CAPTURE THE FLAG

7 YEARS OF LESSONS

MattK 🏴‍☠️🏴‍☠️🏴‍☠️🏴‍☠️🏴‍☠️🏴‍☠️🏴‍☠️

> WHO AM I?
> WHAT'S A CTF?
> MY CTFS - WORK, DC610, DEFCON
> PUZZLE GAMES, ESCAPE ROOMS, AND CTFS
> GAME DESIGN + CTFS
> LESSONS FROM RUNNING CTFS
> FINAL THOUGHTS

AGENDA

WHO AM I?

- 12 years infosec XP
- Red Team / Hunt Team lead
  - Previously IR, intel, talking head
- Puzzlemaster of work CTF (7 years)
- Board member at DC610
- Advisor at DC908
- Escape room and puzzle fan

> WHO AM I?
> WHAT'S A CTF?
> MY CTFS - WORK, DC610, DEFCON
> PUZZLE GAMES, ESCAPE ROOMS, AND CTFS
> GAME DESIGN + CTFS
> LESSONS FROM RUNNING CTFS
> FINAL THOUGHTS

WHAT'S A CTF?

WHAT'S A CTF?

- Competition w/hacking challenges
- Popular at hacker/infosec events, tech + sec companies, colleges
- Players compete for prizes and glory

(usually)

WHAT KINDS OF CHALLENGES?

- Web security
- Network security
- Binary exploitation
- Forensics
- Log analysis
- Cryptography
- Reverse engineering
- Trivia

- Hardware hacking
- Lock picking
- Wireless hacking
- Puzzles

- …almost anything

WHY PLAY CTFS?

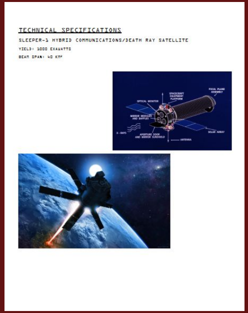
- To win prizes
- To get hands-on experience in new skills
- To show off your skills in topics you already know (“glory”)
- To make new friends
- To have fun

> WHO AM I?
> WHAT’S A CTF?
> MY CTFS - WORK, DC610, DEFCON
> GAME DESIGN + CTFS
> LESSONS FROM RUNNING CTFS
> FINAL THOUGHTS

MY CTFS

MY WORK CTFS

- 7 years running an internal corporate CTF
- Currently ~240 players
- 5 days of CTF, ~120 challenges total
- Team of 9 volunteer challenge creators and testers

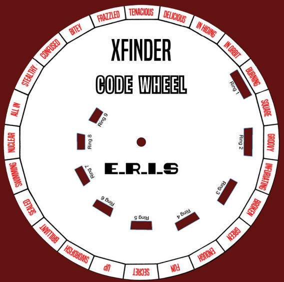

TECHNICAL SPECIFICATIONS

SLEEPER-1 HYBRID COMMUNICATIONS/DEATH RAY SATELLITE

YIELD: 1000 EXAWATTS

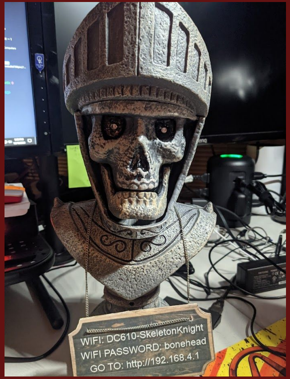
BEAM SPAN: 40 KM²

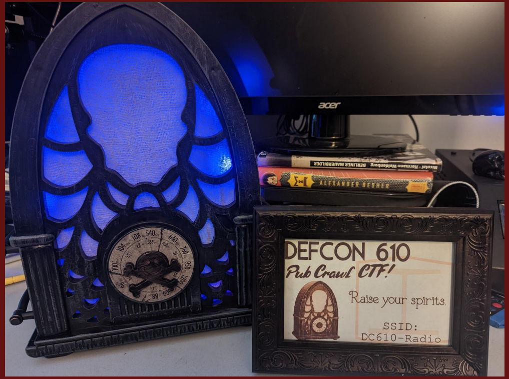
FOCAL PLANE ASSEMBLY
SPACECRAFT EQUIPMENT PLATFORM
OPTICAL MONITOR
MIRROR MODULES AND BAFFLES
X-RAYS
APERTURE DOOR AND MIRROR SUNSHIELD
SOLAR ARRAY
ANTENNA



DC610 PUB CRAWL CTFS

- 5 years creating interactive challenges for pub crawl
- Mostly standalone Wi-Fi APs with several built-in challenges
- Animation, light and sound, video





DC NEXTGEN

- CTF and puzzle box for youth event at Defcon 32
- W/small mods, it worked at the DC610 pub crawl

> WHO AM I?
> WHAT'S A CTF
> MY CTFS - WORK, DC610, DEFCON
> GAME DESIGN + CTFS
> LESSONS FROM RUNNING CTFS
> FINAL THOUGHTS

