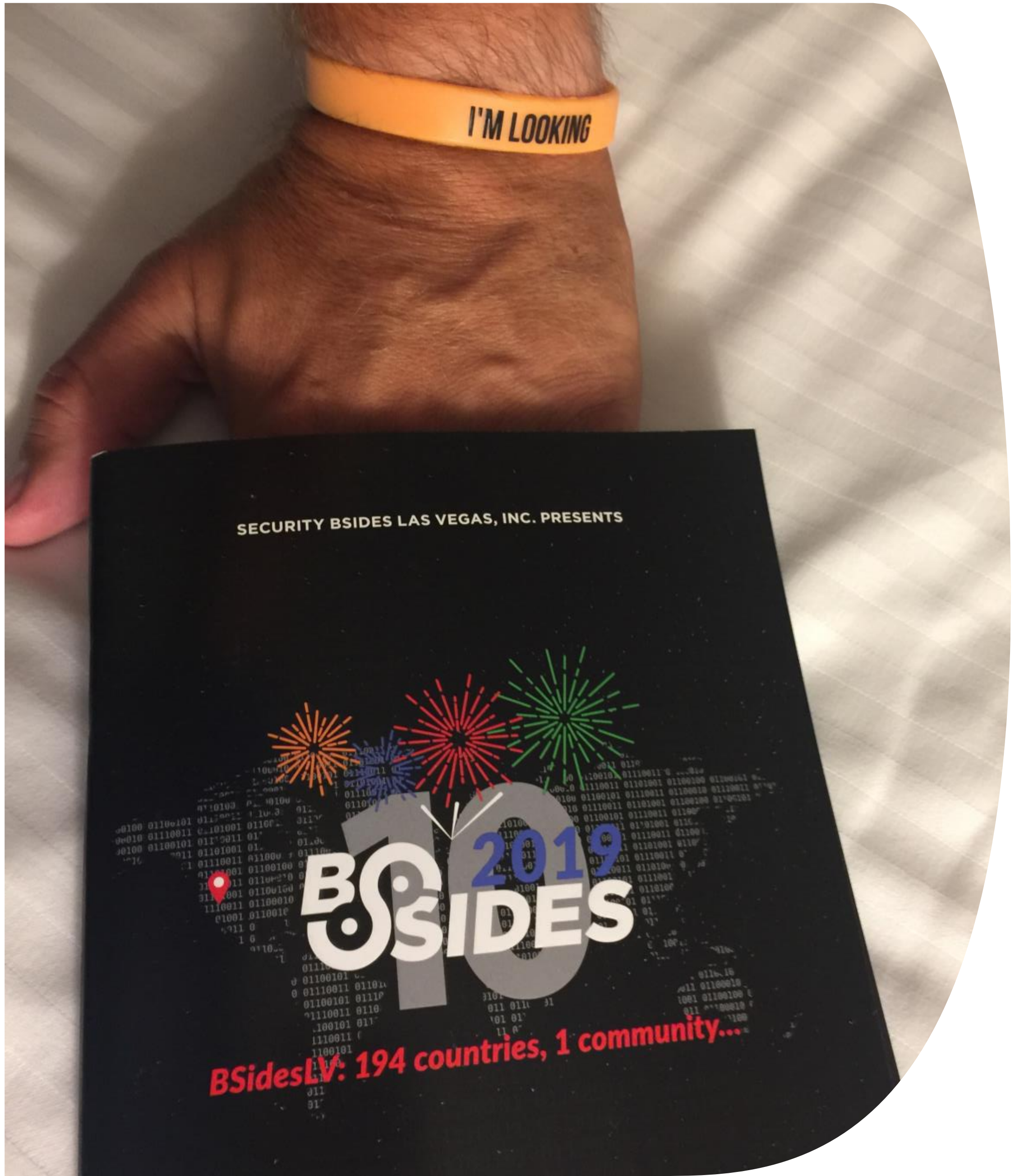
Reporting on BSides Las Vegas and DEF CON

