1 - OWASP top 10 vulnerabilities (max 4 groups)

OWASP is a non-profit organization that captures and catalogues the most common system vulnerabilities. Its goal is to raise awareness about pervasive issues in IT, as well as to lead open-source software projects focused on ensuring web security.

The goal if this work is to analyse and describe protections against the top 10 list of OWASP vulnerabilities. Each group must also select 1/2 vulnerabilities on the list, describe how these can be exploited as attacks, give examples, and explore how one can devise effective countermeasures.

Refs: owasp-top10, owasp-top10-old

Note: no two groups can select the same vulnerabilities.

Assignment #2: The goal is to design a proof-of-concept target application and attack, implement countermeasures, and evaluate their efficacy.

2 - Anonymity and Onion Routing in Tor (max 2 groups)

Tor and the Invisible Internet Project (I2P) are two anonymous networks with the goal of ensuring user anonymity. These networks rely on unidirectional encryption tunnels to hinder eavesdroppers from understanding where traffic is originating, as well as its destination.

The goal of this work is to describe and analyse the mechanisms underlying these networks. Students must select a system for anonymous networks, describe how it can be installed and configured, and analyse how the underlying mechanisms ensure anonymity of users and servers.

Refs: Tor, I2P

Note: no two groups can select the same system

Assignment #2: The goal is to design a proof-of-concept service for this anonymous network, configure it, collect traffic data, and evaluate the anonymity mechanisms used.

3 - De-Anonymity in Tor (max 2 groups)

As the most popular anonymous network, Tor has been the target of many attacks that attempt to breach its anonymity guarantees. This is a crucial security target, as its main goal is to ensure censor-free speech and anonymity even in the presence of malicious governments.

Students must select a peer-reviewed paper describing a threat to anonymity networks, which will be the focus for the assignment. The goal is to analyse the techniques used to breach anonymity of the tor network, and describe potential countermeasures that can be used to strengthen the system against such threats.

Refs: List of papers

Note: no two groups can select the same paper; papers can be no older than 2010

Assignment #2: The goal is to demonstrate how one can capture communication patterns allowing for the de-anonymization of Tor services, and to explore how one can devise effective countermeasures for speecific attack strategies.

4 - Padding Oracle and the Lucky 13 (max 2 groups)

For the security of cryptographic protocols, devil is often found in the details. Lucky 13 is a Padding Oracle attack against which TLS v1.1,1.2 and SSL 3.0 are vulnerable, that relies on exploring a nuance in how these protocols check for message integrity. Specifically, by sending malformed messages to a server, the attacker can distinguish an error arising from incorrect padding, from an error arising from decryption failed.

Students will select a Padding Oracle-based attack (not necessarily Lucky 13), which will be the focus for the assignment. The goal is to explore how the attack works, which systems are vulnerable, and how feasible it is to exploit such vulnerabilities.

Refs: Lucky 13, Padding Oracle

Note: no two groups can select the same padding oracle-based attack

Assignment #2: The goal is to develop a proof-of-concept of such an attack. To ease experimental validation, students can code artificial delays to distinguish errors in decryption.

5 - Securing DNS

DNS (Domain Name System) is the basis of most network connections performed by any computing device. It was design in an earlier time of the web, where security was not a priority, as a result it is not a secure protocol. Given it central role in the communication of any device, it's security (or lack of it) can cause major problems. In this project, students are expected to study DNS security, from both the point of view of providers with a nameserver and/or a name that want to make sure it resolves to their IP addresses, or the point of view of a user wanting to make sure the names are resolved to the right addresses. The goal is to capture the standard mechanisms used, as well as propose the current challenges and tradeoffs for these systems.

Note: If two groups select this topic, different DNS perspectives must be selected.

Refs: DNSsec, DNScrypt , DoT, DoH, DNS security

Assignment #2 The goal is to develop a software-based proof-of-concept that implements secure DNS communications.

6 - Certificate Revocation Issues (max 2 groups)

As systems will inevitably become vulnerable, revocation of permissions is an integral part of PKIs. x.509 certificates allow for revocation mechanisms, which are designed to prevent system breaches from

provoking critical damage. However, adversaries have a wide array of attack opportunities to disrupt and delay the revocation process.

Students should explore the state-of-the-art for certificate revocation mechanisms and their vulnerabilities. The goal is to capture the standard mechanisms used in standard PKIs, as well as propose the current challenges for these systems.

Refs: Certificate revocation challenges, Short-lived Certificates

Note: If two groups select this topic, two methodologies for certificate revocation must be chosen (or a certificateless alternative).

Assignment #2 The goal is to develop a proof-of-concept PKI, demonstrate an attack on the explored revocation mechanisms, and implement the adequate countermeasures.

7 - Ransomware (max 2 groups)

Currently, ransomware is a common term in IT security. It is a malware that blocks access to files of a machine (via encryption), demanding a ransom for data recovery. The maturity of modern cryptographic algorithms ensures that, after encryption, the chance of data recovery without access to the secret key used for encryption is negligible.

Students should explore the methodologies used for ransomware to be installed in machines. Specifically, what are the common network vulnerabilities that allow for this malware to damage modern systems.

Refs: Protecting against ransomware, Ransomware awareness and response

Note If two groups select this topic, two different network vulnerabilities leading to the ransomware attack must be selected.

