THE UNIVERSITY of NEW ORLEANS

CSCI 4621/5621 Intro CyberSecurity

Midterm Review

Vassil Roussev

vassil@cs.uno.edu

DEFINITIONS & PRINCIPLES

- Understand essential definitions
  - *i.e., be able to reason about them in an example situation*
- Understand Security Principles
  - *and how they apply to specific situations*
  - *e.g., think about which principles violations in security breaches*

OS SECURITY POLICIES & MECHANISMS

- Hardware protection
  - *CPU, memory, I/O*
- Access control matrix
  - *ACL, RBAC*
  - *capabilities*
  - *Unix permissions model*

C VULNERABILITIES

- Race conditions
  - *TOCTOU*
    - link file access
    - file squatting
- Integer vulnerabilities in C
  - *conversion*
  - *signedness mismatch*
  - *overflow/underflow*
  - *pointer arithmetic*
- Stack-based overflows
- Heap-based overflows

PRIVILEGE ESCALATION

- Definition
- Examples

Malware

- Definitions & major concerns
- Viruses & worms
  - *history*
  - *behavior*
  - *implementation*
  - *dissemination*
  - *stealth techniques*
- Detection techniques
  - *halting problem*
  - *pros & cons*

Malware [2]

- Ransomware
- Botnets
- Zero-day exploits
- Social engineering
- Malware classification
  - *by objective*
  - *by technique*

STACK SMASHING

- Process memory layout
- Function call conventions/stack layout in C
- Shellcode/no-op sled
- Countermeasures
- Format string exploits
  - *printf parametes & behavior*
  - *arbitrary read implementation*
  - *arbitrary write implementation*