC Berkeley BitBlaze的联合组织者。他的研究领域主要涉及安全体系结构、编程语言及机器学习等。他提出的安全防护方案推动着诸如微软、谷歌、百度等全球顶尖科技公司安全防护水平的提升；他发现的Android和iOS上的安全隐患避免了上亿的用户财产及安全损失。在为百度抵御各种形式的攻击之外，他还发起、指导和推动百度的几个重要的开源安全项目，如Mesalock Linux（内存安全的Linux发行版），Rust SGX SDK，OpenRASP等。

GENERAL WAYS TO FIND AND EXPLOIT PATH TRAVERSAL VULNERABILITIES ON ANDROID APPS

几种通用的安卓平台路径穿越漏洞的挖掘与利用姿势

Xiaobo Xiang (Elphet)
向小波 (Elphet)

Directory traversal vulnerabilities are very common in Android applications. This is also a place that developers ignore easily. Directory traversal vulnerabilities are also very harmful because it can break the application sandbox mechanism of Android.

In this paper, we will introduce the research of directory traversal vulnerabilities on the Android platform. from the aspects of what it is, how to find them, what they will cause and how to exploit them. We will explain these contents in a practical way.

安卓应用在进行文件读写时，对于文件名的完整校验是开发者常常容易忽视的地方，如果攻击者可以通过一些手段控制应用读写的文件名，则可能发生路径穿越漏洞。

路径穿越漏洞是一类品相很好的漏洞，其直接的效果可以突破应用沙箱，进行沙箱内的文件读写，而由于国内安卓生态的乱象、国内安卓应用功能的繁杂，再加上安卓系统本身的一些有趣的特性，致使路径穿越漏洞在一定程度上可以最终达到账号劫持、拒绝服务、甚至克隆攻击与远程任意代码执行的效果。本议题将从此类漏洞的原理出发，结合多个实际的例子，分享从何种业务场景入手挖掘并验证该类漏洞，有哪些通用的漏洞利用技巧，以及如何一步步从路径穿越到任意代码执行。

Xiaobo Xiang (Elphet) is a security researcher of 360 Alpha Team. He has submitted multiple bugs to Google and several other vendors in China. He is a Doctor Candidate in University of Chinese Academy of Sciences (UCAS), who mainly focuses on Android vulnerability reseach. In his spare time, he is keen on participating CTF games as a pwner in the CTF team NeSE (aka Never Stop Exploiting), which is a well-known separate CTF team in China.

Twitter: @b0b0505

向小波（Elphet）是360阿尔法团队的安全研究员，曾多次给谷歌以及国内厂商提交相关漏洞。当前正在中国科学院信息工程研究所攻读博士学位，其研究方向为安卓系统漏洞挖掘与利用，热衷于参加国内外CTF竞赛，是国内知名CTF团队NeSE的pwn选手。

BLASTED TO BITS: MUTILATING MEDIA IN A MINUTE

爆炸：一分钟内销毁存储设备

Zoz

Governments and large organizations all know the importance of destroying retired physical data storage units: the waste stream has the potential to be a major leak of security-relevant information, to competitors, criminal syndicates and the public. Hackers have long appreciated the insights to be gleaned through trashing! But the volumes of data stored today make this process difficult to accomplish instantaneously, and data in the wrong hands is money – or your freedom. If you manage data that might be at risk of physical attack by untouchable agents, could there be a way to ensure its physical destruction in under 60 seconds at the flip of a switch? In this research I investigate multiple paths to forensic-resistant elimination of physical media via thermal, kinetic and high voltage methods. Both magnetic and flash storage devices are investigated, requiring the development of new techniques for high explosives manufacture, delivery and encapsulation, including the use of 3D printing. Surprising results will be presented.

