HITCON GIRLS 成果分享
與 BLACK HAT 之旅

HITCON COMMUNITY 2019

SPEAKERS

- shad0w
  - 台灣停電科技大學研究生，HITCON GIRLS 創始團隊中最晚脫離學生身份的人 (・ω・)ノ
- akee
  - HITCON GIRLS 成員, 不是創始團隊也沒有兼職，只是個單純的成員_(: 3 」∠)_
- Hazel Yen
  - HITCON GIRLS 創始團隊暨總召，比較擅長活在鍵盤後面的生物(゜∀゜)

OUTLINE

- HITCON GIRLS 介紹
- 近期成果與專案
- Black Hat 旅程
- DEF CON 見聞

OUTLINE

- HITCON GIRLS 介紹
- 近期成果與專案
- Black Hat 旅程
- DEF CON 見聞

HITCON GIRLS 介紹

HITCON GIRLS 是以女性為主的資安社群，我們組織各種不同主題的讀書會，來幫助成員們透過合作與分享來克服學習上的瓶頸與互相學習。創造一個鼓勵並激發女性學習資安的環境，並增加科技產業的包容性。

HITCON GIRLS 理念

- 希望聚集對資安感興趣、一起成長的女性，推廣「任何人都可以學習資訊安全」的理念

組織架構

- 籌備團
- 讀書會

組織架構

- 籌備團

(ง๑ ๏̀_๏́)ง

負責活動和場地財務管理，和實作群溝通完善原本的規劃，促成順暢的活動流程，籌備團也是HITCON GIRLS 創立的前身。

- 讀書會

籌備團

- 每年都會辦一場大型的活動
- 資安推廣活動
- 粉絲團、twitter、官網...

組織架構

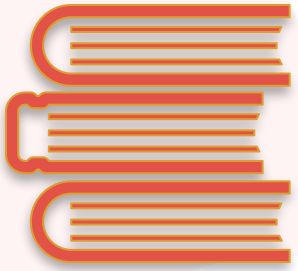
籌備團

負責活動和場地財務管理，和實作群溝通完善原本的規劃，促成順暢的活動流程，籌備團也是HITCON GIRLS 創立的雛形。

讀書會

每個週期會有不定數量的讀書會小組，平時獨立運作舉辦組內讀書會，每個月會有全體交流會，讓大家攝取不同類型的知識。

d(`･∀･)b



讀書會

DFIR 組

數位鑑識與響應分析組，負責蒐集資料，分析駭客到底在犯案現場留下了什麼

惡意程式分析組

針對 Malware 進行分析研究，內容包含靜態與動態分析、各種工具以及分析思路。

WEB PT 組

專門研究網頁滲透測試的手法，如何攻擊、如何防禦都是研究目標

CTF 組

以 CTF 為目標的組別，包山包海什麼都研究，還會不定期出團打 CTF！

不分組

對於各個領域的資安研究都會進行涉獵和分享。

OUTLINE

- HITCON GIRLS 介紹
- 近期成果與專案
- Black Hat 旅程
- DEF CON 見聞

近期成果與專案 - 之於一個社群

- 點數制度
- 總召選舉&行政團隊
- 教練制度
- 英文官網

點數規則的由來

- 「社群」來自於一群擁有共同理念的夥伴，在「對資訊安全有興趣」的匯合下我們組成 HITCON GIRLS。
- 健康的社群，需要傳承與制度。
- 讀書會的經營、活動的籌劃以及組織的營運需要夥伴一起分擔，點數是為了鼓勵「不斷在付出的人」，不論你做的事情是大是小。

點數可以換什麼

項目
HITCON Pacific 一般票贈票一張
HITCON Community 一般票贈票一張
HITCON FreeTalk 入場名額一個
HITCON GIRLS 會議一般票贈票一張
HITCON 包包一個
HITCON 紀念品
特殊活動
(待換購)
二手書 / 資安展社群贈品 / 資安不要的系列 =v="
證件套

不一定有，有就會回饋社群

總召選舉&行政團隊

- 健康的社群，需要傳承與制度
- 讓每個人找到自己的舞台，或許有成員非資安相關，但是她支持社群的理念，她也可以幫忙

總召怎麼選？

- 由非總召的成員成立選舉活動
- 徵「總召候選人」，發表未來營運方針、目標
- 所有成員皆可投票

[HITCON GIRLS] 總召選舉 - Final - Hi GIRLS, 希望大家期中考順利 / 順利放假～ 謝謝大家參加投票，也感謝所有...

Screen Shot 20...

[HITCON GIRLS] 總召選舉 - DAY6(4/23) - *Hi GIRLS,* *希望大家都有個開心的週末～接下

[HITCON GIRLS] 總召選舉 - DAY5(4/20) - Hi GIRLS,

image2.jpeg

[HITCON GIRLS] 總召選舉 - DAY4(4/19) - *Hi GIRLS,* 如果看過前面兩位候選人應該知道這次總召選舉都很厲害...