Christian Dinesen

CiD(a7)NNIT.com

Public

WELCOME
TO Fabulous
LAS VEGAS
NEVADA
YESCO
HERBS

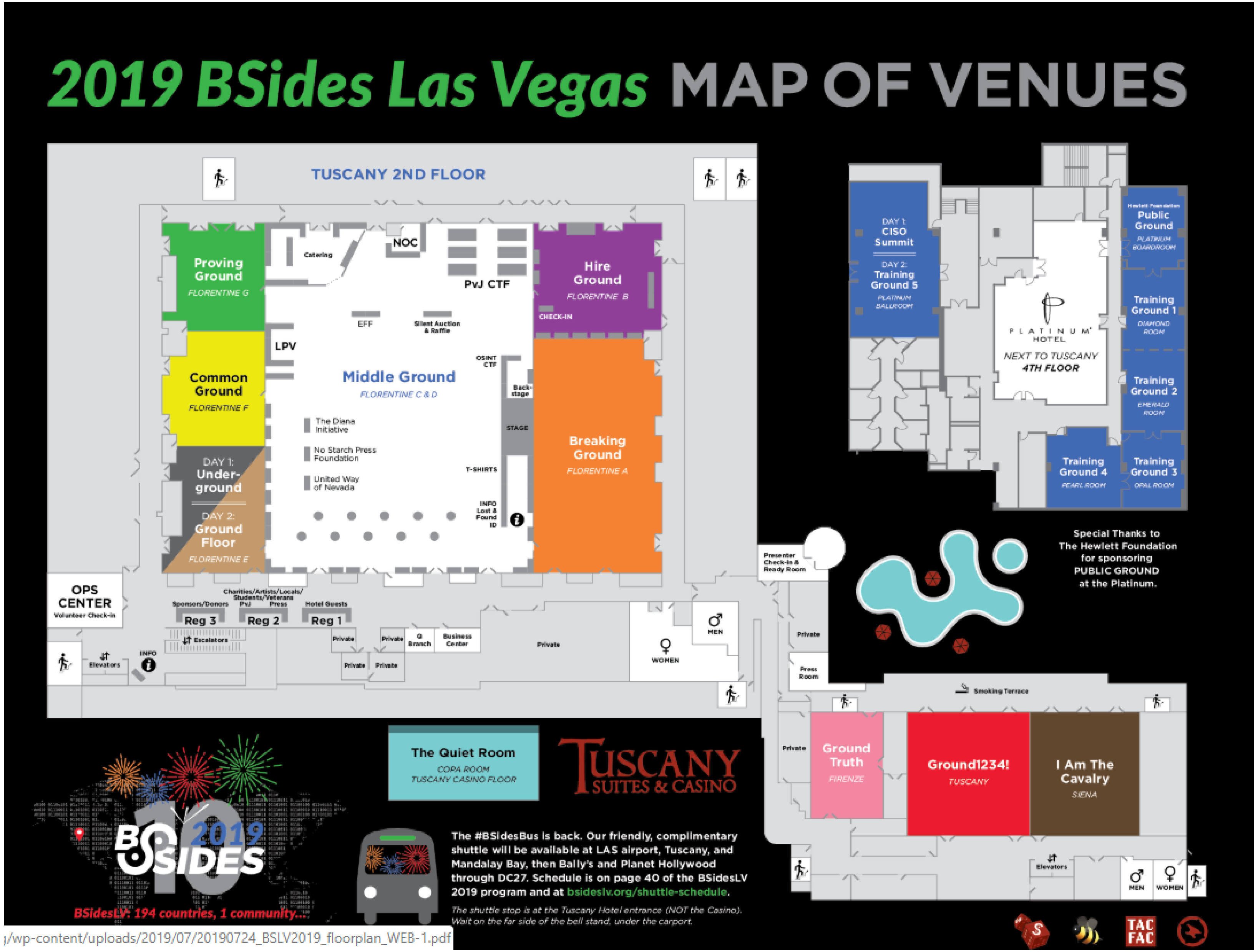

I'M LOOKING
SECURITY BSIDES LAS VEGAS, INC. PRESENTS
10
2019
BSIDES
BSidesLV: 194 countries, 1 community...

In brief

What is BSides Las Vegas

- nonprofit organization
- annual, two-day conference
- for security practitioners and those interested in (or looking to) enter the field.
- Most videos can be found here: https://www.bsideslv.org/streams/

2019 BSides Las Vegas MAP OF VENUES



Special Thanks to
The Hewlett Foundation
for sponsoring
PUBLIC GROUND
at the Platinum.

The #BSidesBus is back. Our friendly, complimentary shuttle will be available at LAS airport, Tuscany, and Mandalay Bay, then Bally's and Planet Hollywood through DC27. Schedule is on page 40 of the BSidesLV 2019 program and at bsideslv.org/shuttle-schedule.

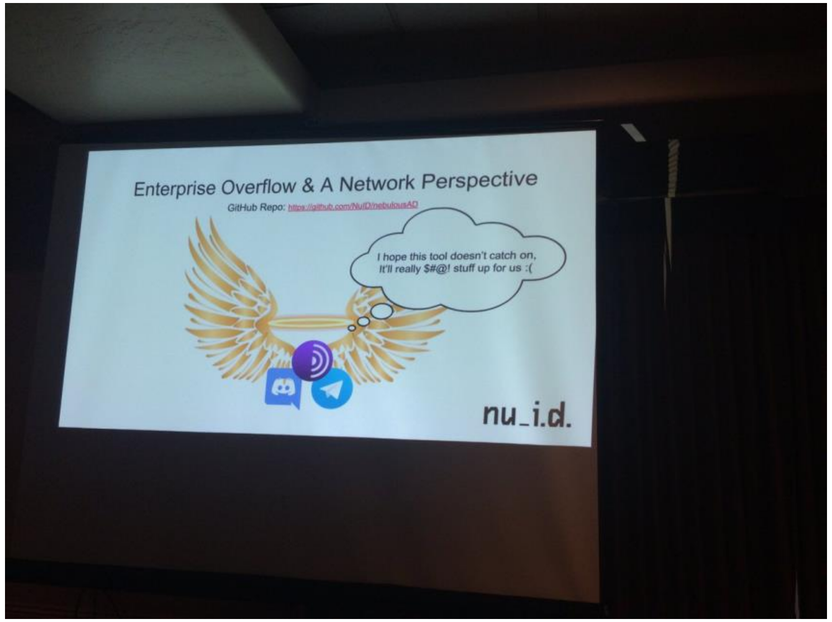
The shuttle stop is at the Tuscany Hotel entrance (NOT the Casino). Wait on the far side of the bell stand, under the carport.

g/wp-content/uploads/2019/07/20190724_BSLV2019_floorplan_WEB-1.pdf

Enterprise Overflow: How Breached Credentials Impact Us All

- If identity is the new perimeter, it is also the new battleground. Each new breach of credential data leads to a ripple effect of identity theft and fraud across enterprises, regardless of industry. A single leaked password from an obscure forum can result in the full compromise of enterprises today. Every week brings a new dump of passwords to add to the conveniently packaged and widely distributed combolists that feed wide-scale credential-based attacks.

- https://www.youtube.com/watch?v=xJgUdNfWbE4&trk



Enterprise Overflow & A Network Perspective

GitHub Repo: https://github.com/NuID/nebulousAD

I hope this tool doesn't catch on,
It'll really $#@! stuff up for us :(
nu_i.d.

Add a little CHAOS to your USB drive

- If you’ve never thought USB devices could become even less trustworthy, then this is the talk for you. We already know USB devices might try to automatically run code when connected, or act like a hyperactive keyboard and mouse, or attempt to physically destroy the host, or masquerade as an innocent charging/data cable. But it can, actually, get worse. Say hello to the Loki Drive, a USB drive with just a little too much chaotic energy. I’ll demonstrate how a USB mass storage device can change the storage it presents to the host computer based on a set of user-defined conditions. On the offensive side this can be used to circumvent USB scanning procedures and on the defensive side this can be used to store private files that will be undetectable without time-consuming analysis.

Hidden Networks Pivoting: Redefining DNS Rebinding Attack (ReDTunnel)

- Infiltrating into internal networks by targeting people into visiting malicious websites is still being used by attackers. However, as the modern browsers are being automatically patched and endpoint protection improves, depending on either a browser 0day or the victim to click and deploy a malware on his machine narrows down attacker’s opportunities. But did you ever wonder how could someone obtain access to internal network by only relying on the victim’s browser as the main weapon?
- In this talk, we will propose an attack concept that brings a whole new attack surface to infiltrate internal networks. The attack will work even on the latest patched browsers and without deploying any malware. By combining and advancing existing concepts of JavaScript reconnaissance techniques and DNS rebinding attacks, internal applications could be now exposed to the outside world while going unnoticed.