政府和知名大企业都明白销毁作废的物理存储设备的重要性：如果被行业竞争者、犯罪者和公众恶意利用，存储在作废物理设备的数据可能导致严重的安全问题。黑客则很欣赏那些记得及时销毁数据的人。但如今的数据存储量使得销毁数据的过程变得极为漫长，而这些未被销毁的数据落入其他人的手中则代表着金钱或者自由。如果你将数据存储在不可接触的代理商手中，那有没有可能在60秒内保证销毁数据呢？在本议题中，我会讨论磁性存储设备和闪存设备，并提出多种销毁数据的方法，最后展示一些惊人的结果。

Zoz is a robotics engineer, rapid prototyping specialist and lifelong enthusiast of the pyrotechnic arts. Once he learned you could use a flamethrower and a coffee creamer bomb to fake a crop circle for TV he realized there are really no limits to creative destruction.

Zoz 是一名机器人工程师，快速原型设计专家，烟花艺术终身爱好者。一次偶然，他学到可以通过喷射器和咖啡伴侣可以伪造电视里出现过的麦田圈，这时他意识到创造性的破坏是没有止境的。

DEF CON GROUPS PANEL

Peter Wesley
Tielei Wang
王铁磊
Changsheng Gao
高昌盛
Xinpeng Liu
刘新鹏
Jun Li
李均
April C. Wright
Jayson E. Street

Have you ever felt frustrated that the super cool DEFCON only happen once a year in Las Vegas? Visa, flights, time, language, distance are all possible reasons that prevent you from enjoying DEFCON. Well, thanks to DEF CON groups, you're able to carry the spirit of DEF CON with you year round, and with local people, transcending borders, languages, and anything else that may separate us! Most importantly, local DEFCON Groups are the platforms to unite us all to achieve causes, to inspire others, regardless of their background, race.

In this talk, you'll hear from DEF CON's founder Dark Tangent, the Ambassador of DEF CON groups Jayson E. Street, DEFCON GROUP 010 founder Jun Li who is also moderating the panel, DEFCON GROUP 617 founder April C. Wright, DEFCON GROUP 86021 founder Tielei Wang, DEFCON GROUP 86755 founder Peter Wesley, DEFCON GROUP 0571 founder Changsheng Gao, DEFCON GROUP 0531 founder Xingpeng Liu . They will first discuss what is hacking, the spirit of hackers, what are the differences between different hacker communities, what interesting experiences can different groups learn from each other, then they will discuss how hacker spirit is contributing to the society in good ways, discuss how to cultivate the next generation of security professionals (aka hackers), finally they will talk about some future projects they might be able to cooperate on, for example go to the remote areas to inspire kid to learn and use technology to change the world.

Founders of their own local DEF CON groups will also discuss the awesome projects of their groups, as well as projects from other groups, to give ideas to take back to your own DEF CON group. Projects we'll discuss range from custom badge build, IoT devices, vintage gaming systems, custom built routers, smarthome devices and more!

你有没有觉得以前DEFCON都在拉斯维加斯举办，而且一年只有一次，你有没有觉得遥远的距离、签证、航班、时间安排、语言等等原因让你错过了参加这个酷炫的安全会议？没关系，多亏了DEFCON GROUP，你能够随时和本地社区的同道中人一起体验到DEFCON精神，国界、语言以及其他一切可能阻隔我们的障碍都被克服。最重要的是本地的这些DEFCON GROUP是让我们团结起来共同去实现一些更大的事业、去启发他人，不论他们来自那个国家、种族以及具有什么样的背景等等。

在这个议题中你可以听到DEFCON创始人Jeff Moss、DEFCON 全球协调人Jayson E.Street、DEFCON GROUP 010 发起人李均、DEFCON GROUP 617 发起人 April C.

