

Introduction to Application Security

Ben Livshits

Microsoft Research

Resume:

Today, more than ever before, security exploits and privacy breaches are on the mind of both computer professionals and the general public. What most people don't realize, however, is that underlying most vulnerabilities are software bugs. This course will introduce students to adversarial mindset, i.e., how to think like an attacker, and will include an overview of the most common types of vulnerabilities in use in exploitation today, including buffer overruns and the most common web vulnerabilities such as cross-site scripting and SQL injection. We will talk about the programming pitfalls behind privacy breaches and focus on several fun case studies involving hacking cars and other physical devices.

Brief summary:

- Introduction to the adversarial mindset.
- Memory safety and buffer overruns.
- Web application security.
- Privacy.
- Tools for static and runtime analysis.
- Hacking for fun and profit: case studies: cars, routers, and other devices.

Bibliography:

Book:

- Foundations of Security, Daswani, Kern, and Kesavan, ISBN 1-59059-784-2.

Papers:

- 25 Years of Vulnerabilities
- Security in the Browser
Web cookies
- Advertising Gets Personal
Privacy practices of browser extensions
- All Your iFRAMEs Point to Us
- Understanding Android Security
Android Permissions
- Four Billion Little Brothers?
TaintDroid: An Information-Flow Tracking System...