Screen Shot 20...

[HITCON GIRLS] 總召選舉 - DAY3(4/18) - *Hi GIRLS,* *緊接著是2號人候選人：小趴！* *小趴是超強的趴姐，也...

S__26681366.jpg

收件匣 [HITCON GIRL... Spark by Readdle

Day1

[HITCON GIRLS] 總召選舉 - DAY1(4/16) - Hi GIRLS, 渡過最BLUE 的星期一，終於有點好消息要帶給大家～～ 經...

為什麼社群要搞得這麼複雜？

搞得好像社群感情很不好？

行政團隊

- 拆分工作的目標是降低每個人的壓力
- 環環相扣的行政流程代表每個人都很重要
- 永遠找得到事情做，沒有的話還可以自己新增……XD

update: 2019.06.30 珣 更新工作詢問

HITCON GIRLS 內部工作清單

※括號內的為需求人數

		負責人	工作時間	工作細節
讀書會	寄信		每個月	事前工作(1)
	場地		每個月	場地(1)
	攝影		每個月	攝影(1)
	召集人		每個月	召集人(1)
給我凝聚力	活動		不定期	活動(1)
FB社團管理	貼文互動		配合活動	貼文互動(不限)
	交流區管理		突發性	交流區管理(1)
Po文管理	粉絲團管理		突發性	粉絲團管理(1)
	Blog 管理		突發性	Blog管理(1)
	Twitter		突發性	
行政	Mail 管理者		突發性	Mail 管理者(1)
官網	官網營運		配合活動	官網營運(1)
	GitHub		配合活動	官網營運(1)
2020 規劃	新生招募		單次活動	新生招募
2020 規劃	總召選舉		單次活動	總召選舉(1)
2020 規劃	紀念品製作		單次活動	紀念品製作

所以到底為什麼要弄得這麼複雜？

- 為了讓社群永存
  - 避免單一人力過勞
  - 傳承後有完整的文件、營運制度可以參考
  - 規範代表限制，同時也代表保障
- 為了讓成員有參與感、發言權
- 有一天，總召不在了，任何人都可以當上領導者