PRESENTATIONS

Wright、DEFCON GROUP 86021 发起人王铁磊、DEFCON GROUP 86755 发起人 Peter Wesley、DEFCON GROUP 0571 发起人腹黑，DEFCON GROUP 0531 发起人刘新鹏等共同探讨什么是”黑”，什么是黑客精神，不同的黑客社区有什么区别，各个黑客社区可以有哪些经验值得相互学习。然后他们会讨论黑客精神是怎样对社会发展作出积极贡献的，如何培养安全从业者，最后他们会讨论未来有哪些可以合作的项目，例如前往偏远地区播撒技术的种子。

各个本地Group发起者还将分享他们的一些酷炫的项目，以及对其他Group的项目给出改进建议等等，这些项目包括个性化胸卡制作，物联网设备，智能家居等等。

Peter Wesley is a security researcher based in Shenzhen, China, where he runs a consultancy specializing in product security services. He has over 20 years experience in IT security, predominately in the Finance and Telecommunications industries, and has previously worked for Huawei Technologies in China, and NBN Co and Hacklabs in Australia. Peter is the organizer of the DC86755, the DEFCON group in Shenzhen.

Tielei Wang is a member of Team Pangu. He was a research scientist at the Georgia Institute of Technology from 2012 to 2014 and received his Ph.D. degree in 2011. His research interests include system security, software security, and mobile security. He discovered a number of zero-day vulnerabilities and won the Secunia Most Valued Contributor Award in 2011. He has published many papers in top research conferences including IEEE Security and Privacy, USENIX Security, ACM CCS, and NDSS, and gave several presentations at BlackHat USA, CanSecWest, POC, and RUXCON. He is the POC of DC86021, the DEFCON group in Shanghai.

Changsheng Gao (aka Fuhei) is an enthusiast of Web security, he is one of the leaders of Whitecap 100 security team, leader of CTF team W&P. He is also the POC of DEFCON GROUP 0571, the DEFCON group in Hangzhou.

Xinpeng Liu is a security researcher from EversecLab, he is focused on web security,botnet tracking and malware analysis. He is speaker of DEFCON GROUP 010. He is the POC of DC0531, the DEFCON group in Jinan.

Jun Li is a security researcher at UnicornTeam in the Radio Security Research Department of 360 Security Technology. He is interested in hardware security, connected car security, wirelfess security. He presented his research about wireless hacking and car hacking at Blackhat, DEFCON, HITB, CanSecWest, Syscan360, etc. He is the author of three books，《无线电攻防大揭秘》、《智能汽车攻防大揭秘》、《Inside Radio: An Attack and Defense Guide》， He is member of DEFCON GROUPS GLOBAL ADVISORY BOARD， the POC of DC010, the first DEFCON group in China.

April C. Wright (@AprilWright) is a hacker, author, teacher, and community leader with over 25 years of breaking, making, fixing, and defending critical global connections. She has held roles on offensive, defensive, operational, and development teams. A security risk specialist for a Fortune 15 company, April has been a speaker and contributor at numerous security conferences, and for US Government and industry organizations such as OWASP and ISSA. She has started multiple small businesses including a non-profit, fulfills the role of Signaler for the DEFCON Groups Core Team, and co-founded Boston DC617.

Jayson E. Street is an author of the “Dissecting the hack: Series”. Also the DEF CON Groups Global Ambassador. Plus the VP of InfoSec for SphereNY. He has also spoken at DEF CON, DerbyCon, GRRCon and at several other ‘CONs and colleges on a variety of Information Security subjects.

*He was a highly carbonated speaker who has partaken of Pizza from Beijing to Brazil. He does not expect anybody to still be reading this far but if they are please note he was chosen as one of Time’s persons of the year for 2006.

Peter Wesley是一名来自澳大利亚的安全研究员，现在主要在中国深圳工作，他运营着一家专注于提供产品安全咨询的咨询公司。他在IT安全领域（主要是金融和通信行业）拥有20多年的经验，他之前在华为以及澳大利亚公司NBN和 Hacklabs工作过。他也是深圳的DEFCON GROUP——DC86755的负责人。

王铁磊是盘古团队核心成员，他2011年获得博士学位，于2012年至2014年乔治亚理工学院任研究科学家。他的研究领域包括系统安全、软件安全、移动安全。他发现了许多0-day漏洞并在2011年被Secunia授予最具价值贡献者奖。他在很多顶级会议上发表过文章，例如IEEE Security and Privacy、USENIX Security、ACM CCS、 NDSS，他在Blackhat、CanSecWest、POC、RUXCON等国际顶级会议连续发表过演讲。他是上海的DEFCON GROUP——DC86021的负责人。