https://www.scorpiones.io/articles/redtunnel-redefining-dns-rebinding-attack

Exploiting Windows Group Policy for Reconnaissance and Attack

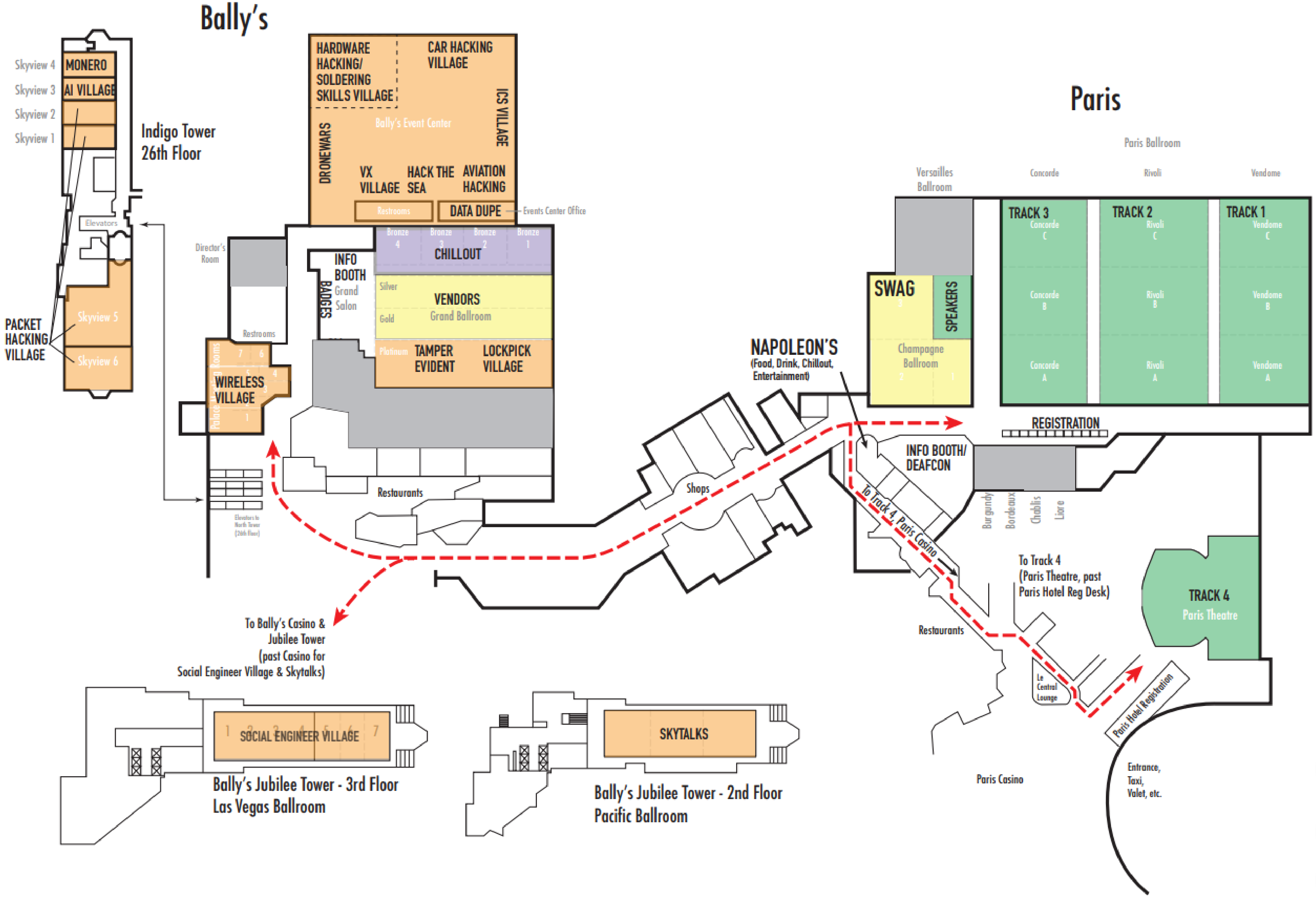
- In this talk, Group Policy expert Darren Mar-Elia (a.k.a. the GPOGUY) looks at Active Directory Group Policy from an attacker’s perspective, illustrating techniques that can be leveraged to gain insight into an organization’s Windows security posture, privileged use and opportunities for compromise. He’ll start by explaining how GP works under the covers, then dig into tools and techniques you can use to take advantage of GP’s “readability” to map out how an organized has deployed security hardening and privileged access, including how you can specifically identify admin tiering and work around it. Then Darren will dig deep into the bowels of GP to show several approaches to exploiting Group Policy, including linking exploits, write-permission/settings abuse, GPT redirection, external paths abuse and some newly documented ideas for abusing GP processing at the client to run arbitrary code. He’ll finish up by presenting some defensive techniques that can be used to harden GP against this kind of abuse

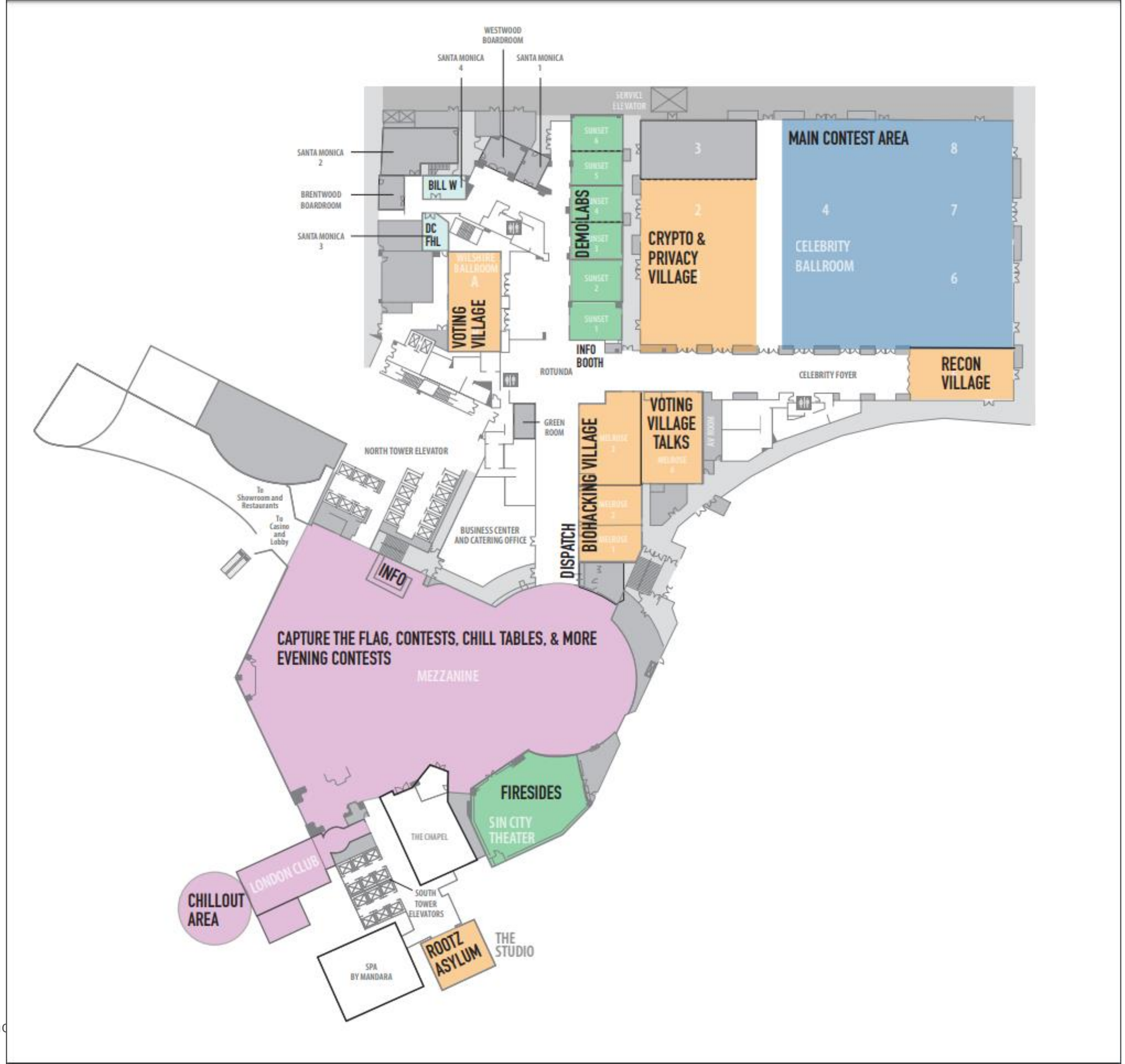
- DEF CON is one of the world's largest hacker conventions 30.000 people
- Held annually in Las Vegas, Nevada.
- For computer security professionals, journalists, lawyers, federal government employees, security researchers, students, and hackers with a general interest in software, computer architecture, hardware modification, and anything else that can be "hacked”.