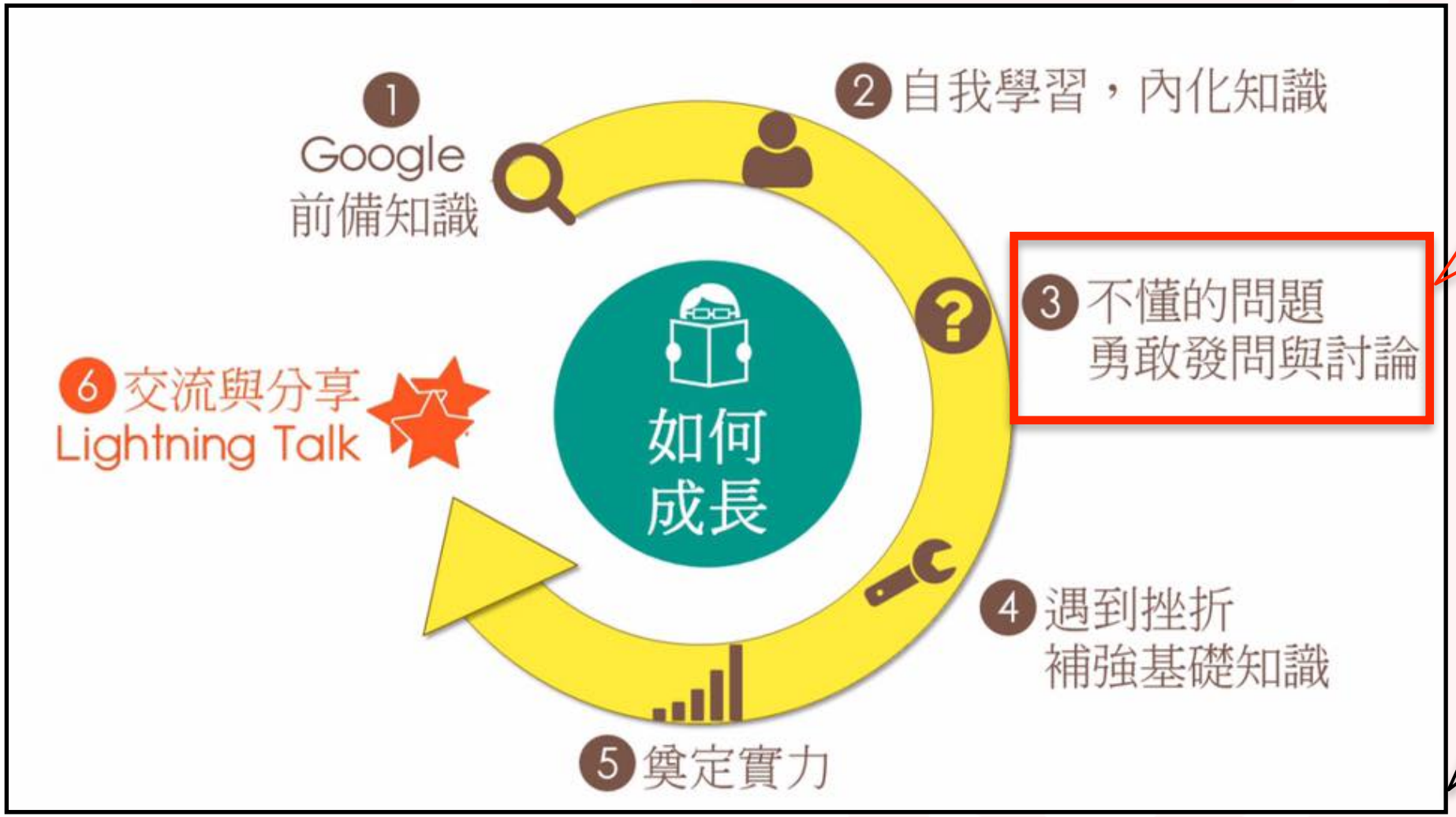
教練制度

- HG 有一個特別的存在叫作「教練」
- 於讀書會有問題時可向他 / 她提問

教練制度的苦衷T^T

- 這就是最容易被說「女生真好」的制度
- 其實呢，Mentor 作法在資安圈很常見
- 其實呢，教練沒有義務要幫我們、回應每個問題
- 其實呢，就跟在研討會抓住 Speaker 發問一樣

曾經有人問過粉絲團如何自主學習



教練在這

但學習還是靠自己

ENGLISH WEBSITE

ENGLISH WEBSITE

- 自從上了英文官網後，來自國外的訊息、互動、活動就變多了呢 (推薦XD)
- 感謝成員幫忙翻譯！

近期成果與專案 - 活動回顧

- 不是刻意，但 HG 活動大概有三種類型
  - 大型活動，開放的、很累的
  - 分享，把知識轉成語言、投影片或影片的類型
  - 邀請型，會請外部的人來分享經驗

活動回顧：大型活動

2014

我們的初始 Workshop

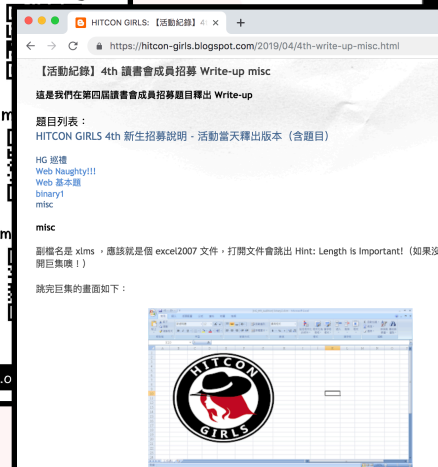
2018

HITCON CMT 2018

2019

第四屆讀書會成員招募 CTF

HG at HITB 活動



活動回顧：分享

2015

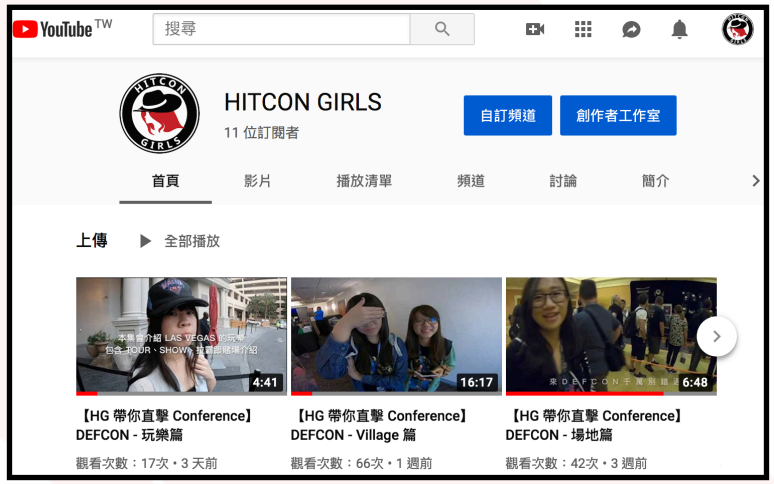
讀書會成果發表

2017

資安萌芽推廣

2019

HG 帶你直擊 Conf



活動回顧：邀請型

2015

週年紀念以及 PPP 分享

2016

Chipchat Party

2017

Birds of a Feather

2019

資安女性分享會

OUTLINE

- HITCON GIRLS 介紹
- 近期成果與專案
- Black Hat 旅程
- DEF CON 見聞

BLACK HAT 旅程 - 前言

- 為何會有這次演講？
  - 共同演講邀約
    - Asuka Nakajima | CTF for GIRLS
    - Suhee Kang | Power of XX
    - Hazel Yen | HITCON GIRLS

