Black Hat USA 2016

written by Mert SARICA | 8 August 2016

İlk defa geçtiğimiz yıl katılma fırsatını yakaladığım dünyaca ünlü Black Hat güvenlik konferansına, NormShield firması sayesinde bu sene tekrar katılacağımı büyük bir mutlulukla geçtiğimiz ay sizlerle paylaşmıştım. Konferans ve öncesinde aldığım kısa notları, 12 saatlik dönüş yolunda sizler için derleyerek daha önce olduğu gibi merak edenler için yazıya dökmeye karar verdim.

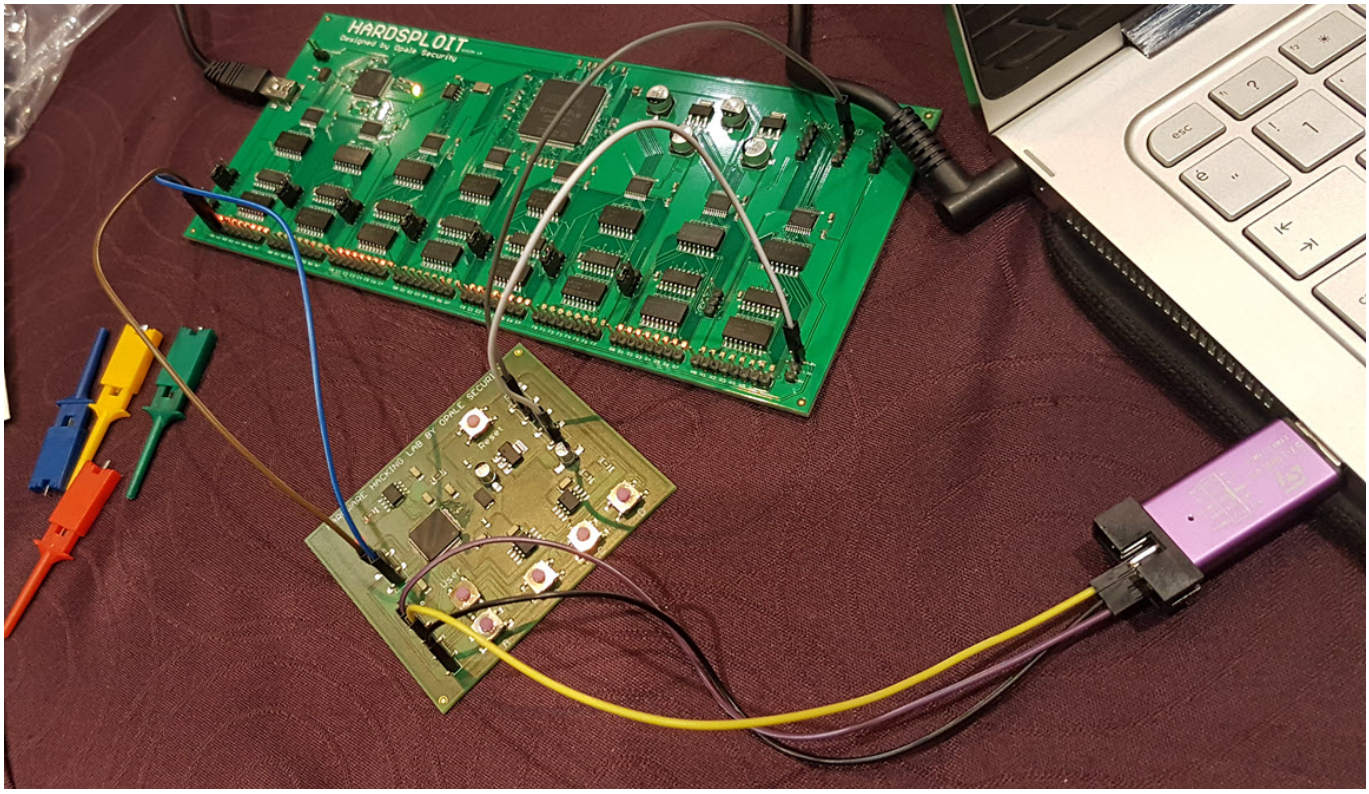
Benden kimseye zarar gelmeyeceğini üçüncü defada artık anlamış olsalar gerek ki, bu defa ABD'ye girişim Intel Security Focus Güvenlik Konferansı başlıklı blog yazımda yaşadıklarımın aksine oldukça rahat oldu. 20 Temmuz itibariyle Los Angeles şehrinde başlayan ABD tatilim, 30 Temmuz itibariyle yerini Las Vegas şehrinde gerçekleşen Black Hat güvenlik etkinliğine bıraktı. Takip edemeyenleriniz için, Black Hat USA 2016 güvenlik etkinliği, bu sene 30 Temmmuz – 4 Ağustos tarihlerinde gerçekleştirildi.

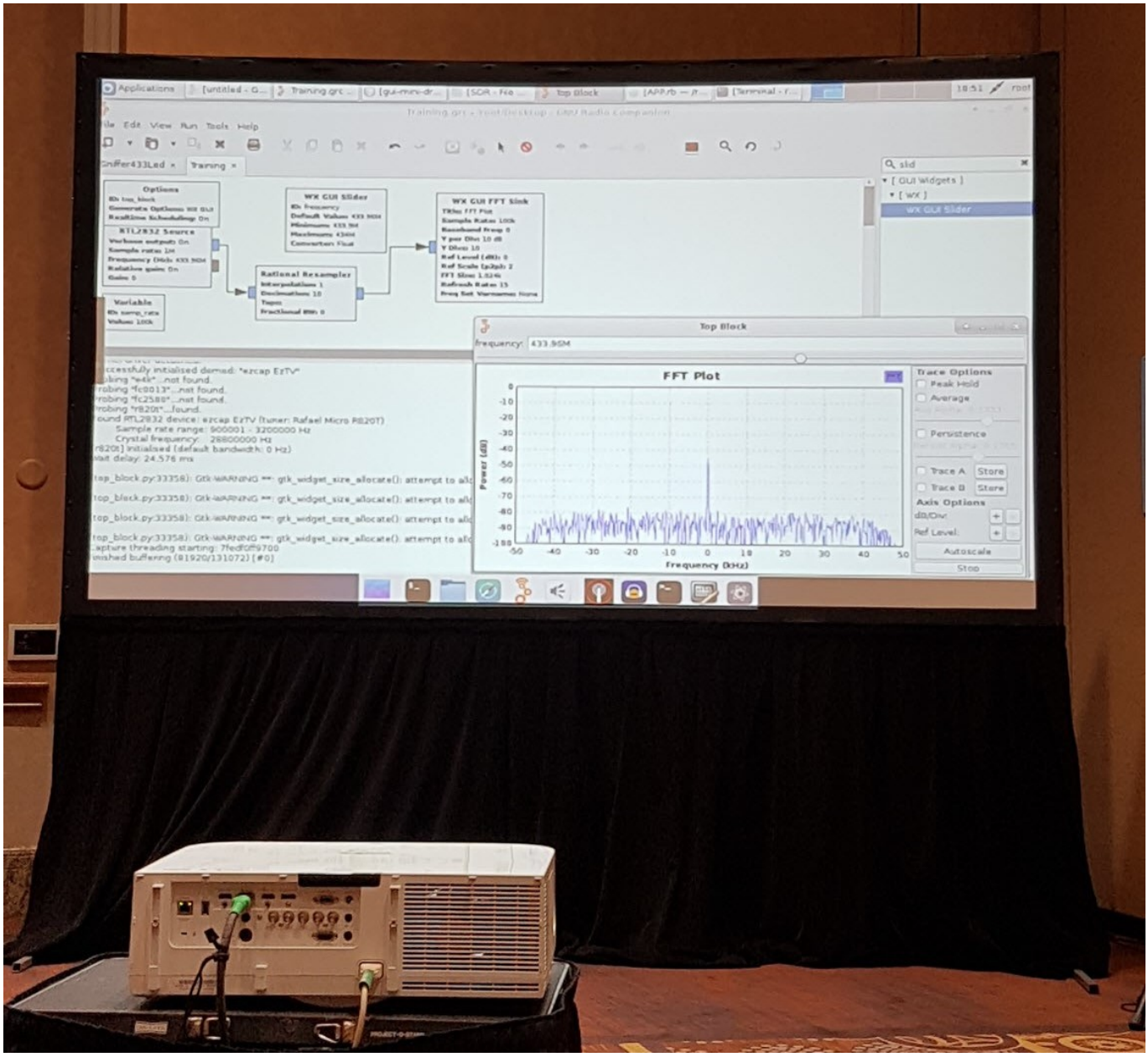
3 ve 4 Ağustos tarihlerinde yapılan sunumlar öncesindeki 4 günde, geçtiğimiz senelerde olduğu gibi birbirinden güzel 70'e yakın güvenlik eğitimi verildi. Ben de, değerli yöneticilerim ve işverenim IBTech sayesinde donanım güvenliği

üzerine yoğunlaşan iki günlük Hardware Hacking With Hardsploit Framework eğitimine katılabildim.