- Some presentation can be found here: https://defcon.org/

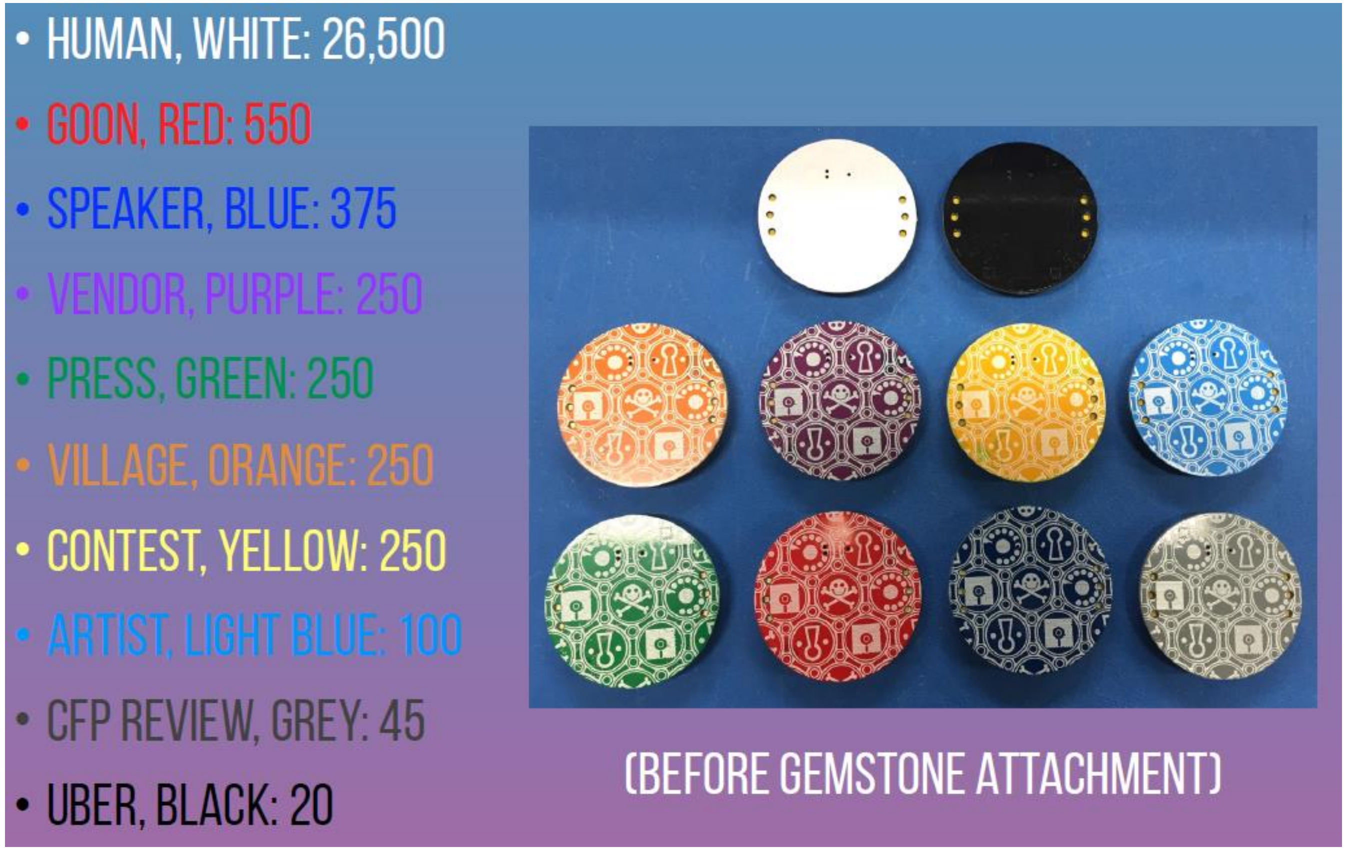
blackhat
DEFCON 2019
DANGERS OF DEFCON BEING IN TOWN
YOU ARE AT RISK OF GETTING HACKED
13 ACTIO NEW