高昌盛（腹黑）是WEB安全爱好者，安全团队白帽100安全攻防实验室负责人之一，CTF战队W&P队长，他是杭州的DFECON GROUP——DC0571的负责人。

刘新鹏是来自恒安嘉新水滴安全实验室的安全研究员，专注于WEB安全、僵尸网络追踪、恶意软件分析等等，他是DEFCON GROUP 010的演讲者之一，也是济南的DEFCON GROUP——DC0531的负责人。

李均是360无线电安全研究部独角兽团队高级安全研究员，他的研究领域包括网联汽车安全、硬件安全、无线安全等等。他曾在DEFCON、 Black Hat、 HITB、CanSecWest、Syscan360等国际著名安全会议发表过关于无线及汽车安全的研究成果。《无线电攻防大揭秘》、《智能汽车攻防大揭秘》、《Inside Radio: An Attack and Defense Guide》等安全书籍的作者。他是中国首个DEFCON GROUP——DC010的发起者，也是DEFCON GROUPs全球顾问委员会成员.

Jayson E. Street是《Dissecting the hack系列》图书的作者之一，同时他也是DEF CON团队的全球大使，SphereNY的信息安全副总裁。他曾在DEFCON、DerbyCon、GRRCon、各种其他CON和学校里进行关于信息安全的各种主题演讲。
*他是一名高度依赖碳酸饮料的演讲者。从北京到巴西，他到处分享披萨。他从不期待有人会读到这部分，不过如果有人看到了，请注意，他曾经被选为时代周刊2006年的年度人物。

THANK YOU!

I want to thank everyone who has supported DEF CON China[Beta]. It takes a lot of people to pull off a conference, and a lot of stress to do it in short order.

Thank you to Zhang Yaqin and Ma Jie from Baidu for their long term vision to bring DEF CON to China and Casper and Alisa from XFuture for making the introductions and encouraging us to take the leap. Without those four people we wouldn’t be here.

Thank you to the speakers, trainers, villages, demo labs, and contest organizers who took this first step with us. Many didn’t know what to expect and so we all had this adventure together. Cool! Thank you for that

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

I want to thank Shen Pengfei, Liu Ye, Tony and Ma Meng from Baidu Security. Thank you to Zhang Jin from XFuture. Also, thank you to our music director Sun Yi Gang.

Thank you to the community supporters, sponsors and press who helped spread the word of our conference and took a risk on us our first year.

Finally I want to thank you, the human, for trying something new and getting involved over this weekend.

We plan to return in 2019, no longer in [Beta] but ready for a v1.0 release!

The Dark Tangent

我想致谢于支持DEF CON 神州的全体人士。在短时间内做一项活动可需不少人的帮忙，也施于大家不少的压力。

百度总裁张亚勤 百度安全总经理马杰。你们长远的眼光协助我们把DEF CON 带到中国来。也同时得感谢未来安全的王英键及赵萱，介绍大家认识。没有这四位的功劳，我们不会在此。

感谢所有的演讲者，研讨会培训者，village乡亲，演示实验室及竞赛的主办者。大家都一起踏出了第一步，尝试了非一般的经历。好酷！谢谢你们。

谢谢你，DEF CON 的工作人员：Nikita, Neil, Darington, Cayce, Will, Charel 及Janet协助办这项活动。Villages 的Zant，研讨会的Tottenkoph， 娱乐的Kampf 及全体CFP评审团。

也感谢百度安全的沈鹏飞，刘叶，于洋和马濛；及未来安全的张晋和我们的音乐会导演孙毅刚。

感谢社区的支持者，赞助商及媒体工作人士。你们帮助我们宣传我们首届会议，并于我们一起同舟共济。

最后，我想致谢于参会嘉宾，尝试度过一个与众不同的周末。

我们计划2019年返回，呈现v1.0 的形式!

The Dark Tangent

KUNTAI HOTEL