Geçtiğimiz aylarda işim gereği elektronik ATM kasa kilidi için sızma testi gerçekleştirmiş bir güvenlik uzmanı olarak, bu eğitimin benim için oldukça verimli geçtiğini ve ufkumu açtığını söyleyebilirim.

Opale Security firması tarafından verilen bu eğitime farklı ülkelerden (Tayvan, Kore, Brezilya, Fransa, Avusturalya), farklı profillerde (yazılımcı, sızma testi uzmanı) katılan yaklaşık 25 kişi vardı. Özellikle Amerikan Hava Kuvvetleri'nden üç kişinin katılması ve bazı katılımcıların eğitimin kendini tanıtma kısmında diğer katılımcılar ile sadece isimlerini paylaşması (Acaba neden? :)) da dikkatimden kaçmadı. Eğitimin ilk günü, Hardsploit aygıtı ile SPI ve I2C belleklerden bilgi toplama (dump), SWD bağlantı noktasından donanım yazılımını (firmware) elde etme (dump) gibi uygulamalar gerçekleştirildi. Eğitimin ikinci gününde ise öğleden önce GNU Radio ve RTL2832U dijital tv alıcısı ile neler yapılabileceği gösterildi. Öğleden sonra ise 1.5 günde öğrenilen bilgilerin pekiştirildiği oldukça keyifli bir çalışma gerçekleştirildi. Katılımcılardan takımlar oluşturuldu ve daha sonra eğitmenler tarafından özel olarak oluşturulmuş quadcopterler (drone) takımlara dağıtıldı. Her bir takımdan drone'a üzerinde bulunan bağlantı noktaları üzerinden cihaza bağlanmaları, donanım yazılımını indirmeleri (dump), zafiyet tespit etmeleri ve diğer ekiplerin mevcut zafiyeti istismar etmesinden önce dronelarındaki bu zafiyeti gidermeleri istendi. Bunlara ilave olarak ayrıca her ekibe dağıtılan ve drone'a komut göndermek için kullanılan vericinin Hardsploit ile incelenmesi ve ardından eğitmenlerin sahip olduğu drone'a komut göndererek (belli periyotlarda eğitmenler kendi dronelarına sinyal göndererek bunu elde etmemizi sağladılar) havalandırmaları istendi. Kısa sürede son derece yoğun geçen bu eğitimden oldukça memnun kaldığımı söyleyebilirim.


HARDSPLOIT
Designed by Opale Security


Top Block
frequency: 433.95M
FFT Plot
Power (dB)
Frequency (kHz)
Trace Options
Peak Hold
Average
Persistence
Trace A
Trace B
Store
Axis Options
dB/Div:
Ref Level:
Autoscale
Stop

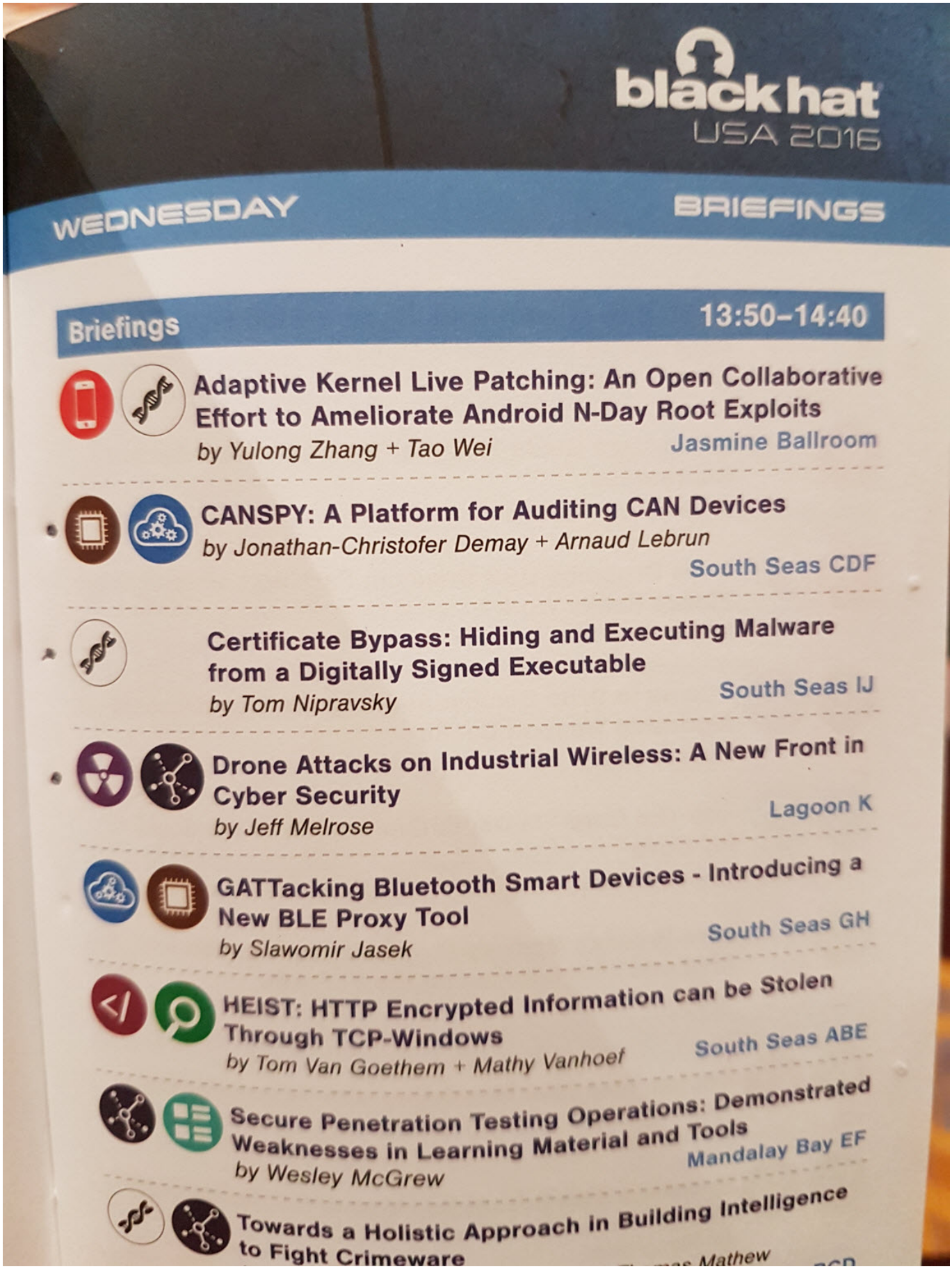

HARDWARE HACKING

Black Hat Konferansı, geleneksel olarak konferansın kurucusu olan Jeff Moss'un açılış konuşması ile başladı. Yaklaşık 8 dakika boyunca konuştuktan sonra sözü Dan Kaminsky'e verdi. Jeff Moss konuşmasında bazı istatistiklere de yer verdi. İlk olarak Black Hat USA 2016'ya tarihi bir katılım olduğunu ve açılış konuşmasında salonda yaklaşık 6400 kişi olduğunu açıkladı! Ardından da 194 öğrenciye burs verdiklerini belirtti. (Açılış konuşmasını merak edenler, aşağıda onlar için kayıt ettiğim videoyu izleyebilirler.)

Geçtiğimiz sene olduğu gibi yine paralelde birbirinden ilgi çekici sunumlar olduğu için hangisine katılacağıma karar vermekte oldukça zorlandım. Sunum sayfasındaki kategori bazlı filtreden faydalanarak “Tersine Mühendislik” ve “Zararlı Yazılım” konularını işleyen sunumlara katılmaya gayret ettim. İkinci gün katıldığım sunumların ilk günkü sunumlara kıyasla benim için daha tatminkar olduğunu söyleyebilirim. Katılım oldukça yüksek olduğu için yine bir sunumdan diğerine gitmek için metrobüs kalabalığını aratmayan bir kalabalığın arasından yolumu bulmaya çalıştım. Bazı sunumlarda işitme engelli katılımcılar için işaret dili ile anlatım yapılmasını da çok takdir ettim.