DEF CON 27 PARIS/BALLY'S FLOORPLAN



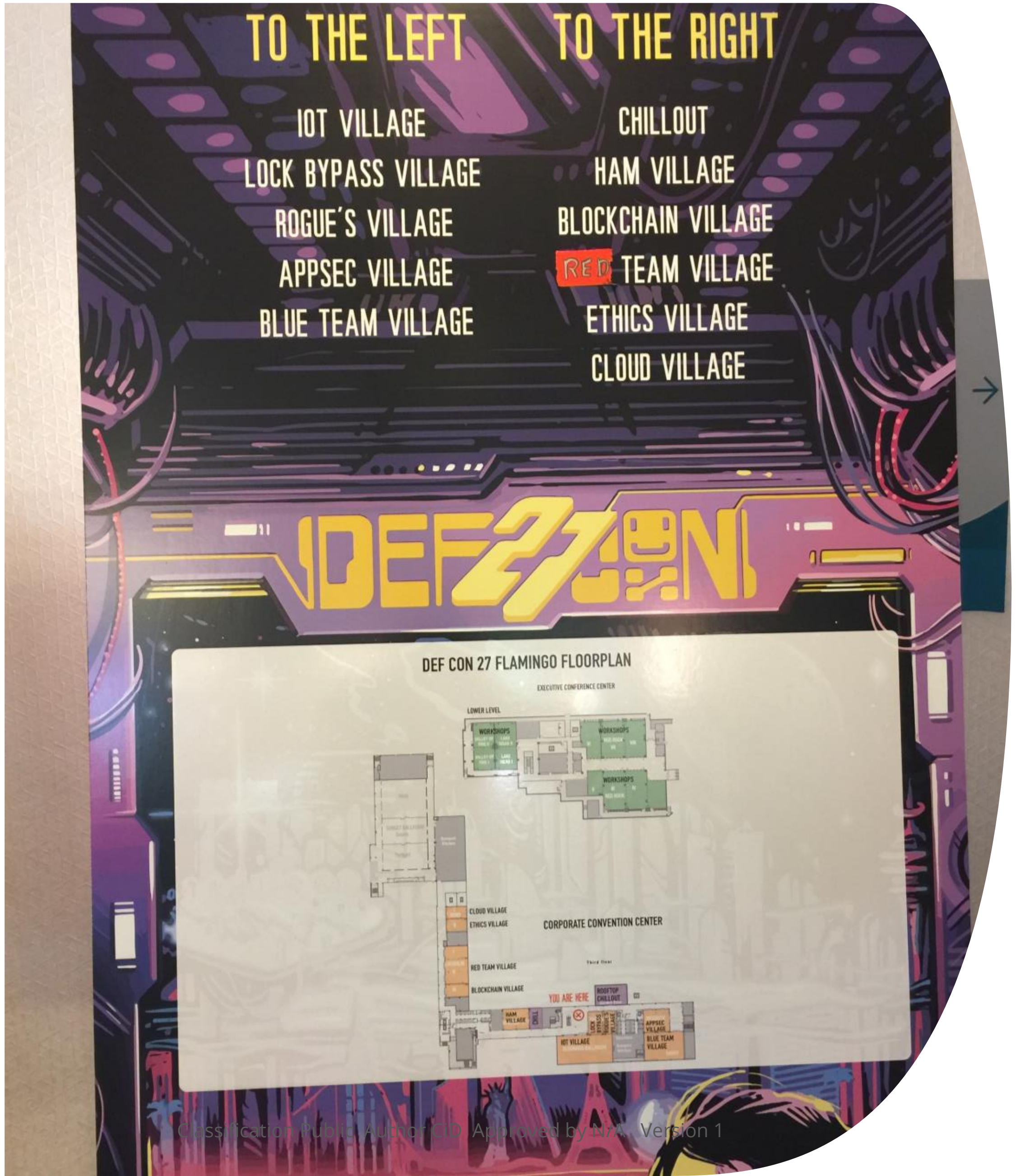

WESTWOOD BOARDROOM
SANTA MONICA 4
SANTA MONICA 1
SERVICE ELEVATOR
SANTA MONICA 2
BILL W
BRENTWOOD BOARDROOM
SANTA MONICA 3
DC FHL
WILSHIRE BALLROOM A
VOTING VILLAGE
SUNSET 6
SUNSET 5
SUNSET 4
SUNSET 3
SUNSET 2
SUNSET 1
DEMO LABS
INFO BOOTH
ROTUNDA
3
2
CRYPTO & PRIVACY VILLAGE
MAIN CONTEST AREA
8
4
7
CELEBRITY BALLROOM
6
RECON VILLAGE
CELEBRITY FOYER
GREEN ROOM
VOTING VILLAGE TALKS
MELROSE 3
MELROSE 4
AV ROOM
BIOHACKING VILLAGE
MELROSE 2
MELROSE 1
DISPATCH
NORTH TOWER ELEVATOR
To Showroom and Restaurants
To Casino and Lobby
BUSINESS CENTER AND CATERING OFFICE
INFO
CAPTURE THE FLAG, CONTESTS, CHILL TABLES, & MORE
EVENING CONTESTS
MEZZANINE
FIRESIDES
SIN CITY THEATER
THE CHAPEL
LONDON CLUB
CHILLOUT AREA
SOUTH TOWER ELEVATORS
ROOTZ ASYLUM
THE STUDIO
SPA BY MANDARA

Defcon Bagde



- HUMAN, WHITE: 26,500
- GOON, RED: 550
- SPEAKER, BLUE: 375
- VENDOR, PURPLE: 250
- PRESS, GREEN: 250
- VILLAGE, ORANGE: 250
- CONTEST, YELLOW: 250
- ARTIST, LIGHT BLUE: 100
- CFP REVIEW, GREY: 45
- UBER, BLACK: 20

(BEFORE GEMSTONE ATTACHMENT)



What is new / different?

- Villages
- Venue
- Number af participants
- Type of participants

IOT
VILLAGE
DEF CON 27
SOHOPELESSLY BROKEN
AV

I Know What You Did Last Summer: 3 Years of Wireless Monitoring at DEF CON

Many people spread a lot of fear, uncertainty and doubt about the wireless environments during DEF CON. This presentation aims to bring some clarity to what is really happening in the airwaves during one of the largest hacker conferences in the world.
d4rkm4tter (Mike Spicer)

Adventures In Smart Buttplug Penetration (testing)

Analysts believe there are currently on the order of 10 billions Internet of Things (IoT) devices out in the wild. Sometimes, these devices find their way up people's butts: as it turns out, cheap and low-power radio-connected chips aren't just great for home automation - they're also changing the way we interact with sex toys. In this talk, we'll dive into the world of teledildonics and see how connected buttplugs' security holds up against a vaguely motivated attacker, finding and exploiting vulnerabilities at every level of the stack, ultimately allowing us to compromise these toys and the devices they connect to.