GAME DESIGN

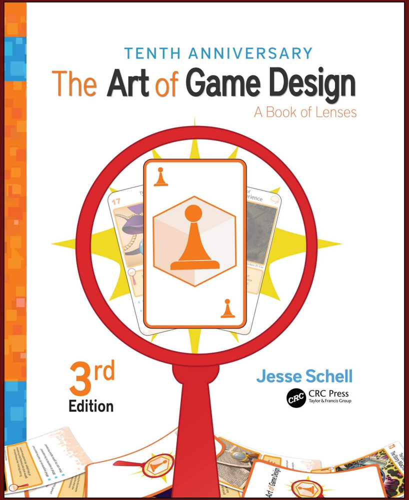
PUZZLE GAMES, ESCAPE ROOMS, AND CTFS

- All kind of the same thing
  - a game with an established set of rules
  - based around solving problems for fun

- Why not cross-pollinate ideas from each?

The Art of Game Design by Jesse Schell

- “A Book Of Lenses”
- LOTS we can apply to CTF creation
  - Definitions of fun
  - Player motivations
  - Interest curves
  - Skill
  - Story + theme



ARE CTFS FUN?

- “Fun is pleasure with surprises” – not a great definition but useful
  - Always create something novel
- Games need to ride the line between **frustration**, **elation**, and **boredom**
- *Not all surprises are fun* if players don’t buy in. (example)
- *A puzzle is a promise.*

CTFS REQUIRE SKILL

- Some players have it, some don't. Cater to both
- Create intro challenges for unskilled, provide hints at a cost
- Create hard challenges for skilled players
- ***Provide "Ringer" and "Casual" brackets***
- Challenges get harder as you progress (but leave time enough to solve everything)
- Parallel challenges when one is too hard

POINTS AND HINTS

(SO HARD TO GET RIGHT)

(And yet, so crucial for player perception of fairness)

Points

- Establish a rubric for difficulty (time-to-complete? complexity?) and assign points based on it
- TEST, ADJUST, RETEST
- Adjust mid-game if no solves for X hours

POINTS AND HINTS

(SO HARD TO GET RIGHT)

(And yet, so crucial for player perception of fairness)

Hints

- Only useful if players TRUST them to be helpful
- Establish expectations
  - Low-cost: nudge towards path
  - Medium-cost: list of needed tools
  - Full cost: walkthrough

GAME STATE

Players want to know:

- What’s my score? Who’s winning?
- What do I need to work on now? What else is available?
- Scoreboard + challenge menu w/solved vs unsolved (CTFd)
- Live event – audio + visual cues

> WHO AM I?
> WHAT'S A CTF
> MY CTFS - WORK, DC610, DEFCON
> GAME DESIGN + CTFS
> LESSONS FROM RUNNING CTFS
> FINAL THOUGHTS

LESSONS

TESTING

- Schedule time!
- More is always better.
- What you don't test, will break.
- You won't have enough time for everything.
- Challenges, scoreboard, infra – all of it.

COMM(UNITY|UNICATION)

Pre-CTF

- FAQ page – “one funnel”
- Reminders to sign up and for game start
- Promotion – someone teach me how

COMM(UNITY|UNICATION)

CTF Day

- Give players a way to talk to each other AND to their teams – even if it's just Discord
- Provide a meeting point for solo players
- Keep an open chat to communicate changes, patches, announcements
- NO DMING THE ADMINS UNLESS APPROVED

COMM(UNITY|UNICATION)

Post-CTF

❖ Spoilers Chat
❖ Feedback session (open)
❖ Questionnaire (private)
❖ Testimonials?

Keep player list for comms next time!

PLAYER FEEDBACK

- Some of it will be helpful
- A lot of it won’t
- Collect it anyway

Save praise + share w/your admins
Plan to fix issues each year

CHALLENGE DESIGN

- Accommodate new players, seasoned ones, experts
- Ramp up challenge if possible
- Always leave enough time to solve hard ones
- Connected challenges – fun, but hard to manage
- Tracks – great but possible bottleneck

> WHO AM I?
> WHAT'S A CTF
> MY CTFS - WORK, DC610, DEFCON
> GAME DESIGN + CTFS
> LESSONS FROM RUNNING CTFS
> FINAL THOUGHTS

THOUGHTS

GRAD PROGRAM

Idea from MIT Mystery Hunt:

After X years of wins, give the most dominant team a place in the Hall of Fame, retire them, and ask them to start making challenges

WHAT DO WE LIKE IN A CTF?

MORE INFO

- *The Art of Game Design: A Book Of Lenses 3rd Edition* by Jesse Schell
- *Five Things New Designers Should Know about Escape Room Puzzle Creation* by Errol Elumir (https://youtu.be/2TUvBd_40Sc)
- *30 Puzzle Design Lessons, Extended Director's Cut* by Elyot Grant (https://youtu.be/oCHciE9CYfA for Part 1)
- *Breaking Brains, Solving Problems: Lessons Learned from 2 Years of Setting puzzles for InfoSec Pros* by Matt Wixey (https://youtu.be/16JWimnLE5A)

https://pastebin.com/ZYQ8QmSe