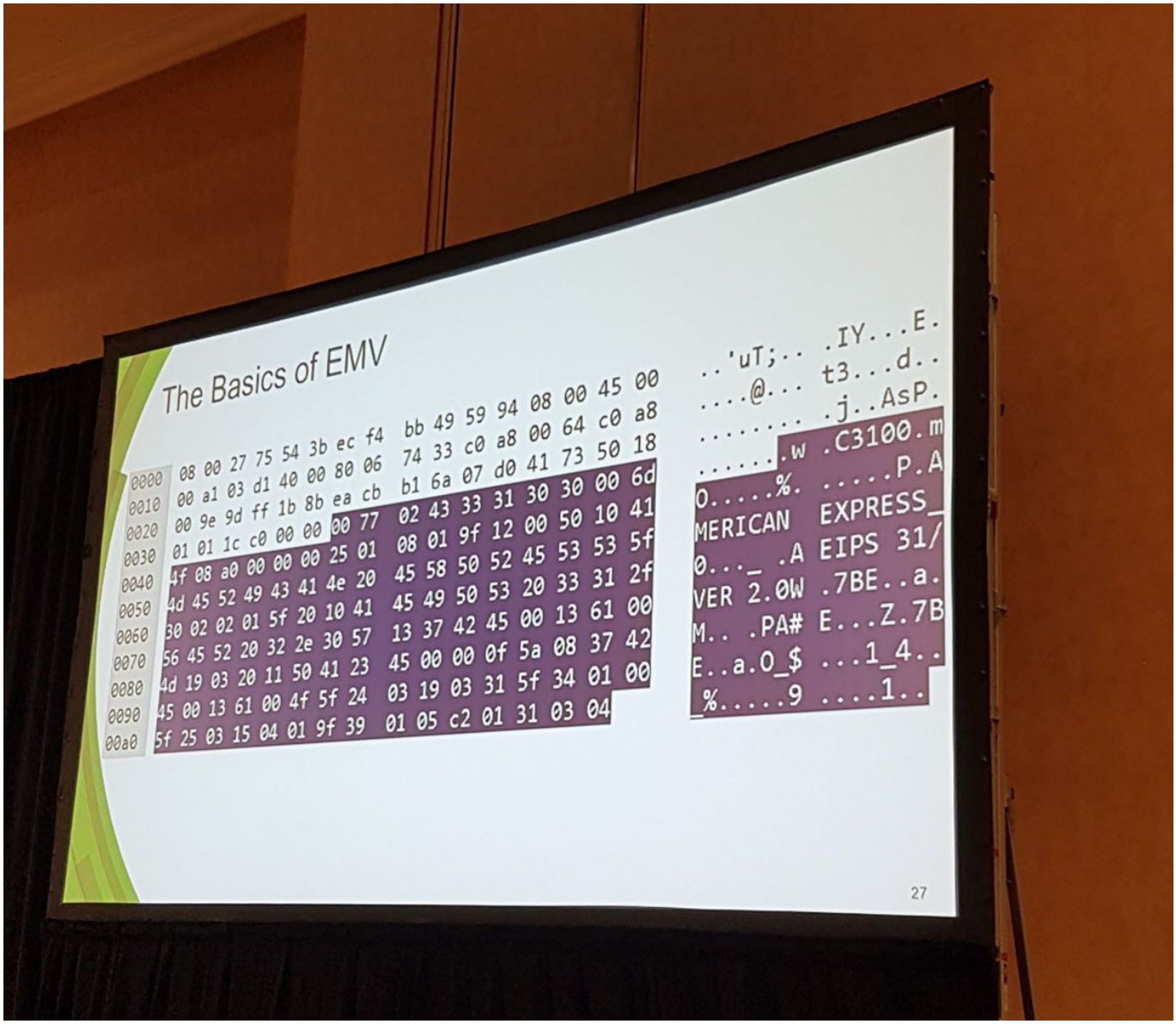

Level 2:
Black Hat Boulevard
Briefings and Trainings Registration
Briefings and Trainings Breakfast and Lunch
Breakers, Lagoon, Mandalay, Reef, Surf Ballrooms
Keynote, NOC, Speaker and Media Offices
black hat
USA 2016
black hat
USA 2016
black hat
USA 2016

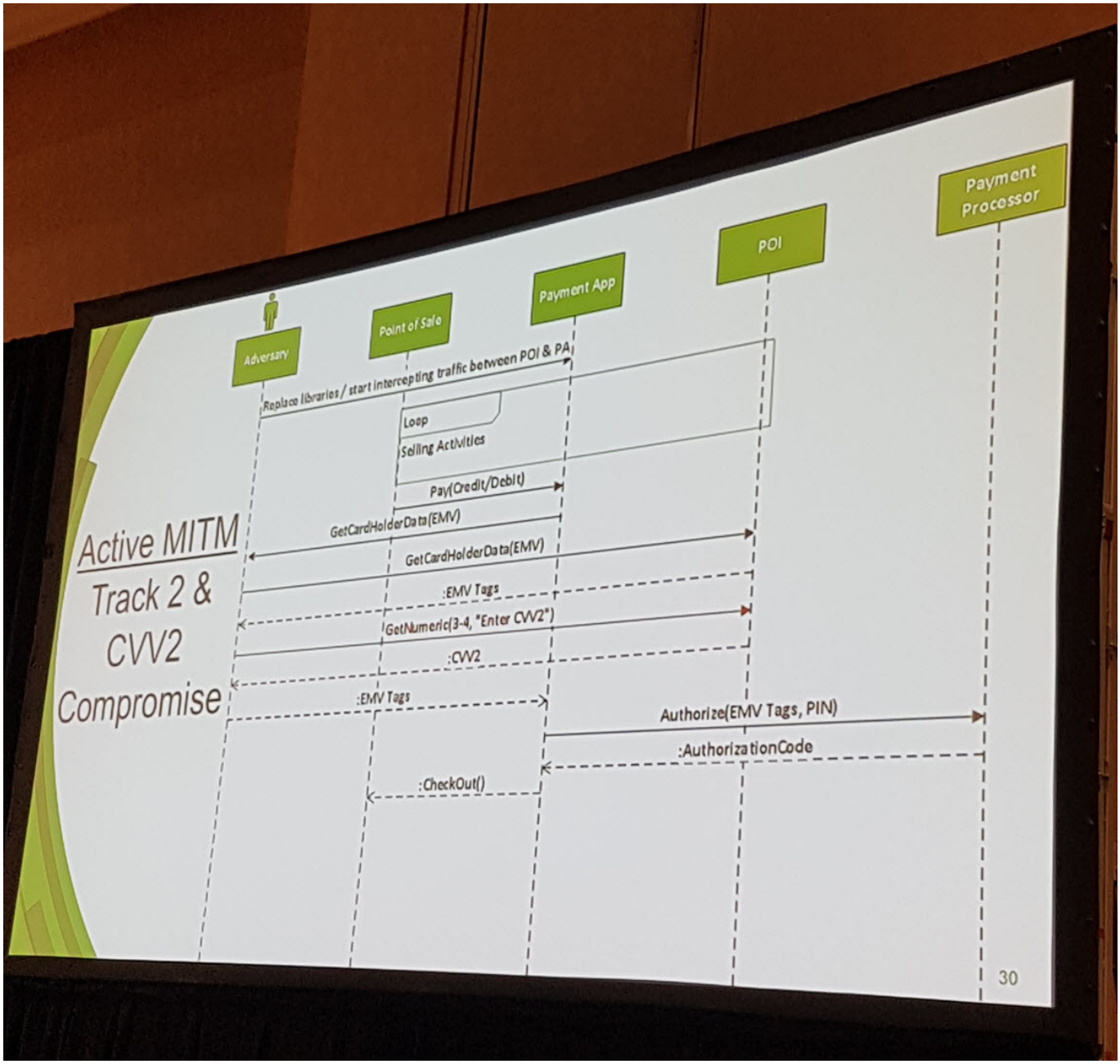

WELCOME TO
black hat®
USA 2016
Briefings Registration
NOC
Black Hat Boulevard
Briefings Breakfasts and Lunches
Keynote
Sales Suite
Sponsored Workshops
Breakers, Lagoon, Reef, Surf Rooms
Mandalay A through H Ballrooms
Speaker and Media Registration
Working Media Center
Event Management Office
Twitter: @BlackHatEvents Hashtag: #BHUSA