https://www.youtube.com/watch?v=CsQ2VWEfduM

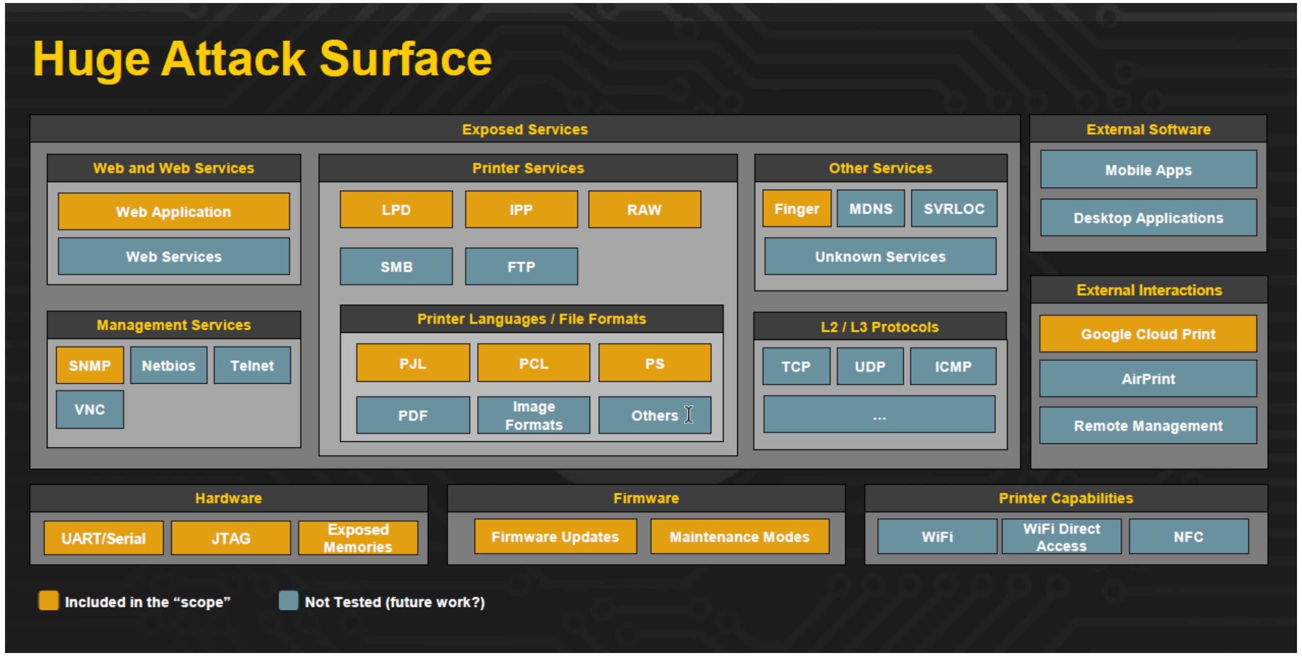
Compromise scenario 1: local hijack

Hacking Congress: The Enemy Of My Enemy Is My Friend

A SIMULATED crisis is unfolding on a national scale, based loosely on the NotPetya attack of 2017. Triggered by a yet-unknown adversary, what started as a an isolated technical issue has quickly escalated into a society-wide event affecting millions of citizens, several industries, and spanning government jurisdictions. Who is in charge, how do they cooperate with others, and how do they make decisions

Why You Should Fear Your “mundane” Office Equipment

The security of common enterprise infrastructure devices such as desktops and laptops has advanced over the years through incremental improvements in operating system and endpoint security. However, security controls for network devices such as enterprise printers are often ignored and thus present a greater potential for exploitation and compromise by threat actors seeking to gain a persistent foothold on target organizations.



Huge Attack Surface

Exposed Services

- Web and Web Services: Web Application, Web Services
- Management Services: SNMP, Netbios, Telnet, VNC
- Printer Services: LPD, IPP, RAW, SMB, FTP
- Printer Languages / File Formats: PJL, PCL, PS, PDF, Image Formats, Others
- Other Services: Finger, MDNS, SVRLOC, Unknown Services
- L2 / L3 Protocols: TCP, UDP, ICMP, ...

External Software: Mobile Apps, Desktop Applications

External Interactions: Google Cloud Print, AirPrint, Remote Management

Hardware: UART/Serial, JTAG, Exposed Memories

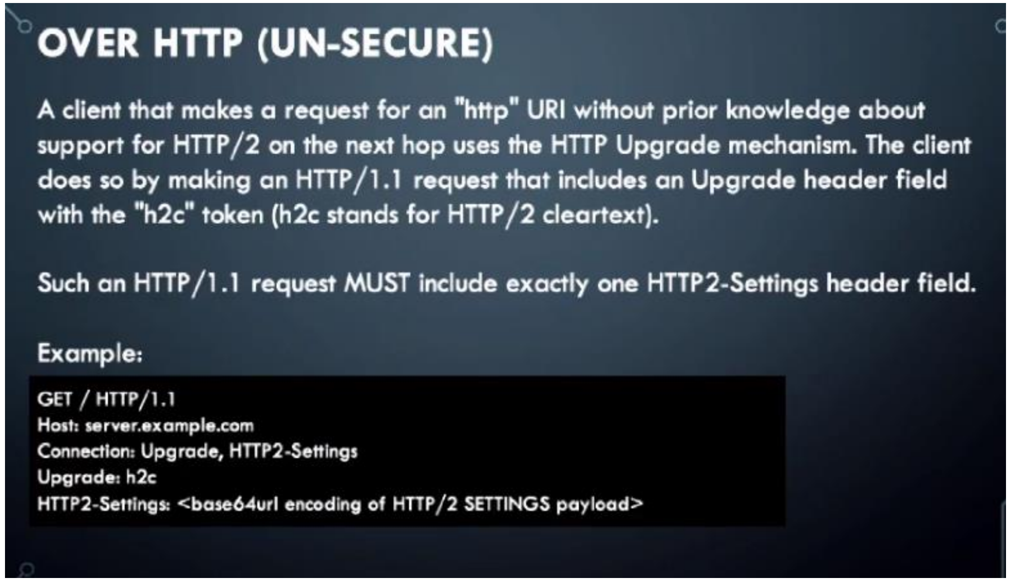
Firmware: Firmware Updates, Maintenance Modes

Printer Capabilities: WiFi, WiFi Direct Access, NFC

🟧 Included in the “scope” 🟦 Not Tested (future work?)

SKYTALK – Let’s talk about WAF (Bypass) Baby

Baby Brett Gravois @Security_Panda



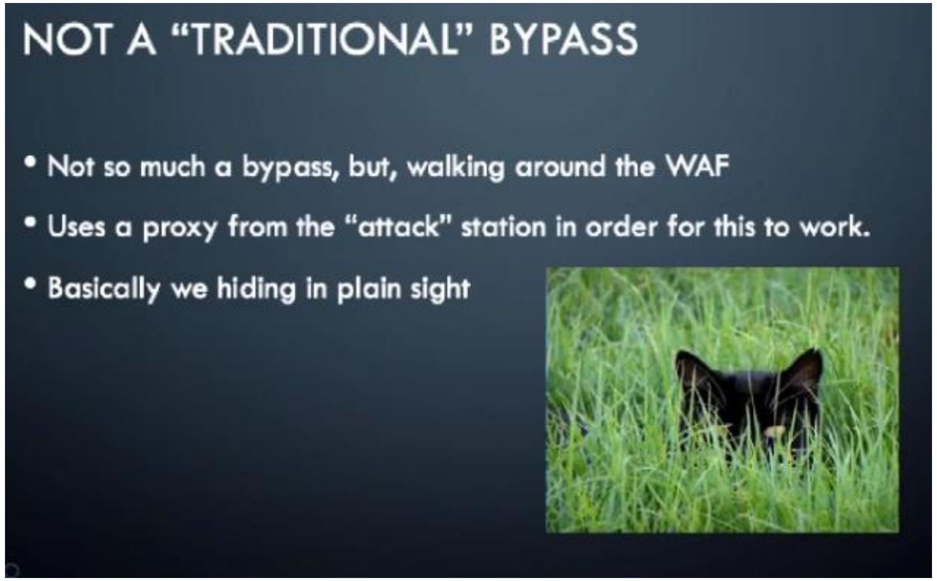
OVER HTTP (UN-SECURE)

A client that makes a request for an "http" URI without prior knowledge about support for HTTP/2 on the next hop uses the HTTP Upgrade mechanism. The client does so by making an HTTP/1.1 request that includes an Upgrade header field with the "h2c" token (h2c stands for HTTP/2 cleartext).

