Deep Dive into Security Engineering: Hackpack

September 16, 2021 / 9:00 PM - 10:00 PM ET

Description

To keep critical systems and sensitive data safe from malicious actors, security engineers must have a deep understanding of the system they are securing while also keeping up with attackers' evolving strategies and motivations. During this workshop, you will take the role of a security engineer to identify security flaws in three different kinds of systems. We will go from the overall architecture to individual lines of code to discover and patch security bugs. We will also discuss state-of-the-art design patterns, tools and frameworks that help us prevent similar flaws in the future.

Learning Outcomes

During this workshop, you'll learn:

- How to identify security vulnerabilities in small web apps, large web apps, and cyber-physical systems
- How to mitigate these vulnerabilities using state-of-the-art frameworks and tools
- Implementation details of popular open-source security tools
- How to read white papers on cybersecurity

Prerequisite Knowledge

Everyone is welcome to join, regardless of their knowledge or skill level! In order to get the most out of this workshop you may want to know the following:

- Basic software engineering skills (e.g. knowing differences between data structures, being able to look through a well-structured codebase and understand the purpose of a given function).
- A general understanding of software architecture (e.g. publisher-subscriber pattern, microservices vs. monolithic architecture).

Pre-Workshop Checklist

Nothing to complete before the workshop!

Timeline (1 hour)

Time	Module	Description
10 min	Intro (becoming a thief)	We will put ourselves into the shoes of an attacker to better understand our role as security engineers.
	Analyzing security risks and developing secure design principles for:	
15 min	Small web apps	Even the smallest web apps can make great targets for attackers. Let's start by looking at common security risks for small web apps, such as cross-site scripting and broken access control.
15 min	Large web apps	We'll examine different kinds of security weaknesses that occur in large web apps, including supply chain attacks. We'll also examine some tools and strategies that can help detect and mitigate vulnerabilities.
15 min	Cyber-physical systems	Cyber-physical systems include safety-critical devices like cars and medical devices. Cyberattacks on these systems can be life-threatening, and we'll examine documented vulnerabilities and secure design principles that may prevent these vulnerabilities.
5 min	Summary and Questions	

Workshop Lead Contact

Katya Potapov
@okcharlie#3081 (Discord handle) kat.p28@gmail.com

Additional Resources

Hack the North Resources

Hack the North 2021 Event Schedule

Check this out to stay up-to-date on activities, workshops, and other key happenings this weekend.

Workshop-Specific Resources

CVE List

A list of publicly disclosed cybersecurity vulnerabilities, identified, defined and catalogued for anyone to search and use. You can follow their Twitter account as well, which notifies followers of new CVEs.

SANS Information Security White Papers

Informative reports published by the SANS institute, an organization that runs many high-quality cybersecurity courses and certifications. Free but requires email registration to access white papers.

';--have i been pwned?

A simple search tool that checks if a person's private information has been revealed in a data breach.