Katıldığım sunumlardan, Breaking Payment Points Of Interaction (POI) sunumunda POS cihazının tuş takımına (Pinpad) ortadaki adam saldırısı (MITM) yapılarak müşteriden Pin girmesini istemeleri ve daha sonrasında aradaki

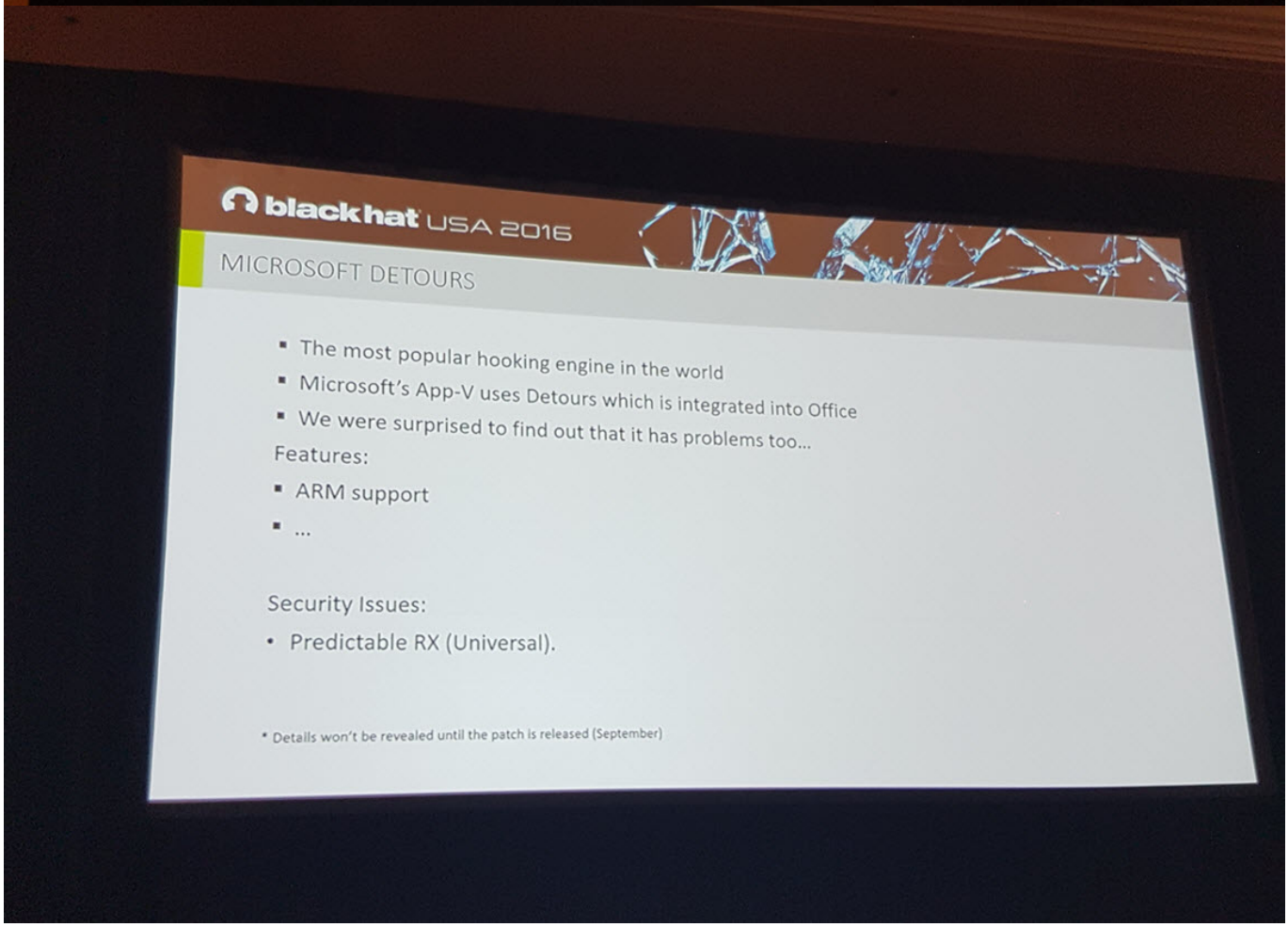
haberleşme şifreli olmadığı için çalabilmeleri, müşteriye gösterilen ekranlara kendi mesajlarını enjekte edebilmeleri oldukça ilginçti.