Such an HTTP/1.1 request MUST include exactly one HTTP2-Settings header field.

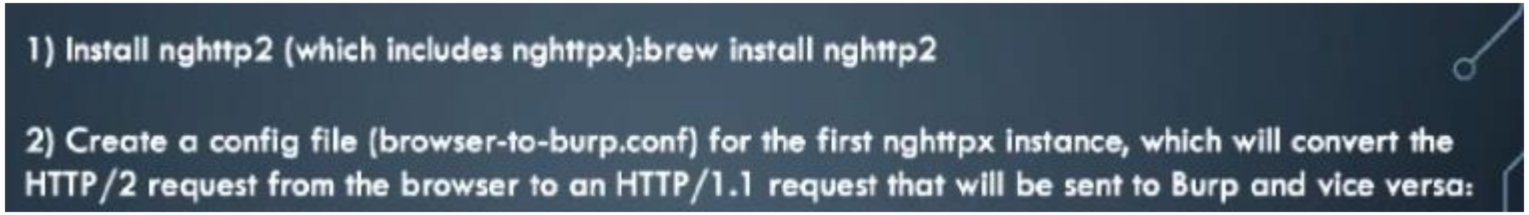
Example:

```
GET / HTTP/1.1
Host: server.example.com
Connection: Upgrade, HTTP2-Settings
Upgrade: h2c
HTTP2-Settings: <base64url encoding of HTTP/2 SETTINGS payload>
```



NOT A “TRADITIONAL” BYPASS

- Not so much a bypass, but, walking around the WAF
- Uses a proxy from the “attack” station in order for this to work.
- Basically we hiding in plain sight



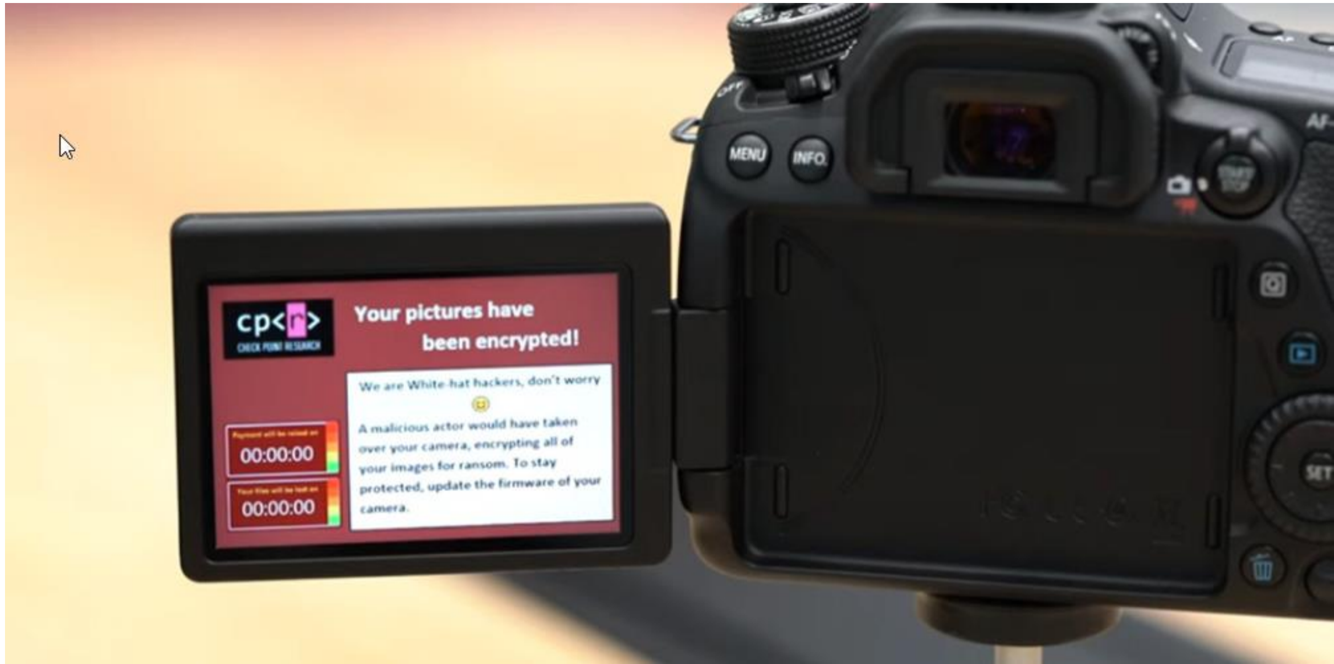
1) Install nghttp2 (which includes nghttpx):brew install nghttp2

2) Create a config file (browser-to-burp.conf) for the first nghttpx instance, which will convert the HTTP/2 request from the browser to an HTTP/1.1 request that will be sent to Burp and vice versa:

(http://www.irongeek.com/i.php?page=videos/nolacon2019/nolacon-2019-c-10-lets-talk-about-waf-bypass-baby-brett-gravois)

Say Cheese - How I Ransomwared Your DSLR Camera

- It's a nice sunny day on your vacation, the views are stunning, and like on any other day you take out your DSLR camera and start taking pictures. Sounds magical right? But when you get back to your hotel the real shock hits you: someone infected your camera with ransomware! All your images are encrypted, and the camera is locked.



Your pictures have been encrypted!

