CS590-SWS/527 Software Security

Software Security Summary

Asst. Prof. Mathias Payer

Department of Computer Science
Purdue University

TA: Kyriakos Ispoglou

https://nebelwelt.net/teaching/16-527-SoftSec/

Spring 2016

Table of Contents

Software security

- Secure coding guidelines
- Defending against attacks
- Best practices
- Update mechanisms

Table of Contents

Attack vectors and threats

- Memory corruption as foundation for attacks
- Control-flow hijack attacks
- Code injection and code reuse attacks
- Data-only attacks
- Recovering data structures
- Reverse engineering
- SQL injection and command injection

Table of Contents

Secure architecture

- Isolation principles and different implementations
- Least privilege principle
- Compartmentalization
- Policies (e.g., at the system call level)
- Simplicity and modularity
- Input validation

Table of Contents

Defense strategy

- Defense in depth (multiple layers)
- Prevention, detection, mitigation
- Make defenses resilient against evasion
- Accountability: auditability

Practical defenses

- Memory safety as an ideal goal
- Trade-offs for realistic defenses
- Address-Space Layout Randomization
- Stack canaries
- Data execution prevention
- Control-Flow Integrity as upcoming defense

Table of Contents

Web security

- Browser security model: isolate tabs
- Different attacker models
- Web security: validate input

Table of Contents

Mobile environments

- Harden the runtime environment
- Sign applications
- Restrict communication between applications
- Enforce security policy and permissions

Questions?

?