Lecture 1: What is Hacking?

Xin Liu

Florida State University

xliu15j@fsu.edu

CIS 5370 Computer Security

https://xinliulab.github.io/cis5370.html

What is Hacking?

Two Steps

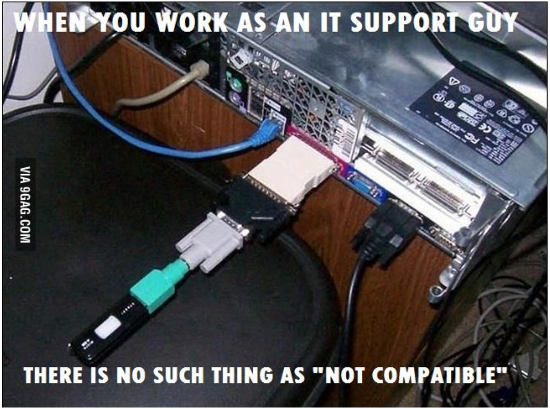
(re-)Use of Unintended Functions

- Unintended Function Discovery
- Creative Re-purpose & Composition

Unintended Function Discovery

Creative Re-purpose & Composition

The ”never give up” example


WHEN YOU WORK AS AN IT SUPPORT GUY
VIA 9GAG.COM
THERE IS NO SUCH THING AS "NOT COMPATIBLE"

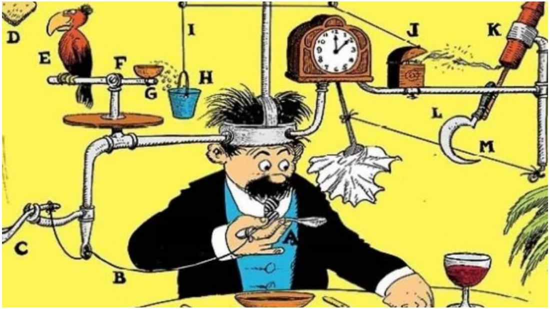
Other hardware examples

Simple Display Emulator with an HDMI-VGA Adapter

Consider the hacker from your current perspective

They're just people
who know computers very well

They compose unintended components in order to achieve unexpected artifacts.

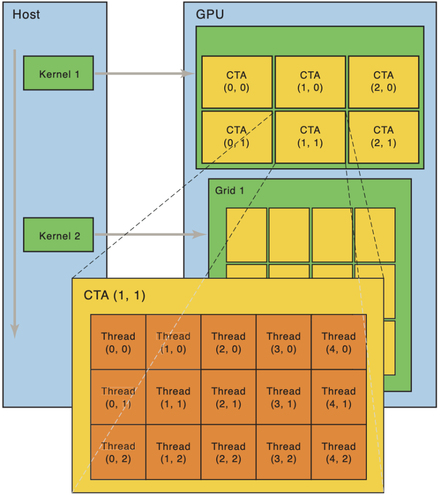


Professor Butts and the Self-Operating Napkin

CUDA: Programming for GPUs

Single Instruction, Multiple Threads

- Many threads execute the same instruction
- Each thread has some thread-local data (e.g., ID)
- Highly optimized design
  - One Program Counter (PC), multiple data elements
  - Successor to VLIW and SIMD architectures



GPU Driver Overview

Reference: Parallel Thread Execution ISA Application Guide

GPU Drivers are Complex Essential Tools in the CUDA Toolchain

- **gcc** → **nvcc**: NVIDIA CUDA Compiler, used to compile CUDA code.
- **binutils** → **cuobjdump**: Disassembler for CUDA binaries.
- **gdb** → **cuda-gdb**: Debugger for CUDA code.
  - Allows debugging directly on the GPU!
- **perf** → **nvprof**: Performance profiling tool to analyze GPU code.
- ...

CUDA brings a complete set of tools to the GPU, similar to what we have for CPUs.

Note: NVIDIA open-sourced its driver in 2022!

- Before that ... Video

How to become a hacker?

(Why hacking is Computer Science?)

Writing Exploits

Exploit code is a ”program”
that is composed by unintended computation abilities,
achieving an unintended goal on the original platform.

Writing Exploits = Programming of Unintended Automata

Takeaways

- Get to know the computers really well - dive into the OS and architecture.
- Keep Coding, coding and coding!