Payment will be raised on
00:00:00

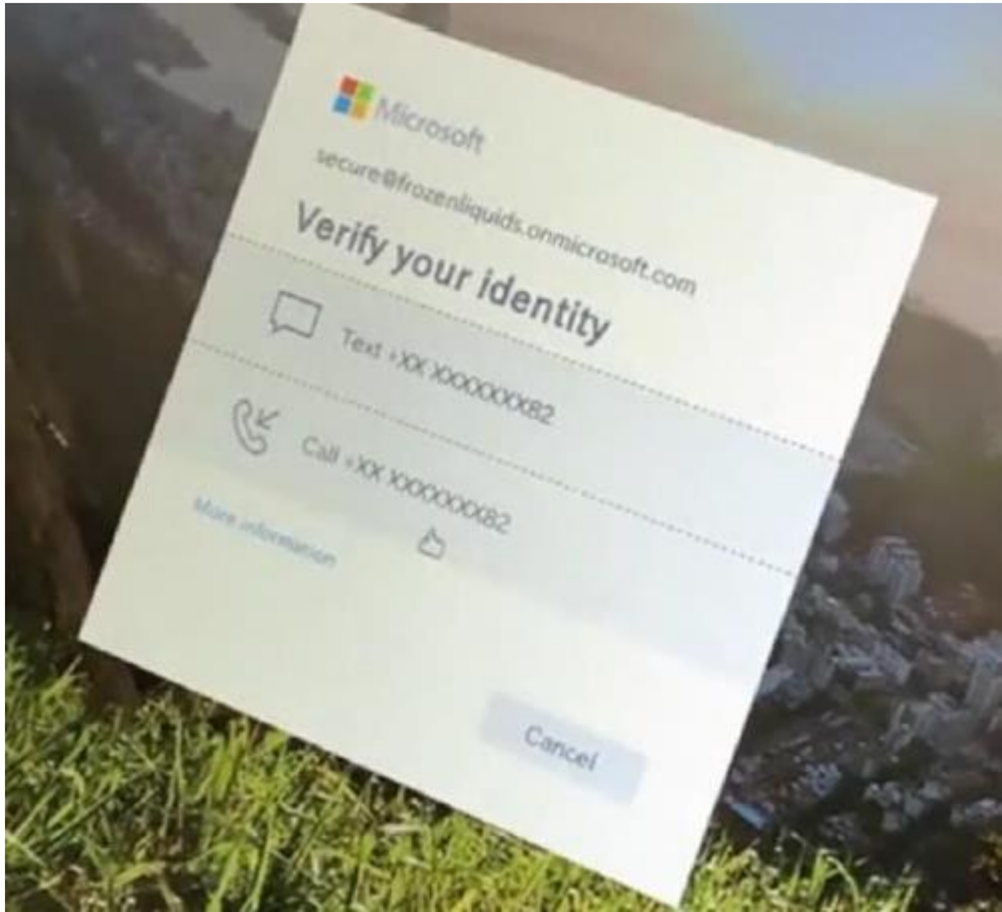
Your files will be lost on
00:00:00

We are White-hat hackers, don't worry 😊

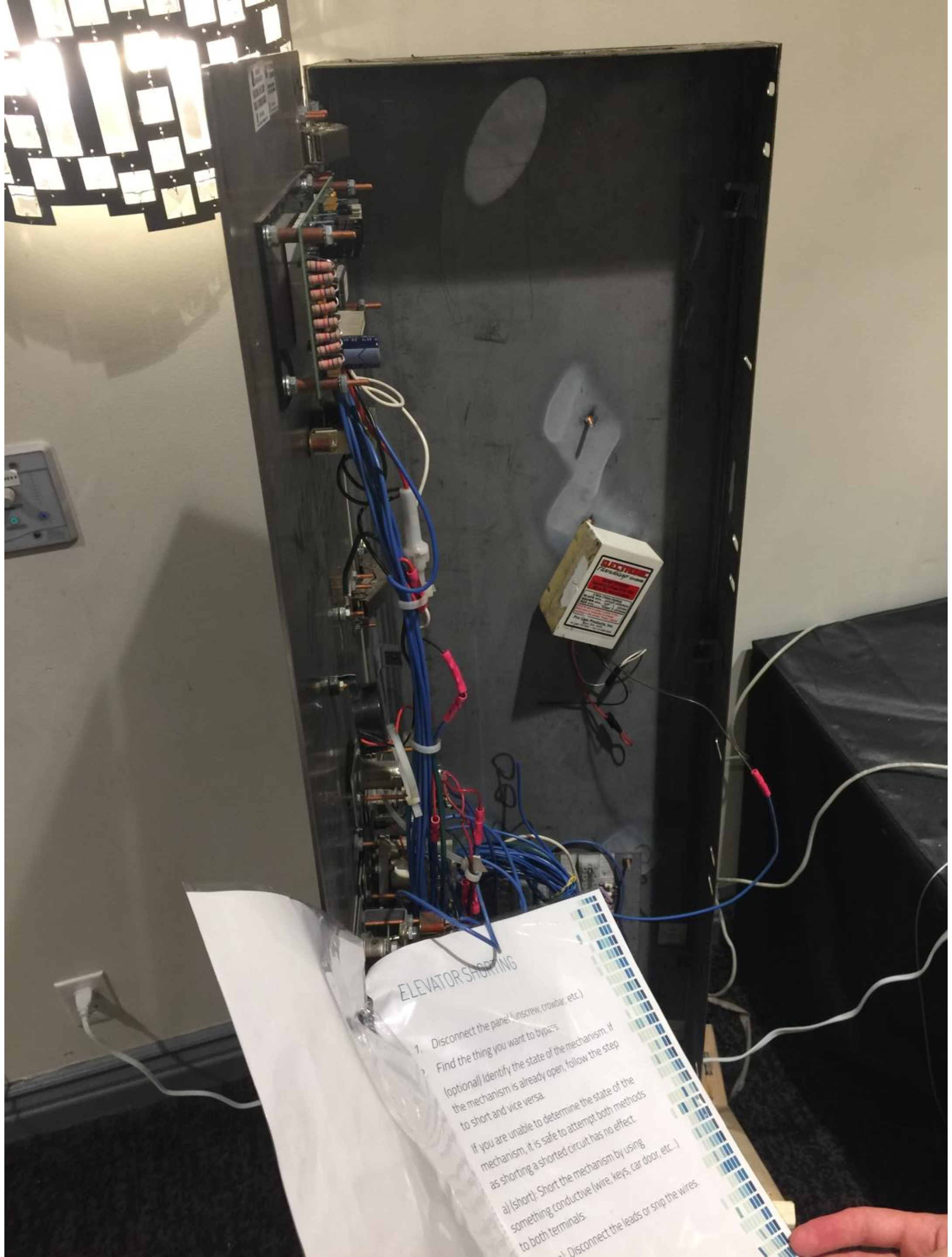
A malicious actor would have taken over your camera, encrypting all of your images for ransom. To stay protected, update the firmware of your camera.

I'm In Your Cloud... Pwning Your Azure Environement

- We start with becoming Domain Admin by compromising Azure AD Sync, sync vulnerabilities that allow for Azure admin account takeover and insecure Single Sign On configurations. Up next is cloud roles and privileges, backdooring Azure AD with service accounts, escalating privileges as limited admin and getting past MFA without touching someone's phone.



Hack the elevator



ELEVATOR SHORTING

1. Disconnect the panel (unscrew, crowbar, etc.)
2. Find the thing you want to bypass

(optional) Identify the state of the mechanism. If the mechanism is already open, follow the step to short and vice versa.

If you are unable to determine the state of the mechanism, it is safe to attempt both methods as shorting a shorted circuit has no effect.

a) (short): Short the mechanism by using something conductive (wire, keys, car door, etc...) to both terminals.

): Disconnect the leads or snip the wires.