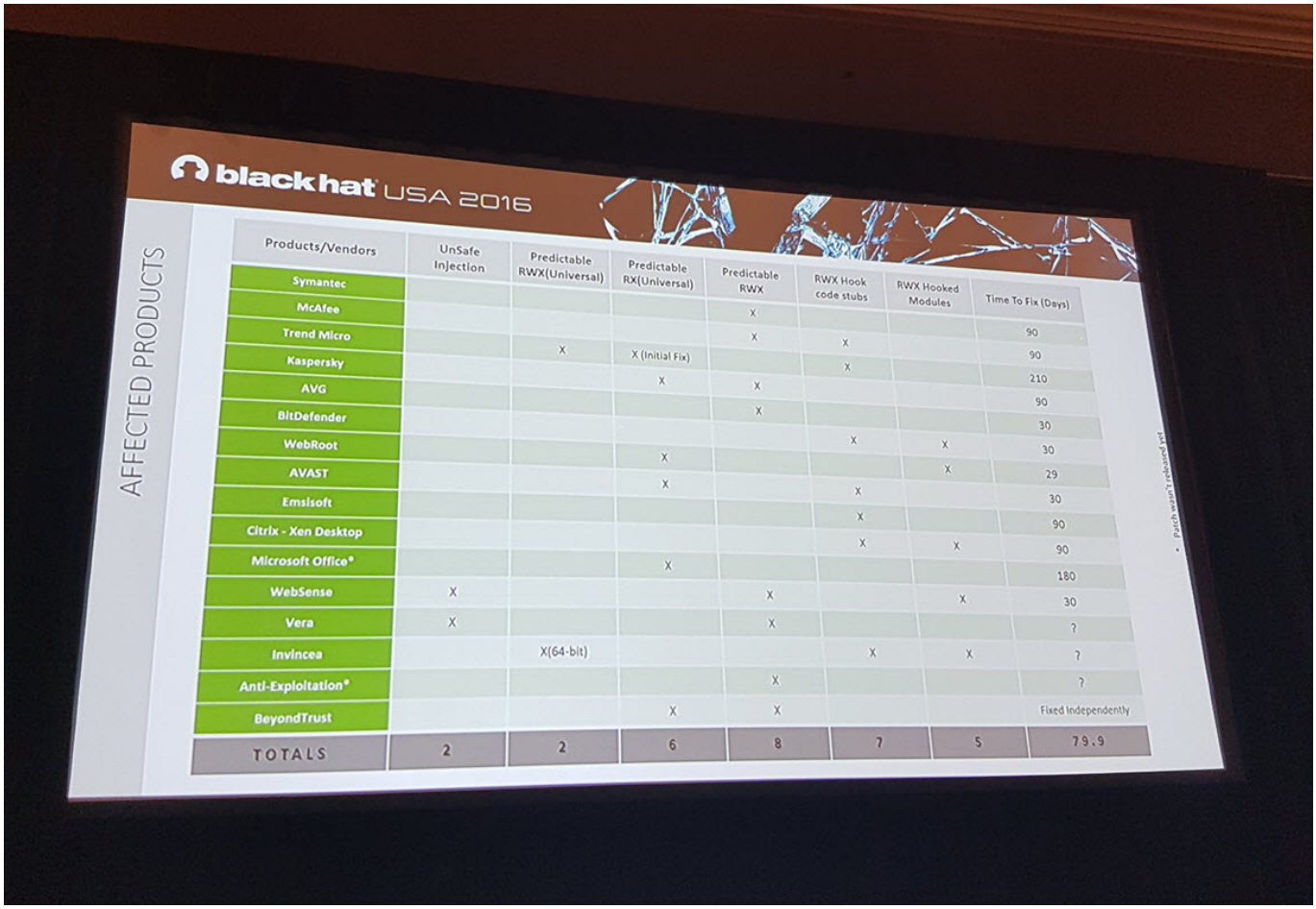

The Basics of EMV
0000 08 00 27 75 54 3b ec f4 bb 49 59 94 08 00 45 00 ..'uT;.. .IY...E.
0010 00 a1 03 d1 40 00 80 06 74 33 c0 a8 00 64 c0 a8 ....@... t3...d..
0020 00 9e 9d ff 1b 8b ea cb b1 6a 07 d0 41 73 50 18 .... .j..AsP.
0030 01 01 1c c0 00 00 00 77 02 43 33 31 30 30 00 6d ....w .C3100.m
0040 4f 08 a0 00 00 00 25 01 08 01 9f 12 00 50 10 41 O.....%. .....P.A
0050 4d 45 52 49 43 41 4e 20 45 58 50 52 45 53 53 5f MERICAN EXPRESS_
0060 30 02 02 01 5f 20 10 41 45 49 50 53 20 33 31 2f 0..._ .A EIPS 31/
0070 56 45 52 20 32 2e 30 57 13 37 42 45 00 13 61 00 VER 2.0W .7BE..a.
0080 4d 19 03 20 11 50 41 23 45 00 00 0f 5a 08 37 42 M.. .PA# E...Z.7B
0090 45 00 13 61 00 4f 5f 24 03 19 03 31 5f 34 01 00 E..a.O_$ ...1_4..
00a0 5f 25 03 15 04 01 9f 39 01 05 c2 01 31 03 04 _%.....9 ....1..
27



Captain Hook: Pirating AVs To Bypass Exploit Mitigations sunumunda ise antivirüs yazılımlarının çengelleme (hook) yöntemini hatalı kullanmaları sebebiyle yüklü oldukları sistemlerin güvenliğini nasıl zayıflattığı ile ilgili kısımlar da oldukça önemliydi.

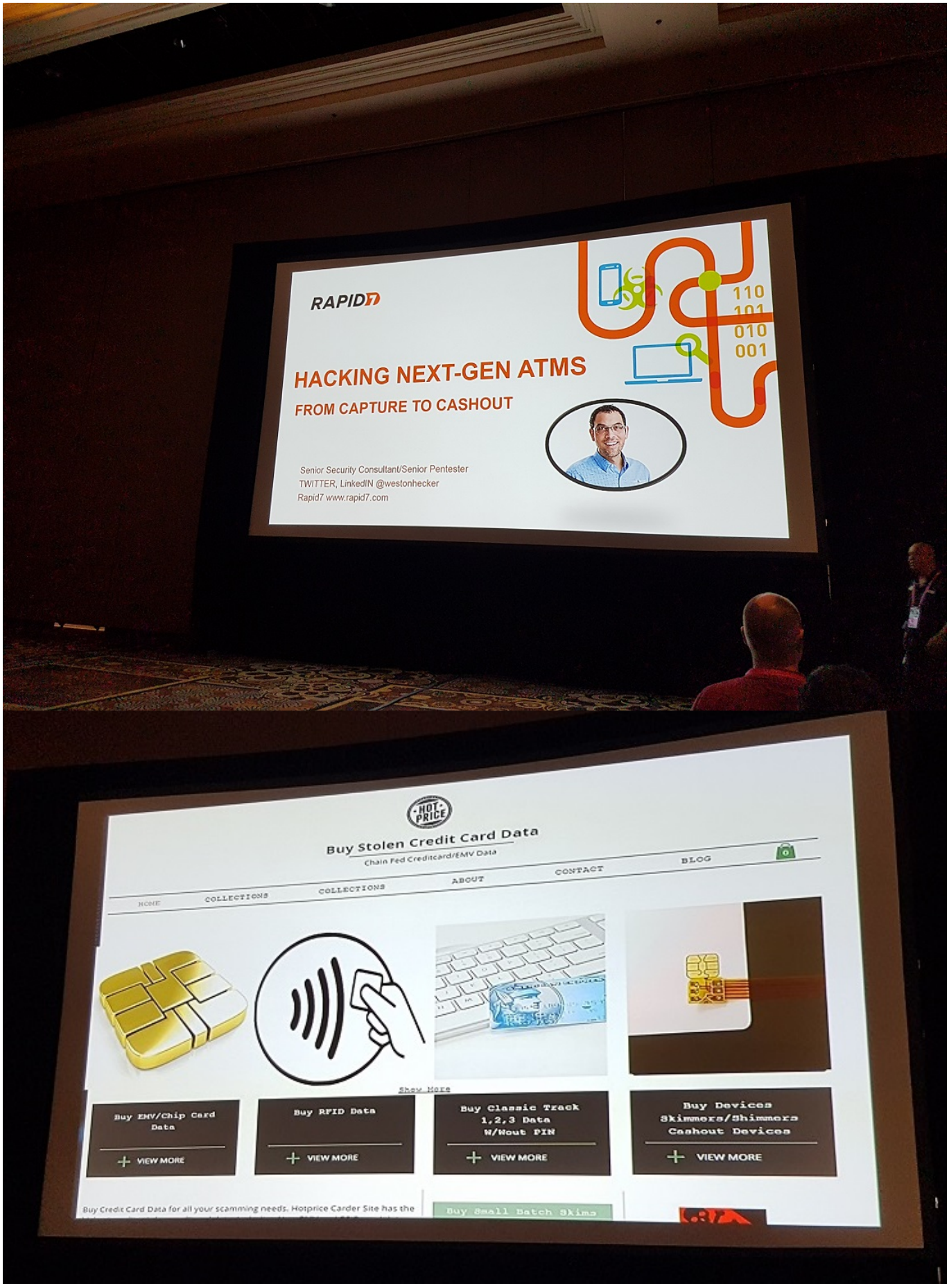

black hat
USA 2016
Captain Hook:
Pirating AVS to Bypass Exploit Mitigations
JULY 30 - AUGUST 4, 2016 / MANDALAY BAY / LAS VEGAS