Women in Security

Building a Female InfoSec Community in Korea, Japan, and Taiwan

South

Suhee Kang, Asuka Nakajima, Hazel Yen

CTF FOR GIRLS

POWER OF XX

推文 284
正在跟隨 403
跟隨者 1,525
喜歡的內容 771
POC_Crew
@POC_Crew
Security Researcher (Suhee, Harry, Jinwook) Organizer of #Zer0Con, #POC and #MOSEC POC2019: Nov. 7~8th
Seoul, Republic of Korea
pocsec.com
2017年10月加入
68 個相片或影片
推文
推文與回覆
媒體
釘選的推文
POC_Crew @POC_Crew · 8月1日
[POC2019 CALL FOR PAPERS OPENS]
CFP Opens: August 1, 2019
CFP Closes: October 10, 2019
POC2019 pursues groundbreaking researches and share very latest work.
[Tracks]
(OS, Mobile, Browser, VM, AI, Cloud, Hardware, AV, Network, Malware, APT, Web, Crypto...)
POC2019

BLACK HAT 旅程 - 關於投稿的大小事

- 講師費 US$1000
- 補助機票 US$1300
- 補助住宿（大約 2~3 萬元左右)
- 可以提前買 DEF CON 門票

BLACK HAT 旅程 - 前言

- 為何會有這趟旅程
  - 天價的門票 (´･ω･`) ||_|| ( || ･ || ) (|| ～ ||) (´;ω;`)

EARLY	REGULAR	LATE	ON-SITE
$2295	$2495	$2795	$2895
ENDS MAY 24	ENDS JULY 12	ENDS AUGUST 2	ENDS AUGUST 8

  - Business Pass $695
    - Business Hall, Arsenal, Sponsored Sessions, Sponsored Workshops, and the Kali Linux Dojo.

BLACK HAT 旅程 - 學生免費專案

- Black Hat Student Scholarship Program
  - 為什麼你想參加 BH
  - 有什麼樣的具體經驗讓你有資格拿 Pass
  - 三個過去的 BH 分享中特別感興趣的內容
- Briefings only
- Black Hat Europe 學生專案申請：Sep. 8 ~ Nov. 8

WHAT IS BLACK HAT?

- 1997 年開始舉辦，是世界上最具代表性的資訊安全研討會之一
- 偏向企業、產業
- 有專業的 Trainings, Workshops，但價格比 Briefings 門票更貴

