UIUCTF Planning

Announcements

- Get questions in #announcemnts poll for Tech Services this Thursday
- Server back up, infra going back up tomorrow
- Killing it at wolvsec CTF rn

Recap

- Art theme decided

- Nick has done amazing work on UIUCTF landing page
  - https://nicholas.sh/uiuctf
  - Still need CTFd theming!

- Need much more pwn, web and **crypto** challenges

Chal Ideas

Nathan

- Nintendo DS Browser pwn
  - no bug yet
- TI OS oday pwn
  - tough deployment logistics
  - no bug yet
- sympy parse_expr oday
- Java obfuscation using invokedynamic
- Eth smart contract RE
  - First solve can get bounty from contract

Ian

- “AI cryptanalysis extraction where the model contains a bunch of a story”
- Z3 wordle
- CDN cache poisoning
- AR Scavenger hunt
- AR puzzle box

Anusha

- Black box model attack using transferred attack methods
- Something easy you can run autoattack on
- Model federation with broken differential privacy (leak weights maybe?)

Kevin

- RestrictedPython oday

Pranav

- Hardware RE/crypto

Hassam

- ZKP problem
- WEP crypto attack
- RAM dump recover private key
- NAND gate RE chal
- Esoteric LLVM backend Lanai RE/(pwn?) chal
- Leaky RNG

Husnain

- Website quine
- Diophantine crypto
- Elliptic curve crypto
- Conway game of life RE
- Library of Babel chal
- Latex RE

Yifei

- SMM cowsay kernel pwn

Nebu

- Predictable private keys on Debian crypto chal

Ankur

- Solana RE (compiles to ebpf)
- Hopefully comes through with some web :P

Kuilin

- Pwn chal no-syscalls-allowed.c
- easy-math already deployed

Ravi

- PwnyOS X
  - Next iteration of PwynOS sequence of custom OS pwn

Richard

- Obfuscated javascript vm (with anti-debugger)
  - Add on from Nathan: Anti debugger should include ways to prevent DOM from being read by employing Kuilin's website trick as well as detecting developer tools and clearing DOM
- Auto rev
- Vim jail/rev

Pete

- easy web = invisible unicode character web backdoor
  - cyberseed *just* did this, so would need to find another clever twist
- branching pwn = each branch uses a secure strcmp, except for one branch which can be side-channeled
  - force people to automatically find which branch is secure and inputs required to get to it
- challenge with generated binaries, claripy constraints must be automatically generated in order to solve each binary
- opensea nfts have javascript, users have to have a certain browser / other restriction to view the “real” nft image

Next meetings

- Next Thursday
  - UIUC Tech Services

- Next Sunday
  - TBD