Assignment #2 The goal is to exemplify how a common network vulnerability can be explored to install a ransomware attack, and implement countermeasures to block the attack.

8 - Intrusion Detection Systems (max 2 groups)

Intrusion detection systems (IDSs) typically monitor incoming and outgoing network packets to detect possible malicious actors attempts to gain control of a system. However, as malicious actors' knowledge and skill increases so must ID systems.

Students should explore the state-of-the-art for intrusion detection systems, focusing on the different approaches and identifying tradeoffs.

Note If two groups select this topic, different improvements must be selected (e.g., ML, eBPF, etc.).

Refs: IDS, SNORT

Assignment #2 The goal is to propose improvements on existing IDS, for example, by adding support to deal with 'zero day' exploits.

9 - Intrusion Prevention Systems (max 2 groups)

Intrusion prevention systems (IPSs) typically work along side intrusion detection systems (IDSs) and manage incoming and outgoing network packets to prevent possible malicious actors attempts to gain control of a system.

Students should explore the state-of-the-art for intrusion prevention systems, focusing on the different approaches and identifying tradeoffs.

Note If two groups select this topic, different improvements must be selected (e.g., ML, eBPF, etc.).

Refs: IPS, SNORT

Assignment #2 The goal is to propose improvements on existing IPS, for example, by adding support to deal with 'zero day' exploits.

10 - Intrusion Detection & Prevention Systems for Specific Scenarios (Smart-Cities, Smart-Industry, in-vehicle networks, etc.)

As new application scenarios and paradigms emerge (e.g., IoT, Autonomous Vehicles, etc.), existing systems and security solutions need to be revamped and adapted to deal with the restrictions and requirements.

In this project, students are expected to explore the state-of-the-art for intrusion detection systems, focusing on how these systems are able to deal with specific application scenarios.

Note If two groups select this topic, different scenarios must be selected.

Assignment #2 The goal of this project is to redesign an IDS to deal with the requirements of a specific scenario.

Refs: IDS, IPS, SNORT

11 - Securing IoT

As the IoT paradigm gains momentum, so does the lack of secure-by-design solutions for supporting these new ecosystems. Everyday devices, from mobile phones to Smart-TV or home appliances (such as refrigherators, dish washers, washing machines, including dish washers), are connected to the Internet and can use different communication protocols. These can be exploited to perform malicious attacks, as evidenced by recent news (Android TV boxes).

In this project, students are expected to study state-of-the-art IoT architectures, focusing on how these systems are able to deal (or not) with traditional security requirements, and how this lack of security is being exploited by malicious actors.

Note If two groups select this topic, different protocols/appliances must be selected.

Assignment #2 Students are expected to present a solution for preventing Smart-Appliances from successfully performing attacks, even if compromised.

Refs: IoT Security Foundation, Architecture of Internet of Things, DesktopECHO

12 - HoneyPots & HoneyNets for detecting intrusions

HoneyPots & HoneyNets are typically used to detect and discover intrusion techniques by attracting malicious actors.

In this project, students are expected to explore the state-of-the-art on this topic, focusing on how these approaches can be used to detect intrusion attempts, gather information and increase the knowledge base used by other systems (e.g., IDSs).

Note If two groups select this topic, different HoneyPot/HoneyNet projects must be selected.

Assignment #2 The goal of this project is to design and develop a HoneyPot or HoneyNet project for gathering information for increasing knowledge base of other systems.

Refs: HoneyNet.org, HoneyNet projects, Awesome HoneyPot projects

13 - Increasing network security with eBPF

eBPF (enhanced Berkeley Packet Filtering) is a technology that allows developers to run programs in the operating system kernel without requiring changes kernel source code or load kernel modules.

In this project, students are expected to study the eBPF technology, and explore how it can be used to increase network security (for example, for monitoring and managing incoming and outgoing connections such as a traditional firewall).

Note If two groups select this topic, different eBPF projects must be selected.

Assignment #2 The goal of this project is to design and develop an eBPF application increasing network security of a system.

Refs: eBPF, eBPF Explained

Rules for project submission and evaluation

- Projects are to be completed in groups of 3 students.
- Projects must be selected until 06/10/2023, using the respective Moodle link.
- Assignment 1 must be a report describing and contextualing the topic and a discussion of the state-of-the-art regarding that topic.
- Assignment 2 is further detail in each topic.
- Assignment 1 must be submitted until 22/11/2023 at 23:59, using the respective Moodle link.
    - Assignment 1 must be presented on the week of 23/11/2023 during class.
- Assignment 2 must be submitted until 10/12/2023 at 23:59, using the respective Moodle link.
    - Assignment 2 must be presented on the week of 11/12/2023 during class.

- All Submissions are done via Moodle. All students of each group are advised to submit the same file.
- The structure for project submission should be as follows, where **X** is the respective group letter:
    - The submission itself must be a **zip** file named: `groupX-project.zip`
    - The submission file must contain all the relevant code, in a folder called `\src`, alongside a `README` file with instructions for execution.
    - The report should be in a single pdf file named `reportX.pdf`
- Submissions that do not follow these specifications risk being discarded from evaluation
- Each project will be defended in a short presentation, to be scheduled later.