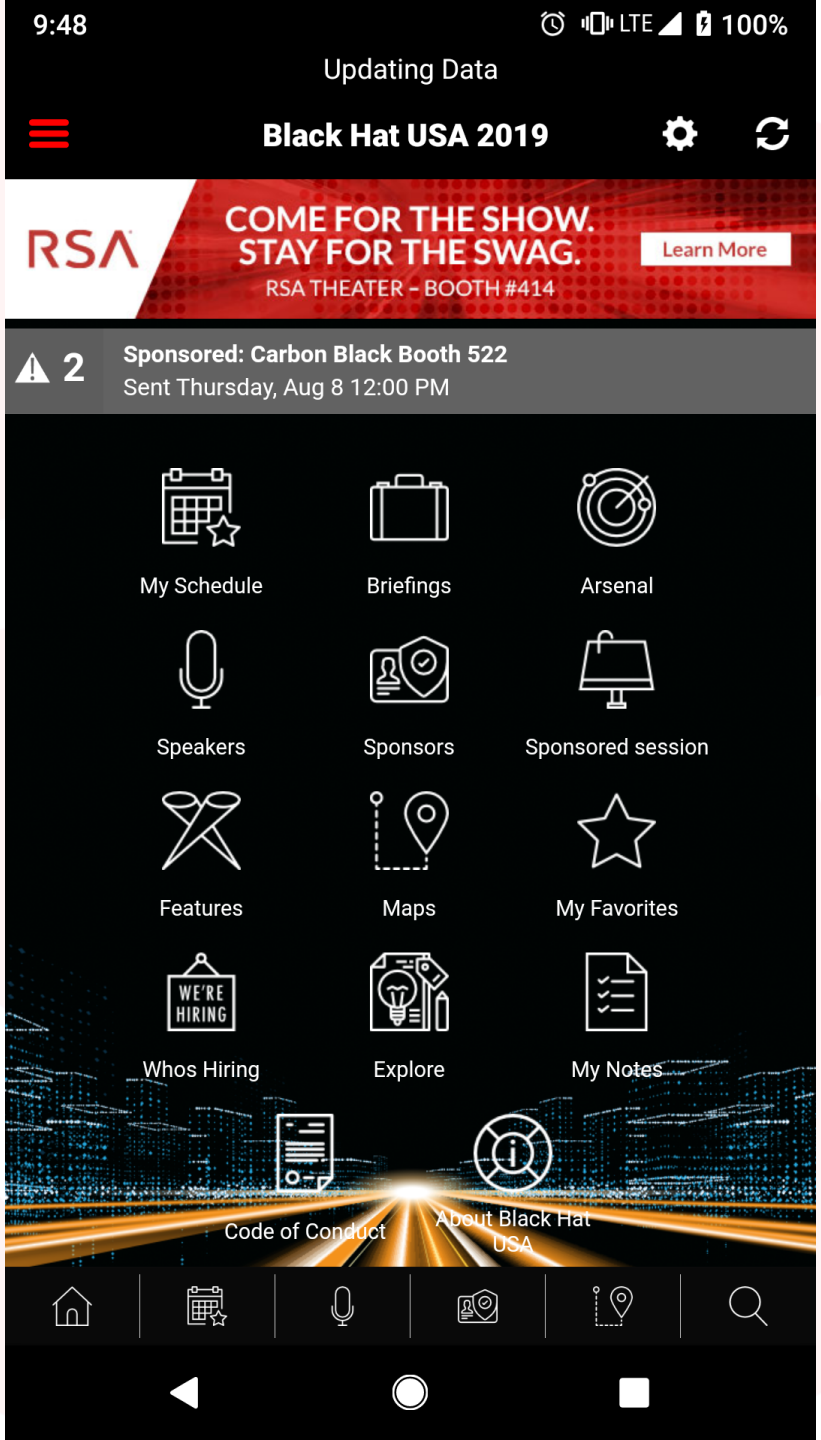
BLACK HAT 旅程

- 炫富的開場
- 完整版可以鎖定 Black Hat Youtube 頻道，雖然他們可能還要再過幾個月才會上傳 ›w‹

122

BLACK HAT 旅程

- 官方 APP 特點
  - 排自己的議程 schedule
  - 每個議程都可以做筆記
  - 地圖（會場超級大）



black hat
USA 2019
black hat USA 2019
Shadow Liu
Master Student
BRIEFINGS

LEGEND
Android, iOS and Mobile Hacking
Code Assessment
Cryptography
Data Forensics and Incident Response
Exploitation & Ethical Hacking
Data Forensics and Incident Response
Hardware/ Embedded
Human Factors
Internet of Things
Malware Defense
Malware Offense
Network Attacks
Network Defense
OSINT
Reverse Engineering
Smart Grid / Industrial Security
Vulnerability Assessment
Web AppSec

FERENCE SCHEDULE
BRIEFINGS DAY 2
THURSDAY // AUGUST 8
8:30 AM - 3:00 PM REGISTRATION // SOUTH HALL, LEVEL 1
8:00 AM - 9:00 AM BREAKFAST // BAYSIDE AB, LEVEL 1
9:00 AM - 9:25 AM
GDPArrrrr: Using Privacy Laws to Steal Identities
by James Pavur
Woke Hiring Won't Save Us: An Actionable Approach to Diversity Hiring and Retention
by Rebecca Lynch
Attack Surface as a Service
by Anna Westelius
Testing Your Organization's Social Media Awareness
by Jacob Wilkin
On Trust: Stories from the Front Lines
by Jamil Farshchi
Mobile Interconnect Threats: How Next-Gen Products May be Already Outdated
by Guillaume Teissier
The Future of Securing Intelligent Electronic Devices Using the IEC 62351-7 Standard for Monitoring
by Andrea Carcano + Alessandro Di Pinto + Younes Dragoni
Death to the IOC: What's next in Threat Intelligence
by Bhavna Soman
WebAuthn 101 - Demystifying WebAuthn
by Christiaan Brand
Islander EI
Islander FG
South Pacific
NORTH HALL // LOWER LEVEL
Breakers GHI
Lagoon GHI
Lagoon JKL
SOUTH HALL // LEVEL 2
Jasmine
South Seas ABE
South Seas CDF
SOUTH HALL // LEVEL 3
9:25 AM - 9:45 AM BREAK
9:45 AM - 10:35 AM
The Enemy Within: Modern Supply Chain Attacks
by Eric Doerr
100 Seconds of Solitude: Defeating Cisco Trust Anchor With FPGA Bitstream Shenanigans
by Ang Cui + Richard Housley + Jatin Kataria
All Your Apple are Belong to Us: Unique Identification and Cross-Device Tracking of Apple Devices
by Xiaolong Bai + Min Zheng
Rough and Ready: Frameworks to Measure Persistent Engagement and Deterrence
by Jason Healey + Neil Jenkins
Breaking Through Another Side: Bypassing Firmware Security Boundaries from Embedded Controller
by Alexandre Gazet + Alex Matrosov
Playing Offense and Defense with Deepfakes
by Mike Price + Matt Price
Planning a Bug Bounty: The Nuts and Bolts from Concept to Launch
by Adam Ruddermann
Denial of Service with a Fistful of Packets: Exploiting Algorithmic Complexity Vulnerabilities
by Nathan Hauke + David Renardy
Information Security in the Public Interest
by Bruce Schneier
Project Zero: Five Years of 'Make 0Day Hard'
by Ben Hawkes
Mandalay Bay CD
Islander EI
Islander FG
ARSENAL DAY 2
THURSDAY // AUGUST 8
OPEN TO ALL PASS TYPES
BRIEFINGS DAY 2
THURSDAY // AUGUST 8
SPONSORED SESSIONS DAY 2
THURSDAY // AUGUST 8
SPONSORED WORKSHOPS DAY 2
THURSDAY // AUGUST 8