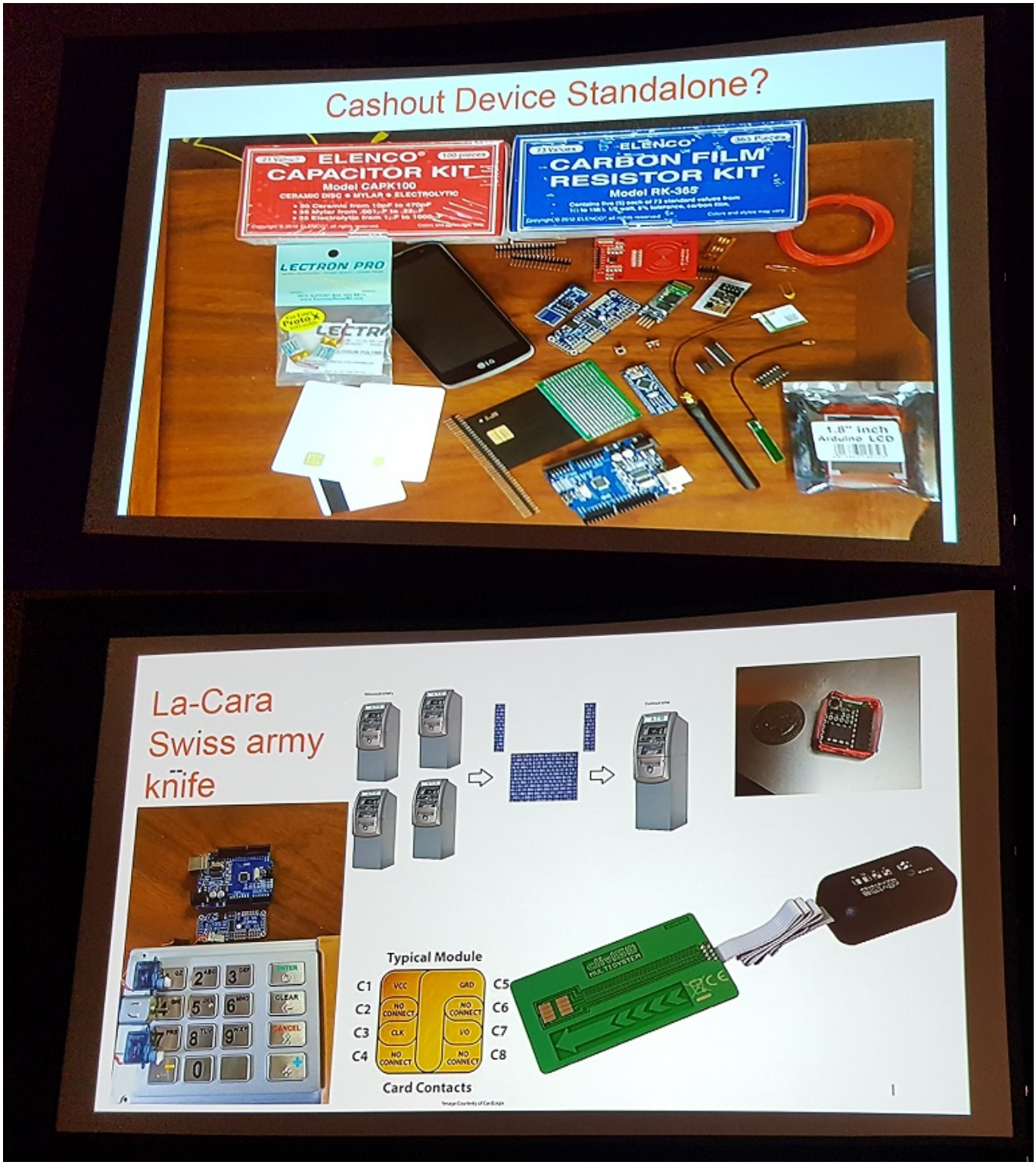

black hat USA 2016
MICROSOFT DETOURS
The most popular hooking engine in the world
Microsoft's App-V uses Detours which is integrated into Office
We were surprised to find out that it has problems too...
Features:
ARM support
...
Security Issues:
Predictable RX (Universal).
* Details won't be revealed until the patch is released (September)



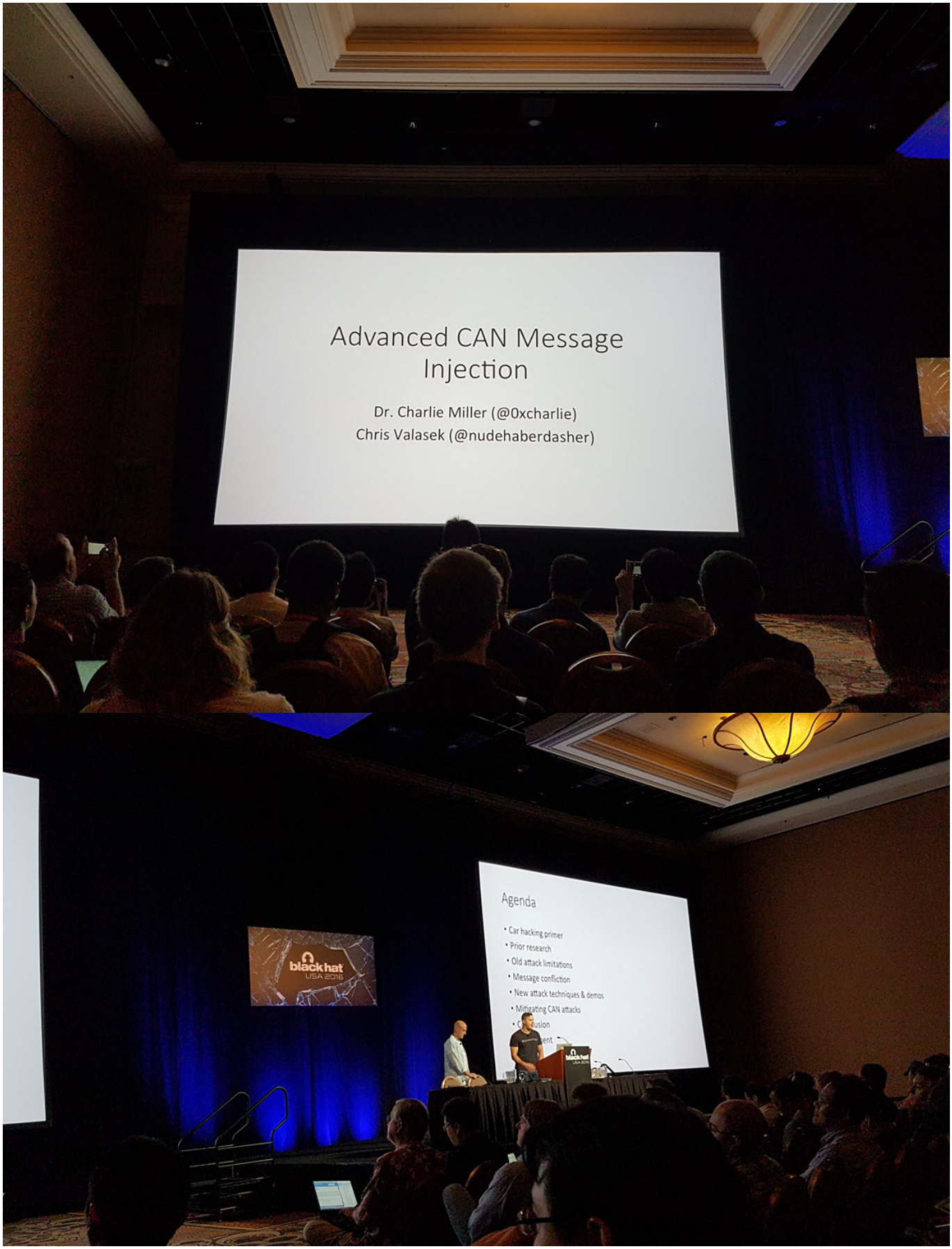
Konferansa damgasını vuran sunumlardan biri olan Hacking Next-Gen ATMs: From Capture To Cashout sunumunda ise Shimmer dediğimiz aygıtlar ile dolandırıcılar tarafından banka hesaplarının ATM üzerinden nasıl boşaltılabilindiği gözler önüne serildi. Ayrıca son zamanlarda dolandırıcıların temassız kredi kartı bilgilerini de satın almaya başladıkları bilgisi, dikkat çeken bir diğer önemli noktaydı.

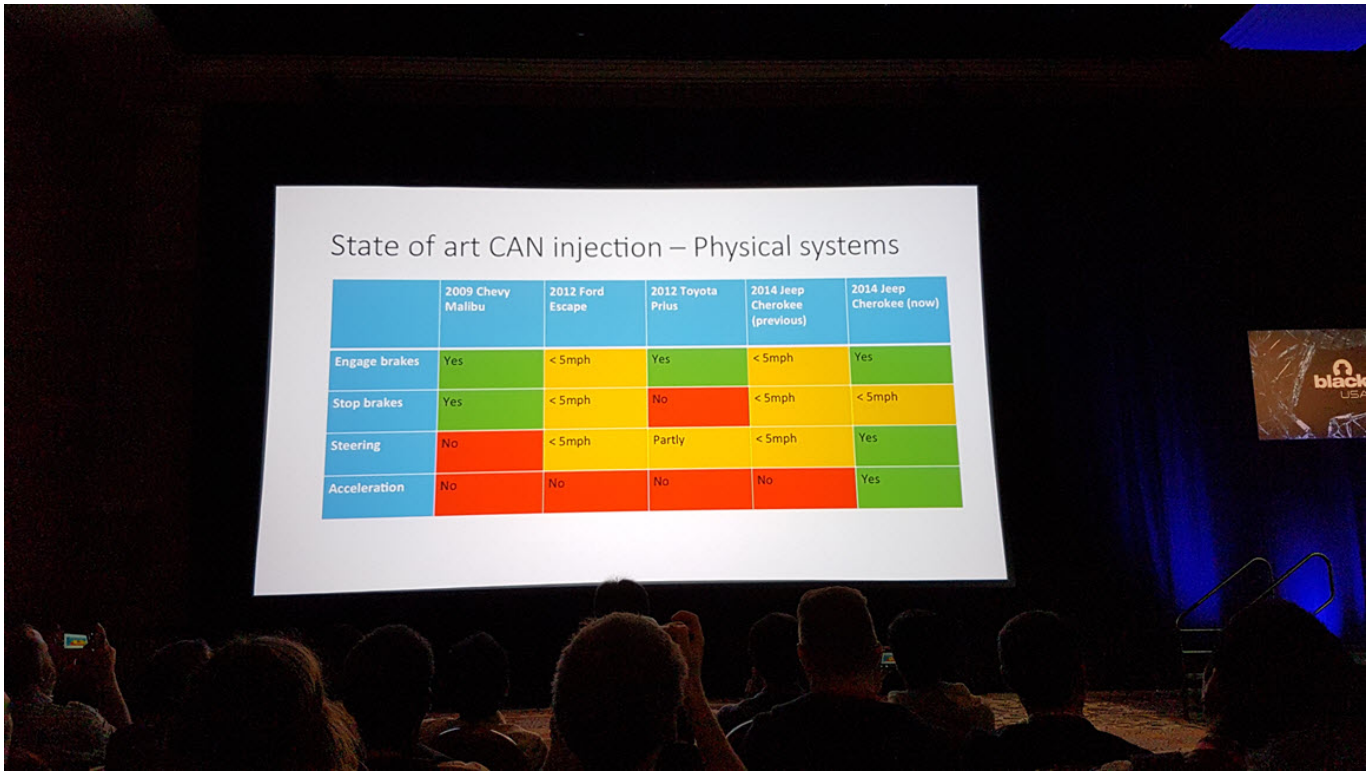
Shimmer, ATM'de kart okuyucu yuvasına yerleştirilen ve günümüzde güvenli olarak kabul edilen Çip & Pin destekli EMV kartın çipi ile ATM'nin çip okuyucusu arasındaki bilgiyi çalan ve dolandırıcılara bu bilgiyi anlık olarak gönderen bir aygıttır. Bu bilgiyi alan dolandırıcı, başka bir ATM'den bu bilgi ile müşterinin banka hesabını boşaltabilmektedir.


