Large Scale Security Engineering: Hackpack

September 15, 2021 / 8:30 PM - 9:30 PM ET

Description

Security teams at large companies have the difficult task of keeping their users' sensitive data safe from ever-changing threats, including stalkers, political hackers, rogue employees and illicit data vendors. We'll be learning more about how these teams secure their systems using large scale automation, encryption, firewalls and more. When we've learned the basics, we'll take a look at some security tools used for real large-scale systems that detect and prevent major security vulnerabilities.

Learning Outcomes

During this workshop, you'll learn:

- Basic security engineering definitions and principles
- How to secure resources (small scale and large scale)
- How to read academic papers on security engineering
- Implementation details of three different tools used to secure large scale systems

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 review the following concepts:

- 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 any given function).
- A general understanding of software architecture (e.g. publisher-subscriber pattern, microservices vs. monolithic architecture).
- A high-level understanding of Kubernetes (e.g. components of the control plane).

Pre-Workshop Checklist

Nothing to complete before the workshop, besides going over the prerequisite knowledge!

Timeline (1 hour)

Time	Module	Description
5 min	Intro to security engineering	Let's go over our goals and motivations as security engineers.
20 min	Scaling up security principles	We'll start by looking at best practices for securing a single resource, then securing ten resources, and so on until we get to thousands of resources.
10 min	Tool 1: TABOR	Going through the research paper for TABOR, an ML model used to detect anomalies in a water treatment system.
10 min	Tool 2: Atomic Red Team	Explaining Atomic Red Team, a suite of tools that map to the MITRE ATT&CK framework.
10 min	Tool 3: kube-hunter	Explaining kube-hunter, a tool that hunts for security weaknesses in Kubernetes clusters.
5 min	Conclusion + Questions	Going over what we've learned today and answering any remaining 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

TABOR

TABOR is a machine-learning model that detects anomalies in industrial control systems. We will be going over this tool's implementation and use cases during the workshop.

Atomic Red Team

Atomic Red Team is a library of tests mapped to the MITRE ATT&CK® framework. We will be going over this tool's implementation and use cases during the workshop.

kube-hunter

kube-hunter hunts for security weaknesses in Kubernetes clusters. We will be going over this tool's implementation and use cases during the workshop.