BLACK HAT 旅程

- Party & Networking Events
  - 由不同的贊助商和社群舉辦
  - 需要事先報名

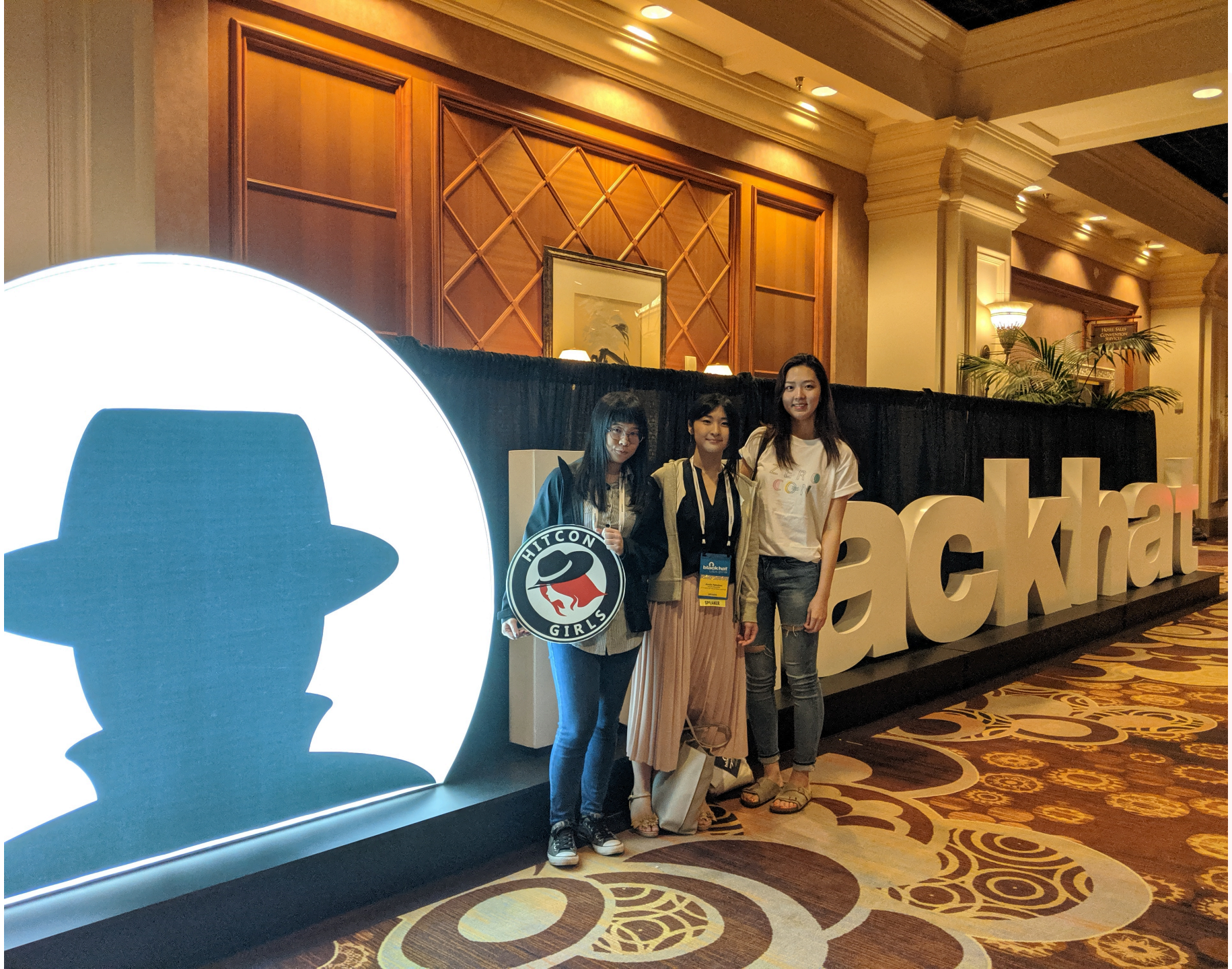
BLACK HAT 旅程

- Career Area 面試區
  - 練習英文溝通的好機會
  - 雖然可能 90% 會因為沒有綠卡而失敗

BLACK HAT 旅程

- 非常禮遇講者
  - 住宿、機票、講師費
  - 演講前調整 mic、演講途中全程幫你控制音量
  - 提供 rehearsal room，且有會後討論室讓講者跟會眾可以盡情討論