RAPID7
HACKING NEXT-GEN ATMS
FROM CAPTURE TO CASHOUT
Senior Security Consultant/Senior Pentester
TWITTER, LinkedIN @westonhecker
Rapid7 www.rapid7.com
110
101
010
001
HOT PRICE
Buy Stolen Credit Card Data
Chain Fed Creditcard/EMV Data
HOME
COLLECTIONS
COLLECTIONS
ABOUT
CONTACT
BLOG
Show More
Buy EMV/Chip Card Data
VIEW MORE
Buy RFID Data
VIEW MORE
Buy Classic Track 1,2,3 Data W/Wout PIN
VIEW MORE
Buy Devices Skimmers/Shimmers Cashout Devices
VIEW MORE
Buy Credit Card Data for all your scamming needs. Hotprice Carder Site has the
Buy Small Batch Skims

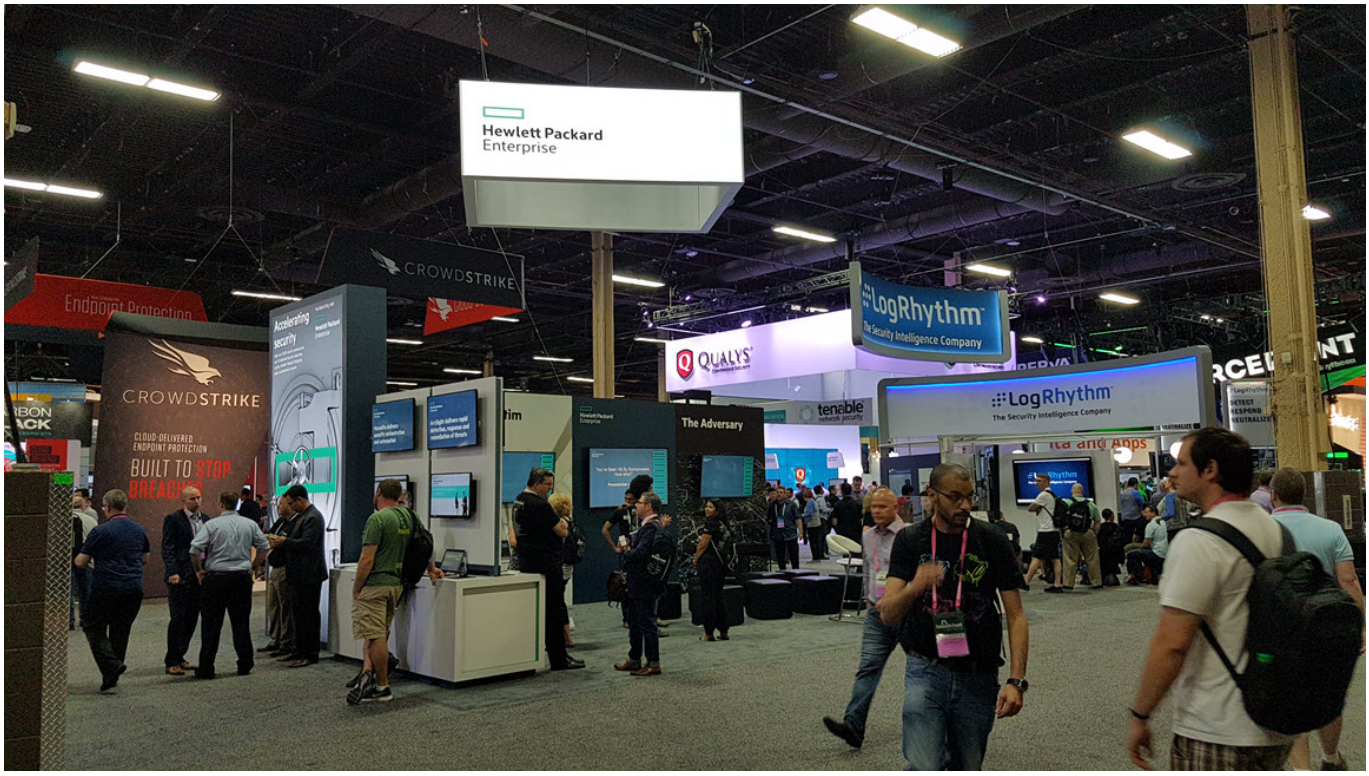


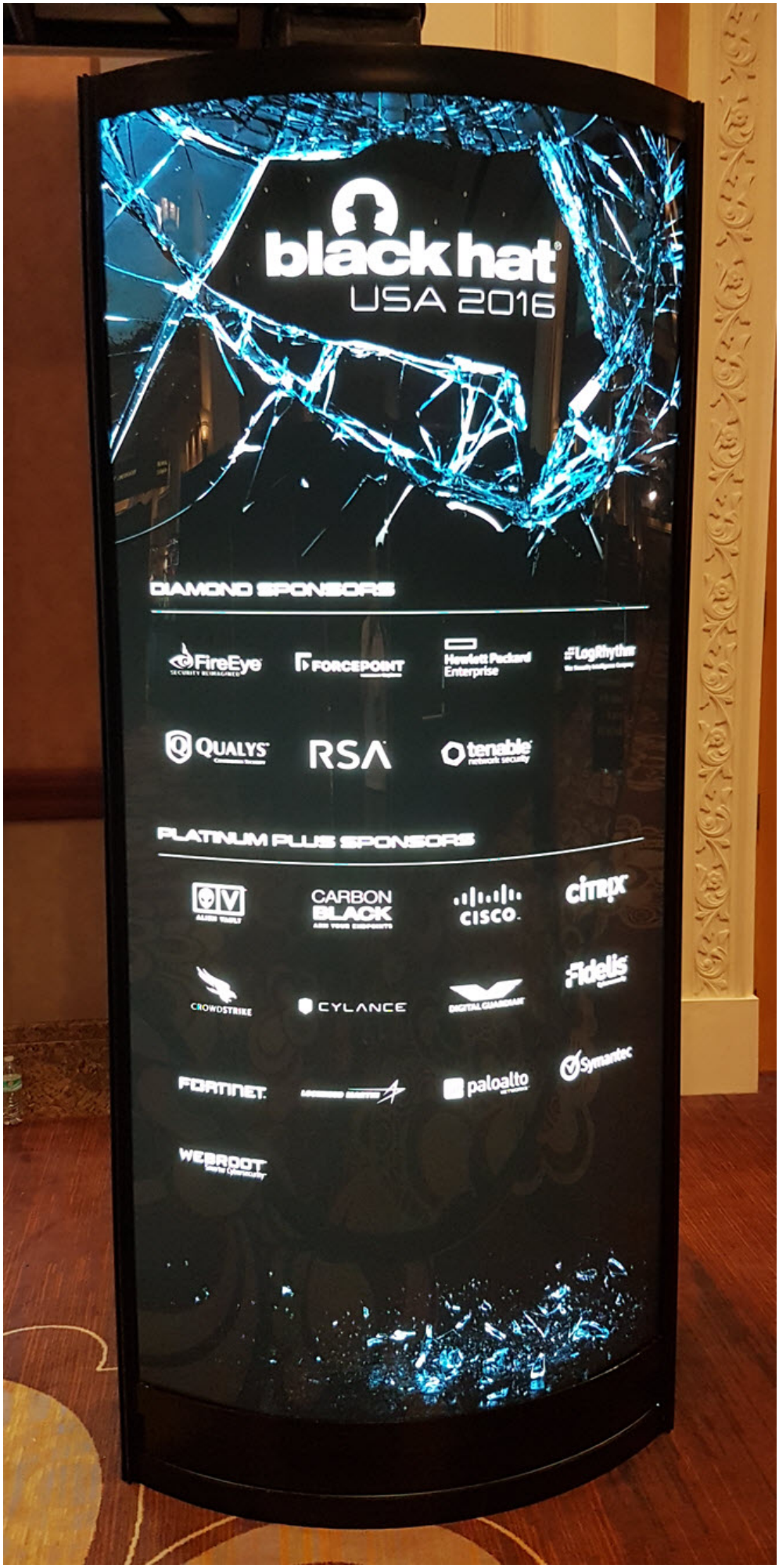
Cherokee Jeep'i hackleyerek ünlerine ün katan Charlie Miller ile Chris Valasek'in Advanced Can Injection Techniques For Vehicle Networks sunumuna geçen sene olduğu gibi yine yoğun bir ilgi vardı. Bu iki güvenlik araştırmacısı sunumlarında, araba üreticilerinin güvenlik adına sistemlerine koydukları kontrolleri nasıl aşabildiklerine ve bunun için hangi adımlardan geçtiklerine yer verdiler.