  - 休息室飲料吧台

black hat
USA 2019
2014.10
2014.12
Study Group
THE BEGINNING OF HITCON GIRLS


HITCON
GIRLS
SPEAKER

BLACK HAT 旅程 - 收獲

- 最頂尖的技術或漏洞分享
- 主動找社群/廠商聊天，拓展人脈
- 所有議程都會錄影並放到 Youtube
- 有錢就好了

OUTLINE

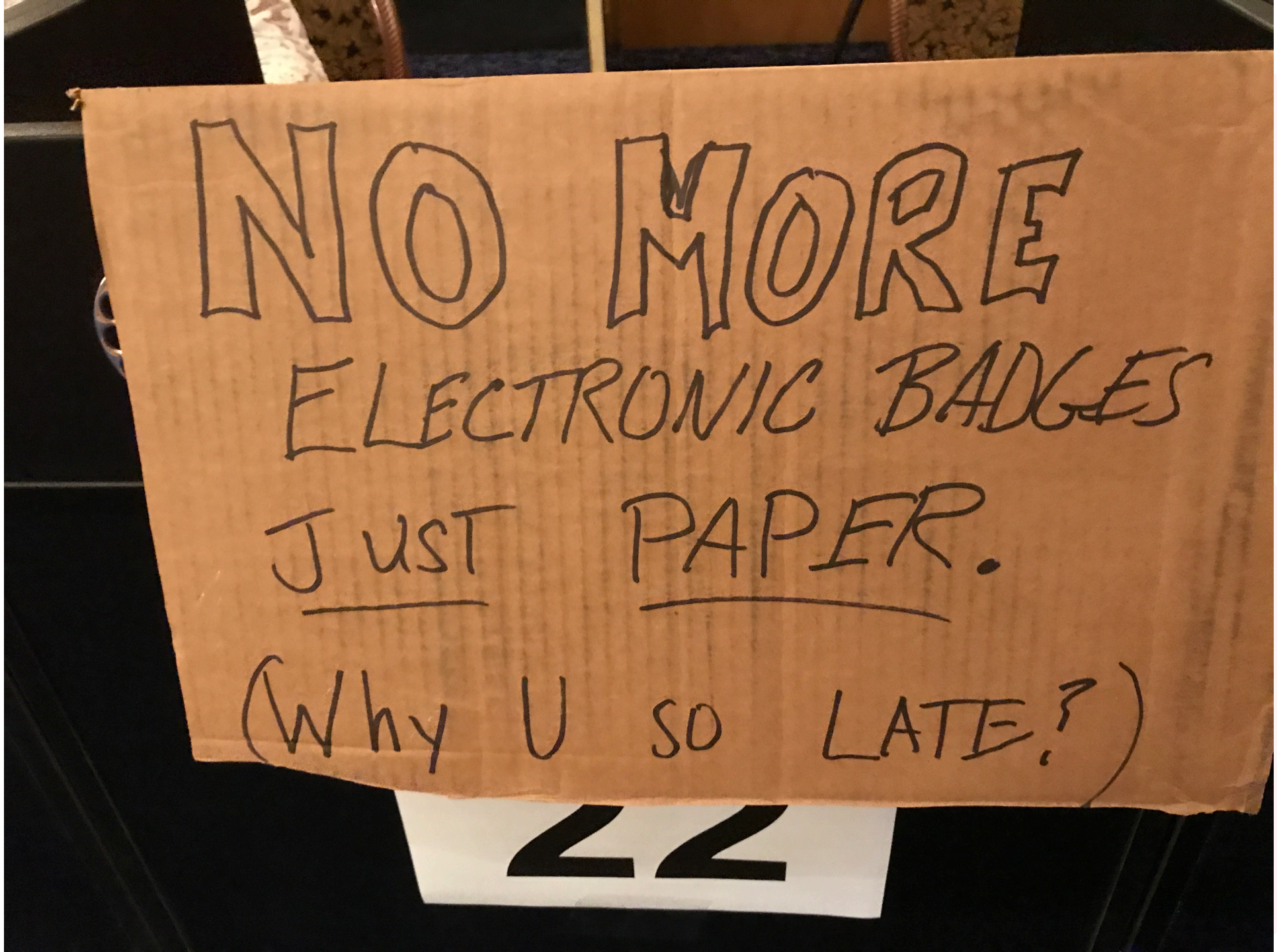
- HITCON GIRLS 介紹
- 近期成果與專案
- Black Hat 旅程
- DEF CON 見聞

WHAT IS DEF CON?

- 1993 年開始舉辦，是世界上最具代表性的資訊安全研討會之一
- 駭客的超大型派對
- 可以自由地與講者及商家交流，或是參與各種競賽和活動

DEF CON 見聞 - BADGE 介紹

- 均一票價 USD 300
- 白色：human
- 藍色：speaker
- 紫色：vendor
- 綠色：press
- 紅色方形：staff
- 紅色圓形：staff 組長


NO MORE
ELECTRONIC BADGES
JUST PAPER.
(Why U SO LATE?)
22

DEF CON 見聞 - 特殊 BADGE

- 要在特定場合參加活動並找到 NPC 才能取得 magic token

DEF CON 見聞 - PRESS TICKET

- 怎麼申請
  - 寄信給 press team
  - 主辦回覆 approve
  - 現場到 Press Room 付錢領取，也是 USD 300
- 規則
  - 允許在會場錄影、拍照和採訪
  - 攝影要經過對方同意，不得使用隱藏式攝影機
  - 不可以拍小孩（潛規則）

DEF CON 見聞 - PRESS TICKET

- 可以做
  - 允許在會場錄影、拍照和採訪
  - 使用媒體室剪輯影片、編輯採訪文稿，提供插座網路 & 飲料吧台！
  - 會在路上各種被攔阻 touch badge

來 DEFCON 就是要去參加 village, contest 啊！聽那些之後會放到 YouTube 的議程要幹嘛 (「`･ω･)「

DEF CON 見聞 - VILLAGE

- DEF CON 的本體
- 每個 village 都會有一個空間，讓 host 自由發揮議程、workshop、contest
- forums 上總共有 33 個，活動不限於會議期間

r00tz

Ham Radio

Biohacking

Blockchain

AppSec

Aviation

ICS

Rogues

Lockpick

Hack the Sea

Hardware Hacking

Voting Hacking

Monero

Car Hacking

Cloud

Red Team

Crypto and Privacy

Drone Warz

IoT

Lock Bypass

Soldering Skills

AI

DEFCON Furs

Ethics

Recon

Skytalks

Wireless

Blue Team

Social Engineer

Packet Hacking

Tamper Evident

VX

Data Duplication

ref: https://forum.defcon.org/node/227570

DEF CON 見聞 - CONTEST AREA

- 由各社群主辦
  - 寫小故事
  - 鬍子
  - 騎腳踏車
  - 酒醉駭客
  - 飲料降溫

DEF CON 見聞 - CONTEST AREA

- Hack Fortress
  - 絕地要塞 2 + 資安比賽
  - 6 TF2 players and 4 hackers
  - 只會玩 FPS 就靠 TF2 打比賽吧 ¯_(ツ)_/¯

DEF CON 見聞 - DEMO LAB

- 各自報名，每個人可以來發表自己寫的工具
- 超小型 talks (每場可能不到五個人聽)
- 可以很好的跟講者討論細節

DEF CON 見聞 - 貼紙文化

- 到處、無所不在、哪邊都會被貼貼紙
- 大家會交流自己有的貼紙，可以跟別人拿 or 交換

DEF CON 見聞

- 只提供水，其他需自理
- 今年場地分散在三間飯店
- 可利用空間很大，但走得很累 へ（。□°）へ

1:51
72%
You walked 68.1 km this week!
REWARDS
5 km
25 km
50 km

DEF CON TIPS

- 會前先上 Forums 看看今年有什麼活動
- 提早決定想參加的，就可以花更多時間投入
- 有些 CTF, contest 需要事先報名否則無法參加
- 想拷貝資料需要自行準備 TB 等級的硬碟 (今年 6TB)
- 準備好飛美國的機票錢 (~￣▽￣)~

Open your mind ʕっ•ᴥ•ʔっ
Just hack it!

Q/A Welcome

<°(@°▽°@)°>

FOLLOW HITCON GIRLS

- 官網：girls.hitcon.org
- 社群：
- 信箱：hgservice@hitcon.org
- ping: Hazel Yen