Advanced CAN Message Injection
Dr. Charlie Miller (@0xcharlie)
Chris Valasek (@nudehaberdasher)
Agenda
• Car hacking primer
• Prior research
• Old attack limitations
• Message confliction
• New attack techniques & demos
• Mitigating CAN attacks
black hat
USA 2015

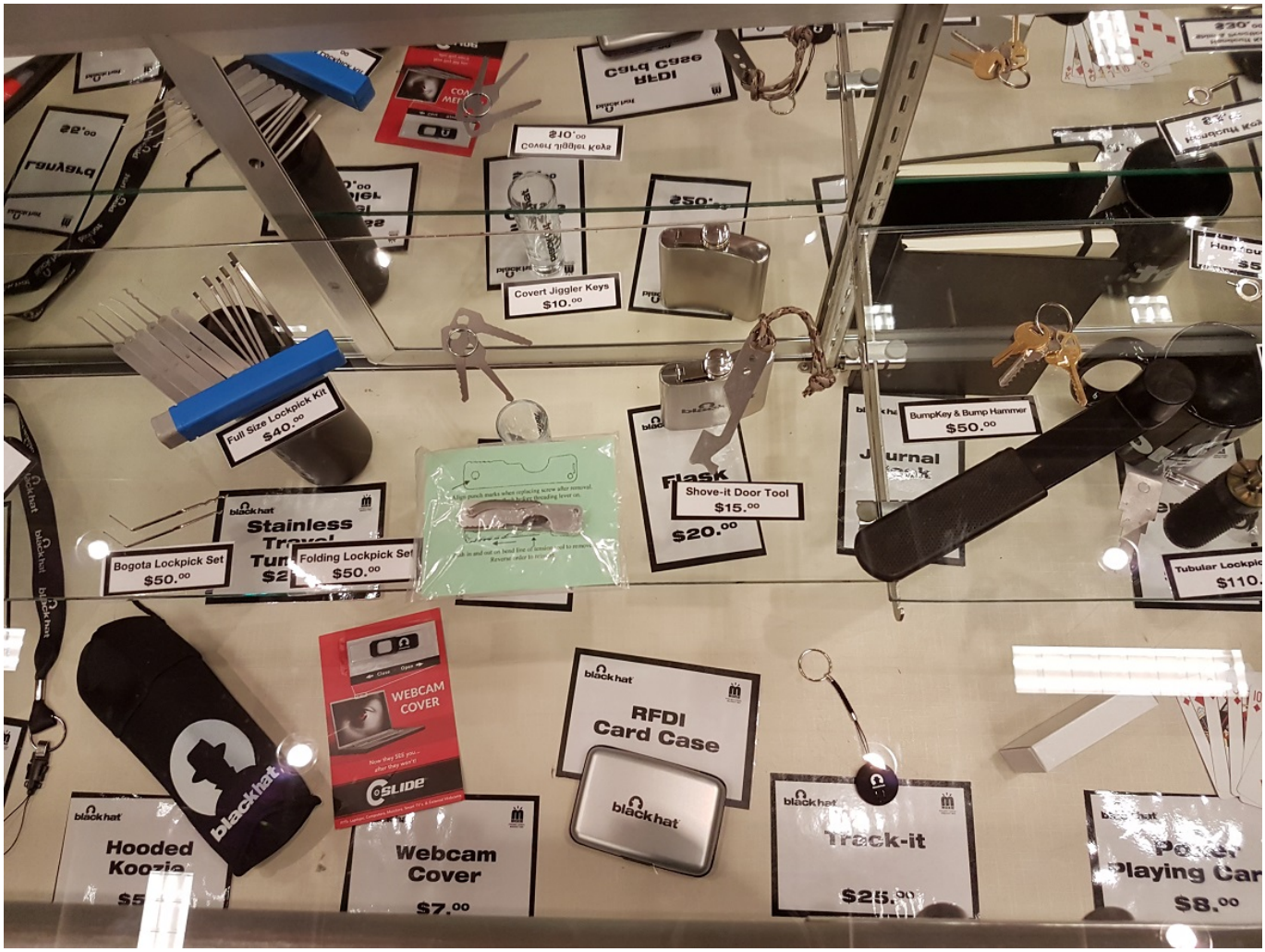


Sunumlar dışında pek tabii yine Business Hall, güvenlik dünyasının markalarına ve bu markaların görkemli stantlarına ev sahipliği yaptı. Black Hat USA 2016'da, Türkiye'de olduğu gibi "madem sponsor oldum o halde ben de konuşacağım" diyen, mikrofonu eline alıp etkinlik programını ve katılımcıların vakitlerini hiçe sayarak uzun süreler konuşup programı sarkıtan sponsor sunumları yoktu. Güvenlik etkinliği düzenlemeye niyetlenip sponsorların kaprisleri ile karşı karşıya kalanlar, sponsorları ikna etme adına aşağıdaki fotoğrafları kendileri ile paylaşabilirler. :)


Hewlett Packard
Enterprise
CROWDSTRIKE
Endpoint Protection
CROWDSTRIKE
CLOUD-DELIVERED
ENDPOINT PROTECTION
BUILT TO STOP
BREACHES
Accelerating
security
QUALYS
LogRhythm
The Security Intelligence Company
tenable
network security
The Adversary
LogRhythm
The Security Intelligence Company


black hat
USA 2016
DIAMOND SPONSORS
FireEye
FORCEPOINT
Hewlett Packard Enterprise
LogRhythm
QUALYS
RSA
tenable
PLATINUM PLUS SPONSORS
CARBON BLACK
cisco
cimpx
Fidelis
CROWDSTRIKE
CYLANCE
Symantec
FORTINET
paloalto
WEBROOT

Black Hat mağazasına her zaman olduğu gibi Black Hat hayranlarının oldukça yoğun ilgisi vardı. Birbirinden ilginç hediyelik eşyalar arasında gezinirken, Twitter takipçilerime yönelik düzenleyeceğim hediye çekilişi için ufak tefek hediyeler almayı ihmal etmedim. :)


Full Size Lockpick Kit
$40.00
Covert Jiggler Keys
$10.00
BumpKey & Bump Hammer
$50.00
Shove-it Door Tool
$15.00
Bogota Lockpick Set
$50.00
Folding Lockpick Set
$50.00
WEBCAM
COVER
SLIDE
RFDI
Card Case
Webcam
Cover
$7.00
Track-it
$25.00
$8.00

Eğitimleriyle, sunumlarıyla, atmosferiyle ve anılarıyla beni her daim büyüleyen Black Hat USA konferansı benim için yine oldukça verimli geçti. Umarım bilgi güvenliğine merakı olan herkes, imkanları dahilinde veya işverenlerinin desteğiyle bu konferansa katılma imkanını birgün yakalar. Black Hat 2017 USA blog yazısı ile tekrar görüşebilir miyiz bilmiyorum fakat görüşebilmeyi ümit ederek herkese güvenli günler dilerim. :)


black hat


412


black hat
USA 2017
SAVE THE DATES
JULY 22-27, 2017
MANDALAY BAY / LAS VEGAS
Hotel Lobby
Casino
Event Center
Restaurants
Parking Garage
Tram